UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 15-1441

In re: Nickelodeon Consumer Privacy Litigation

On Appeal from the U.S. District Court for the District of New Jersey
Case No. 2:12-cv-07829
The Honorable Stanley R. Chesler

APPELLANTS' BRIEF

EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
Facsimile: (732) 248-8273

BARTIMUS FRICKLETON ROBERTSON & GOZA, PC
715 Swifts Highway
Jefferson City, MO 65109
Telephone: (573) 659-4454
Facsimile: (573) 659-4460

Co-Lead Counsel on behalf of All Plaintiffs

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF JURISDICTION

The United States District Court for the District of New Jersey properly exercised jurisdiction under 28 U.S.C. § 1331 because this case arises in part under the laws of the United States, specifically 18 U.S.C. § 2710, 18 U.S.C. § 2510, and 18 U.S.C. § 2701. The District Court exercised supplemental jurisdiction over the Plaintiffs' state law claims under 28 U.S.C. § 1367 because they are related to and arise out of the same case and controversy as the federal claims. In addition, the District Court properly exercised jurisdiction under 28 U.S.C. §1332(d) because this civil action was brought pursuant to Fed. R. Civ. P. 23, over $5 million is in controversy, and a named plaintiff is a citizen of state different from any defendant.

The Third Circuit has jurisdiction over this appeal under 28 U.S.C. § 1291. This appeal is from a final decision of the United States District Court for the District of New Jersey granting the defendants' second motions to dismiss plaintiffs' entire action without leave to amend.

This appeal was timely filed under Fed. Rule App. P. 4. The District Court dismissed the plaintiffs' entire action by Order on January 20, 2015. Plaintiffs filed their Notice of Appeal on February 13, 2015.

STATEMENT OF THE ISSUES

1. Did the District Court err in dismissing Plaintiffs' claim under the Video Privacy Protection Act? In particular, this Court must determine (*See* Appendix ("App'x") at 22-30, 51-53):
    a. Whether the District Court erred by ruling that Plaintiffs did not adequately plead that Viacom disclosed "personally-identifiable information" under the VPPA when it provided to Google each minor child's (1) unique username or alias, (2) gender, (3) age, (4) IP address, (5) browser settings, (6) unique device identifiers, (7) operating system, (8) screen resolution, (9) browser settings, and (10) a unique persistent cookie identifier associated with the videos that the Plaintiffs watched on Viacom's children's websites?
    b. Whether, in concluding Plaintiffs had not adequately alleged disclosure of "personally identifiable information", the District Court made a factual determination that should have been determined by a jury?
    c. Whether Defendant Google can be held liable as a recipient of and participant in Viacom's disclosures?
2. Did the District Court err in dismissing Plaintiffs' claim under the Electronic Communications Privacy Act? In particular, this Court must determine (*See* App'x 30-36):

a. Whether URLs contain "content" under the ECPA, i.e. "any information relating to the substance, purport, or meaning" of a communication? In this case, the URLs included, but were not limited to, URLs with specific names of videos the Plaintiffs requested and viewed.

b. Whether Plaintiffs alleged sufficient facts to show Defendants acted with criminal or tortious intent when their acts violated criminal laws in all 50 states and give rise to the tort of intrusion upon seclusion?

c. Whether Viacom could consent to third-party interceptions of communications with the minor children Plaintiffs?

d. Whether Plaintiffs pled facts sufficient to show an ECPA violation for Google's tracking of the minor children Plaintiffs' communications with non-Viacom websites?

3. Did the District Court err in dismissing Plaintiffs' claim under the California Invasion of Privacy Act by holding that URLs do not contain "any information relating to the substance, purport, or meaning" of a communication? *See* App'x 38-40.

4. Did the District Court err in dismissing Plaintiffs' claim under the Stored Communications Act by holding that Plaintiffs' personal computing devices

and browser-managed files are not "facilities through which" electronic communication services are provided? *See* App'x 36-38.

5. Did the District Court err in dismissing Plaintiffs' claim under the NJCROA by holding that Defendants' unjust enrichment through the unauthorized collection and monetization of the minor children Plaintiffs' PII does not qualify as damage to business or property? *See* App'x 40, 53-54.
6. Did the District Court err and improperly intrude upon the province of the jury by finding Plaintiffs had not sufficiently pled a claim for Intrusion Upon Seclusion? In particular, this Court must determine whether the unauthorized tracking of children's Internet communications adequately alleges facts that a reasonable person may find highly offensive. *See* App'x 40-42, 54-57

STATEMENT OF THE CASE

This case arises from separate class actions consolidated in the District of New Jersey. The Plaintiffs filed seven claims. Defendants moved to dismiss. On July 2, 2014, the District Court granted Defendants' motions – with leave to amend. On September 11, 2014, Plaintiffs filed a second complaint. . Defendants moved again for dismissal. On January 20, 2015, the District Court dismissed all Plaintiffs' claims without leave to amend.

STATEMENT OF THE FACTS

Plaintiffs' factual allegations are deemed true on a motion to dismiss. *Phillips v. City. of Allegheny*, 515 F.3d 224, 233 (3d Cir. 2008). Thus, any conflict between facts alleged in the Complaint and Defendants' subsequent attempts to present this Court with cherry-picked facts outside of discovery must be resolved in Plaintiffs' favor.

A. The Defendants' Unauthorized Disclosures and Tracking

Plaintiffs are minor children under the age of 13 who are registered users of Viacom's children's websites, where the Plaintiffs watched videos, played games, and sent and received communications to and from Viacom. Plaintiffs' Second Consolidated Class Action Complaint ("*Second CAC*") at App'x 108. Unbeknownst to the Plaintiffs and without their or their guardians' lawful consent, Defendants Viacom and Google misused Internet technologies known as cookies to disclose, compile, store, and exploit the video-viewing requests and histories and Internet communications of the minor children Plaintiffs on Nick.com and other websites. *Id.* For a detailed explanation of cookies, see *Id.* at App'x 116-18.

Immediately upon the minor children Plaintiffs' first communication with Viacom's children's websites, Viacom: (1) placed its own first-party cookies on the minor children's computers, and (2) knowingly permitted Defendant Google to place or access its own third-party cookies on the minor children's computers. *Id.* at App'x

127. The placement of these cookies occurred before Plaintiffs or their guardians even had the opportunity to consent – or not consent – to their placement. *Id.* at App'x 128.

Next, Viacom encouraged the minor Plaintiff children visiting the Viacom children's websites to register as a user for each site. *Id.* at App'x 140. During registration, Viacom obtained the child's birthdate and gender, to which it assigned an internal code name. *Id.* at App'x 140-41. Viacom also required the child to create a unique username in the sign-up process. *Id.* Then, Viacom designed its code to allow Google to access each child's profile name and the code name for the child's specific gender and age. *Id.* at App'x 141. In total, for each child's registration, Viacom disclosed to Google each child's (1) unique username or alias; (2) gender; (3) age/birthdate; (4) IP address; (5) browser settings; (6) unique device identifier; (7) operating system; (8) screen resolution; (9) browser version; (10) over time, the content of the child's web communications, including but not limited to the detailed URL requests and video materials requested and obtained from Viacom's children's websites; and (11) a unique DoubleClick persistent cookie identifier used by Google to track Internet communications. *Id.* at App'x 152-53.

Google's third-party cookies are also used to track the specific video requests and viewing histories of minor children through the tracking of detailed URL requests that included the exact titles of the videos requested and received by these

minor children, including, but not limited to URLs like http://www.nick.com/videos/clip/digital-short-penguins-of-madagascar-shorts-skippers-nightmare.html. *Id.* at App'x 130, 141-42. Through this tracking, Viacom knowingly disclosed, and Google knowingly obtained, the specific video and video-game requests and viewing histories of the Plaintiffs on the Viacom children's websites. *Id.* at App'x 130-31.

In addition to tracking the content of Plaintiff children's communications on the Viacom children's websites, Google's cookies also tracked and recorded the content of Plaintiffs' communications immediately and continuously on non-Viacom websites without the consent of the Plaintiffs or their guardians. *Id.* at App'x 138. Viacom knew or had reason to know that Google intentionally intercepted the content of the Plaintiffs' Internet communications with non-Viacom websites despite Google's knowledge that Plaintiffs were minor children. *Id.* at App'x 138-42. Viacom procured Google to intercept the content of the Plaintiffs' communications with other websites, and, upon information and belief, profited from Google's unauthorized tracking on other sites as such information gleaned from the tracking assisted in the sale of targeted advertisements to the Plaintiffs on Viacom's children's websites. *Id.* at App'x 116.

B. Google Tracking is Not Anonymous

The information disclosed by Viacom constitutes identifiable information not only by its content – but more importantly because of its recipient. Taken together, Google's services facilitate its collection of more information about American consumers, including the Plaintiffs and their guardians, than any company in history. This information includes, but is not limited to: (a) first and last names; (b) home or other physical addresses; (c) precise locations of users through GPS; (d) IP addresses; (e) telephone numbers; (f) lists of contacts; (g) the content of Gmail users' email messages; (h) search histories at Google.com and YouTube; (i) web-surfing histories; (j) Android-device activity; and (k) all activity on Google's social network called Google Plus. *Id.* at App'x 137-38.

Google has publicly acknowledged that the types of information disclosed about the plaintiffs in this case contain personally-identifiable information to Google due to its global dominance. *Id.* at App'x 136-37. (Quoting Google promise to "anonymize" log data "by removing part of the IP address (after 9 months) and cookie information (after 18 months).") Further, Google's own Privacy Director has admitted that an IP address alone is personally-identifying to companies with the type of information Google has in its possession. *Id.* Google also publicly admits

that it compiles consumer information in "server logs" that are tied to cookies that uniquely identify the browsers and accounts of American Internet consumers.[1] *Id.*

In short, Google is no ordinary Internet company. It knows more details about American consumers than any company in history. Through its vast web of Internet properties, it compiles detailed profiles on millions of Americans who it individually identifies. It does so with cookies like those at issue in this case. And Viacom knows it.

C. Facts Relating to the "Highly Offensive" Element of Intrusion Upon Seclusion

Plaintiff's *Second CAC* pleads facts which show Defendants' conduct violated social norms as expressed (1) directly by public policy in the form of civil and criminal laws designed to protect privacy, (2) by the standards of Defendants' own industry, and (3) by public opinion.

Specifically, Plaintiffs allege facts showing the Defendants violated the VPPA, the Wiretap Act (or, in the alternative, the Pen Register Act), and the Computer Fraud and Abuse Act and corresponding computer crime laws in all 50 states. *Id.* at App'x 156-57. Plaintiffs allege violation of the Terms of Use of Internet Service Providers and web-browsers, and of the standards of the online advertising industry. *Id.* at App'x 157, 160-61. Finally, Defendants' self-praise to the contrary, the

[1] For a detailed explanation of Google's Internet dominance, see *Second CAC* at App'x 132-36.

complaint alleges facts, through public poll results, showing Americans strongly disapprove of the Defendants' behavior in tracking children. *Id.* at App'x 157-60.

Defendants' illegal tracking is made worse by its scope and its targets. The invasions were perpetrated millions of times on minor children. *Id.* at App'x 160. And, the targeting of children was more intrusive than Internet tracking of adults. *Id.*

STATEMENT OF RELATED CASES

This case has not come before this court previously. Plaintiffs know of no other case or proceeding in any way related, completed, pending, or about to be presented before this Court, any other Court, or state or Federal agency.

Though there is no direct relationship between the cases, Plaintiffs note that similar questions under the Wiretap Act and Stored Communications Act are currently pending before the Third Circuit in the case *In re: Google Cookie Placement Consumer Privacy Litigation*, No. 13-4300.

STANDARD OF REVIEW

Dismissals under Rule 12(b)(6) are reviewed *de novo*. *Balletine v.United States*, 486 F.3d 806, 808 (3d Cir. 2007). To survive a motion to dismiss, a complaint must contain sufficient factual matter to "state a claim for relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that discovery will reveal evidence of the misconduct alleged." Phillips, 515 F.3d at 254 (quoting *Twombly* at 556). All well-pleaded factual allegations are accepted as true and viewed in the light most favorable to the plaintiff. *Ballentine*, 486 F.3d at 810. "Further, [t]he 'issue is not whether a plaintiff will ultimately prevail but whether he or she is entitled to offer evidence to support the claims." *Id.* Where an amended pleading could cure a deficiency in a complaint, this Court requires District Courts to grant leave to amend, even where such relief is not sought. *Shane v. Fauver*, 213 F.3d 113, 116 (3d Cir. 2000). Every claim appealed in this case is subject to this same standard of review.

SUMMARY OF THE ARGUMENT

In its Rule 12(b)(6) analysis, the District Court failed to accept well-pleaded facts as true, engaged in judicial fact-finding, and decided factual issues as if they were matters of law already settled by certain other courts weighing different complaints on different facts, and drew all inferences against, rather than for, the Plaintiffs.

Without giving Plaintiffs the benefit of all reasonable inferences, the District Court's Orders ignore this Circuit's rule that under Rules 8(a)(2) and 12(b)(6) the plaintiffs need only plead facts sufficient to provide defendants fair notice of the plaintiffs' claims and their grounds by pleading facts generating the reasonable inference that discovery will yield evidence supporting the claims. *Phillips v. City of Allegheny*, 515 F.3d 224, 234 (3d Cir. 2008). In violating Rule 8(e)'s mandate that "[p]leadings must be construed so as to do justice," the Orders contradict this Circuit's strong preference for merits resolution. *See, e.g., Glover v. FDIC*, 698 F.3d 139 (3d Cir. 2012). By misapplying Rules 8(a)(2) and 12(b)(6), the District Court's rulings contradicted "[t]he basic purpose of the Federal Rules," which is "to administer justice through fair trials, not through summary dismissals as necessary as they may be on occasion." *Surowitz v. Hilton Hotels Corp.*, 383 U.S. 363, 373 (1966).

LEGAL ARGUMENT

INTRODUCTION

It really isn't anybody's business what books or videos somebody gets. It does not make any different if somebody is up for confirmation as a Supreme Court Justice or they are running the local grocery store. It is not your business. It is not my business. It is not anybody else's business whether they want to watch Disney or they want to watch something of an entirely different nature. It really is not our business.

Senator Patrick Leahy[2]

The "right to privacy" has become firmly woven into the fabric of American jurisprudence and finds expression in common law, state and Federal statutes, and the opinions of the Supreme Court, which has described it as "a most fundamental human right," "the most comprehensive of rights," "the right most valued by civilized men," and one that is "older than the Bill of Rights – older than our political parties, older than our school system." *See Kewanne Oil Co. v. Bicron Corp.*, 416 U.S. 740, 748 (1973), *Olmstead v. United States*, 277 U.S. 438, 478 (1928), *Griswold v. Connecticut*, 381 U.S. 479, 486 (1965). Though it has taken different formulations, the right to privacy has been described as "enforcement of the more general right of the individual to be let alone." Samuel D. Warren, Louis D. Brandeis,

---

[2] *Video and Library Privacy Protection Act of 1988: Joint Hearing on H.R. 4947 and S. 2361*, 100th Cong. 18 (Aug. 3, 1988) (statement of Sen. Leahy). Sen. Leahy also noted, "Privacy is not a conservative or a liberal or a moderate issue. It is an issue that goes to the deepest yearnings of all Americans .... We want to be left alone." S. Rep. 100-599 at 6 (1998).

The Right to Privacy, 4 Harv. L. Rev. 193, 206. (1890). It finds specific federal statutory protection in, among other things, the Video Privacy Protection Act and the Electronic Communications Privacy Act.

This case is about children's privacy. In particular, it is about a scheme through which Viacom, which bills itself as "the number-one entertainment brand for kids," disclosed the video-viewing and Internet communications of minor children to Google, the world's largest data tracking company, without the lawful consent of the minor children or their guardians.

American courts have also long recognized that "children have a very special place in life which law should reflect." *May v. Anderson*, 345 U.S. 528, 536 (1953)(Frankfurter, J., concurring). The Supreme Court has recognized three reasons that courts treat children differently – their "peculiar vulnerability," their "inability to make critical decisions in an informed, mature manner," and "the importance of the parental role in child rearing." *Belotti v. Baird*, 443 U.S. 622, 635 (1979). Congress shares the Supreme Court's view, having enacted statutes providing children with additional, special legal protection concerning the "collection, use, and/or disclosure of personal information from and about children on the Internet." 15 U.S.C. § 6501, et seq. (the Children's Online Privacy Protection Act).

The Plaintiffs, representing a nationwide class of minor children under the age of 13, filed suit through their guardians to vindicate their rights to privacy under

Federal and state statutes and the common law. The District Court erred in dismissing the Plaintiffs' action by misapplying the law to the facts adequately alleged in the Plaintiffs' consolidated complaints and by engaging in judicial fact-finding invading the province of the jury.

I. THE DISTRICT COURT ERRED IN DISMISSING PLAINTIFFS' VPPA CLAIM

A. Plaintiffs Adequately Alleged Disclosure of "Personally-Identifiable Information" Under the VPPA

The VPPA prohibits the disclosure of "personally-identifiable information" about consumers of video-tape service providers to third-parties without the informed, written consent of the consumer. It provides for private enforcement through a cause-of-action against "any act of a person in violation" of the VPPA. 18 U.S.C. § 2710.

To Plaintiffs' knowledge, this case, along with a case currently pending before the 11th Circuit, present a question of first impression for our nation's appellate courts. In particular, this Court must determine the scope of the phrase "personally-identifiable information" ("PII") under the VPPA. The plain-language of the Act itself contains an open-ended definition of PII. However, the District Court erred by interpreting the statute to have an overly restrictive definition that is contrary to that used at common law, in similar federal statutes, and by the Defendants' own industry with respect to children.

1. The VPPA Explicitly and Purposefully Adopts an Open-Ended Definition of PII

The VPPA defines PII to "*include* information that identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3). The use of the word "includes" was not a drafting error. Congress explained, "Unlike other definitions in [the VPPA], paragraph (a)(3) uses the word 'includes' to establish *a minimum, but not exclusive, definition of personally identifiable information.*" S. Rep. 100-599 at 12 (1988).

Congress understood that any definition of PII written in 1988 would soon be made obsolete by new digital communications technology. Decades before the minor children in this case were born, Sen. Patrick Leahy predicted the very practices that gave rise to this case:

> In an era of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones, all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch, who are some of the people they telephone .... I think that is wrong. I think that really is Big Brother, and I think it is something that we have to guard against.

Sen. Leahy, S. Rep. 100-599 at 5-6 (1988).

The VPPA was thus designed to prohibit unauthorized disclosures of video-request and viewing histories that could be used to build digital profiles based on the

videos they and individuals and their families watch – even family-friendly entertainment.[3]

2. Recent District Court Cases Support the Plaintiffs

In addition to the instant case, four other District Courts have recently opined on whether persistent-identifiers may constitute PII under the VPPA, and all four opinions support the Plaintiffs in this case. *In re: Hulu*, No. C11-03764, 2014 WL 1724344 (N.D. Cal. April 28, 2014); *Ellis v. Cartoon Network*, No. 1:14-cv-00484, 2014 WL 5023535 (N.D. Ga. Oct. 8, 2014); *Locklear v. Dow Jones & Co.*, 14-cv-00744 (N.D. Ga. Jan. 23, 2015), and *Eichenberger v. ESPN*, C14-463 TSZ (W.D. Wash., Nov. 24, 2014).

In *Hulu*, the Court ruled the Defendant could be held liable for disclosing persistent cookie identifiers to Facebook, but not comScore, a third-party analytics company which does not have other services that directly take or track the broad swath of information that Facebook and Google do.

In *Ellis*, the Court found no liability for disclosures to a third-party company called Bango, which (like comScore) does not have other services that directly collect and maintain a broad swath of information from American Internet consumers. In *Locklear*, the Court found no VPPA liability for disclosures to Adobe,

[3] The Act was passed in 1988 following the publication of "a profile of Robert H. Bork based on the titles of 146 files *his family had rented* from a video store." S. Rep. 100-599 at 6 (1988).

yet another third-party analytics company that, unlike Google or Facebook, does not directly collect and retain personal information about American consumers. Finally, in *Eichenberger*, the Court found no liability for disclosures to Adobe, but allowed leave to amend because "ESPN could be found liable under the VPPA for disclosing both 'a unique identifier and a correlated look-up table' by which plaintiff could be identified as a particular person who watched particular videos[.]" *Eichenberger* at 2 (citing *Hulu* at 11).

Under this recent line of cases, the question for this Court is whether Google is more like Facebook, which provides direct services to Internet consumers through which it gains access to and keeps data on the consumers' names, addresses, locations, interests, social connections, search histories, and more, or, in the alternative, is Google a second-tier data industry company like comScore, Bango, or Adobe?[4]

Plaintiffs' Second CAC illustrates that Google not only dwarfs comScore, Bango, and Adobe, it also dwarfs Facebook. Google enjoys a ubiquitous presence on the

[4] To be clear, Plaintiffs assert that the Defendants should have been found liable under the VPPA in each of these cited cases, at least two of which are on appeal, because PII under the VPPA includes all unique persistent identifiers capable of individually-identifying American video consumers, regardless of whether the receiving entity is as large and ubiquitous as Facebook or Google. Nevertheless, this case presents an easier question given Google's reach and public admissions about what it knows about individual consumers.

Internet. For a full explanation of Google's Internet dominance, see *Second CAC* at App'x 136-37.

Google has publicly admitted that it connects persistent cookie identifiers, IP addresses, and unique device identifiers with user information in "server logs." *Id.* It has further admitted that, for it, IP addresses and cookie information are not "anonymous." *Id.* Google informs users, "We anonymize this log data by removing part of the IP address (after 9 months) and cookie information (after 18 months)." *Id.* Its own Privacy Director admitted IP addresses are personally-identifiable to companies with information like that which Google retains in its "server logs." *Id.* at App'x 137. Further, Google's own Privacy Policy defines "personal information" in a way that would include IP addresses and cookie identifiers. It defines "Personal information" as "information which you provide to us which personally identifies you, such as your name, email address or billing information, or other data which can be reasonably linked to such information by Google."[5]

In the case of DoubleClick cookies and IP addresses, Google has as much or more information to individually-identify Internet users than ISPs do. These include, but are not limited to: first and last names; physical addresses; precise current locations of users through GPS; IP addresses, telephone numbers; lists of contacts;

[5] See http://www.google.com/policies/privacy/key-terms/#toc-terms-personal-info. Last visited Oct. 15, 2014

the content of email messages, search histories at Google and YouTube; web-surfing history; Android device activity; and all activity on the social networking site Google+. *Id.* at App'x 137-38.[6]

In this case, the Plaintiffs pleaded facts showing Defendant Viacom discloused the following information to Defendant Google: (1) the child's username/alias; (2) the child's gender; (3) the child's birthdate; (4) the child's IP address; (5) the child's browser settings; (6) the child's unique device identifier; (7) the child's operating system; (8) the child's screen resolution; (9) the child's browser version; (10) the child's web-communications; and (11) the child's persistent cookie identifiers placed and tracked by Google through its subsidiary DoubleClick.net, which are used to identify and track Internet users. *Id.* at App'x 152-53.

As explained by well-pleaded facts elsewhere in the Complaint, this information is enough, without more, to identify the minor children Plaintiffs video viewing requests and histories based on information that Google already has in its possession and from its own activities. *Id.* at App'x 153. To put it in the terms of *Hulu* and *Eichenberger*, Viacom has disclosed to Google persistent cookie

[6] The District Court's Second Order erred in finding Plaintiffs needed to plead that they signed up for a particular Google service. Plaintiffs disagree. Nevertheless, Plaintiffs' aver that their parents had Google accounts, and an amended pleading could cure the deficiency. If this Court requires such, District Courts should grant leave to amend, even where such relief is not sought.

identifiers for which Viacom knows Google already has a "correlated look-up table" created through Google's own services.

B. American Courts Have Long Recognized that PII is Contextual

Where the text of a statute does not expressly or exhaustively define a term, recourse to the common law is appropriate. *Clackamas Gastroenterology Assoc. v. Wells*, 538 U.S. 440, 444-48 (2003). In the context of PII, the common law has long treated information known by the recipient to refer to a person as personally-identifiable. For example, the tort of defamation requires the plaintiff to prove, among other things, that the defendant made a defamatory comment "of and concerning the plaintiff." *Taj Mahal Travel, Inc. v. Delta Airlines, Inc.*, 164 F.3d 186, 189 (3d Cir. 1998). As the Restatement (Second) of Torts explains:

> It is not necessary that the plaintiff be designated by name; it is enough that there is a description or reference to him that those who hear or read [it] reasonably understand the plaintiff to be the person intended.

RESTATEMENT (SECOND) OF TORTS, § 564, comt. B. Further, "It is not necessary that everyone recognize the other as the person intended; it is enough that any recipient of the communication reasonably so understands it." *Id.* Finally, even where the Defendant is inept in its description, liability will attach. *Id.* at comment a. ("If it is in fact intended to refer to [the plaintiff], it is enough that it is so understood even though he is so inaccurately described that it is extraordinary that the communication is correctly understood." In *Taj Mahal*, the Third Circuit found the plaintiff had

adequately alleged a communication "of and concerning the plaintiff" even though the defendant did not identify plaintiff by any name or number. In this case, Defendant Viacom has identified each individual Plaintiff with far more information and, as such, this Court should hold that Plaintiffs have adequately alleged facts showing disclosure of PII under the VPPA.

C. Every Federal Fact-Finder to Examine the Issue Has Found that Persistent Unique Identifiers are PII

In addition to the common law, it is also appropriate for courts to look to similar provisions of similar statutes. *See United States v. Knox*, 32 F.3d 733, 753 (3d Cir. 1994). To Appellants' knowledge, every other federal statute containing the phrase PII has been interpreted to include information like the information at issue in this case. These statutes include the Children's Online Privacy Protection Act (COPPA),15 U.S.C. § 6501; the Gramm-Leach Financial Modernization Act, 15 U.S.C. § 6801; the Federal Education Rights and Privacy Act (FERPA), 20 U.S.C. § 1232; and the Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. § 1320.

Like the VPPA, these statutes all define "personally-identifiable information" or a like term in an open-ended fashion. Unlike the VPPA, these statutes delegate fact-finding to determine precise and updated definitions of PII to federal agencies. Every agency interpreting the definition of personally-identifiable information under these acts has found that the information disclosed by Viacom to Google is PII.

Under COPPA, which protects the Internet privacy of American children, the FTC has found that "online contact" information" and "persistent identifier[s] that can be used to recognize a user over time and across different Web sites or online services." These persistent identifiers include, but are not limited to "a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device series number, or unique device identifier." 16 C.F.R. § 312. Likewise, Gramm-Leach and HIPAA, respectively, define PII to include "any information ... collect[ed] through an Internet cookie" and account numbers, device identifiers, URLs, IP addresses, and "any other unique identifying number, characteristic or code." *See* 17 C.F.R. §248.3(u)(2)(F) and 45 C.F.R. § 164.514(e)(2).

Similarly, under FERPA, the Department of Education has found that PII "include[s]" but is not limited to "personal identifier[s]," "indirect identifiers such as the student's date of birth," "other information that . . . is linked or linkable to a specific student that would allow a reasonable person . . . to identify the student with reasonable certainty," or "information requested by a person who the educational agency . . . reasonably believes knows the identity of the student to whom the education record relates." 34 C.F.R. § 99.3.

D. The Defendants' Define PII to Include the Information in This Case

Defendants are both members of the Interactive Advertising Bureau. As members, Defendants' agreed to IAB's Code of Conduct, which requires compliance

with the Self-Regulatory Principles for Online Behavioral Advertising. IAB's Code of Conduct specifically states that members will "not collect 'personal information' as defined in [COPPA] from children they have actual knowledge are under the age of 13 or from sites directed to children under the age of 13 for Online Behavioral Advertising." As such, the Defendants have agreed to the definition of PII in COPPA. *Second CAC* at App'x 150.

E. The District Court's Interpretation of PII is an Outlier Which Intrudes Upon the Province of the Jury

When compared to existing case law on the VPPA, long-held common law rulings, and expert opinions within federal agencies and the data industry, the District Court's interpretation of PII is an outlier. By the plain terms of the VPPA, confirmed by legislative history, Congress purposely chose a broad and open-ended definition of PII to keep pace with technological innovation. To Plaintiffs' knowledge, every fact-finding federal agency charged with determining whether type of information disclosed by Viacom to Google contains PII has found that it does.

The difference between the VPPA and those statutes is that the VPPA does not specifically assign responsibility for enforcement to a federal agency. Instead, it creates a private cause-of-action. For the other statutes, the proper fact-finder is the federal agency charged with enforcement. For the VPPA and its private cause-of-action, the proper fact-finder is a jury.

F. Defendant Google Can Be Held Liable for Knowingly Receiving the Plaintiffs' Video Viewing Histories in Violation of the VPPA

Google is a proper Defendant for a disclosure claim under the VPPA because it is in possession of illegally obtained PII. Parties "who are in possession of personally identifiable information as a direct result of the improper release of such information are subject to suit under the [VPPA]". *Dirkes v. Borough of Runnemede*, 936 F.Supp. 235, 240 (D.N.J. 1996). In *Dirkes*, the Court reasoned that among the relief available to plaintiffs under the VPPA are equitable remedies. 18 U.S.C. 2710(c)(2)(D), *Dirkes,* 936 F.Supp. at 239. In order to effectuate the VPPA's purpose, which is to protect an individual's private information, possessors of illegally obtained information must be able to be hauled into court to prevent further disclosure. *Id.* at 241.

Here, as in *Dirkes*, Plaintiffs allege that Google has illegally received their PII, along with their video viewing histories, from Viacom in direct violation of the VPPA. *Second CAC* at App'x 141-42, 152-53. Like the plaintiffs in *Dirkes*, the Plaintiffs here should be able to seek the remedies available to them under the VPPA to prevent further disclosure of their information.

The District Court opinion's reliance on *Daniel v. Cantrell*, 375 F.3d 377 (6th Cir. 2004) is misplaced. In *Daniel*, the plaintiff had pleaded guilty to sexual molestation of three underage girls. From prison, he filed suit pro se against various retail video store employees and law enforcement officers for alleged violations of

the VPPA relating to the investigation of his crimes. The *Daniel* Court, however, misreads the VPPA.

The VPPA cause-of-action section provides that "[a]ny person aggrieved by *any act of a person* in violation of this section may bring a civil action." 18 U.S.C. § 2710(c)(1). Thus, the cause-of-action section of the VPPA does not limit actions to VTSPs, but instead provides that an action may be brought against any person acting in violation of this section. As the knowing recipient and participant in a scheme involving the disclosure of the plaintiffs' PII, Google was a person in violation of the VPPA and can, accordingly, be held liable.

II. THE DISTRICT COURT ERRED IN DISMISSING PLAINTIFFS' COUNT II (TITLE I OF THE ECPA (THE WIRETAP ACT))

A. Electronic Communications Privacy Act Title I (the Wiretap Act)

The paramount objective of the ECPA "is to protect effectively the privacy of communications." *In re Pharmatrak, Inc.,* 329 F.3d 9, 18 (1st Cir. 2003) (citation omitted). The Act entitles private parties to bring a cause of action for damages and injunctive relief where aggrieved by a defendant's unauthorized interception of electronic communications. *DIRECTTV, Inc v. Pepe,* 431 F.3d 162, 167 (3d Cir. 2005). A properly pled claim under Title I of the ECPA consists of allegations that the defendant: (1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a device. *In re Pharmatrak,* 329 F.3d at 18.

The District Court dismissed Plaintiff's Wiretap Act claim on two bases:

(1) that Plaintiffs had not pled facts showing the Defendants intercepted the "contents" of their online communications; and,

(2) that there was valid consent to the interception by one party to the communication. July 2, 2014 Opinion of District Court at App'x 30-36.

The District Court erred in both respects.

B. The District Court Erred in Finding that Uniform Resource Locators (URLs) are Not Contents Under the ECPA.

The ECPA defines "contents" broadly. It "includes *any* information concerning the substance, purport, or meaning[7] of [a] communication." 18 U.S.C. § 2510(8) (emphasis added). This definition governs both Title I to the ECPA (the Wiretap Act), and its reciprocal counterpart, Title III to the ECPA (the Pen Register Act).[8] Plaintiffs' alleged Defendants' intercepted their online communications, including the URLs that divulged the substance of Plaintiffs' communications with web sites. *See* Master Consolidated Complaint ("*First CAC*") at App'x 90-95, 97-98; and *Second CAC* at App'x 130-31. (Providing three examples URLs). Despite

---

[7]As this definition makes clear, what is the substance, purport or meaning of a communication is largely a factual question a jury should decide.

[8]Combined, the Wiretap and Pen Register Acts cover all aspects of a communication. The Wiretap Act prohibits the interception of "contents," and the Pen Register Act prohibits the recording of non-content "dialing, routing, addressing, or signaling (DRAS)." 18 U.S.C. § 3127(3). URLs contain both content and signaling information.

these allegations, the District Court erred in holding, as a matter of law, that a URL was exclusively a "location identifier" akin to identification and address information and did not include "any information relating to the substance, purport, or meaning" of a communication. July 2, 2014 Opinion of District Court at App'x, 33-36.

C. Defendant Google Has Conceded That Some URLs Contain Content Under the Wiretap Act

A nearly identical question is pending before the Third Circuit in *In re: Google, Inc. Cookie Placement Consumer Privacy Litig.*, No. 13-4300. At oral argument in that case, counsel for Defendant Google conceded that (1) whether a URL contains "content" is a fact-intensive issue not easily subject to judicial dismissal, and (2) many URLs contain content. The following is from the transcript of oral argument held on December 11, 2014 in that case:

> JUDGE KRAUSE: Can you talk to us about whether – again, thinking about this as sort of combined communication, are URLs content?
>
> MR. RUBIN: We don't think the Court gets to that question here.
>
> JUDGE FUENTES: But if we did?
>
> MR. RUBIN: If you did, we don't think that that question is susceptible to a ruling as a matter of law. It's a fact-intensive question.

Transcript of December 11, 2014 Third Circuit Oral Argument in *In re: Google, Inc. Cookie Placement Consumer Privacy Litig.*, No. 13-4300 at App'x 393. Later, the Court returned to the topic of whether URLs contain content:

> JUDGE KRAUSE: Could we go back to content for a moment?
>
> JUDGE FUENTES: Sure.
>
> JUDGE KRAUSE: Do you acknowledge then, that there are URLs – perhaps many URLs – that you would concede constitute content for purposes of the Wiretap Act?
>
> MR. RUBIN: We acknowledge that there may be some URLs that could constitute content.

Id. at App'x 398.

D. Logic and Case Law Support the Conclusion that URLs Contain Content

With the exception of the District Court opinion here and the District Court opinion on appeal in the *In re: Google Cookie Placement* case, every federal court examining whether URLs contain contents under the Wiretap Act have ruled that they can or do. *See* e.g. *United States v. Forrester*, 512 F.3d 500, 510 fn. 6 (9th Cir. 2007); *In re: Pharmatrak*, 329 F.3d 9, 18 (1st Cir. 2003); *Declassified Opinion from the United States Foreign Intelligence Surveillance Court* ("Declassified FISC Opinion") at App'x 163-279; *In re: Application of the United States for an Order Authorizing the Use of a Pen Register*, 396 F.Supp. 2d 45 (D. Mass. 2005); *Sams v. Yahoo*, 2011 WL 1884633 at *11 (N.D. Cal. May 18, 2011); and *In re: Zynga Privacy Litigation*, 750 F.3d 1098 (9th Cir. 2014).

In the Declassified FISC Opinion, the NSA sought to track URLs under the counterpart to the Wiretap Act, the Pen Register Act. Declassified portions of the

opinion reveal the NSA took a position identical to the one the District Court adopted in this case–that URLs are not "contents" because they are dialing, routing, addressing and signaling information (DRAS), and thus, mutually exclusive of "content." Declassified FISC Opinion at App'x 193. The Foreign Intelligence Surveillance Court (hereinafter FISC), which routinely analyzes the ECPA, flatly rejected the NSA's argument, explaining, "The breadth of the terms used by Congress to identify categories of information subject to collection and to define "contents" reinforces the conclusion that DRAS and contents are *not* mutually exclusive categories." Declassified FISC Opinion at App'x 193. The FISC pointed out that while a URL does "constitute[] a form of addressing information," it also "can also include contents." *Id.* [9]

Congress has also confirmed its intention for URLs to be treated as "content" in the PATRIOT Act. *See* P.L. 107-56, PATRIOT Act, House Report No. 107-236(I) at 54 (stating "an order under the statute could not authorize the collection of email subject lines, which are clearly content. Further, an order could not be used to collect information other than "dialing, routing, addressing, and signaling" information, *such as the portion of a URL (Uniform Resource Locator) specifying Web search terms or the name of a requested file or article.* (emphasis added)). Another recently declassified document reveals that the NSA apparently changed

[9] Federal courts have also concluded that mere numbers can constitute "content" as well. See *Brown v. Waddell*, 50 F.3d 285, 87-88 (4th Cir. 1995) (Numbers sent to a pager which are "more extensive … than those in telephone numbers" contain "contents.") and *U.S. Telecom Assoc'n v. FCC*, 227 F.3d 450 (D.C. 2000) ("Post-cut-through digits" entered by a telephone caller after being connected to the recipient of their call "can also represent call content.") If mere numbers punched into a telephone can constitute content, so too must words that detail an Internet user's precise communications with the websites with which they choose to interact.

its position on URLs and, in a subsequent brief to FISC, cited with approval the exact same sentence of legislative history and the same cases cited by Plaintiffs herein. *See* Memorandum of Law and Fact in Support of Application for Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes ("Declassified NSA Brief") at App'x 329-30.

That "contents" and DRAS information are not mutually exclusive for URLs becomes clear upon considering the different parts of a URL. Consider the following real-world URL from the website HubPages.com.:

http://progressivehealth.hubpages.com/hub/How-Do-I-Reduce-Herpes-Breakouts

Broken down, this URL contains the following parts:

1. ***http://***

   This part of the URL identifies the computer *language* (http:) the web-browser and the host web-server will use to communicate.

2. ***progressivehealth.hubpages.com/***

   This part of the URL identifies the *name of the website* and the corresponding host web-server with which this person intended to communicate.

3. ***hub/***

   This part of the URL identifies the *specific electronic folder* on the host webserver that contains the contents of the information the Internet user has requested.

4. ***/How-Do-I-Reduce-Herpes-Breakouts***

   This part of the URL identifies the *precise file or document* contained within the folder the Internet user has requested.

5. ***/hub/How-Do-I-Reduce-Herpes-Breakouts***

> The combination of the folder and the precise file name is called the "*file path.*"[10]

This URL exhibits duality of function. It serves as the address for this particular page on the Internet, but also reveals the substance and meaning of this user's communication with this website. Indeed, if this person had called Hubpages on the phone and requested the article, and if Google had tapped that phone line and intercepted that request, there is no question such conduct would violate the Act.[11] Plaintiffs' allegations about Internet requests are no different. *See In re Application of the U.S.,* 396 F.Supp.2d at 49-50 ("contents" included URL "subject lines, application commands, search queries, requested files names, and file paths."); *U.S. v. Forrester,* 512 F.3d 500, n. 6 (9th Cir. 2008) (URL, unlike IP address, "reveals much more information" about user's Internet activity, including articles viewed).

In this case, Plaintiffs specifically pled the interception of URL "file paths." *First CAC* at App'x 95.[12] Other examples from the Plaintiffs' complaints illustrate

---

[10] See http://technet.microsoft.com/en-us/library/ff919564(v=office.14).aspx for Microsoft's description of the parts of a URL. Last visited October 17, 2013.

[11] Similarly, if the Plaintiffs had called a phone number with an automated answering machine and, through post-cut-through-dialed-digits, indicated that they sought information contained in the file path, that too is protected by the ECPA.

[12] The District Court's reliance on *Zynga* is misplaced. In *Zynga*, the Ninth Circuit explained that URLs contain "content" where they contain a "search term" or "similar communication" which requests "specific information." *In re: Zynga Privacy Litigation*, 750 F.3d 1098, 1109 (9th Cir. 2014). In that case, the plaintiffs

how full-string URLs, which contain application commands, requested file names, file paths, and search queries, contain information "about the substance, purport or meaning" of communications. These URLs include:

(1) www.nick.com/shows/penguins-of-madagascar/;

(2) www.wikihow.com/Deal-With-Your-Parents'-Divorce; and

(3) www.nick.com/digital-short-penguins-of-madagascar-shorts-skippers-nightmare. *Second CAC* at App'x 129-30.

The Plaintiffs and American Internet users in general, do not just accidentally send GET requests with random URLs. Internet communications consist of deliberate acts. To arrive at a given URL, each Plaintiff must either: (1) type the URL directly into their web-browser; or (2) click on a hyper-link which indicates the substance, purport, and meaning of the associated webpage. Both methods involve a conscious choice by the user to request such information.

Each of the URLs listed above conveys content, i.e. information "relating to the substance, purport, or meaning" of a communication. The Plaintiffs could only

---

had only alleged interception of Facebook profile URLs that revealed a username or group name. For example, www.facebook.com/nytimes is the profile page for the New York Times and www.facebook.com/bedelman is the profile page of Facebook user Ben Edelman. *In re: Zynga*, Facebook Response Brief at 8-9, n. 7. The URLs in this case are different. They seek particular content or "specific information," including *file paths*, related to, respectively: (1) Penguins of Madagascar, (2) dealing with a parents divorce, and (3) the Penguins of Madagascar short video titled Skipper's Nightmare.

get to the webpages with those URLs by directly entering them into their web-browsers or by clicking on a hyperlink, either of which would send a "GET" request to Nick.com or WikiHow.com requesting information on the relevant subjects – Penguins of Madagascar, How to Deal with Divorce, and Digital Shorts Penguins of Madagascar Skippers Nightmare.

In turn, Nick.com and WikiHow.com send communications back that contain videos and information directly relating to the topics which are obvious from those URLs. The Wiretap Act protects both the sending and the receipt of electronic communications. While the District Court's focus was on the Plaintiffs' acts of sending the GET request to a website, the Plaintiffs also receive information in response to those GET requests. The URLs listed above contain information relating to the "substance, purport, or mean" of both the Plaintiffs' GET requests to websites as well as the communications received by the Plaintiffs in turn.

As such, the District Court's analysis ignores the reality recognized in the FISC's recently declassified decision that URLS are simultaneously location identifiers and the "contents" of a user's online communication. The concepts are not mutually exclusive. *Declassified FISC Opinion* at App'x 194-195.

Plaintiffs have alleged that dual character here. The interception of Plaintiffs' electronic communications allowed the Defendants to determine that Plaintiffs were making specific requests for information on particular topics – and, in turn, receiving

responses relating to those topics. This amounts to the substance and meaning of a communication. *See In re Application of the United States,* 329 F.Supp.2d at 49.

E. Plaintiffs also Alleged the Interception of Content in the Form of Birthdate and Gender Information

Plaintiffs also allege that Defendant Google's cookies intercepted personal information such as their gender and birthdate that Plaintiffs had provided to Viacom. *Second CAC* at App'x 140-41. Such information, which Plaintiffs intended to communicate to Viacom, also constitutes contents. *See In re: Pharmatrak, Inc.,* 329 F.3d. at 19 (1st Cir. 2003).

F. The District Court Erred in Determining at the Pleading Stage That There Was Consent for the Interception as a Matter of Law

Consent to the interception by a party to the communication is a defense the defendants bear the burden of establishing.[13] *In re Pharmatrak,* 329 F.3d at 19 (1st Cir. 2003). The District Court ruled as a matter of law at the pleading stage, without the parties having conducted any discovery, that Viacom consented for Google to intercept Plaintiffs' online communications. The District Court erred in making this determination as consent does not bar a Wiretap Act claim when a communication is intercepted for the purpose of committing a criminal or tortious act in violation of

[13]Affirmative defenses may not be raised in a motion to dismiss unless there are no disputed issues of fact. *See e.g. Scott v. Kuhlman,* 746 F.2d 1377, 1378 (9th Cir. 1984) (citing Wright & Miller, *Federal Practice and Procedure* § 1277 at 328-30).

the Constitution or laws of the United States or of any State. 18 U.S.C. § 2511(2)(d). Alternatively, Viacom's consent is not sufficient here because the communication involved minors, who, as a matter of law, are incapable of consent.

1. The Master Consolidated Complaint Alleged Facts Showing that Defendants' Interceptions Were Accomplished for a Criminal and Tortious Purpose

18 U.S.C. § 2511 (d) (2) provides:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception *unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State*.

18 U.S.C. § 2511 (d) (2) (emphasis added). The District Court wrongly concluded that Plaintiffs' had not pled facts triggering the "criminal or tortious act" exception to the consent exception of the Federal Wiretap Act.

A cause of action for intrusion upon seclusion sounds in tort. *Rumbauskas v. Cantor,* 649 A.2d 853, 854 (N.J. 1994). Thus, a person intending to intrude upon the seclusion of another necessarily acts with a tortious purpose by violating the other's right to be let alone. Plaintiffs' complaint included a cause of action for intrusion upon seclusion and alleged that the Defendants intentionally intruded upon the Plaintiffs' solitude or seclusion by taking information from the privacy of their own homes. *Second CAC* at App'x 155-61; *First CAC* at App'x 104. Said

differently, the Complaint alleged that the Defendants acted with the purpose of intruding upon the minor Plaintiffs' right to be let alone—that is, a purpose that the law recognizes to be tortious. The Complaint also alleged that the defendant's acted with a criminal purpose by violating numerous federal and state statutes, including 18 U.S.C. § 1030 (a)(2)(C) of the Computer Fraud and Abuse Act. These allegations were sufficient to show that the Defendants acted with a tortious and/or criminal purpose.

The District Court incorrectly reasoned that the instant case was about "illegal means" and not an "illegal purpose." Respectfully, the District Court's analysis conflates allegations of an illegal purpose (i.e. to intrude upon Plaintiffs' right to be let alone) with allegations concerning the benefits the Defendants intended to derive from that purpose. As the Ninth Circuit has stated: "For this [Wiretap] claim to survive . . . [Plaintiff] had to come forward with evidence to show that [the defendant] taped the conversation . . . *for the purpose of violating Cal. Penal Code § 632,* [or] *for the purpose of invading her privacy . . . .*" *Detersa v. ABC*, 121 F.3d 460, n. 4 (9th Cir. 1997). Plaintiffs specifically alleged that the Defendants intercepted Plaintiffs' Internet communications "for the tortious purpose of intruding upon the Plaintiffs' seclusion" and for criminal purposes in violation of numerous federal and state statutes, including the Computer Fraud and Abuse Act. These allegations were sufficient to allow Plaintiffs to go forward and conduct discovery

on these issues. The fact that the Defendants sought to monetize the information they obtained as a result of intruding upon the Plaintiffs' seclusion does not make the criminal and tortious act exception inapplicable.

2. Whether Viacom Consented to the Interception is Irrelevant Because Plaintiffs are Minors

The ability of a minor to provide consent has never been treated in the same way as an adult. The age of a minor is "more than a chronological fact." *Eddings v. Okl.,* 455 U.S. 104, 115(1982). "It is a fact that generates commonsense conclusions about behavior and perception." *J.D.B. v. North Carolina*, 131 S.Ct. 2394, 2403 (2011).. The Supreme Court has reiterated this concept repeatedly and unequivocally. *See e.g., Bellotti,* 443 U.S. at 635 (plurality opinion) (Children "often lack the experience, perspective, and judgment to recognize and avoid choices that could be detrimental to them"); see also *Gall v. United States,* 552 U.S. 38, 58(2007); *Roper v. Simmons,* 543 U.S. 551, 569 (2005); *Johnson v. Texas,* 509 U.S. 350, 367(1993).

It is a basic tenet that interactions involving minors cannot be judged by the same standard as those between two adults. The better rule (and the one this Court should adopt) is that "when one party to a conversation is under the age of eighteen, the *only* person who can consent to an interception is a . . . judge" or parental guardian. *See Bishop v. State*, 241 Ga.App. 517, 522 (1999) (emphasis in original). See also *L.C. v. Central Pa. Youth Ballet*, No. 1:09-cv-2076, 2010 WL 2650640 at

*3 (M.D. Pa., July 2, 2010)(Denying defendant's motion to dismiss and holding intentional disclosure of recorded conversation with minor child violates ECPA).

G. Plaintiffs Adequately Alleged Interceptions of the Minor Children Plaintiffs' Communications on Non-Viacom Websites Without Consent

The District Court failed to address directly Plaintiffs' Wiretap claim relating to interceptions of their communications with non-Viacom websites. *See First CAC* at App'x 96-98. Consent under the ECPA cannot be "casually inferred." *In re: Pharmatrak*, 329 F.3d 9, 20 (1st Cir. 2003). Just as a medical patient may consent to one form of treatment but refuse another, so too may a party consent to access to "only a subset of its communications." *Id.* at 19. The non-Viacom websites where Google tracked the plaintiffs may have consented to the interception of some of some communications, but there is nothing to suggest they consented to the interceptions of communications with Internet users that Google knew to be minor children. And if they did consent to such interceptions, it is a fact-issue to be determined by discovery. Accordingly, these interceptions are not subject to the same "consent" defense because Defendants cannot plausibly claim that the non-party non-Viacom websites knew or consented to the tracking of minor children on their websites. For these interceptions (and for the interceptions discussed above), Viacom can also be held liable for procuring Google to violate the ECPA. *See Lonegan v. Hasty*, 436 F.Supp.2d 419, 428 (E.D. N.Y. 2006) (concluding procurement liability still exists under the ECPA). *Id.* Thus, Plaintiffs may maintain a cause of action against Viacom

for facilitating Google's violations of Plaintiffs' rights under the ECPA. *First CAC* at App'x at 97.

III. THE DISTRICT COURT ERRED IN DISMISSING PLAINTIFFS' CLAIM UNDER CAL. PENAL CODE § 631 (THE CALIFORNIA INVASION OF PRIVACY ACT)

A. For The Same Reasons Set Forth in Point II Regarding "Content," the District Court Erred in Dismissing Plaintiffs' California Wiretap Claim

The California Wiretap Act is codified at Cal. Penal Code § 631. California courts have interpreted this provision consistent with the federal Wiretap Act, with one crucial exception. California's act is an *all-party consent* statute. That is, an interceptor must show it obtained the consent of *all* parties to a communication to avoid liability. Cal. Penal Code § 631(a). The complaints make clear that Plaintiffs did not, and indeed, legally could not have consented to Defendants' interception of their communications with the Viacom children's websites and other websites irrespective of whether Viacom consented to the interception. *First CAC* at App'x 96-97.

Recognizing this, the District Court dismissed Plaintiffs' California Wiretap Act claim on the basis that the Plaintiffs had not alleged facts showing the interception of "content." For the same reasons set forth above, the District Court erred. Accordingly, this Court should reverse the District Court's dismissal of Plaintiffs' California Wiretap claim and remand the matter so that discovery may commence.

IV. THE DISTRICT COURT ERRED IN DISMISSING PLAINTIFFS' CLAIM UNDER 18 U.S.C. § 2701 (STORED COMMUNICATIONS ACT)

A. Plaintiffs Properly Pled a Stored Communications Act Claim

The Stored Communications Act (SCA) provides a cause of action against "whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided, or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system . . . ." 18 U.S.C. § 2701(a).

The District Court erred in dismissing Plaintiffs' SCA claims by holding that Plaintiffs' personal computing devices and/or browser-managed files do not qualify as "facilities through which" any electronic service is provided under the SCA.

Under the plain-language of the SCA, a "facility" can be anything "through which an electronic communication service is provided." 18 U.S.C. § 2701(a). This definition includes facilities operated by third party Electronic Communication Service ("ECS") providers, such as Internet Service Providers ("ISPs"), email servers, and electronic bulletin boards. *See Chance v. Avenue A, Inc.*, 165 F.Supp.2d 1153, 1160 (W.D. Wash. 2001). By the statute's plain language, the broad term "facility" also includes personal devices and software that serve as conduits for third-party ECS services. 18 U.S.C. § 2701(a).

Under the plain language of the statute, the "facility" analysis is two-fold. First, there must an ECS provided; and, second, there must be something (i.e., a facility) through which that service is provided. 18 U.S.C. § 2701(a).

1. Plaintiffs' Internet Service Providers and Web Browsers Provide Electronic Communications Services as Defined in 18 U.S.C. § 2510 (15)

The ECPA defines an "electronic communication service" broadly to include "*any* service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (emphasis added). Both ISPs, like Comcast, and web browsers, like Google Chrome and Apple Safari, satisfy this definition. (Complaint ¶¶ 24,166-167). ISPs are physical infrastructure that help fulfill web browsers' requests. In turn, web browsers provide a service Internet users employ to send and receive electronic communications over the Internet.[14] 18 U.S.C. § 2510(15).

2. Plaintiffs' Computers and the Browser Managed Files Within Them That Store Information are "Facilities"

In light of the plain language of 18 U.S.C. 2701(a), anything that acts as a "conduit" for ECS qualifies as a "facility" for purposes of the SCA. *See, Quon v.*

---

[14] For a description of why a browser is an ECS. *See Google's explanation of its own Chrome browser.* http://googleblog.blogspot.com/2008/09/fresh-take-on-browser.html (last visited February 4, 2014) ("We search, chat, email and collaborate in a browser. And in our spare time, we shop, bank, read news and keep in touch with friends -- all using a browser.").

Arch Wireless Operating Co., Inc., 529 F.3d 892, 902 (9th Cir. 2008) (noting that electronic communications pass through a "conduit") (reversed on other grounds by *City of Ontario, Cal. v. Quon,* 560 U.S. 746 (2010)).

Here, both Plaintiffs' computers and the browser managed files contained within them are "facilities" because they act as the "conduit[s]" through which ISPs and web-browsers provide ECS. *See, Chance*, 165 F.Supp.2d at 1161; *Expert Janitorial, LLC v. Williams*, No. 3:09-CV-283, 2010 WL 908740 at *5 (E.D. Tenn. 2010); *Becker v. Toca*, No. 07-7202, 2008 WL 4443050 at * 4 (E.D. La.2008).

Cases holding otherwise have conflated the concept of a "facility" and an ECS provider. Yet, there is nothing in the statute which requires that a "facility" must also be the ECS provider or something in the complete control of the ECS provider. 18 U.S.C. § 2701(a).

Plaintiffs do not contend that their personal computers, or the browser managed files on those computers, are ECS providers. *First CAC* at App'x 100. Instead, as "facilities," they are merely the conduits for electronic communication services provided by third party ISPs and web browsers. *Id.* at App'x 99-100 (identifying ISPs and web browsers as providers of ECS). In other words, Plaintiffs' personal computers and browser managed files are the things "*through which* an electronic communication service is provided." 18 U.S.C. § 2701(a) (emphasis added); *see In re Intuit Privacy Litig.*, 138 F.Supp.2d 1272, 1282 n. 3

(C.D. Cal. 2001) (the SCA "does not require that Plaintiffs' computers to be 'communication service providers' only that they be a facility through which an electronic communication service is provided.")

Accordingly, this Court should reverse the District Court's dismissal of Plaintiffs' California Wiretap claim and remand the matter so that discovery may commence.

V. PLAINTIFFS PROPERLY PLED A DAMAGE IN BUSINESS OR PROPERTY UNDER THE NEW JERSEY CONSUMER RELATED OFFENSES ACT

The NJCROA provides a right of action for damages to any person (1) "damaged in business or property." *See* N.J.S.A. § 2A:38A–3. Plaintiffs' factual allegations, properly construed, are more than sufficient to support their claim. Plaintiffs allege sufficient damages that ties the NJCROA to unjust enrichment in a quasi-contractual setting. *See Second CAC* at App'x 155.

The NJCROA states "[a] person or enterprise damaged in business or property as a result of any of the following actions may sue the actor therefor[.]" N.J.S.A. 2A:38A-3. Plaintiffs need not show the precise value of the damage caused because the NJCROA tasks a jury with that charge. *See* N.J.S.A. § 2A:38A-4 ("[t]he value of damage, loss, property or income involved in any lawsuit shall be determined by the trier of fact."). Thus, Plaintiffs need only point to some damage in business or property and need not allege specific value at this early stage in the proceedings.

The *Second CAC* alleges that:

> Through conversion and without consent, Defendants harvested Plaintiffs' personal information for their unjust enrichment and to the financial detriment of Plaintiffs and Class Members. . . Plaintiffs, Class Members, and/or their parents and/or guardians would have at least expected remuneration for their personal information at the time it was conveyed.

Second CAC at App'x 155.

Plaintiffs present unjust enrichment not as an independent action in tort, but as a measure of damages under the NJCROA in a quasi-contractual sense. *See Goldsmith v. Camden County Surrogate's Office*, 975 A.2d 459, 463 (App. Div. 2009) (stating quasi-contracts permit unjust enrichment as available remedy). In a quasi-contract, "there is no agreement; but they are clothed with the semblance of contract for the purpose of the remedy, and the obligation arises not from consent, as in the case of true contracts, but from the law or natural equity." *Callano v. Oakwood Park Homes Corp.*, 219 A.2d 332, 334 (N.J. App. Div. 1966). Usually, a contract defines the duty, but "in the case of **quasi-contracts** the duty defines the contract. Where a case shows that it is the duty of the defendant to pay, the law imparts to him a promise to fulfill that obligation. The duty which thus forms the foundation of a **quasi-contractual** obligation is frequently based on the doctrine of unjust enrichment." *Id.*

To show unjust enrichment a party must demonstrate "that it expected remuneration from the defendant at the time it performed or conferred a benefit on defendant and that the failure of remuneration enriched defendant beyond its

contractual rights." July 2, 2014 Opinion at 38, citing *VRG Corp. v. GKN Realty Corp.*, 641 A.2d 519, 554 (N.J. 1994). A plaintiff need only show that if they had known all the facts "he would have expected remuneration from defendant. . . ." *Id.*, citing *Mu Signa, Inc. v. Affine, Inc.*, No. 12-cv-1323 (FLW), 2013 WL 3772724, at *10 (D.N.J. July 17, 2013).

Here, when the minor Plaintiffs first visited Nick.com, they were greeted by a picture of Sponge Bob Square Pants and asked to enter information including their name, gender and date of birth. *Second CAC* at App'x 140. Right above Sponge Bob is the following language: "HEY GROWN-UPS: We don't collect ANY personal information about your kids. Which means we couldn't share it even if we wanted to!" *Id.* (emphasis in original). The form itself belies this statement, as the form asks for Plaintiffs' personally identifiable information (PII) in the form of gender and birthdate. *Id.* Additionally, Plaintiffs allege the illegal harvesting, conveyance and use of Plaintiffs' IP address, browser settings, and video viewing histories. *Id.* at App'x 141. At the time that the minor Plaintiffs provided their PII, they had no way of knowing how the information would be used. Had they known, and more importantly had their parents or legal guardians known, that Defendants would monetize their PII, Plaintiffs would not have provided their PII without compensation or would have at least had the option not to provide that information

in the first place. Defendants, through nefarious business practices, hid this from Plaintiffs, denying them of that choice.

Undoubtedly, Plaintiffs' PII has monetary value to Defendants.[15] So too does Plaintiffs' PII have value to Plaintiffs as this is part of the basis for the privacy interest alleged in the Second Complaint's intrusion upon seclusion claim. Had Plaintiffs known that the information they provided would be harvested and illegally conveyed to Defendants for advertising purposes, they would have had a choice not to send the information. As such, now Plaintiffs have no choice about what happens to the PII Defendants harvested and conveyed, but they should at least be compensated, and rightly would have expected compensation, for the benefit Defendants received. Thus, this Court should deny Defendants' motions because Plaintiffs have demonstrated an injury in business or property as required by the NJCROA.

VI. THE DISTRICT COURT ERRED IN DISMISSING PLAINTIFFS' CLAIMS FOR INTRUSION UPON SECLUSION

Plaintiffs' well-pled facts confirm Defendants' conduct is actionable under the common law privacy tort of intrusion upon seclusion. Plaintiffs' facts demonstrate in detail (1) intentional intrusions by Defendants (2) upon the solitude or seclusion of Plaintiffs and their private affairs, which (3) would be highly

[15] The precise amount attributed to that value is contested by both parties, but it is not important at this point in the proceeding. *See* N.J.S.A. § 2A:38A-4.

offensive to a reasonable person. *See Hennessey v. Coastal Eagle Point Oil Co.*, 609 A.2d 11, 17 (N.J. 1992), quoting RESTATEMENT (SECOND) OF TORTS, § 652B. Accordingly, Plaintiffs sufficiently stated an intrusion claim, and the District Court erred in holding otherwise.

In its Order on Defendants' first Motion to Dismiss, the District Court agreed Plaintiffs allege facts "demonstrating … [i] Plaintiffs had a reasonable expectation that certain aspects of their online identities remain private and [ii] that Defendants intruded upon those private concerns" July 2, 2014 District Court Opinion at App'x 42. Thus, the District Court found Plaintiffs' Complaint sufficient with respect to the first two elements of an intrusion claim. The District Court concluded, however, that Plaintiffs failed to set forth sufficient facts demonstrating Defendants' intrusions "would be highly offensive to a reasonable person." *Id.* The District Court therefore dismissed the claim without prejudice to allow Plaintiffs to re-plead. *Id.* Plaintiffs' amended their Complaint to include additional facts illustrating the "highly offensive" nature of Defendants' conduct. *Second CAC* at App'x 156-61. Nevertheless, the District Court again dismissed the claim, concluding as a matter of law that Defendants' alleged conduct is not "highly offensive." January 20, 2015 District Court Order at App'x 55. The District Court erred in that regard and this Court should remand for further proceedings.

A. The Determination of Whether Conduct is "Highly Offensive" is Generally a Fact Question and Should Have Been Treated As Such in This Case

Ordinarily, the determination of whether an intrusion is "highly offensive" is a question of fact. *See, e.g., Desmond v. Phillips & Cohen Assocs.*, 724 F. Supp. 2d 562, 569 (W.D. Pa. 2010); *Vurimindi v. Fuqua Sch. of Bus.*, 435 Fed. Appx. 129, 136 (3d Cir. 2011) (unpublished) (confirming district court erred in dismissing intrusion claim at pleadings stage).[16] And, while there are occasions where courts have decided the issue as a matter of law,[17] such a determination is appropriate "only … if reasonable persons can draw only one conclusion from the [facts alleged]." *Remsburg v. Docusearch*, 816 A.2d 1001, 1008 (N.H. 2003). In other words, at this stage, the issue may be decided against Plaintiffs as a matter of law only if no reasonable person could take the facts alleged in Plaintiffs' Complaint, which must be accepted as true and viewed in the light most favorable to Plaintiffs, and conclude

---

[16]*See also Toomer v. Garrett*, 574 S.E.2d 76, 90 (N.C. Ct. App. 2002) ("The kinds of intrusions that have been recognized under this tort include 'physically invading a person's home or other private place, eavesdropping by wiretapping or microphones, peering through windows, persistent telephoning, unauthorized prying into a bank account, and opening personal mail of another.'"); *Dalley v. Dykema Gossett*, 788 N.W.2d 679 (Mich. App. 2010) ("Whether a reasonable person would find an intrusion objectionable constitutes a factual question best determined by a jury."); *Ruzicka Elec. & Sons, Inc. v. IBEW*, 427 F.3d 511 (8th Cir. 2005) ("Whether a defendant obtained information through a method objectionable to the reasonable person is 'ordinarily a question for the jury.'").

[17]*See Boring v. Google*, 362 F. App'x 273, 279 (3rd Cir. 2010).

the subject conduct is "highly offensive." This is not such a case, and the District Court erred in holding otherwise.

On this point, a reasonable person could conclude Defendants' unauthorized interception, tracking, recording, and dissemination of young children's personal information and Internet communications is "highly offensive." This is especially true when Defendants' conduct is viewed against social norms regarding the protection of children and the right to privacy, as embodied in various sources of public policy, including, constitutional and legislative enactments, common law principles, and industry standards. Indeed, the actions by Defendants are strikingly similar to the actionable behavior described in §652B of the Restatement, and cited by this Court in *O'Donnell v. United States*—"wiretapping a ... phone or using binoculars to view inside a ... residence." *See O'Donnell v. U.S.*, 891 F.2d 1079, 1083 n.3 (3d Cir. 1989). As such, the District Court erred in deciding this issue as a matter of law.

B. Defendants' Unauthorized Intrusion into the Private Matters of Children Violated Their Reasonable Expectations of Privacy In a Highly Offensive Manner

The tort of intrusion is premised on a substantial interference with a plaintiff's seclusion—"a kind that would be highly offensive to the ordinary reasonable man, as the result of conduct to which the reasonable man would strongly object.'" *Castro v. NYT Television*, A.2d 1173, 1177 (N.J. App. Div. 2006), citing RESTATEMENT

(SECOND) OF TORTS § 652B, cmt. b). Whether an intrusion is "highly offensive" "turns on what a person's reasonable expectation of privacy is with respect to the item or area searched or intruded upon." *Torsiello v. Strobeck*, 955 F. Supp. 2d 300, 315 (D.N.J. 2013), citing *White v. White*, 781 A.2d 85 (N.J. Super. Ct. Ch. Div. 2001).[18] Applying that standard here, it is clear Plaintiffs properly stated an intrusion claim. Plaintiffs sufficiently allege facts confirming Plaintiffs had a reasonable expectation of privacy in their personal information and Internet communications, and that Defendants' alleged intrusions would be "highly offensive" to a reasonable person.

1. Plaintiffs Had a Reasonable Expectation of Privacy In the Information Obtained and Disseminated by Defendants

It is beyond dispute Plaintiffs had a reasonable expectation of privacy with respect to their personal information and communications. Indeed, as noted above, the District Court found Plaintiffs allege facts "demonstrating . . . Plaintiffs had a reasonable expectation that certain aspects of their online identities remain private . . . . July 2, 2014 District Court opinion at App'x 42. Plaintiffs' expectation of privacy is derived from, and supported by, general social norms[19] as embodied in

---

[18] *See also State v. Hempele*, 576 A.2d 793, 802 (N.J. 1990) (holding that "expectations of privacy are established by general social norms").

[19] *See Torsiello*, 955 F. Supp. 2d at 315 (stating "expectations of privacy are established by general social norms").

various sources of public policy, including, constitutional and legislative enactments, common law principles, and industry standards.

For example, the United States Constitution provides the most basic evidence of "social norms," serving as "a national expression of public policy, a moral compass to help us focus on the values that are at stake in this case." *Soliman v. Kushner Companies, Inc.*, 77 A.3d 1214, 1223-24 (N.J. App. Div. 2013). "[T]he right to privacy is 'grounded' in the Fourteenth Amendment of the United States Constitution's concept of 'personal liberty. . . . [which] safeguards at least two different kinds of interests: 'the individual interest in avoiding disclosure of personal matters,' and 'the interest in independence in making certain kinds of important decisions.'" *Id.* at 1223. Privacy is "a most fundamental human right," "the most comprehensive of rights," "the right most valued by civilized men," and one that is "older than the Bill of Rights..." *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 487 (1974), *Olmstead v. United States*, 277 U.S. 438, 478 (1928), *Griswold v. Connecticut*, 381 U.S. 479, 486 (1965).[20]

[20] This right and expectation of privacy has not diminished merely because we are live in the "Information Age." In *Riley v. California*, for example, the Supreme Court unanimously held Americans have a right to privacy in the data contained on personal computing devices, and it expressed particular concern for the privacy of "Internet search and browsing history." *Riley v. California*, 134 S.Ct. 2473, 2489-90 (2014).

Furthermore, as the District Court observed, "the right to privacy created by . . . the New Jersey constitution provides greater protection than the privacy right created by the federal Constitution" July 2, 2014 District Court Opinion at App'x 41 (citing *State v. Reid*, 945 A.2d 26, 32-34 (N.J. 2008)). "New Jersey 'explicitly recognizes a right to 'informational privacy,' which encompasses any information that is identifiable to an individual.'" *Id.* (citing *State. v. Reid*, 914 A.2d 310, 314 (N.J. Sup. Ct. App. Div. 2007)); *Doe v. Poritz*, 662 A.2d 367, 412 (N.J. 1995) ("We have found a constitutional right of privacy in many contexts, including the disclosure of confidential or personal information."). "'Personal information [is] any information, no matter how trivial, that can be traced or linked to an identifiable individual.'" *Id.* (quoting *Reid*, 914 A.2d at 314).

Civil and criminal statutes similarly evidence social norms regarding the preservation and protection of private information. *See, e.g., Latture v. Emmerling*, No. 304833, 2013 WL 5225243, at *4 (Mich. App. 2013) ("Criminal activity is an objectionable method of obtaining information."); *Clayton v. Richards*, 47 S.W.3d 149, 154 at n. 1 (Tex. App.—Texarkana 2001) ("Unlawful interception of wire, oral, or electronic communications is a criminal act under [Texas law]. Courts … give weight to the fact that conduct is a crime when determining if it also amounts to a tort."); *Nader v. General Motors Corp.*, 25 N.Y.2d 560 (N.Y. App. 1970) ("[T]o the extent the two challenged counts charge it with wiretapping and eavesdropping, an

actionable invasion of privacy has been stated."); *see also*, *inter alia*, the Video Privacy Protection Act, the Wiretap Act, the Pen Register Act, the Computer Fraud and Abuse Act and corresponding computer crime laws in all 50 states.

Finally, nowhere are these social norms clearer than with young children, whom the Supreme Court has recognized "have a very special place in life which law should reflect." *May v. Anderson*, 345 U.S. 528, 536 (1953). According to the Supreme Court, children are entitled to enhanced protection under the law precisely because: (1) children possess "peculiar vulnerability;" (2) children are unable "to make critical decisions in an informed, mature manner;" and (3) of the "importance of the parental role in child rearing." *Belotti*, 443 U.S. at 635. Recognizing these interests, Congress enacted the Children's Online Privacy Protection Act ("COPPA") in 1998 to protect against the collection of personal information over the Internet from children under the age of 13. *See* 15 U.S.C. §§ 6501-06. These social norms are also reflected in Defendants' own industry, which has established Terms of Use and other standards protecting young children from the collection and disclosure of personal information. *Second CAC* at App'x 126-27, 150, 157, 160-61.

Given these constitutional and legislative enactments, common law principles, and industry standards, Plaintiffs clearly allege a reasonable expectation of privacy with respect to their personal information and communications.

2. Defendants' Conduct in Obtaining and Disseminating Plaintiffs' Private Information was Highly Offensive

In their Second CAC, Plaintiffs allege the information obtained and disclosed by Defendants is "personal information" subject to an expectation of privacy for the reason that it can be traced or linked to identifiable individuals. *Second CAC* at App'x 131-38. Consistent with the established social norms described above, Plaintiffs allege Defendants, without seeking or obtaining the permission of Plaintiffs or their parents, invaded the privacy rights of millions of children under the age of 13 by obtaining, tracking, and disclosing personal information and Internet communications from the privacy of their homes, including the following: (1) the child's username/alias, (2) the child's gender, (3) the child's birthdate, (4) the child's IP address, (5) the child's browser settings; (6) the child's unique device identifier; (7) the child's operating system; (8) the child's screen resolution; (9) the child's browser version; (10) the child's web communications, including but not limited to detailed URL requests and video materials requested and obtained from Viacom's Nick.com website; and (11) the DoubleClick persistent cookie identifiers. *Second CAC* at App'x 131-38, 141-42, 152-57, 160. Plaintiffs further allege Defendant Viacom discloses this information to Google, knowing Google's ubiquity and ability to use the information to identify individuals. *Id.* at App'x 131-38,152-53. Additionally, Plaintiffs allege Defendants placed significantly more tracking technologies on children's websites than adult websites to take advantage of the

Plaintiffs' vulnerability as children. *Id.* at App'x 122, 160. Thus, Plaintiffs allege Defendants obtained and disclosed personal information and Internet communications knowing the same could be traced or linked to identifiable young children. *Id.* at 131-38, 153.

As Plaintiffs allege, given the special place of children in society, a reasonable person could find Defendants' unauthorized intrusions into the private matters of children under the age of 13 are "highly offensive" in that they exploit the vulnerability of children and disregard the importance of the parental role. Moreover, based on Defendants' unauthorized collection and disclosure of information that can be traced or linked to an identifiable individual, a reasonable person could find Defendants' intrusions "highly offensive" because they violate the social norms embodied in the "informational privacy" and confidential/personal information protections of the New Jersey Constitution, and fly in the face of a "most fundamental human right" enshrined in the U.S. Constitution.

Plaintiffs further allege that Defendants' intrusions are highly offensive because they violate the social norms embodied in: (1) the Terms of Use of Plaintiffs' Internet Service Providers and web-browsers, which prohibit the use of those services in criminal activity, unlawful activity, and the tracking of Internet communications without consent; and (2) the standards of the online advertising industry, including the Interactive Advertising Bureau's Code of Conduct, in which

Defendants agreed to "not collect 'personal information' as defined in the Children's Online Privacy Protection Act ('COPPA') from children they have actual knowledge are under the age of 13 or from sites directed to children under the age of 13 for Online Behavioral Advertising." *Id.* at App'x 150, 157, 160-61.

In addition, Plaintiffs allege Defendant Viacom's intrusions are "highly offensive" because they violate the social norms embodied by the Video Privacy Protection Act, the Wiretap Act, the Pen Register Act, the Stored Communications Act, the Computer Fraud and Abuse Act and corresponding computer crime laws in all 50 states. *Id.* at App'x 156-57.

The District Court, however, discounted these allegations inasmuch as it believed Defendants' activities did not violate the VPPA, Wiretap Act, or SCA in the first place. January 20, 2015 District Court Opinion at App'x 55. For the reasons explained above, the District Court erred in those regards. It also failed to consider whether Defendants' actions violated the Pen Register Act or the Computer Fraud and Abuse Act and corresponding laws in all 50 states.

The Pen Register Act prohibits the non-consensual interception of "dialing, routing, addressing, or signaling" information and is punishable by up to a year in prison. See 18 U.S.C. § 3121(c). Defendants' prevailed in their motions to dismiss plaintiffs' Wiretap claims on the basis that a URL is nothing more than "addressing" information. As explained above, a URL contains both addressing information and

content. However, there is no dispute that URLs contain information protected by the Pen Register Act.

Additionally, the Computer Fraud and Abuse Act prohibits: (1) intentional access to a computer (2) without authorization or exceeding authorized access, and (3) thereby obtaining information from a protected computer. 18 U.S.C. § 1030(a)(2)(C). On these points, Plaintiffs further allege Defendants intentionally accessed Plaintiffs' computers by placing tracking cookies on them and utilized those tracking cookies to intercept and record the Plaintiffs' personal information and communications without authorization and with knowledge that the Plaintiffs were minor children. *Second CAC* at App'x 109, 127-28, 130-31, 140-42, 150-53. Such conduct violates the elements of the CFAA set forth above. *Id.* at App'x 157. The fact that the CFAA and laws in every state provide criminal penalties to Defendants' alleged conduct supports the plausibility of Plaintiffs' allegations that Defendants' conduct is "highly offensive" to a reasonable person.

When properly considered, a reasonable person, viewing Defendants' conduct against the privacy protections embodied in those statutes, could find Defendants' intrusions "highly offensive."

Finally, Plaintiffs' Complaint sets forth additional facts confirming Defendants conduct was "highly offensive." In particular, Plaintiffs' Complaint includes facts pulled from the results of public surveys about basic principles of

children's online privacy. *Second CAC* at App'x 157-59. Among other things, those survey results confirm:

- 86% of Americans oppose advertisers tracking "a child's behavior online even if they give the child free content" (70% "*strongly disagree*" with this practice);
- 80% oppose the tracking of children even where an advertiser does not "know a child's name and address" (67% "*strongly disagree*" with this practice);
- 91% believe advertisers should receive a parent's permission before placing tracking software on a minor child's computing device (82% "*strongly agree*" in parental consent); and
- 90% support federal law requiring parental permission before the collection of personal information of a minor child online.

Id. at 157-60.

The District Court erred in dismissing these facts as "inapposite to the legal issue." January 20, 2015 District Court Opinion at App'x 56. If, as the Restatement and New Jersey law teach, an intrusion is deemed "highly offensive" because it results from "conduct to which the reasonable man would strongly object," *see Castro*, 895 A.2d at 1177, then Plaintiffs clearly pled sufficient facts alleging Defendants' unauthorized interception, tracking, recording, and dissemination of the personal information or communications of children is "highly offensive." Indeed, the facts alleged confirm that more than 65% of Americans "strongly" oppose advertisers tracking children online, and more than 80% "strongly" support parental

consent requirements. *Second CAC* at App'x 158-59. Thus, an ordinary reasonable person could find Defendants' actions, taken without parental consent, to be "highly offensive." The District Court erred in holding otherwise.

In short, Plaintiffs plausibly allege Defendants' intrusions into the private matters of young children are "highly offensive" to a reasonable person. The District Court therefore erred in concluding no reasonable juror could find Defendants' conduct "highly offensive." This Court should so hold.

CONCLUSION

For the aforementioned reasons, Plaintiffs respectfully request that this Court reverse the ruling of the District Court.

Respectfully Submitted,

/s/ Barry R. Eichen

Barry R. Eichen
Evan J. Rosenberg
EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
beichen@njadvocates.com
erosenberg@njadvocates.com

James P. Frickleton
Edward D. Robertson III
BARTIMUS FRICKLETON ROBERTSON & GOZA, PC

11150 Overbrook Rd., Suite 200
Leawood, KS 66211
Telephone: (913) 266-2300
jimf@bflawfirm.com
krobertson@bflawfirm.com

Edward D. Robertson, Jr.
Mary D. Winter
BARTIMUS FRICKLETON ROBERTSON & GOZA, PC
715 Swifts Highway
Jefferson City, MO 65109
Telephone: (573) 659-4454
chiprob@earthlink.com
marywinter@earthlink.com

Jay Barnes
BARNES & ASSOCIATES
219 East Dunklin St.
Jefferson City, MO 65101
jaybarnes5@zoho.com

Thomas Rosenfeld
GOLDENBERG HELLER ANTOGNOLI & ROWLAND PC
2227 South State Route 157
Edwardsville, IL 62025
618-656-5150
tom@ghalaw.com

Adam Voyles
LUBEL VOYLES LLP
5200 Montrose Blvd., Suite 800
Houston, TX 77086
713-284-5200
Adam@lubelvoyles.com

Douglas Campbell
Frederick Donald Rapone
CAMPBELL & LEVINE LLC
1700 Grant Building

Pittsburgh, PA 15219
(412) 261-0310
dac@camlev.com
fdr@camlev.com

Andrew Lyskowski
BERGMANIS LAW FIRM LLC
380 West US Highway 54, Suite 201
Camdenton, MO 65020
(573) 346-2111
alyskowski@ozarklawcenter.com

Mark C. Goldenberg
Kevin P. Green
GOLDENBERG HELLER ANTOGNOLI & ROWLAND PC
2227 SOUTH ROUTE 157
P.O. BOX 959
EDWARDSVILLE, IL 62025
(618)656-5150
kevin@ghalaw.com

CERTIFICATION OF BAR MEMBERSHIP

I hereby certify that I am a member of the bar of the Court of Appeals for the Third Circuit.

/s/ Barry R. Eichen
Barry R. Eichen
EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
beichen@njadvocates.com

CERTIFICATION OF WORD COUNT

This brief complies with the type-volume limitation of Fed. R. App. P. 28(e)(2)(A)(i) because this brief contains 13,791 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in 14-point Times New Roman font.

/s/ Barry R. Eichen
Barry R. Eichen
EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
beichen@njadvocates.com

CERTIFICATION OF SERVICE UPON COUNSEL

I hereby certify that on April 27, 2015, I electronically filed the foregoing using the Court's CM/ECF system, which sent a notification of such filing to all counsel of record.

Also, as per Fed. R. App. P. 25(a)(2)(B)(ii), I sent copies of the foregoing to the Office of the Clerk of Court and a copy to all Defendants counsel of record for delivery within 3 days.

/s/ Barry R. Eichen
Barry R. Eichen
EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
beichen@njadvocates.com

CERTIFICATION OF IDENTICAL COMPLIANCE OF BRIEFS

I certify that the E-Brief and Hard Copies of the brief are identical.

/s/ Barry R. Eichen
Barry R. Eichen
EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
beichen@njadvocates.com

CERTIFICATION OF VIRUS CHECK

I hereby certify that a virus check was performed on the E-Brief using Microsoft Security Essentials Version 1.197.699.0 and that no viruses were found.

/s/ Barry R. Eichen
Barry R. Eichen
EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
beichen@njadvocates.com

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 15-1441

In re: Nickelodeon Consumer Privacy Litigation

On Appeal from the U.S. District Court for the District of New Jersey
Case No. 2:12-cv-07829
The Honorable Stanley R. Chesler

APPELLANTS' APPENDIX – VOLUME 1
(Appellant 000001-000058)

EICHEN CRUTCHLOW
ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
Facsimile: (732) 248-8273

BARTIMUS FRICKLETON
ROBERTSON & GOZA, PC
715 Swifts Highway
Jefferson City, MO 65109
Telephone: (573) 659-4454
Facsimile: (573) 659-4460

Co-Lead Counsel on behalf of All Plaintiffs

TABLE OF CONTENTS

CERTIFICATE OF SERVICE

I, Barry R. Eichen, hereby certify that on April 27, 2015, I caused the following documents to be electronically filed with United States Court of Appeals for the Third Circuit by using the CM/ECF system; and caused a copy of the foregoing documents to be served *via* U.S. Mail to all counsel listed below and the Court.

Dated: April 27, 2015

/s/ Barry R. Eichen
Barry R. Eichen

Barry R. Eichen
EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
Facsimile: (732) 248-8273

Co-Lead Counsel on behalf of Plaintiffs

SERVICE LIST

ATTORNEYS FOR DEFENDANT VIACOM, Inc.

Stephen M. Orlofsky
Seth J. Lapidow
BLANK, ROME, LLP
301 Carnegie Center, 3rd Floor
Princeton, NJ 08540

Bruce P. Keller
Jeffrey S. Jacobson
DEBEVOISE & PLIMPTON LLP
919 Third Avenue
New York, NY 10022

ATTORNEYS FOR GOOGLE, INC.

Jeffrey J. Greenbaum
Joshua N. Howley
SILLS CUMMIS & GROSS PC
One Riverfront Plaza
Newark, NJ 07102-5400

Colleen Bal
Michael H. Rubin
WILSON SONSINI GOODRICH & ROSATI, PC
One Market Plaza
Spear Tower, Suite 3300
San Francisco, CA 94105-1126

Tonia O. Klausner
WILSON SONSINI GOODRICH & ROSATI, PC
1301 Avenue of the Americas, 40th Floor
New York, NY 10019

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

IN RE: NICKELODEON CONSUMER PRIVACY LITIGATION	**Circuit Court Docket No. _____**
	MDL No. 2443
	District Docket No. 2:12-cv-07829
	District Court Judge: Stanley R. Chesler
This Document Relates to:	
All Actions	**NOTICE OF APPEAL TO THE THIRD CIRCUIT COURT OF APPEALS**

Notice is hereby given that MDL Class Plaintiffs appeal to the United States Court of Appeals for the Third Circuit from an Order entered in this action on January 20, 2015.

Date: February 13, 2015

By: /s/ Barry R. Eichen

Barry R. Eichen
EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
Facsimile: (732) 248-8273

Co-Lead Counsel on behalf of Plaintiffs

(Please see additional sheets for appellants and appellees counsel)

2:12-cv-07829 In Re: Nickelodeon Consumer Privacy Litigation

Attorneys for Appellants

(representing AV, CAF, CTF, MP, TP, KT, NJ, TM, and Stephanie Fryar)

Barry R. Eichen
Evan J. Rosenberg
EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
beichen@njadvocates.com
erosenberg@njadvocates.com

James P. Frickleton
Edward D. Robertson III
BARTIMUS FRICKLETON ROBERTSON & GOZA, PC
11150 Overbrook Rd., Suite 200
Leawood, KS 66211
Telephone: (913) 266-2300
jimf@bflawfirm.com
krobertson@bflawfirm.com

Edward D. Robertson, Jr.
Mary D. Winter
BARTIMUS FRICKLETON ROBERTSON & GOZA, PC
715 Swifts Highway
Jefferson City, MO 65109
Telephone: (573) 659-4454
chiprob@earthlink.com
marywinter@earthlink.com

Thomas Rosenfeld
GOLDENBERG HELLER ANTOGNOLI & ROWLAND PC
2227 South State Route 157
Edwardsville, IL 62025
618-656-5150
tom@ghalaw.com

Adam Voyles
LUBEL VOYLES LLP
5200 Montrose Blvd., Suite 800
Houston, TX 77086
713-284-5200
Adam@lubelvoyles.com

Douglas Campbell
Frederick Donald Rapone
CAMPBELL & LEVINE LLC
1700 Grant Building
Pittsburgh, PA 15219
(412) 261-0310
dac@camlev.com
fdr@camlev.com

Jay Barnes
BARNES & ASSOCIATES
219 East Dunklin St.
Jefferson City, MO 65101
jaybarnes5@zoho.com

Andrew Lyskowski
BERGMANIS LAW FIRM LLC
380 West US Highway 54, Suite 201
Camdenton, MO 65020
(573) 346-2111
alyskowski@ozarklawcenter.com

MARK C. GOLDENBERG
Kevin P. Green
GOLDENBERG HELLER ANTOGNOLI & ROWLAND PC
2227 SOUTH ROUTE 157
P.O. BOX 959
EDWARDSVILLE, IL 62025
(618)656-5150
kevin@ghalaw.com

Attorneys for Appellees

ATTORNEYS FOR DEFENDANT VIACOM, Inc.

Stephen M. Orlofsky
Seth J. Lapidow
BLANK, ROME, LLP
301 Carnegie Center, 3rd Floor
Princeton, NJ 08540
orlofsky@blankrome.com
lapidow@blankrome.com

Bruce P. Keller
Jeffrey S. Jacobson
DEBEVOISE & PLIMPTON LLP
919 Third Avenue
New York, NY 10022
bpkeller@debevoise.com
jsjacobs@debevoise.com

ATTORNEYS FOR GOOGLE, INC.

Jeffrey J. Greenbaum
Joshua N. Howley
SILLS CUMMIS & GROSS PC
One Riverfront Plaza
Newark, NJ 07102-5400
jgreenbaum@sillscummis.com
jhowley@sillscummis.com

Colleen Bal
Michael H. Rubin
WILSON SONSINI GOODRICH & ROSATI, PC
One Market Plaza
Spear Tower, Suite 3300
San Francisco, CA 94105-1126
cbal@wsgr.com
mrubin@wsgr.com

Tonia O. Klausner
WILSON SONSINI GOODRICH & ROSATI, PC
1301 Avenue of the Americas, 40th Floor
New York, NY 10019
tklausner@wsger.com

CERTIFICATE OF SERVICE

I hereby certify that on February 13, 2015, I electronically filed the foregoing with the Clerk of the Court for the United States District Court for the District of New Jersey by using the CM/ECF system. I certify that for all participants in the case that are registered CM/ECF users, and service will be accomplished via the CM/ECF system.

Date: February 13, 2015

By: /s/ Barry R. Eichen

Barry R. Eichen
EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
Facsimile: (732) 248-8273

Co-Lead Counsel on behalf of Plaintiffs

NOT FOR PUBLICATION

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN RE NICKELODEON CONSUMER PRIVACY LITIGATION	**MDL No. 2443 (SRC)**
	Civil Action No. 12-07829
	Civil Action No. 13-03755
	Civil Action No. 13-03729
	Civil Action No. 13-03757
THIS DOCUMENT RELATES TO: THE CONSOLIDATION ACTION	**Civil Action No. 13-03731**
	Civil Action No. 13-03756
	OPINION

CHESLER, District Judge

The Plaintiffs in this multidistrict consolidated class action lawsuit are children younger than thirteen who allege that Defendants Viacom Inc. and Google Inc. ("Viacom" and "Google" and, collectively "Defendants") have violated their privacy rights, in contravention of federal law and the laws of California and New Jersey. This matter is before the Court on the Defendants' motions to dismiss the Master Consolidated Class Action Complaint ("MCC"), filed pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). [Docket Entries 43 & 44.] Plaintiffs have opposed [Docket Entry 52], and the Court has opted to rule on the parties' submissions, and without oral argument. See Fed. R. Civ. P. 78. For the foregoing reasons, the Court finds that the MCC fails to state a claim upon which relief can be granted. Counts II, III, IV, and VII are dismissed with prejudice. Count I is dismissed with prejudice as to Google, and without prejudice as to Viacom. Counts V and VI are dismissed without prejudice as to both Defendants.

I. Background

Viacom owns and operates three websites geared towards children – Nick.com, Nickjr.com, and Neopets.com. Viacom "encourage[s]" users of these websites to "register and establish profiles" on these sites. (See MCC ¶ 85.) Viacom collects certain information about users who register on its sites, including gender and birthdate; Viacom then assigns a code name to each discrete user based on that user's gender and age – allegedly called (by Viacom internally) the "rugrat" code. (Id. at ¶ 89).[1] Children who register for accounts on Viacom's sites also create "unique" profile names that are tied to each child's "profile page." (Id. at ¶ 90.) Each named Plaintiff in this consolidated action is a registered user of one or more of the Viacom websites. (See id. at ¶ 4.)

Children who use these Viacom websites can stream videos or play video games on them – it is unclear from the MCC whether a user must be registered on a Viacom site before watching a video or playing a game. Nevertheless, the MCC alleges that the act of viewing a video or playing a video game creates an "online record," which Viacom collects and later disseminates to Google, who collects and compiles it. (See id. at ¶¶ 96-101.) According to the MCC, the "video viewing" record is a long string of alphanumeric characters that contains two relevant pieces of information – the name of the video "requested" by the website user and the "rugrat" code that describes the age and gender of the user. (See id. at ¶¶ 98-99.)

Before all of this happens, however, Viacom has placed a text file – the aforementioned "cookie" – on Plaintiffs computers; this is done without Plaintiffs consent, or the consent of their

[1] "Rugrat" is both a colloquial term for a child or toddler and also the name of an animated television series that aired on Nickelodeon in the 1990s and 2000s. The rugrat codes provided as examples in the MCC – "Dil," for a six-year-old boy, and "Lou," for a twelve-year-old boy – are names of characters from that show.

parents. (Id. at ¶ 72.) This cookie allows Viacom to acquire certain information – in addition to username, gender, and birthdate collected at the time of registration – about each Plaintiff "who [is] a registered user of Viacom's children's websites." (See id. at ¶ 81.) This information includes a Plaintiff's: "IP address"; "browser settings"; "unique device identifier"; "operating system"; "screen resolution"; "browser version"; and certain "web communications," specifically "detailed URL [Uniform Resource Locator] requests and video materials requested and obtained from Viacom's children's websites." (Id. at ¶ 81.)[2] The MCC alleges that Viacom shares this information with Google, apparently by allowing Google to access the information "contained within Viacom's first party cookies." (See id. at ¶ 75, 81.)

Contemporaneously, Viacom also "knowingly permit[s]" Google to place its own text files – so-called "third-party cookies" – on Plaintiffs' computers; in the alternative, Viacom allows Google to access the information already stored within "third-party cookies" Google may have previously deposited on the device. (Id. at ¶ 73.) Either way, the MCC alleges that Viacom somehow affirmatively authorizes Google's use of cookies to track certain of Plaintiffs' internet usage. The fruits of Google's data tracking include "the URLs . . . visited by the Plaintiffs, the Plaintiffs' respective IP addresses and each Plaintiff's [sic] browser setting, unique device identifier, operating system, screen resolution, browser version, detailed video viewing histories and the details of their Internet communications with" the Viacom sites. (Id. at ¶ 77.) Google's cookies also assign to each Plaintiff a "unique numeric or alphanumeric identifier" that becomes "connected to" the information Viacom discloses to Google about that Plaintiff – namely, the username, gender, birthdate, IP address, etc. (See id. at ¶ 82.) The information is used by Google for the same reason that Viacom uses it -- "to sell targeted advertising" based upon

[2] As described in the MCC, a URL is the address of a resource connected to web, such as a video file. (See MCC ¶ 78.)

Plaintiffs' "individualized web usage, including videos requested and obtained." (See id. at ¶ 84.)

In summary, the MCC alleges that Plaintiffs visit certain Viacom-owned websites and willingly provide Viacom with their gender and age when they register as users of the sites. While this is happening, Viacom places a text file ("cookie") on Plaintiffs' computers without their consent or that of their parents; this text file allows Viacom to collect certain information about the computer that the Plaintiff is using and what the Plaintiff does while on Viacom's website. This information is shared with Google, or at minimum Google is allowed to access the Viacom text file containing it. In addition to the sharing of information from Viacom to Google, Google is also collecting information about Plaintiffs by virtue of its own text files, which Google has placed onto Plaintiffs' computers – again, without their consent – at the behest of (or aided by) Viacom. These "cookies," much like Viacom's, allow Google to collect certain information about Plaintiffs' computers and their website viewing history. Finally, if a registered user watches a video on one of the Viacom websites, Viacom makes a record of that activity, which includes the name of the video watched and the age and gender of the viewer. This information is then shared with Google, who compiles it with similar previously collected information about that particular child.

As the Court reads the MCC, that is the factual basis of the misconduct alleged.[3] Against this backdrop, the MCC alleges seven causes of action. The first three are violations of federal

[3] The Court cannot in connection with this motion credit the allegations made in Paragraphs 66 and 83, which without factual support both state "upon information and belief" that Viacom and Google were able to link online activity and information with offline activity and information, and thereby "identify specific users." (See MCC ¶ 66; see also id. at ¶ 83 ("Defendants . . . were able to identify specific individuals and connect online communications and data . . . to offline communications and data.").) These statements are entirely conclusory, and therefore of little utility in response to a motion to dismiss for failure to state a claim. See Bistrian v. Levy, 696

statutes – the Video Protection and Privacy Act ("VPPA"), 18 U.S.C. § 2710; The Federal Omnibus Crime Control and Safe Streets Act of 1968 ("the Wiretap Act"), as amended by the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2510-2522; and the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-2712. The other four are state law causes of action based upon the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 631; New Jersey's Computer Related Offenses Act ("CROA"), N.J. Stat. Ann. §§ 2A:38A-1 to -6; invasion of privacy under New Jersey law based on intrusion upon seclusion; and unjust enrichment under New Jersey law.[4] Jurisdiction is therefore exercised pursuant to 28 U.S.C. § 1331, 28 U.S.C. § 1367, and the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2), because the MCC pleads minimum diversity and an amount in controversy greater than $5 million. (MCC ¶ 21.)[5] The MCC defines two Plaintiff classes: (1) a "U.S. Resident Class" comprised of children who visited the Viacom websites and had cookies placed on their computers by Viacom and Google;

F.3d 352, 365 (3d Cir. 2012) ("[W]e peel away those allegations that are no more than conclusions and thus not entitled to the assumption of truth."); Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009). There are simply no facts pleaded in the MCC which indicate when or how either Defendant linked the online information it collected with extra-digital information about the Plaintiffs.

[4] The MCC does not specify which state's law applies to the intrusion upon seclusion and unjust enrichment torts. Plaintiffs, perhaps wary of the maxim that a complaint cannot be amended by a brief opposing a motion to dismiss, undertake an abridged choice of law analysis to support their conclusion that New Jersey law governs the tort claims. (See Opp. Br. at 55-57.) This conclusion was unclear from the MCC itself, because New Jersey law does not generally recognize an independent "unjust enrichment" cause of action. See, e.g., Goldsmith v. Camden County Surrogate's Office, 975 A.2d 459, 462-63 (N.J. Super. Ct. App. Div. 2009) (stating that an unjust enrichment principle normally underpins "a claim of quasi-contractual liability" (quoting Nat'l Amusements, Inc. v. New Jersey Tpk. Auth., 619 A.2d 262 (N.J. Sup. Ct. Law Div. 1992))).

[5] Neither Viacom nor Google challenge the assertion of CAFA jurisdiction over this action. Because CAFA provides the Court with an independent basis for subject matter jurisdiction over this lawsuit, the Court cannot decline pendent jurisdiction over the state law claims. (See Viacom Mov. Br. at 32.)

and (2) a "Video Subclass" comprised of all of the children in the Resident Class who were also registered users of the Viacom websites, "engaged with one or more video materials on such site(s)," and had their "video viewing histories" disclosed to Google by Viacom. (MCC ¶ 103.) The VPPA claim is brought on behalf of the Video Subclass only; all other counts are brought on behalf of the Resident Class.

II. Whether Plaintiffs Have Standing to Sue

Both Defendants raise a threshold argument that Plaintiffs have no standing under Article III of the Constitution to bring this suit. (Viacom Mov. Br. at 12; Google Mov. Br. at 11-14.) The "irreducible constitutional minimum of standing contains three elements" – injury-in-fact, causation, and redressability. See Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1992); Danvers Motor Co., Inc. v. Ford Motor Co., 432 F.3d 286, 290-91 (3d Cir. 2005). Defendants have not challenged causation and redressability here; rather, Defendants focus their argument exclusively on injury-in-fact, and in particular on whether or not the MCC plausibly alleges that Plaintiffs were economically harmed by Defendants' collection of their personal information. (See, e.g., Viacom Mov. Br. at 13-14.) Defendants contend that it does not, and because Plaintiffs have suffered no economic injury – a "paradigmatic" or "classic" form of injury-in-fact, see Danvers, 432 F.3d at 291, 293 – the MCC must be dismissed for lack of standing.

Were it necessary to decide the question, the Court might be inclined to agree. The MCC describes at some length why the personal information collected and aggregated by Defendants has a pecuniary value to companies who monetize popular websites by selling targeted advertising on those sites. (See, e.g., MCC ¶ 49 ("To the advertiser, targeted ads provided [sic] an unprecedented opportunity to reach potential consumers. The value of the information that

Defendants take from people who use the Internet is well known . . . . Personal information is now viewed as a form of currency.").) Even assuming this proposition to be true, it does not follow that personal information of the type collected by Viacom and Google has actual monetary value to Plaintiffs themselves, a fact necessary to Plaintiffs' theory of economic injury. (See Opp. Br. at 12 ("The [MCC] alleges a violation of Plaintiffs' financial interests to support their allegations that personally identifiable information . . . has monetary value and is a commodity . . . .").) In other words, the MCC presupposes the proposition that Plaintiffs could sell their personal information if they wanted to because Viacom and Google might already do so. In the parlance of standing, this theory is "abstract or conjectural or hypothetical," and therefore not "legally . . . cognizable." See Danvers, 432 F.3d at 291. It is also indistinguishable from the belief that a football fan could sell her eyeballs to a TV network for four cents because an advertiser pays $4 million to reach 100 million viewers during the Super Bowl. See In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 525 (S.D.N.Y. 2001) ("Demographic information is constantly collected on all consumers by marketers, mail-order catalogues and retailers. However, we are unaware of any court that has held the value of this collected information constitutes damage to consumers or unjust enrichment to collectors.")

But whether or not Plaintiffs have alleged injury-in-fact in the form of economic harm is not dispositive to the standing analysis. Injury-in-fact is nothing more or less than an "invasion of a legally protected interest which is . . . concrete and particularized . . . [and] actual or imminent, not conjectural or hypothetical." Pichler v. UNITE, 542 F.3d 380, 390 (3d Cir. 2008) (quoting Lujan, 504 U.S. at 560-61). The "legally protected interest" can be – and often is – property-based or financial. But it need not be. See Alston v. Countrywide Financial Corp., 585

F.3d 753, 763 (3d Cir. 2009) (addressing standing under the federal Real Estate Settlement Procedures Act and stating that "[a] plaintiff need not demonstrate that he or she suffered actual monetary damages"). Indeed, it has long been the case that "[t]he actual or threatened injury required by Art. III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing . . . ." See Warth v. Seldin, 422 U.S. 490, 500 (1975) (internal quotation and marks omitted); see also Pichler, 542 F.3d at 390-91. Thus, where a plaintiff states a valid claim for violation of an individual right or set of rights conferred via statute the issue of monetary harm is generally superfluous to the standing inquiry. This is why the Third Circuit has both explicitly and implicitly treated inquiries into statutory standing and whether a statutory claim has been stated as one and the same. Baldwin v. Univ. of Pittsburgh Med. Ctr., 636 F.3d 69, 73 (3d Cir. 2011) ("A dismissal for lack of statutory standing is effectively the same as a dismissal for failure to state a claim."); Pichler, 542 F.3d at 390-91 (affirming dismissal for lack of standing where plaintiffs did not meet the definition of "individual" under the Drivers Protection Privacy Act, 18 U.S.C. §§ 2721-2725, and thus had no cause of action).

In short, if Plaintiffs can state valid claims for violations of statutes that codify certain of their privacy rights, the Court will not prevent Plaintiffs from suing to enforce those rights because of doubts about whether they have suffered concrete monetary harm. Cf. In re Google Inc. Cookie Placement Consumer Privacy Litig., 2013 WL 5582866, at *3 (D. Del. Oct. 9, 2013) ("Google Cookie") (concluding that complaint based upon placement of Google third-party cookies did not allege sufficient injury-in-fact but proceeding to analysis of "whether plaintiffs have pled sufficient facts to establish a plausible invasion of rights created by the various statutes asserted"); In re Zynga Privacy Litig., No. 10-cv-04680, 2011 WL 7479170, at *2 (N.D. Cal.

June 15, 2011) ("Plaintiffs have Article III standing, because they allege a violation of their statutory rights under the Wiretap Act."), aff'd, -- F.3d --, 2014 WL 1814029 (9th Cir. May 8, 2014). Consequently, the Court must now turn to Defendants' argument that the facts alleged in the MCC do not state claims for violations of the various statutes asserted.[6] If Defendants are correct, any need to revisit the standing question will be rendered unnecessary. See Alston, 585 F.3d at 758 (addressing "lingering" Article III concerns only after determining that plaintiffs had stated a claim under the Real Estate Settlement Procedures Act).

III. Whether The MCC States A Plausible Claim for Relief

A. Legal Standard

A complaint will survive a motion under Rule 12(b)(6) only if it states "sufficient factual allegations, accepted as true, to 'state a claim for relief that is plausible on its face.'" Iqbal, 556 U.S. at 678 (quoting Bell Atlantic v. Twombly, 550 U.S. 554, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Id. (citing Twombly, 550 U.S. at 556). Following Iqbal and Twombly, the Third Circuit has held that to prevent dismissal of a claim the complaint must show, through the facts alleged, that the plaintiff is entitled to relief.

[6] Viacom invites the Court to follow Sterk v. Best Buy Stores, L.P., No. 11 C 1894, 2012 WL 5197901 (N.D. Ill. Oct. 17, 2012), and hold that Plaintiffs are required to plead "an injury beyond a statutory violation" to have standing. (Viacom Reply Br. at 6 n.1.) The Court must decline. Insofar as Sterk holds that pleading a violation of a statutory right without more is not an injury-in-fact, the case is incompatible with binding Third Circuit authority. See Alston, 585 F.3d at 763; Pichler, 542 F.3d at 390 (basing standing analysis on whether plaintiffs suffered "an invasion of a legally protected interest" created by the DPPA). Such inconsistency notwithstanding, the Court agrees with the In re Hulu Privacy Litigation Court's characterization of Sterk as a case of limited persuasive authority which is best understood in context. See No. C 11-03764, 2013 WL 6773794, at *8 (N.D. Cal. Dec. 20, 2013) (noting that Sterk found no VPPA injury where defendants Best Buy Stores, L.P. and BestBuy.com LLC only disclosed plaintiff's "DVD purchase history and other information to their parent company, Best Buy Co., Inc." (citing 2012 WL 5197901, at *1-3, *5)).

Fowler v. UPMC Shadyside, 578 F.3d 203, 211 (3d Cir. 2009). In other words, the facts alleged "must be enough to raise a right to relief above the speculative level . . . ." Eid v. Thompson, 740 F.3d 118, 122 (3d Cir. 2014) (quoting Twombly, 550 U.S. at 555). While the Court must construe the complaint in the light most favorable to the plaintiff, it need not accept a "legal conclusion couched as factual allegation." Baraka v. McGreevey, 481 F.3d 187, 195 (3d Cir. 2007); Fowler, 578 F.3d at 210-11; see also Iqbal, 556 U.S. at 679 ("While legal conclusions can provide the framework of a complaint, they must be supported by factual allegations."). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, will not suffice." Iqbal, 556 U.S. at 678.

B. The VPPA Claim Against Google

Whether the MCC states a claim against either Viacom or Google for violation of the federal VPPA is a question of statutory interpretation. See In re Hulu Privacy Litig., 2014 WL 1724344, *6-7 (N.D. Cal. Apr. 28, 2014). The Court will therefore address the merits of certain of Defendants' text-based arguments, starting with Google's contention that it is not a "video tape service provider" within the ambit of the VPPA, and thus as a matter of law could not have violated Plaintiffs' rights under that statute. (See Google Mov. Br. at 28-29.)

1. Only VTSPs Can be Civilly Liable for Violations of the VPPA, and the MCC Does Not Allege that Google is A VTSP

It is well established that "every exercise of statutory interpretation begins with an examination of the plain language of the statute." United States v. Diallo, 575 F.3d 252, 256 (3d Cir. 2009) (quoting Rosenberg v. XM Ventures, 274 F.3d 137, 141 (3d Cir. 2001)). 18 U.S.C. § 2710(b), entitled "Video tape rental and sales records," provides that "[a] video tape service provider who knowingly discloses, to any person, personally identifiable information concerning

any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection [(c)]."[7] Section 2710(c), entitled "Civil action," states that "[a]ny person aggrieved by an act of a person in violation of this section may bring a civil action in a United States district court." Reading these two provisions together, the Act limits the right to sue to those persons "aggrieved" by "violation[s] of" the VPPA itself, and the VPPA is violated when a "video tape service provider . . . knowingly discloses . . . personally identifiable information concerning" that "aggrieved" person. It is thus apparent on the face of the VPPA that an "aggrieved" person's claim must be against a "video tape service provider" ("VTSP"). The great majority of courts to address the issue have reached the same conclusion. See, e.g., Daniel v. Cantrell, 375 F.3d 377, 381, 82 (6th Cir. 2004) ("[U]nder the plain language of the statute, only a 'video tape service provider' . . . can be liable."); Hulu, 2014 WL 1724344, at *7 ("[t]he VPPA prohibits a 'videotape service provider' from" knowingly disclosing "personally identifiable information" (citing § 2710(b))).

Plaintiffs contend otherwise. Relying exclusively on Dirkes v. Borough of Runnemede, 936 F. Supp. 235 (D.N.J. 1996), Plaintiffs argue that any party who is "in possession of personally identifiable information as a direct result of the improper release of such information" is subject to VPPA liability. (Opp. Br. at 22 (quoting Dirkes, 936 F. Supp. at 240).) According to Plaintiffs, the Dirkes decision establishes a "law" of the District of the New Jersey, and thus in this district VPPA liability is not limited to VTSPs only. (See Opp. Br. at 22, 24 ("this Court should follow the law of this district" (citing Dirkes, 936 F. Supp. at 239)).) There is, however,

[7] The actual text of the VPPA says that "such provider shall be liable to the aggrieved person for the relief provided in subsection (d)." § 2710(b). This appears to be a typo, because subsection (d) is a rule of evidence which renders inadmissible personally identifiable information, whereas subsection (c) describes the remedies available to a VPPA plaintiff in a civil action. See Sterk v. Redbox Automated Retail, LLC, 672 F.3d 535, 537 (7th Cir. 2012).

no such thing as "law of the district," and "[t]he doctrine of *stare decisis* does not compel one district court judge to follow the decision of another," even where the facts of the two cases are the same. Threadgill v. Armstrong World Indus., Inc., 928 F.2d 1366, 1371 (3d Cir. 1991). While the Court has the highest regard for the author of the Dirkes opinion, the Court is not persuaded that Dirkes correctly interprets the relevant VPPA provisions.

Instead, the Court agrees with the Sixth Circuit's discussion in Daniel that Dirkes reaches the holding it does – *i.e.*, that persons other than VTSPs can be liable under the VPPA – based on a misreading of the statute. See Daniel, 375 F.3d at 382-83. Dirkes appears to be based upon the false premise that "the plain language of the [VPPA] does not delineate those parties against whom an action under this Act may be maintained." See 936 F. Supp. at 240. This is simply not the case. Certainly, subsection (c) – which Dirkes focuses on but puzzlingly reads in isolation – does not explain who can be liable in a VPPA suit; and that makes sense, because subsection (c) deals exclusively with the victims of the conduct denounced by the statute. See § 2710(c) ("[a]ny person aggrieved by an act of a person in violation of this section may bring a civil action"). Elsewhere, however, the VPPA does explain "those parties" who can be sued under the Act – namely, VTSPs. See § 2710(b) ("a [VTSP] . . . shall be liable to the aggrieved person"). Thus, it is only by ignoring the very subsection that establishes the contours of a VPPA cause of action that Dirkes concludes that the possible universe of VPPA defendants is infinite. See 936 F. Supp at 240 (finding that the court "need not identify all potential categories of defendants in this opinion").

Moreover, Dirkes understands Congress to be granting to federal judges "broad remedial powers" to remedy VPPA violations because the Act states that "[t]he court may award . . . such

other . . . relief as the court determines to be appropriate." See 936 F. Supp. at 241 (quoting 18 U.S.C. § 2710(c)(2)(D)). Dirkes chooses to exercise those powers by expanding the scope of permissible VPPA defendants, "to prevent the further disclosure of information." See id. But again, this is contrary to the plain language of the VPPA itself. The "such other . . . relief" language describes the type of remedy – like statutory damages and attorneys' fee – that "[t]he court may award"; it does not indicate against whom such relief may be awarded. That indication comes from § 2710(b), which states that a VTSP "who knowingly discloses . . . personally identifiable information concerning any consumer . . . shall be liable" to that person.

In short, as the Sixth Circuit correctly highlights Congress provides a detailed definition of a VTSP in § 2710(a) and makes the cause of action created in § 2710(b) contingent on actions taken by VTSPs; it does violence to this plain language to read § 2710(c) in isolation and conclude that anyone can violate the statute. See Daniel, 375 F.3d at 383. This Court, fortified by the Sixth Circuit's persuasive analysis in Daniel, therefore holds that only VTSPs can be liable for violations of the VPPA.

Having determined that only VTSPs can violate the VPPA, the Court finds that the VPPA claim against Google must be dismissed because the MCC does not allege Google is a VTSP. According to the VPPA, a VTSP is a person "engaged in the business . . . of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure." By referencing these two subparagraphs, the statute broadens the definition of VTSP to include: (1) "any person if the disclosure [of information by the VTSP] is solely of the names and addresses of consumers and

if" certain other factors are met, see § 2710(b)(2)(D); and (2) "any person if the disclosure is incident to the ordinary course of business of the video tape service provider," see § 2710(b)(2)(E). Notably, the term "ordinary course of business" is defined to include "only debt collection activities, order fulfillment, request processing, and the transfer of ownership." § 2710(a)(2).

None of these definitions fit Google here. The MCC does not allege that Google is "engaged in the business" of renting, selling, or delivering either video tapes or "similar audio materials" – instead, it describes Google as (1) the global epicenter of Internet search and browsing activity"; (2) an "advertising company"; and (3) an "[e]nterprising online marketer[]" who utilizes its third-party cookies "to sell advertising that is based upon a particular person's prior Internet activity." (See id. at ¶¶ 19, 35, 37.) Moreover, Google is not a VTSP by virtue of the alleged disclosures made to it by Viacom – the MCC does not allege that the disclosures made to Google are "solely . . . the names and addresses of consumers," see § 2710(b)(2)(D), and it does not allege that the disclosures are made in the "ordinary course of [Viacom's] business," as that term is defined in the statute. See id. §§ 2710(a)(2), 2710(b)(2)(E).

Plaintiffs contend that, despite what the MCC alleges (or fails to allege), Google is in fact a VTSP because it owns YouTube, a provider of "[o]nline video services" that is considered to be a VTSP "within the meaning of the VPPA." (See Opp. Br. at 25 (quoting Hulu, 2012 WL 328296, at *4-6).) Even if this is true, "after-the-fact allegations" like these, which are contained in a brief filed in opposition to a motion to dismiss but not in the complaint itself, do not factor into the Rule 12(b)(6) analysis. See Frederico v. Home Depot, 507 F.3d 188, 201-02 (3d Cir.

2007). Thus, the MCC is still deficient on this score, regardless of how Plaintiffs characterize Google in their brief.

But even if Plaintiffs were given leave to amend the MCC so they could allege Google is a VTSP because of its ownership of YouTube, it would not help. The presence of "personally identifiable information," defined at 18 U.S.C. § 2710(a)(3) and discussed in greater detail *infra*, is a mandatory prerequisite to a cognizable VPPA suit. "Personally identifiable information," however, is contingent on the request or receipt of "specific video material or services from a [VTSP]." See § 2710(a)(3). Thus, the VPPA only contemplates civil actions against those VTSP from whom "specific video materials or services" have been requested. It is readily apparent that is not the case with Google here, nor could it ever be – YouTube videos are irrelevant to this lawsuit, which focuses exclusively on three Viacom websites and the Defendants' data collection activities in regards to those sites. The VPPA's legislative history confirms that Google's ownership of YouTube does not bring Google within the Act's ambit in this case. See S. Rep. No. 100-599, at 12 (1988) ("Senate Report"), as reprinted in 1988 U.S.C.C.A.N. 4342-1 ("The definition of personally identifiable information includes the term 'video' to make clear that simply because a business is engaged in the sale or rental of video materials or services does not mean that all of its products or services are within the scope of this bill.") As least as far as Google is concerned, this is a lawsuit about online advertising practices, not online videos.

2. 18 U.S.C. § 2710(e) Cannot be the Basis for A Civil Claim Against Google

As the foregoing analysis reveals, only those persons "aggrieved" by an act in violation of the VPPA may bring a civil action, and one can only be "aggrieved" for purposes of the

statute when a VTSP "knowingly discloses" his or her "personally identifiable information." See § 2710(b). Since Plaintiffs have not alleged that Google is a VTSP, they cannot state a VPPA claim against it. Nevertheless, Plaintiffs contend that Google is liable for damages and other relief provided by the Act for a violation of § 2710(e) ("Destruction of old records"), which requires "person[s] subject to [the VPPA]" to timely "destroy personally identifiable information." Plaintiffs' lone allegation in this regard, found in Paragraph 131 of the MCC, is wholly conclusory, and is not supported by any factual allegations whatsoever – for instance, the MCC does not describe how long Google retains Plaintiffs' information, a fact that would seem integral to a suit based upon the failure to destroy "old records." Plaintiffs' VPPA claim against Google, insofar as it is predicated upon § 2710(e), must therefore be dismissed. See Iqbal, 556 U.S. at 678 ("Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, will not suffice.").

More importantly, it is readily apparent that non-compliance with § 2710(e) cannot serve as the basis of a VPPA action. See Daniel, 375 F.3d at 384 ("only § 2710(b) can form the basis of liability"); Redbox, 672 F.3d at 538. While Dirkes holds to the contrary, the Court is satisfied that the reasoning applied in the Daniel and Redbox opinions is more persuasive. Both the Sixth and Seventh Circuits untangle the same statutory text and explain why the placement of the VPPA's civil action provision – immediately following subsection (b)'s disclosure prohibitions, but before the prohibitions contained in subsections (d) and (e) – is not an accident; rather, it is evidence that Congress intended the VPPA's right of action to be "limited to enforcing the prohibition of disclosure." See Redbox, 672 F.3d at 538; Daniel, 375 F.3d at 384 ("If these later sections [subsections (d) and (e)] were to be a basis for liability, it would make sense that the

section on civil actions [subsection (c)] would come at the end of the statute, rather than preceding these sections."). The manner in which the civil action provision is drafted further strengthens this conclusion – subsection (c)(4) states that "[n]o liability shall result from lawful disclosure permitted by this section." It is unclear why Congress would add this caveat – redundant, to be sure, but still there – if it did not intend liability to be limited only to violations of subsection (b), which explains how an unlawful disclosure occurs.[8]

In sum, the Court does not agree with Plaintiffs that § 2710(e) authorizes a civil VPPA action, let alone one against a non-VTSP entity. The VPPA claim against Google, predicated on Google's alleged failure to destroy old records and unsupported by factual allegations, fails as a matter of law and will be dismissed with prejudice.

C. The VPPA Claim Against Viacom

In contrast, the MCC expressly pleads that Viacom is a VTSP within the terms of the statute. (See MCC ¶ 126 ("The home page of Nick.com advertises it as the place to watch '2000+ FREE ONLINE VIDEOS' . . . .").) Viacom makes a tepid attempt to contest this characterization, arguing in a footnote of its moving brief (and a paragraph of the reply) that the VPPA does not apply to entities that stream videos online. (See Viacom Mov. Br. at 19 n.4; Reply Br. at 12-13.) Because, however, the Court finds that the VPPA claim against Viacom must fail for other reasons, it is unnecessary to determine whether or not Viacom is a VTSP by

[8] The VPPA's legislative history, while unnecessary to consult to decide the question, further supports the conclusion that the remedies in subsection (c) are only available for violations of subsection (b). See, e.g., Senate Report at 7 (statement of Sen. Leahy) ("In the event of an unauthorized disclosure, an individual may bring a civil action for damages."); id. at 8 ("The civil remedies section puts teeth into the legislation, ensuring that the law will be enforced by individuals who suffer as the result of unauthorized disclosures."); id. at 14 ("Section 2710(c) imposes liability where an individual, in violation of the act, knowingly discloses personally identifiable information concerning any consumer.").

virtue of its provision of online streaming videos.[9] Specifically, the Court finds merit in Viacom's argument that the VPPA claim fails because the information allegedly acquired and disclosed by Viacom is not "personally identifiable information" as that term is defined by the statute. (Viacom Mov. Br. at 18-20.) In short, there is simply nothing on the face of the statute or in its legislative history to indicate that "personally identifiable information" includes the types of information – anonymous user IDs, a child's gender and age, and information about the computer used to access Viacom's websites – allegedly collected and disclosed by Viacom.

As already discussed, § 2710(b) establishes the elements of a VPPA cause of action; the statue is violated when a VTSP "knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider . . . ." "Personally identifiable information" ("PII") is a defined term – PII "includes information which identifies a person as having requested or obtained specific video materials or services from a [VTSP]." § 2710(a)(3). Quoting this definition, Viacom argues that PII is "information sufficient to identify a person, by real name, in the real world, as having obtained a 'specific video' . . . ." (See Viacom Mov. Br. at 20.) Viacom suggests that "[i]t is clear that Congress had 'the names and addresses of consumers' in mind" when drafting its definition of PII. (See id.)

This reading, however, does not jive with the VPPA's plain language. If Congress wanted to define PII as any "information which identifies a person by name or mailing address as having requested or obtained specific video materials," it could have. Those words, however, are nowhere to be found in the definition. Moreover, subsection (b)(2), which establishes certain

[9] The Court notes that the only other court to address the issue of whether providers of streaming videos are VTSPs has found that they are, at least for pleading purposes. See Hulu, 2012 WL 3282960, at *6 (rejecting argument by online video content provider that "the VPPA does not expressly cover digital distribution" of video materials). Viacom does not suggest a persuasive reason why the Hulu Court's conclusion was incorrect.

exceptions to the prohibition against disclosure, explains that a VTSP "may disclose [PII] concerning any consumer . . . to any person if the disclosure is solely of the names and addresses of consumers and if" certain other factors are met. See § 2710(b)(2)(D). That language implies that "names and addresses" are but a subset of PII; otherwise, why include the "if the disclosure is" clause at all? The Court therefore reads the statute to comport with common sense – "a person" can be identified by more than just their name and address. See Hulu, 2014 WL 1724344, at *11 ("One can be identified in many ways: by a picture, by pointing, by an employee number, by the station or office or cubicle where one works . . . .").

That does not mean the universe of PII is as broad as Plaintiffs suggest either. Indeed, the Hulu decision, which engages in an exhaustive analysis of the VPPA's text and legislative history, holds that PII is information that must link "a specific, identified person and his video habits" – what the Hulu Court characterizes as any information "akin" to a name. See 2014 WL 1724344, at *12, 14. This is a cogent and reasonable reading of the statute, which on its face establishes that PII is "information" that itself must both "identif[y] a person" and further identify that "person" in connection with "specific video materials or services" "requested or obtained" from a VTSP. See § 2710(a)(3). At bottom, then, this Court concludes that PII is information which must, without more, itself link an actual person to actual video materials.

To the extent of any ambiguity in the statute's definition of PII, the VPPA's legislative history comports with this reading. As the parties highlight, the VPPA was passed in direct response to the publication of a newspaper profile about then-Supreme Court nominee Judge Robert Bork based upon the titles of movies he had rented from a local video store. See Senate Report, at 5. This disclosure was resoundingly denounced. In the words of Senator Patrick

Leahy, "[i]t is nobody's business what Oliver North or Robert Bork or Griffin Bell or Pat Leahy" – all identified, specific people – "watch on television or read or think about when they come home." Id. The Senate Report's discussion of PII echoes this emphasis on preventing the dissemination of the video viewing habits of identifiable individuals:

> This definition [of PII] makes clear that personally identifiable information is intended to be transaction oriented. It is information that identifies a particular person as having engaged in a specific transaction with a [VTSP] . . . . Thus, for example, a video tape service provider is not prohibited from responding to a law enforcement agent's inquiry as to whether a person patronized a [VTSP] at a particular time or on a particular date.

Id. at 12. Conspicuously absent from this treatment is any discussion about PII being tied to the actual names or addresses of individuals; but so too is any indication that PII can be anonymous information which may after investigation lead to the identification of a specific person's video viewing habits.

And it is this conclusion that is fatal to the VPPA claim against Viacom. The MCC alleges that Viacom disclosed the following information to Google about each Plaintiff: anonymous username; IP address; browser setting; "unique device identifier"; operating system; screen resolution; browser version; and "detailed URL requests and video materials requested and obtained" from the Viacom websites, requests which presumably contain the "rugrat" (gender and age) code and the title of a video. None of this information, either individually or aggregated together, could without more serve to identify an actual, identifiable Plaintiff and what video or videos that Plaintiff watched. Much of this information – screen resolution, browser version and setting, operating system, etc. – is not even anonymized information about

the Plaintiff himself; it is anonymized information about a computer used to access a Viacom site.

Additionally, Plaintiffs themselves highlight that merely acquiring an IP address does not itself identify an individual – Plaintiffs argue (but do not plead) that "IP addresses are looked up easily to reveal geolocation information." (See Opp. Br. at 20 n.13.) But even "geolocation information" does not identify a specific individual. Indeed, it will often have the opposite effect: to adopt an example used by the parties, the computer on which this Opinion was written is located in Newark, New Jersey, but the IP address associated with it is geographically located in Philadelphia – presumably where the Third Circuit's computer servers are. Knowing anonymized information about a computer, and an IP address associated with that computer, will not link actual people (children or adults) to their specific video choices, any more than knowing that an Opinion was written on an HP Compaq running Windows XP located at a Philadelphia IP address will link an actual judge to a specific case.

The closest the MCC comes is the allegation that Viacom disclosed to Google specific profile names and a URL containing: (1) Viacom's internal "rugrat" code; (2) the name of a specific video; and (3) information identifying a Google "third-party" cookie. (See MCC ¶¶ 98-99.) But even assuming Google knew which codes names where associated with certain age and gender combinations – and the MCC is less than clear on this point[10] – this information does not link an identified person to a specific video choice. Instead, as Plaintiffs themselves highlight, all Google knows from the disclosure of this information (plus the computer specific information

[10] Specifically, the MCC alleges that "Viacom also provided Google with the code name for the child's specific gender and age." (MCC ¶ 93.) This allegation could be read in two ways – Viacom (1) provided Google with a key to decipher the "rugrat" code (*e.g.*, Dil = six-year-old boy), or (2) provided a code name that only Viacom knew corresponded to a specific age and gender.

discussed above) is "a child's username, sex, age, type of computer," and IP address. (See Opp. Br. at 20.) This is simply not information that, without more, identifies a person – an actual, specific human being – as having rented, streamed, or downloaded a given video, especially given the absence of factual allegations regarding how (and if) Plaintiffs' unique usernames were linked to their actual names. Certainly, this type of information might one day serve as the basis of personal identification after some effort on the part of the recipient, but the same could be said for nearly any type of personal information; this Court reads the VPPA to require a more tangible, immediate link.

None of the cases Plaintiffs cite alter this conclusion. Plaintiffs again cite to Dirkes (see Opp. Br. at 16), but Dirkes is inapposite, since it dealt with the disclosure of the plaintiffs' real names and a history of the pornographic videotapes they rented from a local video store. See 936 F. Supp. at 236. This information is so clearly PII that Dirkes, if anything, serves only to illustrate how far Plaintiffs in this case attempt to stretch that term's definition. Plaintiffs also make much out of an earlier decision in the Hulu litigation, in which the court rejected Hulu's motion to dismiss based upon, *inter alia*, the argument that Hulu was not a VTSP within the terms of the VPPA. See 2012 WL 3282960, at *4-8. That decision is also unhelpful. There, Hulu never argued that the type of information it disclosed was not PII, and thus the court in that case did not make any findings about whether the types of information allegedly disclosed by Hulu were PII or not. More importantly, the allegations in Hulu differ in critical ways from those here. The Hulu plaintiffs alleged, among other things, that Hulu transmitted "their Facebook IDs, connecting the video content information to Facebook's personally identifiable user registration information." See id. at *2. No such allegations exist in this case – the closest

the MCC comes is to allege that Viacom gives Google the video viewing histories of anonymous children categorized by age and gender. (See MCC at ¶¶ 98-99.)

The most recent decision in the Hulu litigation, denying in part Hulu's motion for summary judgment, emphasizes just how important the disclosure of Facebook-related identification information was to the survival of the VPPA claim in that case. In that decision, the court analyzed whether any of three different types of disclosures came close enough to "linking identified persons to the video they watched" to resist judgment as a matter of law. The disclosures were: (1) a "URL web address containing the video name and the Hulu user's unique seven-digit Hulu User ID"; (2) a unique user ID that allowed comScore (a company hired to calculate viewership) "to link the identified user and the user's video choices with information . . . gathered from other websites that the same user visited;" and (3) a transmission to Facebook containing information "about what the Hulu user watched and who the Hulu user is on Facebook." See Hulu, 2014 WL 1724344, at *9, *13. The court held that only the last disclosure – which identified the user's "actual identity on Facebook" – was actionable. See id. Critically, the court found that

> a Facebook user – even one using a nickname – generally is an identified person on a social network platform. The Facebook User ID is more than a unique, anonymous identifier. It personally identifies a Facebook user. That it is a string of numbers and letters does not alter the conclusion. Code is a language, and languages contain names, and the string is the Facebook user name.

Id. at 14. None of the allegedly disclosed information in this case – anonymous information about home computers, IP addresses, anonymous usernames, even a user's gender and age – serves to identify an actual, identifiable person and link that person to a specific video choice.

Simply put, in a socially networked world a Facebook ID is at least arguably "akin" to an actual name that serves without more to identify an actual person. This Court, however, need not decide that issue, because the same simply cannot be said about the information allegedly disclosed here.

The fact that Plaintiffs are all minors does not alter the analysis either. Certainly, the ease by which children access the internet implicates important policy concerns, and Congress has legislated in this area, passing the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§ 6501-6506. But as Viacom highlights, Plaintiffs do not allege that either party has violated COPPA, and considering the broader rulemaking authority granted by Congress to the Federal Trade Commission ("FTC") under COPPA, FTC rules implementing that statute are irrelevant to this Court's VPPA analysis. See § 6501(8)(F) (granting FTC authority to expand statutory definition of "personal information" beyond, *inter alia*, names, address, Social Security numbers, and telephone numbers). The VPPA by its very terms applies equally regardless of the age of the consumer, and nothing in the Act's legislative history indicates any Congressional intent to transform disclosures of non-PII into VPPA violations because the subject of the disclosure is younger than thirteen. See Hulu, 2014 WL 1724344, at *12 (noting that COPPA, which specifically protects children online, "implicates different privacy concerns and resulted in broader definitions of personal information," while "[b]y contrast" "the VPPA prohibits only disclosure of a particular viewer's watched videos").[11]

[11] Also immaterial are certain public statements reproduced in Plaintiffs' opposition brief and attributed to Viacom, in which Viacom announced that YouTube would strip "personally identifiable information" from data before transferring that data to Viacom pursuant to a court order. (See Opp. Br. at 19.) Statements made by Viacom about the anonymity of information disclosed to it by a Google subsidiary say nothing about whether the information allegedly disclosed by Viacom to Google in this case is itself anonymized, or something more nefarious. Insofar as Plaintiffs intend the underlying Viacom/Google copyright litigation to serve as legal

In sum, Plaintiffs do not state a VPPA claim against Viacom because they fail to allege the disclosure of personally identifiable information by Viacom to Google. The VPPA claim against Viacom will be dismissed. This dismissal, predicated upon Plaintiffs' failure to plead facts showing Viacom disclosed PII, will be without prejudice. Phillips v. County of Allegheny, 515 F.3d 224, 236 (3d Cir. 2008) ("where a complaint is vulnerable to a 12(b)(6) dismissal, a district court must permit a curative amendment, unless an amendment would be inequitable or futile").

D. The Wiretap Act Claim

The Wiretap Act creates a civil cause of action "against those who intentionally use or disclose to another the contents of a wire, oral, or electronic communication, knowing or having reason to know that the information was obtained in violation of the statute." Bartnicki v. Vopper, 200 F.3d 109, 114-15 (3d Cir. 1999) (citing 18 U.S.C. §§ 2511(1), 2520(a)). The Third Circuit has held that "private parties can bring a cause of action for damages and injunctive relief where aggrieved by a defendant's . . . unauthorized interception of electronic communications." DIRECTV, Inc. v. Pepe, 431 F.3d 162, 167 (3d Cir. 2005). Plaintiffs allege that Google "intentionally intercepted the contents of [Plaintiffs'] electronic communications" through its placement and use of cookies, while Viacom "procured Google" to so intercept and "profited" from this "unauthorized tracking of the Plaintiffs' Internet communications." (MCC ¶¶ 147, 156-57.) The Wiretap Act claim fails as a matter of law as to both Defendants, and will be dismissed with prejudice.

---

authority, the Court notes that the Opinion and Order which precipitated Viacom's excerpted statement actually supports the Defendants' position. See Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 262 (S.D.N.Y. 2008) (quoting with approval defendants' statement that a "login ID is an anonymous pseudonym that users create for themselves when they sign up with YouTube" which "cannot identify specific individuals" without more).

Indeed, the claim is defective for two distinct reasons. First, Defendants' correctly highlight that the Wiretap Act is a "one-party consent" statute, i.e., it is not unlawful under the Act for a person to "intercept . . . electronic communication" if the person "is [1] a party to the communication or [2] where one of the parties to the communication has given prior consent to such interception . . . ." § 2511(d)(2). Defendants argue that as alleged in the MCC, all communications in this case were either directly between themselves (or their cookies) and Plaintiffs' computers, or intercepted with the express consent of websites like Viacom. (See Viacom Mov. Br. at 25; Google Mov. Br. at 17.)[12]

Plaintiffs do not seriously dispute this. Instead, Plaintiffs attempt to invoke the "criminal or tortious act" exception to the Wiretap Act's one-party consent regime based on the MCC's allegation of a common law privacy tort against Defendants. (See Opp. Br. at 28-29 ("Plaintiffs' allegation of intrusion upon seclusion is sufficient to invoke the tort/crime exception of the [Wiretap Act], and negate the relevance of Viacom's consent."). While Plaintiffs are correct that consent will not absolve liability where a "communication is intercepted for the purpose of committing any criminal or tortious act," see § 2511(2)(d), that exception does not help them here. Courts have almost uniformly found that the "criminal or tortious act" exception applies only where defendant has "the intent to use the illicit recording to commit a tort or crime beyond the act of recording itself." See Caro v. Weintraub, 618 F.3d 94, 98 (2d Cir. 2010); see also

[12] Paragraph 155 of the MCC alleges that Google uses its cookies to "track the Plaintiffs' communications with other websites on which Google places advertisements," "in addition to intercepting the Plaintiffs' communications with the Viacom children's websites . . . ." Plaintiffs contend that this single paragraph "provides a separate and unchallenged basis" for a Wiretap Act claim against Google. (Opp. Br. at 37.) Even if the Court were to credit this conclusory allegation, made with no factual support, it provides no independent basis for a Wiretap Act claim, as the MCC alleges that all websites upon which Google serves ads consent to the placement of cookies by Google to accomplish that task. (See MCC ¶¶ 38-45 (describing how "[w]ebsite owners" allow "third-party companies such as Google to serve advertisements directly," which involve the placement of "third-party cookies on individuals' computers").)

Sussman v. Am. Broadcasting Cos., 186 F.3d 1200, 1202-03 (9th Cir. 1999) ("Under section 2511, 'the focus is not upon whether the interception itself violation another law; it is upon whether the purpose for the interception – its intended use – was criminal or tortious.'" (internal quotation omitted)). The instant lawsuit is one about allegedly illegal means – "the scheme to track the Plaintiffs' communications," (see MCC ¶ 195) – not an illegal purpose, and in such a circumstance, the Wiretap Act claim against Defendants must fail. Sussman, 186 F.3d at 1202-03 ("Where the purpose is not illegal or tortious, but the means are, the victims must seek redress elsewhere.").

L.C. v. Central Pa. Youth Ballet, 09-cv-2076, 2010 WL 2650640 (E.D. Pa. July 2, 2010), cited by Plaintiffs for the proposition that violating the Wiretap Act itself "operates to negate single party consent," (see Opp. Br. at 29), does not help Plaintiffs here. That case involved the video-taping and intentional distribution of an interview with a child – conducted by the ballet school where that child was a student – concerning the sexual assault of that child by another student at the school. See 2010 WL 2650640, at *2. Thus, the case is immediately problematic because it is unclear what the illegal interception was – it appears plaintiff L.C. agreed to a video-taped interview, but his parents did not. See id. at *2 (stating that defendants "proceeded to tape record an interview with L.C. concerning the . . . sexual assault without his parents' knowledge"). Even if L.C. can be read to support the (questionable) proposition that one-party consent is ineffective where an illegal interception of a communication occurs with the express purpose to later disclose the intercepted information, see id. at *3, such a rule would be inapplicable to this case, which is only about Defendants' "scheme" to track Plaintiffs' online communications. There are no facts pleaded to indicate that the interceptions in this case were

motivated by anything other than Defendants' desire to monetize Plaintiffs' internet usage, and thus the "criminal or tortious act" exception embodied in § 2511(2)(d) is inapplicable.

Plaintiffs also contend that § 2511(2)(d) does not protect Defendants here because Plaintiffs are minors, and thus "Defendants' consent is [i]rrelevant." (Opp. Br. at 29.) Specifically, Plaintiffs argue that "a minor's ability to contract and consent to an agreement has never been treated the same way as an adult." (See id.) This is undoubtedly true, and were this a contract case such an argument might have force. But this is not a contract case, and Plaintiffs have cited no authority for the proposition that the Wiretap Act's one-party consent regime depends on the age of the non-consenting party. Moreover, the sextet of Supreme Court decisions Plaintiffs cite have no application to these facts – they are a mix of death penalty, criminal sentencing, and abortion cases that have no bearing on the Court's task in this case, which is to determine whether Plaintiffs have stated plausible claims for the causes of action alleged. Their rhetoric notwithstanding, Plaintiffs have provided no legal basis to treat minors any differently than adults under the Wiretap Act.

The Wiretap Act claim must also fail because there are no allegations that Defendants intercepted "contents" of communications, as required by the Act. See Bartnicki, 200 F.3d at 115. In this regard, the Court agrees with the District of Delaware's cogent and persuasive Google Cookie decision, which holds that "contents" as defined in the Act consist of "information the user intended to communicate, such as the spoken words of a telephone call." 2013 WL 5582866, at *4 (citing United States v. Reed, 575 F.3d 900, 916 (9th Cir. 2009)). The converse of this rule is that "'personally identifiable information that is automatically generated by the communication' is not 'contents' for purposes of the Wiretap Act.'" See id. at *5

(quoting In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012)). The Ninth Circuit, in a recently published opinion, has expressly adopted a nearly identical standard. See Zynga, -- F.3d --, 2014 WL 1814029, at *7 ("we hold that under ECPA [the Wiretap Act], the terms 'contents' refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication").

Nothing allegedly intercepted in this case can pass muster under this standard. Plaintiffs argue that IP addresses and URLs in particular contain or are themselves "contents" for purposes of the Wiretap Act. (See Opp. Br. at 30.) IP addresses – the unique numbers generated by an ISP to identify a device connected to the internet and "voluntarily turned over to direct" computer servers, United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010) – are simply not "contents" of a communication. See, e.g., In re Application of the U. S. for an Order Authorizing use of A Pen Register and Trap on [xxx] Internet Service Acc't, 396 F. Supp. 2d 45, 48 (D. Mass. 2005) ("If . . . the government is seeking only IP addresses of the web sites visited and nothing more, there is no problem."). Indeed, in the analogous Fourth Amendment context, email and IP addresses can be collected without a warrant because they "constitute addressing information and do not necessarily reveal any more about the underlying contents of communications than do phone numbers," which can be warrantlessly captured via pen registers. Zynga, 2014 WL 1814029, at *9 (quoting United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008)); see also Christie, 624 F.3d at 574 ("[defendant] therefore had no reasonable expectation of privacy in his IP address and so cannot establish a Fourth Amendment violation."). Plaintiffs suggest no compelling reason (in fact, no reason at all) why Congress intended such "addressing

information" to be treated any differently for purposes of the Wiretap Act – neither does the text of the Act itself.

Instead, Plaintiffs' opposition brief focuses exclusively on the argument that URLs are contents.[13] The District of Delaware's Google Cookie decision, however, correctly highlights that "URLs [i.e., Uniform Resource Locators] do not change and are used to identify the physical location of documents" on servers connected to the internet. 2013 WL 5582866, at *5. This characterization is consistent with the MCC filed in this case, which describes one URL in particular as the "file path" for a specific video file contained in a folder on a web server owned or operated by Viacom. (See MCC § 78.) Characterized as such, the URLs in this case have less in common with "the spoken words of a telephone call," Google Cookie, 2013 WL 5582866, at *4, than they do with the telephone number dialed to initiate the call.

It thus rings hollow when Plaintiffs argue that the electronic video requests allegedly intercepted here are no different than the contents – i.e., the spoken words – of a telephone call to a video store. (See Opp. Br. at 34.) In the latter case, the video title spoken over the phone by a customer is the "substance, purport, or meaning" of the call itself, § 2510(8); in the former, the video title contained in the intercepted URL is the "physical" location of that video on the servers of the website generating the URL. Stated differently, words entered by a user into a Google search might themselves be considered contents if reproduced in a URL that is subsequently disclosed. See Zynga, 2014 WL 1814029, at *9 ("[u]nder some circumstances, a

[13] The Court cannot credit Plaintiffs' argument that Google intercepted communications containing birthdate and gender information. (See Opp. Br. 35.) Such an argument is foreclosed by the MCC itself, which expressly alleges that Viacom disclosed Plaintiffs' gender and age information, either directly or through the "rugrat" code. (See MCC ¶¶ 81, 98-99.) Indeed, the entirety of Plaintiffs' VPPA claim is premised on these very allegations. Plaintiffs cannot have it both ways – either Viacom told Google the age and sex of its users, or Google intercepted that information as Plaintiffs provided it to Viacom.

user's request to a search engine for specific information could constitute a communication such that divulging that search term to a third party" could result in disclosure of contents (citing In re Pen Register & Trap Application, 396 F. Supp. 2d at 49)). But the file path and video title information contained in the URLs allegedly intercepted in this case are static descriptions more akin to "identification and address information." See id. As such, the Wiretap Act claim must be dismissed for the additional reason that Plaintiffs fail to allege that Google intercepted the "contents" of an electronic communication at Viacom's behest.

E. The SCA Claim

Plaintiffs also allege that Google has violated the Stored Communications Act, 18 U.S.C. § 2701(a), which by operation of § 2707(a) creates a civil cause of action against: "whoever . . . intentionally accesses without authorization [or intentionally exceeds authorization to access] a facility through which an electronic communication service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is electronic storage in such system . . . ." (MCC §§ 165, 170.)[14] "Facility" is undefined, but "electronic communication service" is defined as any "service which provides to users thereof the ability to send or receive wire or electronic communications." § 2510(15).

Enacted as Title II of the Electronic Communications Privacy Act of 1986, the SCA was Congress's attempt to fill the possible gaps in Fourth Amendment protection created by the proliferation of third-party storage of electronic communications. Google Cookie, 2013 WL 5582866, at *6 ("because [copies of user e-mail created and retained by e-mail service providers

[14] Confusingly, the MCC states that the SCA claim is brought against Defendant Google only (see MCC at 40), yet later on the MCC also alleges that "Defendants" intentionally accessed their computers without authorization. (MCC § 165.) This latter allegation would imply that the SCA claim is in fact brought against Viacom as well. During briefing, however, all parties took the position that Plaintiffs intended to plead an SCA cause of action again Google only, and the Court will adopt that approach as well.

are] subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection" (quoting S. Rep No. 99-541 (1986), as reprinted in 1986 U.S.C.C.A.N. 3555, 3557)); see also Zynga, 2014 WL 1814029, at *4 (finding that the SCA "covers access to electronic information stored in third party computers"). The SCA thus protects individuals from the unauthorized acquisition or modification of certain of their communications while those communications are stored on someone else's computer. Garcia v. City of Laredo, Tex., 702 F.3d 788, 793 (5th Cir. 2012) ("the words of the statute were carefully chosen: '[T]he statute envisions a *provider* (the [internet service provider] or other network service provider) and a *user* (the individual with an account with the provider), with the *user's communications in the possession of the provider*.'" (internal quotation omitted)), cert. denied, 133 S. Ct. 2859 (2013).

Under the Act's plain language, Plaintiffs' SCA claim would appear to be a nonstarter – this is a case where Defendants' alleged privacy violations stem from "cookies" placed on Plaintiffs' (or their parents') own computers, not any third-party device. (See generally MCC ¶¶ 72-82.) Recognizing this, Plaintiffs argue that their own personal computers should be considered "facilities" for purposes of the SCA, and that Google can plausibly be liable for its unauthorized access of information found there. (See Opp. Br. at 47.) But as Google correctly highlights, Plaintiffs' approach is problematic. (Google Reply Br. at 15-17.) First, it runs contrary to the vast majority of published and non-published decisions that have considered the issue. See Cousineau v. Microsoft Corp., No. 11-cv-1438, 2014 WL 1232593, at *7 (W.D. Wash. Mar. 25, 2014) (collecting cases); Morgan v. Preston, No. 13-cv-0403, 2013 WL 5963563, at *5 (M.D. Tenn. Nov. 7, 2013) ("the overwhelming body of law" supports the

conclusion that "an individual's personal computer is not a 'facility through which an electronic communication service is provided'"). Moreover, Plaintiffs' interpretation of the statute does violence to the SCA's user/provider dichotomy, see Garcia, 702 F.3d at 793, and would empower service providers to grant access to their users' personal computer's without such users' authorization. § 2701(c) ("the person or entity providing a wire or electronic communications service" can authorize access to a facility). Such a result would be illogical, and "[s]tatutes should be interpreted to avoid untenable distinctions and unreasonable results whenever possible." Am Tobacco Co. v. Patterson, 456 U.S. 63, 71 (1982).

Plaintiffs' interpretation of the SCA is untenable, and this Court – in agreement with the great majority of decisions to address the issue – finds that the SCA is not concerned with access of an individual's personal computer. The SCA claim against Google fails as a matter of law will be dismissed with prejudice.

F. The State Law Claims

Plaintiffs also fail to state a plausible claim under any of the state law theories alleged.[15]

1. The California Invasion of Privacy Act Claim (Count IV)

In its wiretapping provision, the California Invasion of Privacy Act makes it a crime to "willfully and without the consent of all parties to the communication" read or "learn the contents or meaning of any message, report, or communication while the same in transit or passing over any wire, line or cable . . . ." Cal. Penal Code § 631(a). Persons injured by a violation of Section 631(a) may bring a civil action for money damages or injunctive relief. See id. at § 637.2. The MCC alleges that Viacom "knowingly serv[ed] as the conduit through which

[15] Because the Court finds that Plaintiffs fail to plead a viable state law claim, the Court need not reach Viacom's argument that COPPA preempts those claims. (Viacom Mov. Br. at 32.)

Google placed its [cookies] in positions to intercept the content of Plaintiffs' Internet communications." (MCC ¶ 184.)

Defendants argue that because the MCC does not allege facts demonstrating the interception of "contents" for purposes of the Wiretap Act, it also cannot allege the interception of "contents or meaning" for CIPA purposes. (See Viacom Mov. Br. at 34; Google Mov. Br. at 23.) Both Defendants cite the Google Cookie decision for this proposition. See 2013 WL 5582866, at *5-6 (dismissing the Wiretap Act and CIPA claims because "plaintiffs' allegations do not demonstrate that Google intercepted any 'contents or meaning'"). Plaintiffs do not argue that this aspect of Google Cookie was wrong, nor do they contend that "contents or meaning" means something different under California law than "contents" does under federal law; instead, Plaintiffs argue the intercepted information "takes on new meaning [*i.e.*, becomes contents] when it is matched up with an individual child via a cookie's unique identifier." (Opp. Br. at 43.) This argument is misguided. Plaintiffs' wiretap claims – including the CIPA count – are predicated upon the interception of electronic communication, not its use. (See MCC ¶ 180). Thus, whatever Google or Viacom allegedly do with the Plaintiffs' online information after it is intercepted has no bearing upon the question of whether that information could properly be considered "contents" at the time of interception. And, as the Court has discussed in detail supra, URLs and IP addresses are not properly considered "contents" in the wiretapping context.

In short, courts read CIPA's wiretapping provision and the federal Wiretap Act to preclude identical conduct. See Google Cookie, 2013 WL 5582866, at *6; Hernandez v. Path, Inc., No. 12-cv-1515, 2012 WL 5194120, at *3, *5 (N.D. Cal. Oct. 19, 2012) (dismissing Wiretap Act and CIPA wiretapping claim because of plaintiff's failure to allege "interception"

for purposes of both statutes). Absent a compelling suggestion otherwise, this Court will do the same, and holds that CIPA claim must fail for the same reason that the Wiretap Act claim fails – there are no allegations that plausibly demonstrate the interception of the "contents or meaning" of Plaintiffs' communications. The CIPA claim will be dismissed with prejudice.

2. The New Jersey Computer Related Offenses Act Claim (Count V)

The New Jersey CROA claim will be dismissed as well. The CROA is an anti-computer-hacking statute which provides a civil remedy to "[a] person or enterprise damaged in business or property as the result of" certain enumerated actions. N.J. Stat. Ann. 2A:38A-3; see also Marcus v. Rogers, 2012 WL 2428046, at *4 (N.J. Sup. Ct. App. Div. June 28, 2012) ("This statute plainly requires a plaintiff to prove that he or she was 'damaged in business or property.'"). The MCC, however, is devoid of factual allegations regarding the "business or property" damage Plaintiffs have suffered as a result of Defendants collecting and monetizing their online information. Plaintiffs attempt to rescue their CROA claim by rehashing arguments made in the standing context – namely, that Defendants' use of cookies permitted the "acquisition and use of Plaintiffs' personal information for marketing purposes," which Plaintiffs equate to "property" damage. (See Opp. Br. at 53.) This contention fails for the same reason it failed vis-a-vis standing – just because Defendants can monetize Plaintiffs' internet usage does not mean Plaintiffs can do so as well. Without allegations demonstrating plausible damage to "business or property," Plaintiffs cannot state a claim for relief under the CROA, and Count V will be dismissed without prejudice. See Phillips, 515 F.3d at 236.

3. The Invasion of Privacy Claim (Count VI)

New Jersey recognizes the common law privacy tort of "intrusion upon seclusion."

Soliman v. Kushner Cos., Inc., 77 A.3d 1214, 1224 (N.J. Sup. Ct. App. Div. 2013) (quoting Hennessey v. Coastal Eagle Point Oil Co., 609 A.2d 11, 17 (N.J. 1992)). This tort imposes civil liability for invasion of privacy on "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person." Hennessey, 609 A.2d at 17 (quoting Restatement (Second) of Torts, § 652B). The privacy invasion "need not be physical"; indeed, it may arise from "some other form of investigation or examination" into an individual's "private concerns." See id. To succeed with a claim for intrusion upon seclusion, a plaintiff "must establish that he possessed a reasonable expectation of privacy" in the affairs or concerns intruded upon. See G.D. v. Kenny, 15 A.3d 300, 320 (N.J. 2011). Plaintiffs allege Defendants "took information from the privacy of the Plaintiffs' homes," thereby "intentionally intrud[ing] upon the Plaintiffs' solitude or seclusion . . . ." (MCC ¶ 195.)

The Court notes that the right to privacy created by the New Jersey constitution provides greater protection than the privacy right created by the federal Constitution. See State v. Reid, 945 A.2d 26, 32-34 (N.J. 2008) (stating that Article I, Paragraph 7 of the New Jersey constitution "provides more protection than federal law affords" and holding that under New Jersey law an individual has a protectable "privacy interest in the subscriber information he or she provides to an Internet service provider"). Moreover, New Jersey explicitly "recognizes a right to 'informational privacy,'" which encompasses "any information that is identifiable to an individual." State v. Reid, 914 A.2d 310, 314 (N.J. Sup. Ct. App. Div. 2007) (internal quotation omitted), aff'd as modified, 945 A.2d 26; Doe v. Poritz, 662 A.2d 367, 412 (N.J. 1995) ("We have found a constitutional right of privacy in many contexts, including the disclosure of

confidential or personal information."). This information includes both "assigned" information, like names and addresses, but also "generated" information, such as medical records and phone logs. See Reid, 914 A.2d at 314 ("[P]ersonal information will be defined as any information, no matter how trivial, that can be traced or linked to an identifiable individual."). Thus, it is not implausible that the MCC as constituted alleges facts demonstrating that for purposes of New Jersey law Plaintiffs had a reasonable expectation that certain aspects of their online identities remain private and that Defendants intruded upon those private concerns. While Defendants' use of cookies to acquire or intercept IP addresses and URLs is an insufficient basis upon which to predicate claims for the federal statutes alleged, it is entirely unclear from the parties' submissions that the same would be true under New Jersey law and its expansive view of individual privacy.

But the Court need not address that question at this juncture, because the MCC lacks allegations demonstrating that the alleged intrusion is "highly offensive" to a reasonable person, see Hennessey, 609 A.2d at 17, and thus the intrusion upon seclusion claim must fail for that reason. Paragraph 197, which states without more that Defendants' intrusion "would be highly offensive to a reasonable person" is, of course, entirely conclusory, and thus properly disregarded on a motion to dismiss for failure to state a claim. See Bistrian, 696 F.3d at 365. The MCC otherwise does not explain factually how Defendants' collection and monetization of online information would be offensive to the reasonable person, let alone exceedingly so. The intrusion upon seclusion claim will be dismissed; because it does not appear at this juncture that leave to amend would be futile, however, this dismissal will be without prejudice. See Phillips, 515 F.3d at 236.

4. The Unjust Enrichment Claim (Count VII)

As stated supra, New Jersey law does not recognize "unjust enrichment" as an independent cause of action sounding in tort. Goldsmith, 975 A.2d at 462-63. "The Restatement of Torts does not recognize unjust enrichment as an independent tort cause of action. Unjust enrichment is of course a familiar basis for imposition of liability in the law of contracts." Castro v. NYT Television, 851 A.2d 88, 98 (N.J. Sup. Ct. App. Div. 2004) (citing Restatement (Second) of Contracts § 345(d)). Indeed, "[t]he unjust enrichment doctrine requires that the plaintiff show that it expected remuneration from the defendant at the time it performed or conferred a benefit on defendant and that the failure of remuneration enriched defendant beyond its contractual rights." VRG Corp. v. GKN Realty Corp., 641 A.2d 519, 554 (N.J. 1994); see also Mu Signa, Inc. v. Affine, Inc., No. 12-cv-1323 (FLW), 2013 WL 3772724, at *10 (D.N.J. July 17, 2013) (finding unjust enrichment only appropriate where, "if the true facts were known to plaintiff, he would have expected remuneration from defendant, at the time the benefit was conferred" (internal quotation omitted)).

This is not a quasi-contract case, and an unjust enrichment claim is inappropriate based upon the facts pleaded here. There are no allegations that Plaintiffs conferred any benefit on Defendants, nor are there any allegations that Plaintiffs expected or should have expected any sort of remuneration from them. Plaintiffs argue that the Defendants "received a direct benefit" from the information they collected from Plaintiffs. (Opp. Br. at 60.) But receipt of a benefit by a defendant and conferral of a benefit by a plaintiff are two different things, and it simply is not reasonable for a consumer – regardless of age – to use the internet without charge and expect compensation because a provider of online services has monetized that usage. The Court is

unaware of any legal authority that would find the relationship described in the MCC to be unjust in the contractual or quasi-contractual sense, and Plaintiffs do not suggest a cogent reason for the Court to find as such here. The common law "unjust enrichment" claim will be dismissed with prejudice.

IV. Conclusion

For the foregoing reasons, the Court will grant the motions to dismiss filed by Defendants Viacom Inc. and Google Inc. [Docket Entries 43 & 44.] The VPPA claim against Google is dismissed with prejudice, inasmuch as it is apparent that Plaintiffs cannot plead facts that would make Google a video tape service provider as that term is defined in the statute. The Wiretap Act, Stored Communication Act, California Invasion of Privacy Act, and state law unjust enrichment claims fail as a matter of law and will be dismissed with prejudice. The VPPA claim against Viacom, and the intrusion upon seclusion and New Jersey Computer Related Offenses Act claims against both Defendants, will be dismissed without prejudice, since it appears that the Plaintiffs could possibly plead facts sufficient to cure the defects in those claims. Plaintiffs will have forty-five (45) days to file an Amended Master Consolidated Class Action Complaint. An appropriate form of Order will be filed herewith.

s/ Stanley R. Chesler
STANLEY R. CHESLER
United States District Judge

Dated: July 2nd, 2014

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN RE NICKELODEON CONSUMER PRIVACY LITIGATION	**MDL No. 2443 (SRC)**
	Civil Action No. 12-07829
	Civil Action No. 13-03755
	Civil Action No. 13-03729
	Civil Action No. 13-03757
THIS DOCUMENT RELATES TO: THE CONSOLIDATION ACTION	**Civil Action No. 13-03731**
	Civil Action No. 13-03756
	ORDER

CHESLER, District Judge

This matter having come before the Court upon the motions to dismiss the Master Consolidated Class Action Complaint, filed by Defendants Viacom Inc. and Google Inc. ("Viacom" and "Google" and, collectively "Defendants") pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) [Docket Entries 43 & 44]; and Plaintiffs have opposed the motions [Docket Entry 52]; and the Court having opted to rule on the papers submitted, and without oral argument, pursuant to Federal Rule of Civil Procedure 78; and for the reasons expressed in the Opinion filed herewith; and good cause shown,

IT IS on this 2nd day of July, 2014,

ORDERED that Defendants' motions to dismiss [Docket Entries 43 & 44] be and hereby are **GRANTED**; and it is further

ORDERED that Counts II, IV, and VII, for violation of the federal Wiretap Act, violation of the California Invasion of Privacy Act, and common law unjust enrichment, be and hereby are **DISMISSED WITH PREJUDICE** as to both Defendants; and it is further

ORDERED that Count III, brought against Google for violation of the federal Stored Communications Act, be and hereby is **DISMISSED WITH PREJUDICE**; and it is further

ORDERED that Count I, for violation of the federal Video Protection and Privacy Act, be and hereby is **DISMISSED WITH PREJUDI**CE as to Google, and **DISMISSED WITHOUT PREJUDICE** as to Viacom; and it is further

ORDERED that Counts V and VI, for violation of the New Jersey Computer Related Offenses Act and common law invasion of privacy, be and hereby are **DISMISSED WITHOUT PREJUDICE** as to both Defendants; and it is further

ORDERED that Plaintiffs shall have leave to file an Amended Master Consolidated Class Action Complaint within forty-five (45) days of this Order.

s/ Stanley R. Chesler
STANLEY R. CHESLER
United States District Judge

NOT FOR PUBLICATION

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN RE NICKELODEON CONSUMER PRIVACY LITIGATION	**MDL No. 2443 (SRC)**
	Civil Action No. 12-07829
	Civil Action No. 13-03755
	Civil Action No. 13-03729
	Civil Action No. 13-03757
THIS DOCUMENT RELATES TO: **ALL CASES**	**Civil Action No. 13-03731**
	Civil Action No. 13-03756
	OPINION

CHESLER, District Judge

This matter comes before the Court upon the motion by Defendants Viacom Inc. ("Viacom") and Google Inc. ("Google") (collectively "Defendants"), to dismiss the Second Consolidated Class Action Complaint ("SAC") filed by Plaintiffs minor children and their father ("Plaintiffs"). For the reasons set forth in an Opinion dated July 2, 2014 ("the July 2 Opinion"), the Court dismissed with prejudice a number of Plaintiffs' claims. The Court also granted Plaintiffs leave to amend certain of its other theories of relief. Specifically, the Court dismissed without prejudice Plaintiffs' Video Privacy Protection Act ("VPPA") claim against Viacom, and their intrusion upon seclusion and New Jersey Computer Related Offenses ("CROA") claims against both Defendants. The issue now before the Court is whether Plaintiffs have cured the deficiencies in those counts. For the reasons that follow, and for those laid out in the July 2 Opinion, the Court finds that Plaintiffs have not cured the enumerated defects. Accordingly, the Court will grant Defendants' motions to dismiss the SAC with prejudice.

I. BACKGROUND

a. Facts

This is a multidistrict consolidated class action lawsuit, and Plaintiffs are children under the age of thirteen who claim that Defendants Viacom and Google have infringed upon their privacy rights. In its July 2 Opinion, the Court extensively reviewed the factual allegations involved, and the Court incorporates that background into this Opinion. For convenience, the Court will briefly restate the contours of the case. The Court assumes the following to be true for purposes of this motion only.

Viacom runs websites for children, including Nick.com, and it encourages users of those web sites to register profiles on them. Viacom collects information about the users who register, including their gender and birthday, and it then assigns a code name to each user based on that information. Children who register also create names associated with their profiles.

Children can stream videos and play video games on these sites, which creates a record of their gender and birthday, as well as the name of the video they played. Viacom sends this record to Google. Viacom also places a text file called a "cookie" onto Plaintiffs' computers without their consent. Cookies allow Viacom to gather additional information about these users, including their IP address, device and browser settings, and web traffic. Viacom shares this cookie information with Google. Additionally, Viacom allows Google to place its own text file "cookies" on Plaintiffs' computers and to access information from those cookies. This lets Google track certain aspects of Plaintiffs' Internet usage. Google's cookies also assign to each Plaintiff an identifier that is associated with other information Viacom has provided. Both Google and Viacom use all of this gathered information to target Plaintiffs with advertising.

b. Procedural History and the Instant Motions

The Court incorporates by reference the procedural history set forth in its July 2 Opinion. In that Opinion, the Court found some of Plaintiffs' claims to be deficient but potentially curable. Specifically, it held that Plaintiffs' VPPA claim against Viacom failed because the data that Viacom discloses is not "personally identifiable information." It further found that Plaintiffs' CROA claim failed because Plaintiffs had not alleged that they suffered any "business or property" damage. With respect to the intrusion upon seclusion claim, the Court found that Plaintiffs had not alleged an intrusion that would be "highly offensive" to a reasonable person. The Court granted Plaintiffs leave to amend these claims.

In response to the Court's July 2 Opinion, Plaintiffs filed the SAC in September of 2014, alleging certain additional facts which they believe cure the aforementioned deficiencies.

Defendants moved to dismiss on October 14, 2014. In support of their motions, Defendants assert that Plaintiffs' SAC suffers from the same fundamental defects. Namely, they urge that Plaintiffs still fail to allege the disclosure of any personally identifiable information; that there are no new allegations of requisite damages; and that the conduct at issue still falls short of the kind of "highly offensive" behavior that is cognizable under tort law.

Plaintiffs oppose the motions, highlighting new allegations included in the SAC. Specifically, Plaintiffs allege that Google could learn Plaintiffs' actual identities by using a "DoubleClick cookie identifier," and by combining the information Viacom provides it with data it already gathers from its other websites and services. Plaintiffs urge that newly alleged facts render Defendants' conduct "highly offensive" and establish the requisite damages.

II. DISCUSSION

a. Legal Standard

A complaint will survive a motion under Rule 12(b)(6) only if it states "sufficient factual allegations, accepted as true, to 'state a claim for relief that is plausible on its face.'" Iqbal, 556 U.S. at 678 (quoting Bell Atlantic v. Twombly, 550 U.S. 554, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Id. (citing Twombly, 550 U.S. at 556). Following Iqbal and Twombly, the Third Circuit has held that to prevent dismissal of a claim the complaint must show, through the facts alleged, that the plaintiff is entitled to relief. Fowler v. UPMC Shadyside, 578 F.3d 203, 211 (3d Cir. 2009). In other words, the facts alleged "must be enough to raise a right to relief above the speculative level[.]'" Eid v. Thompson, 740 F.3d 118, 122 (3d Cir. 2014) (quoting Twombly, 550 U.S. at 555).

While the Court must construe the complaint in the light most favorable to the plaintiff, it need not accept a "legal conclusion couched as factual allegation." Baraka v. McGreevey, 481 F.3d 187, 195 (3d Cir. 2007); Fowler, 578 F.3d at 210-11; see also Iqbal, 556 U.S. at 679 ("While legal conclusions can provide the framework of a complaint, they must be supported by factual allegations."). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, will not suffice." Iqbal, 556 U.S. at 678.

The Court will apply these principles to assess whether Plaintiffs have cured the pleading deficiencies in their (1) VPPA claims against Viacom; (2) CROA claims against both Defendants; and (3) intrusion upon seclusion claim against both Defendants.

b. The VPPA Claim Against Viacom

Section 2710(b) of the VPPA establishes the elements needed to state a claim under the statute. The VPPA is violated when a video tape service provider ("VTSP") "knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider[.]" For reasons explained extensively in the July 2 Opinion, nothing on the face of the VPPA or its legislative history suggest that "personally identifiable information" ("PII") includes information such as anonymous user IDs, gender and age, or data about a user's computer. In its July 2 Opinion, the Court found that the IP addresses and other information collected here could not, either individually or in the aggregate, identify a Plaintiff and what video they had watched.

The issue is whether Plaintiffs have alleged new facts which make it plausible that the information collected does indeed identify Plaintiffs. The Court finds that they have not.

Plaintiffs argue that because of Google's ubiquitous presence on the Internet, it can learn a lot from even limited information. Plaintiffs note that Google owns a vast network of services -- including Google.com, Gmail, YouTube, and so forth -- which collects ample data about users of those services, sometimes including their full names. Plaintiffs contend that with that information already in hand, Google can take the information Viacom sends it and indeed ascertain personal identities.

The Court has already concluded, however, that PII "is information which must, without more, itself link an actual person to actual video materials." In re Nickelodeon Consumer Privacy Litig., No. 12-cv-7829, 2014 WL 3012873, at *10 (D.N.J. July 2, 2014). Nothing in the amended Complaint changes the fact that Viacom's disclosure does not -- "without more" -- identify individual persons. Id.; see also Ellis v. Cartoon Network, Inc., No. 1:14-cv-484-TWT,

2014 WL 5023535, at *3 (N.D. Ga. Oct. 8, 2014) (quoting In re Hulu Privacy Litigation, No. C-11-03764-LB, 2014 WL 1724344, at *13 (N.D.Cal. Apr. 28, 2014) ("The emphasis is on disclosure, not comprehension by the receiving person.").

Even if the Court were to consider what Google could do with the information, rather than the nature of the information itself, Plaintiffs' claim would still fail because it is entirely theoretical. According to Plaintiffs, in order for Google to connect the information that Viacom provides it with the identity of an individual Plaintiff, one of the Plaintiffs would need to have registered on one of Google's services. Crucially, however, Plaintiffs have alleged no facts whatsoever that a Plaintiff ever registered with Google. Such an allegation is necessary for the theoretical combination of information to actually yield one of the Plaintiff's identities. It appears that Google would not even allow a child under the age of thirteen to register for its services, which would rule out the entire class of Plaintiffs, all of whom are under that age.

At bottom, the SAC simply includes no allegation that Google can identify the individual Plaintiffs in this case, as opposed to identifying people generally, nor any allegation that Google has actually done so here. In that respect, Plaintiffs' VPPA claim resembles one that another court rejected as deficient:

> Although ESPN could be found liable under the VPPA for disclosing both "a unique identifier and a correlated look-up table" by which Plaintiff could be identified as a particular person who watched particular videos, Plaintiff does not allege sufficient facts to support his theory that Adobe already has a "look-up table." Even if Adobe does "possess a wealth of information" about individual consumers, it is speculative to state that it can, and does, identify specific persons as having watched or requested specific video materials from the WatchESPN application.
>
> [Eichenberger v. ESPN, No. 2:14-cv-00463-TSZ (W.D. Wash. Nov. 24, 2014) (Docket Item 38 at 2) (minute order dismissing complaint) (internal citation omitted)].

Here too, the SAC does not allege that Google actually "can, and does, identify" any of the Plaintiffs. The theory upon which Plaintiffs rely to cure this claim is thus wholly speculative. The Court will dismiss Plaintiffs' VPPA claim with prejudice.

c. The CROA Claims Against Both Defendants

The New Jersey CROA is an anti-computer-hacking statute which provides a civil remedy to "[a] person or enterprise damaged in business or property as the result of" certain enumerated actions. N.J. Stat. Ann. 2A:38A-3; see also Marcus v. Rogers, 2012 WL 2428046, at *4 (N.J. App. Div. June 28, 2012) ("This statute plainly requires a plaintiff to prove that he or she was 'damaged in business or property.'").

The Court notes at the outset, as it did in its July 2 Opinion, that because the CROA targets computer hacking, it is dubious whether the law also covers situations like this, in which Plaintiffs' computers have not been hacked nor has their information been stolen. Cf. Mu Sigma, Inc. v. Affine, Inc., No. 12-1323 (FLW), 2013 WL 3772724, at *10 (D.N.J. July 17, 2013) (finding CROA claim deficient in part because it did "not specify how or whether Defendants allegedly stole its data or what in particular was stolen"). By relying upon another statute that does not appear apt to the circumstances, Plaintiffs again seek to fit square pegs into round holes.

Even assuming that the statute applies, the Court earlier dismissed the CROA claim because Plaintiffs failed to allege "business or property" damage stemming from Defendants' conduct. The Court found that just because Defendants could monetize Plaintiffs' Internet usage did not necessarily mean that Plaintiffs could do the same. In the SAC, Plaintiffs now rhetorically frame their damages in terms of unjust enrichment in a quasi-contractual setting. Despite the new semantics, Plaintiffs are pointing to the same exact concept in an attempt to

satisfy the damages requirement. The Court again rejects comparisons between this scenario and unjust enrichment or a quasi-contract, for reasons stated in the July 2 Opinion.

In relevant part, Plaintiffs fail to allege that they could have monetized the PII collected, or if they could, that Defendants' conduct prohibited them from still doing so. See In re Google Cookie Placement Consumer Privacy Litig., 988 F. Supp. 2d 434, 442 (D. Del. 2013) ("[The Complaint] details that online personal information has value to third-party companies and is a commodity that these companies trade and sell . . . . [Yet] plaintiffs have not sufficiently alleged that the ability to monetize their PII has been diminished or lost by virtue of Google's previous collection of it."); see also Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1028-30 (N.D. Cal. 2012) (rejecting allegations that the unauthorized taking of consumer information constitutes injury or damages under other theories of relief).

Plaintiffs have again failed to identify any property or business damage, as is required. Cf. Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1159 (W.D. Wash. 2001) ("Unlike a computer hacker's illegal destruction of computer files or transmission of a widespread virus which might cause substantial damage to many computers as the result of a single act, here the transmission of an internet cookie is virtually without economic harm."). The Court will accordingly dismiss the CROA claim with prejudice.

d. The Intrusion Upon Seclusion Claims Against Both Defendants

New Jersey recognizes "intrusion upon seclusion," a common law privacy tort. Soliman v. Kushner Cos., 77 A.3d 1214, 1224 (N.J. App. Div. 2013) (quoting Hennessey v. Coastal Eagle Point Oil Co., 609 A.2d 11, 17 (N.J. 1992)). That claim imposes civil liability upon one "who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his

private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person." Hennessey, 609 A.2d at 17 (quoting Restatement (Second) of Torts, § 652B) (emphasis added); see also Castro v. NYT Television, 895 A.2d 1173, 1177 (N.J. App. Div. 2006) (quoting same).

Although the question of what constitutes "highly offensive" conduct is sometimes appropriate for juries, see Vurimindi v. Fuqua Sch. of Bus., 435 F. App'x 129, 136 (3d Cir. 2011) (finding that claim should have survived pleading stage), courts are also empowered to make that determination if it can be decided as a matter of law. Boring v. Google, 362 F. App'x 273, 279 (3d Cir. 2010) ("[Plaintiffs] suggest that the District Court erred in determining what would be highly offensive to a person of ordinary sensibilities at the pleading stage, but they do not cite to any authority for this proposition. Courts do in fact, decide the 'highly offensive' issue as a matter of law at the pleading stage when appropriate.") (citing Diaz v. D.L. Recovery, 486 F.Supp.2d 474, 475–80 (E.D.Pa.2007)).

Here, as in the July 2 Opinion, the Court finds as a matter of law that Defendants' alleged conduct falls short of the "highly offensive" behavior which is cognizable under this theory. Plaintiffs suggest that additional facts pleaded in the SAC render Defendants' conduct "highly offensive" in light of social norms. Specifically, they urge that Defendants' activities violated various statutes and public opinion as expressed through polling.

With respect to the alleged statutory violations, the Court has already determined that Defendants' conduct does not violate the statutes upon which Plaintiffs rely. With respect to public polling, Plaintiffs cite to sentiments that are not directly on point. Plaintiffs highlight, for example, statistics suggesting that a large majority of the public opposes tracking children's online activity. Yet such a statistic does not answer the relevant inquiry: what a reasonable

person finds "highly offensive." That which the public generally supports or opposes does not equate to that which an ordinarily reasonable person finds "highly offensive." Indeed, a large majority of voters may disapprove of a given politician's job performance, but that would not indicate that a reasonable person finds the politician's performance "highly offensive." The Court therefore finds Plaintiffs' polling allegations inapposite to the legal issue. It may indeed strike most people as undesirable that companies routinely collect information about anonymous web users to target ads in a more sophisticated way; yet this theory of relief requires more. See Rush v. Portfolio Recovery Associates, 977 F. Supp. 2d 414, 433 n.23 (D.N.J. 2013) ("[A]n intrusion on seclusion claim requires a showing of conduct more offensive than that which merely annoys, abuses, or harasses.").

Surveying the classic intrusion-upon-inclusion claims demonstrates that this tort supports allegations of truly exceptional conduct. See, e.g., Leang v. Jersey City Bd. of Educ., 198 N.J. 557, 589-90 (2009) (coworker falsely reported that teacher threatened students' lives, causing teacher to undergo psychiatric evaluation); Soliman v. Kushner Cos., 77 A.3d 1214, 1218 (N.J. App. Div. 2013) (defendants hid video recording equipment in bathrooms); Del Mastro v. Grimado, No. BER-C-388-03E, 2005 WL 2002355 (N.J. Super. Ct. Ch. Div. Aug. 19, 2005) (plaintiff's ex-boyfriend distributed erotic photos of her without permission). The Court finds that the collection and disclosure of anonymous browsing history and other similar information falls short of that kind of "highly offensive" behavior. See, e.g., In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (finding unauthorized disclosure of mobile device information to not be egregious breach of social norms); Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (finding disclosure of LinkedIn data insufficiently offensive).

In a final effort to salvage this claim, Plaintiffs urge that the Court should consider Defendants' conduct "highly offensive" because it involves children. It is, of course, apparent to the Court that children do indeed warrant special attention and heightened protections under our laws and social norms. To be sure, however, the Court's role in this decision is not to pass on the morality nor the wisdom of companies tracking the anonymous web activities of children for advertising purposes. The Court does not, by way of this Opinion, find Defendants' conduct beneficial. The Court's only task is to assess whether Plaintiffs' claims pass muster under the federal pleading standards vis-à-vis the authorities upon which those claims rest. Here, Plaintiffs' SAC is an exercise in attempting to fit square pegs into round holes. Although Plaintiffs have identified conduct that may be worthy of further legislative and executive attention, they have not cited any existing and applicable legal authority to supports their claims.

III. CONCLUSION

For the foregoing reasons, the Court will grant Defendants' motions to dismiss [Docket Entries 77 & 78]. An appropriate form of Order will be filed herewith.

s/ Stanley R. Chesler
STANLEY R. CHESLER
United States District Judge

Dated: January 20th, 2015

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN RE NICKELODEON CONSUMER PRIVACY LITIGATION	**MDL No. 2443 (SRC)**
	Civil Action No. 12-07829
	Civil Action No. 13-03755
	Civil Action No. 13-03729
	Civil Action No. 13-03757
THIS DOCUMENT RELATES TO: **ALL CASES**	**Civil Action No. 13-03731**
	Civil Action No. 13-03756
	ORDER

CHESLER, District Judge

This matter having come before the Court upon Defendants' motions to dismiss Plaintiffs' Second Consolidated Class Action Complaint; and Plaintiffs having opposed the motions; and the Court having opted to rule on the papers and without oral argument, pursuant to Federal Rule of Civil Procedure 78; and for the reasons expressed in the Opinion filed herewith; and for good cause shown,

IT IS on this 20th day of January, 2015,

ORDERED that Defendants' motions to dismiss [Docket Entries 77 & 78] be and hereby are **GRANTED**; and it is further

ORDERED that the Second Consolidated Class Action Complaint is **DISMISSED WITH PREJUDICE** as to both Defendants.

s/ Stanley R. Chesler
STANLEY R. CHESLER
United States District Judge

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 15-1441

In re: Nickelodeon Consumer Privacy Litigation

On Appeal from the U.S. District Court for the District of New Jersey
Case No. 2:12-cv-07829
The Honorable Stanley R. Chesler

APPELLANTS' APPENDIX – VOLUME 2
(Appellant 000059-000420)

EICHEN CRUTCHLOW
ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
Facsimile: (732) 248-8273

BARTIMUS FRICKLETON
ROBERTSON & GOZA, PC
715 Swifts Highway
Jefferson City, MO 65109
Telephone: (573) 659-4454
Facsimile: (573) 659-4460

Co-Lead Counsel on behalf of All Plaintiffs

TABLE OF CONTENTS

CERTIFICATE OF SERVICE

I, Barry R. Eichen, hereby certify that on April 27, 2015, I caused the following documents to be electronically filed with United States Court of Appeals for the Third Circuit by using the CM/ECF system; and caused a copy of the foregoing documents to be served *via* U.S. Mail to all counsel listed below and the Court.

Dated: April 27, 2015

/s/ Barry R. Eichen
Barry R. Eichen

Barry R. Eichen
EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
Facsimile: (732) 248-8273

Co-Lead Counsel on behalf of Plaintiffs

SERVICE LIST

ATTORNEYS FOR DEFENDANT VIACOM, Inc.

Stephen M. Orlofsky
Seth J. Lapidow
BLANK, ROME, LLP
301 Carnegie Center, 3rd Floor
Princeton, NJ 08540

Bruce P. Keller
Jeffrey S. Jacobson
DEBEVOISE & PLIMPTON LLP
919 Third Avenue
New York, NY 10022

ATTORNEYS FOR GOOGLE, INC.

Jeffrey J. Greenbaum
Joshua N. Howley
SILLS CUMMIS & GROSS PC
One Riverfront Plaza
Newark, NJ 07102-5400

Colleen Bal
Michael H. Rubin
WILSON SONSINI GOODRICH & ROSATI, PC
One Market Plaza
Spear Tower, Suite 3300
San Francisco, CA 94105-1126

Tonia O. Klausner
WILSON SONSINI GOODRICH & ROSATI, PC
1301 Avenue of the Americas, 40th Floor
New York, NY 10019

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

IN RE NICKELODEON CONSUMER PRIVACY LITIGATION	)	**C.A. 12-7829 (SRC)(CLW)**
	)	**MDL No. 2443**
	)	
	)	**Judge Stanley R. Chesler**
	)	
	)	**MASTER CONSOLIDATED**
This Document Relates to:	)	**CLASS ACTION COMPLAINT**
	)	
All Actions	)	
	)	

I. INTRODUCTION AND OVERVIEW

1. This class action seeks damages and injunctive relief on behalf of all minor children under the age of 13 in the United States who visited the websites Nick.com, NickJr.com, or NeoPets.com. Defendant Viacom Inc., (hereinafter "Viacom") owns and operates these websites, each of which has a target audience of minor children.

2. Specifically, this case is about Defendant Viacom and Defendant Google Inc.'s (hereinafter "Google") misuse of Internet technologies ("cookies") to disclose compile, store and exploit the video viewing histories and Internet communications of children throughout the United States in contravention of federal and state law. With neither the knowledge nor the consent of their parents, unique and specific electronic identifying information and content about each of these children was accessed, stored, and utilized for commercial purposes.

3. This case is brought to enforce the privacy rights of these children, and to enforce federal and state laws designed to uphold those rights.

II. NATURE OF THE ACTION

4. The named Plaintiffs are minor children under the age of 13 who were registered users of the websites Nick.com, Nickjr.com and NeoPets.com.

5. The Defendants utilized Internet technologies commonly known as "cookies" to track and share the plaintiffs' and putative class members' video-viewing histories on Nick.com, Nickjr.com and NeoPets.com without plaintiffs' informed written consent.

6. The Defendants further utilized these technologies to track plaintiffs' and the putative class members' Internet communications without plaintiffs' authorization or consent.

7. Plaintiffs are informed and believe the Defendants' conduct is systematic and class wide.

8. The Defendants' conduct violated federal and state laws designed to protect the privacy of American citizens, including children. Such conduct gives rise to the following statutory and common law causes-of-action:

a. Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710, et seq.;

b. Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2510, et seq.;

c. Violation of the Stored Communications Act, 18 U.S.C. § 2701, et seq.;

d. Violation of the California Invasion of Privacy Act, Cal. Penal Code §631(a), et seq.;

e. Violation of the New Jersey Computer Related Offenses Act, N.J.S.A. 2A:38A-1, et seq.;

f. Intrusion Upon Seclusion; and

g. Unjust Enrichment.

III. THE PARTIES

A. Plaintiffs

9. Plaintiffs C.A.F., C.T.F., M.P. and T.P. are minor children under the age of 13 who reside in the State of New Jersey. At all relevant times, they have been registered users of the websites Nick.com and/or NickJr.com.

10. Plaintiff L.G. is a minor child under the age of 13 who resides in the State of California. At all relevant times, L.G. has been a registered user of the website Nick.com and/or NickJr.com.

11. Plaintiff T.M. is a minor child under the age of 13 who resides in the State of Illinois. At all relevant times, T.M. has been a registered user of the websites Nick.com, NickJr.com and/or NeoPets.com.

12. Plaintiff N.J. is a minor child under the age of 13 who resides in the State of Missouri. At all relevant times, N.J. has been a registered user of the website Nick.com and/or NickJr.com.

13. Plaintiff A.V. is a minor child under the age of 13, who resides in the State of New York. At all relevant times, A.V. has been a registered user of the website Nick.com and/or NickJr.com.

14. Plaintiff Johnny Doe is a minor child under the age of 13, who resides in the State of Texas. At all relevant times, he has been a registered user of the website Nick.com, NickJr.com and/or NeoPets.com.

15. Plaintiff K.T. is a minor child under the age of 13, who resides in the state of Pennsylvania. At all relevant times, K.T. has been a registered user of the website Nick.com and/or NickJr.com.

B. Defendant Viacom

16. Defendant Viacom, Inc. is a publicly-traded Delaware corporation with headquarters at 515 Broadway, New York, New York 10036. Defendant Viacom does business throughout the United States and the world, deriving substantial revenue from interstate commerce within the United States.

17. Defendant Viacom publicly proclaims its Nickelodeon division to be "the number-one entertainment brand for kids."[1]

C. Defendant Google

18. Defendant Google, Inc. is a publicly traded Delaware corporation with headquarters at 1600 Amphitheatre Parkway, Mountain View, California 94043. Defendant Google does business throughout the United States and the world, deriving substantial revenue from interstate commerce within the United States.

19. Google has, by design, become the global epicenter of Internet search and browsing activity. Underscoring its vast Internet reach, Google describes its "mission" as "to organize the world's information and make it universally accessible and useful."[2]

IV. JURISDICTION AND VENUE

20. This Court has personal jurisdiction over Defendants because all Defendants have sufficient minimum contacts with this District in that they all operate businesses with worldwide reach, including but not limited to the State of New Jersey.

[1] Viacom.com, Viacom Company Overview, http://www.viacom.com/brands/pages/nickelodeon.aspx (last visited October 7, 2013).
[2] Google.com, Google Company Overview, http://www.google.com/about/company (last visited October 7, 2013).

21. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §1331 because this action arises in part under federal statutes, namely 18 U.S.C. §2710, et seq. (the Video Privacy Protection Act), 18 U.S.C. §2510, et seq. (the Electronic Communications Privacy Act), and 18 U.S.C. § 2701 et seq. (the Stored Communications Act). This Court further has subject matter jurisdiction pursuant to 28 U.S.C. §1332(d) (the Class Action Fairness Act) because the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and a member of the class is a citizen of a State different from any Defendant.

22. This Court has supplemental jurisdiction over the remaining state law claims pursuant to 28 U.S.C. §1367 because the state law claims form part of the same case or controversy under Article III of the United States Constitution.

23. Venue is proper in this District pursuant to 28 U.S.C. §1391 because a substantial amount of the conduct giving rise to this cause of action occurred in this District and because the United States Judicial Panel on Multidistrict Litigation transferred this case to this District for consolidated pretrial proceedings pursuant to Transfer Order in MDL No. 2443, entered on June 11, 2013.

V. FACTS COMMON TO ALL COUNTS

A. How Do Internet Users Access Websites?

24. In order to access and communicate on the Internet, people employ web-browsers such as Apple Safari, Microsoft Internet Explorer, Google Chrome, and Mozilla Firefox.

25. Every website is hosted by a computer server, which communicates with an individual's web-browser to display the contents of webpages on the monitor or screen of their individual device.

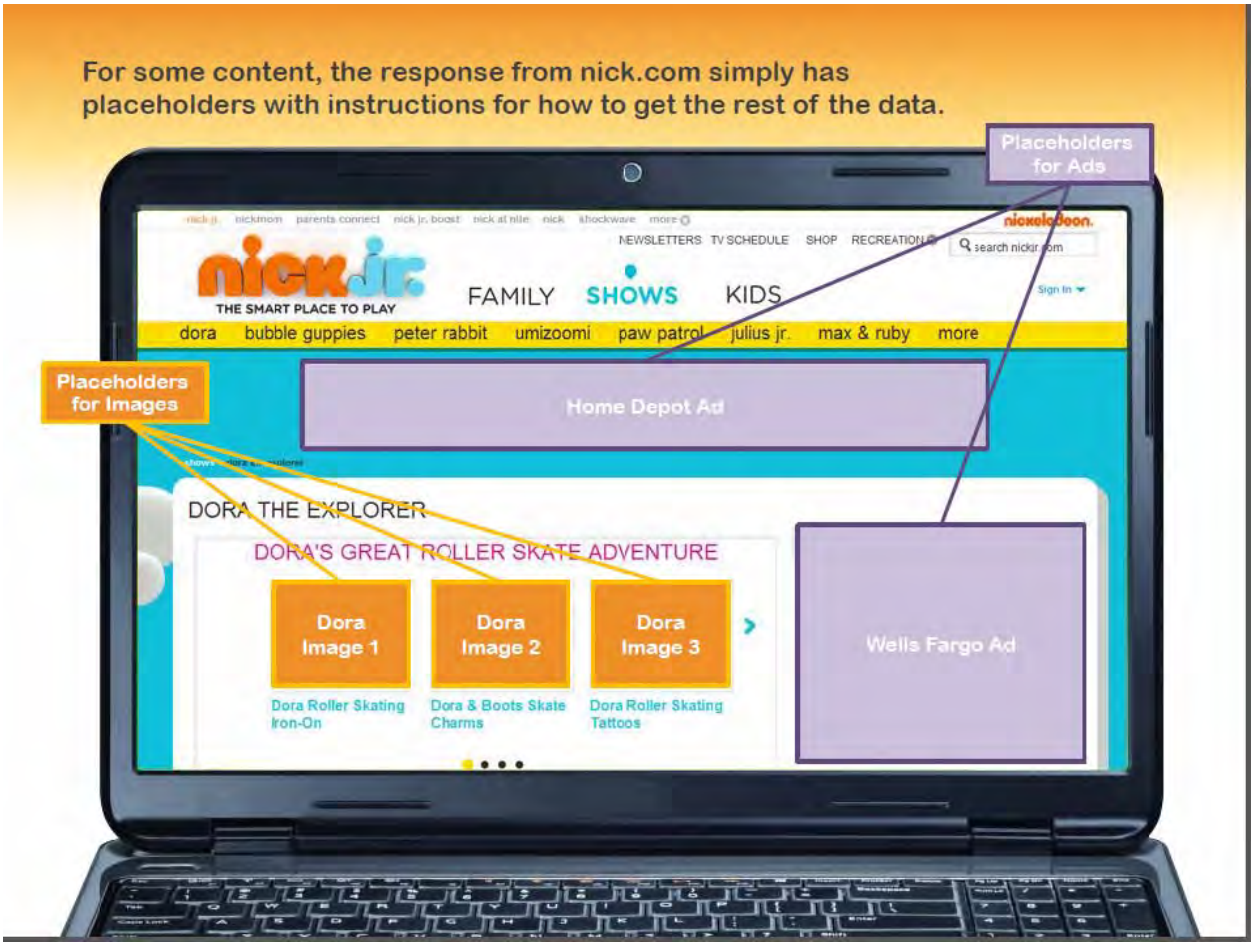
26. The basic command web browsers use to communicate with website servers is

called the "GET" command.

27. For instance, when a child types "www.nick.com" into the navigation bar of his or her web-browser and hits "Enter," the child's web browser sends a "GET" command to the Nick.com host server. The "GET" command instructs the Nick.com host server to send the information contained on Nick.com to the child's browser for display. Graphically, the concept is illustrated as follows:

28. Although a single webpage appears on the child's screen as a complete product, a single webpage is in reality an assembled collage of independent parts. Each different element of a webpage – *i.e.* the text, pictures, advertisements and sign-in box – often exist on distinct servers, which are sometimes operated by separate companies.

29. To display each of these parts of the webpage as one complete product, the host server leaves part of its website blank.



30. Upon receiving a GET command from a child's web browser, the website host server contemporaneously instructs the child's web browser to send other GET commands to other servers responsible for filling in the blank parts of the web page.

31. Those other servers respond by sending information to fill in the blank portions of the webpage.

B. Targeted Internet Advertising: How Does it Work?

32. In the Internet's formative years, advertising on websites followed the same model as traditional newspapers. Just as a sporting goods store would choose to advertise in the sports section of a traditional newspaper, advertisers on the early Internet paid for ads to be placed on specific web pages based on the type of content displayed on the web page.

33. Computer programmers eventually developed technologies commonly referred to as Internet "cookies," which are small text files that web servers can place on a person's computing device when that person's web browser interacts with the website host server.

34. Cookies can perform different functions; and some cookies were eventually designed to track and record an individual's activity on websites across the Internet.

35. In general, cookies are categorized by:

(1) "time" – the length of time they remain on a user's device; and

(2) "party" – describing the relationship (first or third party) between the Internet user and the party who places the cookie:

a. Cookie Classifications by *Time:*

i. "Session cookies" are placed on a person's computing device only for the time period during which the person is navigating the website that placed the cookie. The person's web browser normally deletes session cookies when he or she closes the browser; and

ii. "Persistent cookies" are designed to survive beyond a single Internet-browsing session. The party creating the persistent cookie determines its lifespan. As a result, a "persistent cookie" can record a person's Internet browsing history and Internet communications for years. By virtue of their lifespan, persistent cookies can track a person's communications across the Internet. Persistent cookies are also sometimes called "tracking cookies."

b. Cookie Classifications by *Party*

i. "First-party cookies" are set on a person's device by the website the person intends to visit. For example, Defendant Viacom sets a collection of Nick.com cookies when a child visits Nick.com. First-party cookies can be helpful to the user, server and/or website to assist with security, login

and functionality; and

ii. "Third-party cookies" are set by website servers other than the server the person intends to visit. For example, the same child who visits Nick.com will also have cookies placed on his or her device by third-party web servers, including advertising companies like Google. Unlike first-party cookies, third-party cookies are not typically helpful to the user. Instead, third-party cookies typically work in furtherance of data collection, behavioral profiling and targeted advertising.

36. In addition to the information obtained by and stored within third party cookies, third party web servers can be granted access to profile and other data stored within first party cookies.

37. Enterprising online marketers, such as defendants, have developed ways to monetize and profit from these technologies. Specifically, third party persistent "tracking" cookies are used to sell advertising that is customized based upon a particular person's prior Internet activity.

38. Website owners such as Viacom can now sell advertising space on their web pages to companies who desire to display ads to children that are customized based on the child's Internet history.

39. Moreover, many commercial websites with extensive advertising allow third-party companies such as Google to serve advertisements directly from third-party servers rather than through the first party website's server.

40. To accomplish this, the host website leaves part of its webpage blank. Upon receiving a "GET" request from an individual's web browser, the website server will,

unbeknownst to that individual, immediately and contemporaneously re-direct the user's browser to send a "GET" request to the third-party company charged with serving the advertisements for that particular webpage.

41. Some websites contract with multiple third-parties to serve ads such that the website will contemporaneously instruct a user's browser to send multiple "GET" requests to multiple third-party websites.

42. In many cases, the third party receives the re-directed "GET" request and a copy of the user's request to the first-party website before the content of the initial request from the first-party webpage appears on the user's screen.

43. The transmission of such information is contemporaneous to the user's communication with the first-party website.

44. The third-party server then responds by sending the ad to the user's browser – which then displays it on the user's device.

45. In the process of placing advertisements, third-party advertising companies also implant third-party cookies on individuals' computers. They further assign each specific user a unique numeric or alphanumeric identifier that is associated with that specific cookie.

46. The entire process occurs within milliseconds and the web page appears on the individual's web browser as one complete product, without the person ever knowing that multiple GET requests were executed by the browser at the direction of the web site server, and that first party and third party cookies were placed. Indeed, all the person has done is type the name of a single web page into his or her browser. Graphically, the concept is illustrated as follows:

47. Because advertising companies serve advertisements on multiple sites, their cookies also allow them to monitor an individual's communications over every website and webpage on which the advertising company serves ads. And because that cookie is associated with a unique numeric or alphanumeric identifier, the data collected can be utilized to create detailed profiles on specific individuals.

48. By observing the web activities and communications of tens of millions of Internet users, advertising companies, including Defendant Google, build digital dossiers of each individual user and tag each individual user with a unique identification number used to aggregate their web activity. This allows for the placement of "targeted" ads.

C. The Personal Information Defendants Collect: What is Its Value?

49. To the advertiser, targeted ads provided an unprecedented opportunity to reach potential consumers. The value of the information that Defendants take from people who use the Internet is well understood in the e-commerce industry. Personal information is now viewed as a form of currency. Professor Paul M. Schwartz noted in the Harvard Law Review:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.[3]

50. Likewise, in the Wall Street Journal, privacy expert and fellow at the Open Society Institute, Christopher Soghoian, noted:

> The dirty secret of the Web is that the "free" content and services that consumers enjoy come with a hidden price: their own private data. Many of the major online advertising companies are not interested in the data that we knowingly and willingly share. Instead, these parasitic firms covertly track our web-browsing activities, search behavior and geolocation information. Once collected, this mountain of data is analyzed to build digital dossiers on millions of consumers, in some cases identifying us by name, gender, age as well as the medical conditions and political issues we have researched online.
>
> Although we now regularly trade our most private information for access to social-networking sites and free content, the terms of this exchange were never clearly communicated to consumers.[4]

51. In the behavioral advertising market, "the more information is known about a consumer, the more a company will pay to deliver a precisely-targeted advertisement to him."[5]

---

[3] Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2056-57 (2004).

[4] Julia Angwin, *How Much Should People Worry About the Loss of Online Privacy?*, THE WALL STREET JOURNAL (Nov. 15, 2011).

[5] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change – A Proposed Framework for Business and Policymakers – Preliminary FTC Staff Report*, December

52. In general, behaviorally targeted advertisements based on a user's tracked internet activity sell for at least *twice* as much as non-targeted, run-of-network ads.[6]

53. Upon information and belief, most of the Defendants' advertising clients pay on a cost-per-click basis.

54. The Defendants also offer cost-for-impression ads, which charge an advertising client each time the client's ad displays to a user.

55. In general, behaviorally-targeted advertisements produce 670 percent more clicks on ads per impression than run-of-network ads. Behaviorally-targeted ads are also more than twice as likely to convert users into buyers of an advertised product as compared to run-of-network ads.[7]

56. The cash value of users' personal information can be quantified. For example, in a recent study authored by Tim Morey, researchers studied the value that 180 Internet users placed on keeping personal data secure. Contact information was valued by the study participants at approximately $4.20 per year. Demographic information was valued at approximately $3.00 per year. Web browsing histories were valued at a much higher rate: $52.00 per year. The chart below summarizes the findings[8]:

2010, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf at 37 (last visited October 22, 2013).

[6] NetworkAdvertising.org, *Study Finds Behaviorally-Targeted Ads More Than Twice As Valuable, Twice As Effective As Non-Targeted Online Ads*, http://www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf (last visited September 16, 2013).

[7] Howard Beales, *The Value of Behavioral Advertising*, 2010 http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf (last visited September 16, 2013).

[8] Tim Morey, *What's Your Personal Data Worth?*, January 18, 2011, http://designmind.frogdesign.com/blog/what039s-your-personal-data-worth.html (last visited September 16, 2013).

57. In 2012, Defendant Google convened a panel called "Google Screenwise Trends" through which Google paid Internet users to track their online communications through gift cards, with most valued at $5. Though it is unclear whether Google continues to operate Screenwise Trends in the United States,[9] the project remains active in the U.K., where users are paid £15 for staying with Screenwise Trends for 30 days after sign-up and an additional £5 for every 90 days users remain with the panel.[10] Google's Screenwise Trends program demonstrates conclusively that Internet industry participants, including the Defendants, recognize the enormous value in tracking user's Internet communications.

58. Targeting advertisements to children adds *more* value than targeting to adults because children are generally unable to distinguish between content and advertisements. This is

[9] See Screenwisepanel.com, Sign-in Page, https://www.screenwisepanel.com/member/Index.aspx?ReturnUrl=%2fmember, (last visited Sept. 25, 2013) (plaintiffs believe this is the sign-in page for Screenwise Trend users in the United States, indicating the program is still in existence).

[10] See Screenwisetrendspanel.com, Rewards, https://www.screenwisetrendspanel.co.uk/nrg/rewards.php (last visited Sept. 25, 2013).

especially true in the digital realm where children are less likely to identify and counteract the persuasive intent of advertising. This results in children, especially those below the age of 8, accepting advertising information contained in commercials "uncritically . . . [and as] truthful, accurate, and unbiased."[11]

59. An investigation by the Wall Street Journal revealed that "popular children's websites install more tracking technologies on personal computers than do the top websites aimed at adults."[12]

D. Internet Tracking: Is it Anonymous?

60. Though industry insiders claim publicly that tracking is anonymous, experts in the field disagree. For instance, in a widely cited blog post for The Center for Internet and Society at Stanford Law School titled "There is No Such Thing as Anonymous Online Tracking," Professor Arvind Narayanan explained:

> In the language of computer science, clickstreams – browsing histories that companies collect – are not anonymous at all; rather, they are pseudonymous. The latter term is not only more technically appropriate, it is much more reflective of the fact that at any point after the data has been collected, the tracking company might try to attach an identity to the pseudonym (unique ID) that your data is labeled with. Thus, identification of a user affects not only future tracking, but also retroactively affects the data that's already been collected. Identification needs to happen only once, ever, per user.

[11] Report of the APA Task Force on Advertising and Children at 8 available at http://www.apa.org/pi/families/resources/advertising-children.pdf; see also, Louis J. Moses, *Research on Child Development: Implications for How Children Understand and Cope with Digital Marketing*, MEMO PREPARED FOR THE SECOND NPLAN/BMSG MEETING ON DIGITAL MEDIA AND MARKETING TO CHILDREN, June 29-30, 2009, http://digitalads.org/documents/Moses_NPLAN_BMSG_memo.pdf (last visited October 22, 2013).

[12] Steve Stecklow, *On the Web, Children Face Intensive Tracking*, THE WALL STREET JOURNAL, September 17, 2010, http://online.wsj.com/article/SB10001424052748703904304575497903523187146.html (last visited September 16, 2013).

> Will tracking companies actually take steps to identify or deanonymize users? It's hard to tell, but there are hints that this is already happening: for example, many companies claim to be able to link online and offline activity, which is impossible without identity.[13]

61. Moreover, any company employing re-identification algorithms can precisely identify a particular consumer:

> It turns out there is a wide spectrum of human characteristics that enable re-identification: consumption preferences, commercial transactions, Web browsing, search histories, and so forth. Their two key properties are that (1) they are reasonably stable across time and contexts, and (2) the corresponding data attributes are sufficiently numerous and fine-grained that no two people are similar, except with a small probability.
>
> The versatility and power of re-identification algorithms imply that terms such as "personally identifiable" and "quasi-identifier" simply have no technical meaning. While some attributes may be uniquely identifying on their own, any attribute can be identifying in combination with others.[14]

62. The Federal Trade Commission has recognized the impossibility of keeping data derived from cookies and other tracking technologies anonymous, stating that industry, scholars, and privacy advocates have acknowledged that the traditional distinction between the two categories of data [personally identifiable information and anonymous information] has eroded and is losing its relevance.[15]

63. For example, in 2006, AOL released a list of 20 million web search queries connected to "anonymous" ID numbers, including one for user No. 4417749. Researchers were

---

[13] Arvind Narayanan, *There is No Such Thing as Anonymous Online Tracking*, The Center for Internet and Society Blog, July 28, 2011, http://cyberlaw.stanford.edu/blog/2011/07/there-no-such-thing-anonymous-online-tracking (last visited September 16, 2013).

[14] Arvind Narayanan, *Privacy and Security Myths of Fallacies of "Personally Identifiable Information*," Communications of the ACM, June 2010, http://www.cs.utexas.edu/users/shmat/shmat_cacm10.pdf (last visited September 16, 2013).

[15] FTC.gov, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report, December 2010, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (last visited September 16, 2013).

quickly able to identify specific persons with the so-called anonymous ID numbers. As explained by the New York Times:

> The number was assigned by the company to protect the searcher's anonymity, but it was not much of a shield.
> . . . .
> [T]he detailed records of searches conducted by Ms. Arnold and 657,000 other Americans, copies of which continue to circulate online, underscore how much people unintentionally reveal about themselves when they use search engines – and how risky it can be for companies like AOL, Google, and Yahoo to compile such data." [16]

64. Another technological innovation is the use of "browser fingerprinting," which allows websites to "gather and combine information about a consumer's web browser configuration – including the type of operating system used and installed browser plug-ins and fonts – to uniquely identify and track the consumer.[17]

65. Another recent innovation, as Prof. Narayanan predicted, is for companies to connect online dossiers with offline activity. As described by one industry insider:

> With every click of the mouse, every touch of the screen, and every add-to-cart, we are like Hansel and Gretel, leaving crumbs of information everywhere. With or without willingly knowing, we drop our places of residence, our relationship status, our circle of friends and even financial information. Ever wonder how sites like Amazon can suggest a new book you might like, or iTunes can match you up with an artist and even how Facebook can suggest a friend?
>
> Most tools use first-party cookies to identify users to the site on their initial and future visits based upon the settings for that particular solution. The information generated by the cookie is transmitted across the web and used to segment visitors' use of the website and to compile statistical reports on website activity. This leaves analytic vendors – companies like Adobe, Google, and IBM – *the ability to combine online with offline data*, creating detailed profiles and serving

[16] Michael Barbaro and Tom Zeller, Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. Times., Aug. 9, 2006, http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=print (last visited September 16, 2013).
[17] FTC.gov, *supra* note 15 at 36.

targeted ads based on users' behavior.[18]

66. On information and belief, the Defendants in this case are able to link online and offline activity and identify specific users, including the plaintiffs and children that form the putative class.

67. The Defendants, in fact, have marketed their ability to target individual users by connecting data obtained from first-party and third-party cookies.

68. Specifically, Defendant Viacom holds itself out to advertisers as being able to target users with "pinpoint accuracy" to reach "specific audiences on every digital platform" by "connecting the dots between first and third-party data to get at user attributes including interests, behaviors, demo, geolocation, and more."[19] Viacom does this through its "Surround Sound" service powered through Adobe's Audience Manager product. Viacom Vice President for Digital Products, Josh Cogswell, has said publicly the product can be used to target "kids" and, regarding Viacom's audience, "We know who you are across our sites."

69. Moreover, Defendant Google's website informs potential ad buyers that it can identify web users with Google's DoubleClick.net cookies:

> For itself, Google identifies users with cookies that belong to the doubleclick.net domain under which Google serves ads. For buyers, Google identifies users using a buyer-specific Google User ID which is an encrypted version of the doubleclick.net cookie, derived from but not equal to that cookie.[20]

---

[18] Tiffany Zimmerman, *Data Crumbs*, June 19, 2012, http://www.stratigent.com/community/analytics-insights-blog/data-crumbs (last visited September 16, 2013) (emphasis added).

[19] Viacom.com, Serving Advertisers in Surround Sound, March 26, 2012, http://blog.viacom.com/2012/03/serving-advertisers-in-surround-sound-2/ (last visited September 16, 2013) ("Kids" admission at 5:17 of video; "We know who you are across our sites," at 6:25 of video).

[20] Google.com, Google Developer Cookie Guide, https://developers.google.com/adexchange/rtb/cookie-guide (last visited September 16, 2013).

70. In addition, Defendant Google announced a new service in December 2012 called the DoubleClick Search API Conversion Service that will allow advertisers to integrate offline activity with online tracking.[21]

71. Viacom and Google use the individual information collected from the Plaintiffs to sell targeted advertising to them based on their individualized web usage and the content of the their web communications, including, but not limited to, videos requested and obtained.

E. Viacom and the Third Party Tracker Defendants: How Do They Track Children's Internet Use?

72. Immediately upon the Plaintiffs' first communication with the Viacom children's websites, Defendant Viacom automatically placed its own first party cookies on the computing devices of the Plaintiffs.

73. Additionally, immediately upon the Plaintiffs' first communication with the Viacom children's websites, Viacom knowingly permitted Defendant Google to place its own third-party cookies on the computing devices of the Plaintiffs, or alternatively, to access the information stored within those cookies if the cookies already existed on the user's device by virtue of Plaintiffs having visited another website affiliated with Google.

74. Viacom allowed Google to place and/or access cookies from its doubleclick.net domain.

75. Upon information and belief, Viacom also provided Google with access to the profile and other information contained within Viacom's first party cookies.

76. The placement and/or access of these cookies occurred before either the Plaintiffs or their legal guardians had the opportunity to consent to their placement and/or access to the

[21] Google.com, DS API Interface – Conversion Service Overview, https://support.google.com/ds/answer/2604604?hl=en (last visited September 16, 2013).

Plaintiffs' Internet communications.

77. Google's third-party cookies tracked, among other things, the URLs (Uniform Resource Locators) visited by the Plaintiffs, the Plaintiffs' respective IP addresses and each Plaintiff's browser setting, unique device identifier, operating system, screen resolution, browser version, detailed video viewing histories and the details of their Internet communications with Viacom's children's websites.

78. A URL is composed of several different parts.[22] For example, consider the following URL: http://www.nick.com/shows/penguins-of-madagascar/:

a. **http://**: This is the protocol identified by the web browser to the web server which sets the basic language of the interaction between browser and server. The back-slashes indicate that the browser is attempting to make contact with the server;

b. **www.nick.com**: This is the name that identifies the website and corresponding web server, with which the Internet user has initiated a communication;

c. **/shows/**: This part of the URL indicates a folder on the web server, a part of which the Internet user has requested;

d. **/penguins-of-madagascar/**: This is the name of the precise file requested; and

e. **/shows/penguins-of-madagascar/**: This combination of the folder and exact file name is called the "file path".

[22] Microsoft.com, URL Path Length Restrictions (Sharepoint Server 2010), Aug. 5, 2010, http://technet.microsoft.com/en-us/library/ff919564(v=office.14).aspx, (last visited October 21, 2013).

79. Graphically, the concept is illustrated as follows:

80. The URLs visited by plaintiffs and putative class members contain, among other things, substantive content. For instance, in the foregoing example the URL file path contains the substance, purport and meaning of the user's communication with Nick.com, namely, it identifies the exact title of the video the user has requested and received.

81. On its web sites, Viacom further disclosed to Google at least the following about each Plaintiff who was a registered user of Viacom's children's websites: (1) the child's username; (2) the child's gender; (3) the child's birthdate; (4) the child's IP address; (5) the child's browser settings; (6) the child's unique device identifier; (7) the child's operating system;

(8) the child's screen resolution; (9) the child's browser version; and (10) the child's web communications, including but not limited to detailed URL requests and video materials requested and obtained from Viacom's children's websites.

82. Google's third party cookies assigned to each Plaintiff a unique numeric or alphanumeric identifier that then became connected to (1) the child's username; (2) the child's gender; (3) the child's birthdate; (4) the child's IP address; (5) the child's browser setting; (6) the child's unique device identifier; (7) the child's operating system; (8) the child's screen resolution; (9) the child's browser version; and (10) the child's web communications, including but not limited to detailed URL requests and video materials requested and obtained from Viacom's children's websites.

83. Upon information and belief, with the information they obtain, Defendants Viacom and Google were able to identify specific individuals and connect online communications and data, including video viewing histories of the Plaintiffs, to offline communications and data.

84. Viacom and Google used the individual information collected from the Plaintiffs to sell targeted advertising to them based on their individualized web usage, including videos requested and obtained.

F. Viacom and the Third Party Tracking Defendants: What Did They Know About the Gender and Age of Viacom Users?

85. Upon arriving on the Viacom Children's websites, Viacom encouraged its users to register and establish profiles for those websites.

86. During the registration process, Viacom obtained the birthdate and gender of its users.

87. Viacom gave its users an internal code name based upon their answers to the

gender and birth date questions.

88. For instance, Viacom gave 6 year-old males the code name "Dil", and 12 year-old males the code name "Lou".

89. Viacom calls this coding mechanism the "rugrat" code.

90. When a child registered for an account, the child would also create a unique profile name that was tied to that child's profile page.

91. Viacom associated each profile name with a first party identification cookie that had its own unique numeric or alphanumeric identifier.

92. Viacom allowed Google to access each child's profile name.

93. Viacom also provided Google with the code name for the child's specific gender and age.

94. Google was then able to associate the child's age, gender, and other information with its own DoubleClick cookie's unique numeric or alphanumeric identifier so that each time the DoubleClick cookie was accessed, Google would know the specific child they were tracking.

G. How Did Defendants Viacom and Google Share the Video Viewing Histories of Minor Children?

95. The Viacom children's websites offer children the ability to view and/or interact with video materials.

96. When a child viewed a video, or played a video game on a Viacom site, an online record of the activity was made.

97. Viacom provided Google with the online records disclosing its users' video viewing activities.

98. For instance, the following video viewing activity of a Nick.com user was provided to Google and stored within Google's doubleclick.net domain cookies:

> http://ad.doubleclick.net/adi/nick.nol/atf_i_s/club/clubhouses/***penguins_of_madagascar*** [23] ;sec0=clbu;sec1=clubhouses;sec2=penguins_of_madagascar;cat=2;***rugrat=Dil*** [24] ;lcategory=pom_teaser;show=pom_teaser;gametype=clubhouses;demo=D;site=nick;lcategory=nick;u= ***. . . [the user's unique third party cookie alphanumeric identifier appears at the end of the string]***)

99. The online record Viacom provided to Google included the code name that specified the child's gender and age, which in the foregoing example is rugrat=Dil, denominating a male user, age 6.

100. Because Google also received an online record when a child logged in or visited his or her profile page, Google could use its unique numeric or alphanumeric identifier to associate the video materials watched by a specific child with the profile name and profile page of that specific child.

101. From this data, Google was able to compile a history of any particular child's video viewing activity.

102. At no point did Viacom or Google seek or receive the informed, written consent of any Plaintiff or their parent to disclose the video materials requested and obtained by the Plaintiffs from Viacom's children's websites to a third-party at the time such disclosure was sought and effectuated.

VI. CLASS ACTION ALLEGATIONS

103. This putative class action is brought pursuant to Federal Rule of Civil Procedure 23(b)(2) and 23(b)(3). The Plaintiffs bring this action on behalf of themselves and all similarly situated minor children under the age of 13 as representatives of a class and a subclass defined as follows:

[23] *Penguins of Madagascar* is the name of the video requested by this user.
[24] "Dil" is the code name Viacom gives to male users, age 6.

> **U.S. Resident Class**: All children under the age of 13 in the United States who visited the websites Nick.com, NickJr.com, and/or NeoPets.com, and had Internet cookies that tracked their Internet communications placed on their computing devices by Viacom and Google.
>
> **Video Subclass**: All children under the age of 13 in the United States who were registered users of Nick.com, NickJr.com, and/or NeoPets.com, who engaged with one or more video materials on such site(s), and who had their video viewing histories knowingly disclosed by Viacom to Google.

104. Each Plaintiff meets the requirements of both the U.S. Resident Class and Video Subclass.

105. The particular members of the proposed Class and Subclass are capable of being described without managerial or administrative difficulties. The members of the Class and Subclass are readily identifiable from the information and records in the possession or control of the Defendants.

106. The members of the Class and Subclass are so numerous that individual joinder of all members is impractical. This allegation is based upon information and belief that Defendants intercepted the video-viewing histories and Internet communications of millions of Nick.com, NickJr.com and NeoPets.com users.

107. There are questions of law and fact common to the Class and Subclass that predominate over any questions affecting only individual members of the Class or Subclass, and, in fact, the wrongs suffered and remedies sought by the Plaintiffs and other members of the Class and Subclass are premised upon an unlawful scheme participated in by each of the Defendants. The principal common issues include, but are not limited to, the following:

a. Whether Viacom constitutes a video tape service provider as defined in the Video Privacy Protection Act;

b. Whether the Plaintiffs constitute consumers as defined in the Video Privacy Protection Act;

c. The nature and extent to which video materials requested and obtained by Viacom website users were disclosed in violation of the Video Privacy Protection Act;

d. Whether the Defendants "intercepted" the electronic communications of members of the Class in violation of the Electronic Communications Privacy Act;

e. Whether the Defendants utilized "devices" to intercept the online communications of the class;

f. Whether the Defendants intercepted "content" as described in the Electronic Communications Privacy Act;

g. Whether the Defendants intercepted the online communications of the Plaintiffs for a criminal or tortious purpose;

h. Whether the actions taken by the Defendants violate the Stored Communications Act;

i. Whether the Defendants accessed a "facility" as described in the Stored Communications Act;

j. Whether the Defendants accessed a facility without authorization as described in the Stored Communications Act;

k. Whether the actions taken by the Defendants violate the California Invasion of Privacy Act;

l. Whether the actions taken by the Defendants violate the New Jersey Computer Related Offenses Act;

m. Whether or not Viacom should be enjoined from further disclosing information

about the video materials its minor children users watch on its sites, and whether Google should be enjoined from further accessing such information without the proper consent of Plaintiffs;

n. Whether or not the Defendants should be enjoined from further intercepting any electronic communications without the proper consent of the Plaintiffs;

o. Whether the Defendants intruded upon the Plaintiffs' seclusion;

p. Whether the Plaintiffs are entitled to recover profits gained at their expense by the Defendants under a claim for unjust enrichment;

q. The nature and extent of all statutory penalties or damages for which the Defendants are liable to the Class and Subclass members; and

r. Whether punitive damages are appropriate.

108. The common issues predominate over any individualized issues such that the putative class is sufficient cohesive to warrant adjudication by representation.

109. The Plaintiffs' claims are typical of those of the members of the Class and Subclass and are based on the same legal and factual theories.

110. Class treatment is superior in that the fairness and efficiency of class procedure in this action significantly outweighs any alternative methods of adjudication. In the absence of class treatment, duplicative evidence of Defendant's alleged violations would have to be provided in thousands of individual lawsuits. Moreover, class certification would further the policy underlying Rule 23 by aggregating class members possessing relatively small individual claims, thus overcoming the problem that small recoveries do not incentivize plaintiffs to sue individually.

111. The Plaintiffs, by and through their Next Friends, will fairly and adequately

represent and protect the interests of the members of the Class. The Plaintiffs have suffered injury in their own capacity from the practices complained of and are ready, willing, and able to serve as Class representatives. Moreover, Plaintiffs' counsel is experienced in handling class actions and actions involving unlawful commercial practices, including such unlawful practices on the Internet. Neither the Plaintiffs nor their counsel has any interest that might cause them not to vigorously pursue this action. The Plaintiffs' interests coincide with, and are not antagonistic to, those of the Class members they seek to represent.

112. Certification of a class under Federal Rule of Civil Procedure 23(b)(2) is appropriate because the Defendants have acted on grounds that apply generally to the Class such that final injunctive relief is appropriate respecting the Class and Subclass as a whole.

113. Certification of a class under Federal Rule of Civil Procedure 23(b)(3) is appropriate in that the Plaintiffs and the Class Members seek monetary damages, common questions predominate over any individual questions, and a plaintiff class action is superior for the fair and efficient adjudication of this controversy. A plaintiff class action will cause an orderly and expeditious administration of Class members' claims and economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured. Moreover, the individual members of the Class are likely to be unaware of their rights and not in a position (either financially or through experience) to commence individual litigation against these Defendants.

114. Alternatively, certification of a plaintiff class under Federal Rule of Civil Procedure 23(b)(1) is appropriate in that inconsistent or varying adjudications with respect to individual members of the Class would establish incompatible standards of conduct for the Defendants or adjudications with respect to individual members of the Class as a practical matter

would be dispositive of the interests of the other members not parties to the adjudication or would substantially impair or impede their ability to protect their interests.

COUNT I – VIOLATION OF THE VIDEO PRIVACY PROTECTION ACT

Children's Video Subclass v. All Defendants

115. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

116. Online video streaming is quickly replacing the traditional brick and mortar video rental store.

117. The Video Privacy Protection Act, 18 U.S.C. § 2710, (hereinafter "VPPA"), makes it illegal for a video tape service provider to knowingly disclose personally identifiable information concerning any consumer of such provider to a third-party without informed written consent by the consumer given at the time such disclosure is sought.

a. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials."

b. As defined in 18 U.S.C. § 2710(a)(3), "personally identifiable information" is that which "identifies a person as having requested or obtained specific video materials or services from a video tape service provider."

c. As defined in U.S.C. § 2710(a)(1) a "consumer" means "any renter, purchaser or subscriber of goods or services from a video tape service provider."

118. As specified in 18 U.S.C. § 2710(b)(2)(B) at the time this action was filed, valid consent under the VPPA is the "informed, written consent of the consumer given at the time the

disclosure is sought."[25]

119. The Video Privacy Protection Act of 1988 was passed for the explicit purpose of protecting the privacy of specific individuals' video requests and viewing histories.

120. At the time of its passage, Congress was well aware of the impact of ever-changing computer technology. Upon the VPPA's introduction, the late Senator Paul Simon noted:

> There is no denying that the computer age has revolutionized the world. Over the past 20 years we have seen remarkable changes in the way each of us goes about our lives. Our children learn through computers. We bank by machine. We watch movies in our living rooms. These technological innovations are exciting and as a nation we should be proud of the accomplishments we have made. Yet, as we continue to move ahead, we must protect time honored values that are so central to this society, particularly our right to privacy. *The advent of the computer means not only that we can be more efficient than ever before, but that we have the ability to be more intrusive than ever before.* Every day Americans are forced to provide to businesses and others personal information without having any control over where that information goes. These records are a window into our loves, likes, and dislikes.

S. Rep. No. 100-599 at 7-8 (1988) (emphasis added).

121. Senator Patrick Leahy also remarked at the time that new privacy protections were needed:

[25] After years of lobbying by online video service providers, Congress amended the "consent" portion of the VPPA. This action was brought under this previous definition of "consent." The new definition, also found in 18 U.S.C. § 2710 (b)(2)(B) provides that consent must be "informed, written consent (including through an electronic means using the Internet of the consumer that – (i) is in a form distinct and separate from an form setting forth other legal or financial obligations of the consumer; (ii) at the election of the consumer—(I) is given at the time the disclosure is sought; or (II) is given in advance for a set period of time, not to exceed 2 years or until consent is withdrawn by the consumer, whichever is sooner; and (iii) the video tape service provider has provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election."

> It is nobody's business what Oliver North or Robert Bork or Griffin Bell or Pat Leahy watch on television or read or think about when they are home . . . . In an era of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones, all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch, who are some of the people they telephone . . . . I think that is wrong. I think that really is Big Brother, and I think it is something that we have to guard against.

S. Rep. No. 100-599 at 5-6 (1988).

122. Sen. Leahy later explained:

> It really isn't anybody's business what books or what videos somebody gets. It doesn't make any difference if somebody is up for confirmation as a Supreme Court Justice or they are running the local grocery store. It is not your business. It is not anybody else's business, whether they want to watch Disney or they want to watch something of an entirely different nature. It really is not our business."[26]

123. The sponsor of Act, Rep. Al McCandless, also explained:

> There's a gut feeling that people ought to be able to read books and watch films without the whole world knowing. Books and films are the intellectual vitamins that fuel the growth of intellectual thought. The whole process of intellectual growth is one of privacy – of quiet, and reflection. This intimate process should be protected from the disruptive intrusion of a roving eye.

S. Rep. No. 100-599 at 7.

124. Online video service providers were well-aware of the restrictions imposed by the VPPA. For instance, in 2012, online video service provider Netflix lobbied for legislation to amend the Act to no longer require consent every time it sought to disclose a video requested or viewed by a customer.

[26] GPO.gov, House Report 112-312, December 2, 2011, http://www.gpo.gov/fdsys/pkg/CRPT-112hrpt312/html/CRPT-112hrp312.htm (last visited September 16, 2013.

125. As stated clearly in the legislative history to the VPPA amendments of 2012:

> Since 1988, Federal law has authorized video tape service providers to share customer information with the 'informed, written consent of the consumer at the time the disclosure is sought.' This consent must be obtained each time the provider wishes to disclose.

House Report 112-312 at 4. (2012).

126. Viacom is engaged in the business of the delivery of pre-recorded video cassette tapes or similar audio visual materials as defined by the VPPA in that:

a. The home page of Nick.com advertises it as the place to watch "2000+ FREE ONLINE VIDEOS and "play "1000+ FREE ONLINE GAMES." The homepage prominently features a rotating section enticing users to click and watch various videos with action buttons that say "Watch now," "Check it out," or, in the case of games, "Play Now." In addition, two of the first three links in the top bar on the homepage refer to audio-visual materials. *See* Nick.com (last visited September 24, 2013).

b. The home page of NickJr.com advertises it as the place to watch Dora the Explorer, Bubble Guppies, UmiZoomi, and dozens of other children's shows. It also provides users the ability to play online video games. Immediately upon visiting NickJr.com, the page loads videos that play in the upper right hand portion of the home-page.

c. The home page of NeoPets.com advertises it as the place to play dozens of video games, which are similar audio-visual materials.

127. Plaintiffs and members of the putative video sub-class are "consumers' under the VPPA in that they are registered users of the Viacom children's websites and, therefore, constitute subscribers to the video services Viacom provides on its websites.

128. Viacom violated the VPPA by knowingly disclosing to Google the Plaintiffs' personally identifiable information through the specific video materials and services requested and obtained from Viacom by the Plaintiffs without the Plaintiffs' written consent.

129. Google violated the VPPA by knowingly obtaining Plaintiffs' personally identifiable information in the form of the specific video materials and services requested and obtained by Plaintiffs from Viacom.

130. Defendant Google knowingly accepted the Plaintiffs' personally identifiable information regarding video materials and services through its use of the doubleclick.net cookies and other computer technologies.

131. On information and belief, Google further violated the VPPA by failing to destroy plaintiffs' personally identifiable information as provided in 18 U.S.C. § 2710 (e).

132. As a result of the above violations and pursuant to 18 U.S.C. § 2710, the Defendants are liable to the Plaintiffs and the Class for "liquidated damages of not less than $2,500 per plaintiff; reasonable attorney's fees and other litigation costs; injunctive and declaratory relief; and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendants in the future."

COUNT II – THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

U.S. Resident Children v. All Defendants

133. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

134. Enacted in 1986, the Electronic Communications Privacy Act ("ECPA") amended the Federal Wiretap Act by extending to data and electronic transmissions the same protection already afforded to oral and wire communications. The ECPA prohibits the unauthorized interception of the contents of electronic transmissions such as those made by Plaintiffs in this

case.

135. Representative Kastenmeier discussed the scope the ECPA amendments were designed to reach:

> . . . [L]egislation which protects electronic communications from interceptions…should be comprehensive, and *not limited to particular types or techniques of communicating* . . . . Any attempt to . . . protect only those technologies which exist in the marketplace today . . . is destined to be outmoded within a few years….what is being protected is *the sanctity and privacy of the communication.* We *should not attempt to discriminate for or against certain methods of communication* . . . .[27]

136. Moreover, Senator Leahy discussed the purpose of the ECPA:

> Today Americans have at their fingertips a broad array of telecommunications and computer technology, including . . . *computer-to-computer links* . . . . When title III was written 18 years ago, Congress could barely contemplate forms of telecommunications and computer technology we are starting to take for granted today . . . . Senate bill 2575 . . . is designed to . . . provide a reasonable level of Federal privacy protection to these new forms of communication.[28]

137. As described herein, Google intentionally intercepted the contents of electronic communications of minor children under the age of 13 who visited Nick.com, NickJr.com, and NeoPets.com through Google's use of devices that tracked and recorded the Plaintiffs' web communications, including but not limited to their Internet browsing histories and without consent.

138. Google's DoubleClick.net cookies tracked at least the following information regarding each individual Plaintiff: (1) unique IP address; (2) browser setting; (3) unique device identifier; (4) operating system; (5) screen resolution; (6) browser version; (7) and web

[27] 132 Cong. Rec. H4039-01 (1986) 1986 WL 776505 (comments from Rep. Kastenmeier) (emphasis added).
[28] 132 Cong. Rec. S14441-04 (1986) 1986 WL 786307 (comments from Sen. Leahy) (emphasis added).

communications, including but not limited to detailed and unique URL requests (which included video materials requested and obtained from Viacom's children's websites).

139. The specific Uniform Resource Locators the Plaintiffs typed into and sent through their web browsers are "contents" within the meaning of the ECPA because they include "any information concerning the substance, purport, or meaning of that communication" as defined in 18 U.S.C. § 2510 (8).

140. Specifically, URLs that expose the "file path" contain content under the ECPA. As an example, the URL http://www.nick.com/shows/penguins-of-madagascar/ is content because it contains "information concerning the substance, purport, or meaning of that communication," namely, it identifies the exact title of the video shown on the communication requested and received by the Internet user from Viacom.

141. If an individual called Blockbuster Video to request that Blockbuster mail the video "Penguins of Madagascar" to that individual, and if a third party intercepted the substance of that call, the third party would have intercepted "contents" because it would have received information concerning the substance, purport, or meaning of the individual's communication with Blockbuster, namely, the request for a specific video.

142. The only difference in this case is that the plaintiffs' communications with Viacom in requesting certain videos were executed with a keyboard. Google, thus, intercepted the "contents" of the plaintiffs' requests to Viacom for specific videos; and, as those requests contain the substance, purport and meaning of plaintiffs' communications with Viacom, namely, the request for a specific video, such information constitutes content as defined in the ECPA.

143. Congress also intended for URLs to constitute "content" under the ECPA. In modifying the Pen Register Act through the Patriot Act, the House Committee Report states:

> This section updates the language of the statute to clarify that the pen/register authority applies to modern communication technologies…Moreover, the section clarifies that orders for the installation of pen register and trap and trace devices may obtain any non-content information—"dialing, routing, addressing, and signaling information"—utilized in the process of transmitting of wire and electronic communications. Just as today, such an order could not be used to intercept the contents of communications protected by the wiretap statute. The amendments reinforce the statutorily prescribed line between a communication's contents and non-content information, a line identical to the constitutional distinction drawn by the U.S. Supreme Court in *Smith v. Maryland*, 442 U.S. 735, 741-43 (1979).
>
> Thus, for example, an order under the statute could not authorize the collection of email subject lines, which are clearly content. Further, an order could not be used to collect information other than "dialing, routing, addressing, and signaling" information, *such as the portion of a URL (Uniform Resource Locator) specifying Web search terms or the name of a requested file or article.*[29]

144. Google's tracking and interceptions began immediately upon the Plaintiffs' first communications with Defendant Viacom's children's websites and before any consent could be obtained from the Plaintiffs' and Class Members' guardians.

145. Google's cookies tracked and recorded the content of the web communications of the Plaintiffs and class members contemporaneous to, and, in some cases, before the Plaintiffs' communications with other websites were consummated such that the tracking and recording was contemporaneous with the Plaintiffs' communications and while the communications were in transit.

146. After Plaintiffs registered with the Viacom site, Google also accessed their individual username, gender, and birthdate.

147. Defendant Google's doubleclick.net "id", cookies:

[29] H.R. Rep. 107-236(I) at 53-54 (emphasis added).

a. Were placed on Plaintiffs' computing devices before each Plaintiff created an account or logged-in to the respective Viacom children's websites;

b. Remained on the Plaintiffs' computing devices even after individual users who were minor children under the age of 13 had created an account or logged-in and informed Viacom that they were minor children under the age of 13; and

c. Are capable of determining each individual user's response to Viacom's "birthdate" question in the form which was necessary to create a user account and collects information about the user's age via computer code.

148. The transmission of data between the Plaintiffs' computing devices and Viacom's children's websites and other non-Viacom websites hosted by servers are "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

149. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5).

a. Each individual cookie that Google used to track the Plaintiffs' communications;

b. The Plaintiffs' browsers which Google used to place and extract data from each Defendant's individual cookies;

c. The Plaintiffs' computing devices;

d. Each Defendant's web server; and/or

e. The plan Google carried out to effectuate its purpose of tracking the electronic communications of minor children.

150. The Plaintiffs, minor children under the age of 13, did not, and as a matter of law could not have, consented to the tracking of their web usage and communications.

151. The Plaintiffs' legal guardians did not consent to the tracking of Plaintiffs' web usage and communications.

152. Viacom, as a matter of law, could not have consented to the tracking of the web usage and communications of minor children under the age of 13 using their websites without the consent of their guardians.

153. The Defendants' actions were done for the tortious purpose of intruding upon the Plaintiffs' seclusion as set forth in this Complaint.

154. The Defendants' actions were done for criminal purposes in violation of numerous federal and state statutes, including, but not limited to 18 U.S.C. § 1030(a)(2)(C) of the Computer Fraud and Abuse Act.

155. Upon information and belief, in addition to intercepting the Plaintiffs' communications with the Viacom children's websites, Google used the cookies to track the Plaintiffs' communications with other websites on which Google places advertisements and related tracking cookies despite Google's knowledge that the Plaintiffs were minor children and without the consent of the Plaintiffs, their guardians, or the other websites with which the Plaintiffs were communicating.

156. Viacom procured Google to intercept the content of Plaintiffs' Internet communications with other websites.

157. Upon information and belief, Viacom profited from Google's unauthorized tracking of the Plaintiffs' Internet communications with other websites as such information assisted in the sale of targeted advertisements to children on the Viacom sites.

158. Viacom knew or had reason to know that Google intentionally intercepted the content of the Internet communications of the Plaintiffs on non-Viacom websites with tracking cookies deposited and/or accessed on Viacom's websites despite Google's knowledge that the

Plaintiffs were minor children and that it did not have either the Plaintiffs' or their guardians' consent to intercept their Internet communications.

159. As a direct and proximate cause of such unlawful conduct, the Defendants violated the ECPA in that they:

a. Intentionally intercepted or procured another person to intercept the contents of wire and/or electronic communications of the Plaintiffs;

b. Upon belief predicated upon further discovery, intentionally disclosed to another person the contents of Plaintiffs' wire or electronic communications, knowing or having reason to know that the information was obtained through the interception of wire or electronic communications in violation of 18 U.S.C. § 2511(1)(a); and

c. Upon belief predicated upon further discovery, intentionally used or endeavored to use the contents of Plaintiffs' wire or electronic communications, knowing or having reason to know that the information was obtained through the interception of wire or electronic communications in violation of 18 U.S.C. § 2511(1)(a).

160. As a result of the above violations, and pursuant to 18 U.S.C. § 2520, the Defendants are liable to the Plaintiffs and the Class in the sum of statutory damages consisting of the greater of $100 for each day each of the class members' data was wrongfully obtained or $10,000 per violation, whichever is greater; injunctive and declaratory relief; punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendants in the future, and reasonable attorney's fees and other litigation costs.

COUNT III – THE STORED COMMUNICATIONS ACT

U.S. Resident Children v. Google

161. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

162. The Stored Communications Act (hereinafter "SCA") provides a cause of action against any person who "intentionally accesses without authorization a facility through which an electronic communication service is provided," or any person "who intentionally exceeds an authorization to access that facility; and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage in such a system." 18 U.S.C. § 2701(a).

163. The SCA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof;" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

164. The SCA defines an "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

165. Defendants intentionally accessed without authorization or intentionally exceeded authorization to access facilities through which an electronic communications services was provided when they used the instrumentalities described in this Complaint to access the Plaintiffs' web-browsers and computing devices for purposes of tracking the Plaintiffs' Internet communications.

166. The web browsers utilized by the Plaintiffs on their computing devices provide electronic communications services to the Plaintiffs because they "provide to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

167. The Internet Service Providers to which the Plaintiffs use or subscribe to provide electronic communication services to the Plaintiffs because they "provide to users thereof the

ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

168. Neither the Plaintiffs' browsers nor the Internet Service Providers authorized the extent of the Defendants' access to the Plaintiffs' computing devices.

169. The Plaintiffs' respective web browsers store cookie and other information in browser-managed files on the Plaintiffs' computing devices. These browsers are also facilities under the SCA because they comprise the software necessary for and "through which (the) electronic communications service is provided."

170. Google intentionally accessed Plaintiffs' web browsers without authorization when Google accessed Plaintiffs' browsers immediately upon the Plaintiffs' visiting Viacom's children's websites and after sign-up without obtaining the consent of the Plaintiffs or their guardians.

171. The Plaintiffs' computing devices are facilities under the SCA because they comprise the hardware necessary for and "through which (the) electronic communications service is provided."

172. The cookies in the browser-managed files that Plaintiffs' web browsers store are updated regularly to record users' browsing activities and communications as they happen. For that reason, when Google accesses these facilities to acquire Plaintiffs' electronic communications, it acquires profile information and related just-transmitted electronic communications out of random access memory ("RAM"). Google acquires the profile information and related electronic communications out of electronic storage, incidental to the transmission thereof.

173. Upon information and belief, the acquisition of electronic communications from the Plaintiffs' web browsers and computing devices included the contents of communications the

Plaintiffs had with non-Viacom websites that are not affiliated with Google.

174. Plaintiffs and Class Members were harmed by Defendant's violations, and pursuant to 18 U.S.C. § 2707(c), are entitled to actual damages including profits earned by Defendants attributable to the violations or statutory minimum damages of $1,000 per person, punitive damages, costs, and reasonable attorney's fees.

COUNT IV – THE CALIFORNIA INVASION OF PRIVACY ACT

U.S. Resident Children v. All Defendants

175. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

176. California Penal Code § 631(a) provides, in pertinent part:

> Any person who . . . willfully and without the consent of *all* parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars . . . .

(emphasis added).

177. The Defendants' tracking, access, interception, and collection of the Plaintiffs' and Class Members' personal information and Internet communications, including web-browsing and video-viewing histories, was done without authorization or consent of either the Plaintiffs and Class Members or their guardians.

178. Google's corporate headquarters are located in California.

179. On information and belief, a substantial portion of the putative class and plaintiff L.G. reside in the State of California and accessed the Viacom Children's websites from

computing devices in the state of California.

180. Upon information and belief, Google directed and used the tracking, access, interception, and collection of the Plaintiffs' and Class Members' personal information and Internet communications in the state of California.

181. As a result of Google's actions in California, every act of tracking and every interception of the Plaintiffs' and Class Members' personal information and Internet communications took place, in part, in California, regardless of the location of each individual Plaintiff and Class Member.

182. Plaintiffs and Class Members did not consent to any of the third-party tracker Defendants' actions in intercepting and learning the contents of their communications with Viacom's children's websites and other websites.

183. Plaintiffs and Class Members, as a matter of law, could not have consented to Google's actions in intercepting and learning the contents of their communications with Viacom's children's websites and other websites.

184. Viacom aided, conspired with, and permitted Google to violate California Penal Code § 631(a) when Viacom permitted, acquiesced to, facilitated, and participated in the activity alleged herein by knowingly serving as the conduit through which Google placed its devices in positions to intercept the content of Plaintiffs' Internet communications. Viacom then profited from Google's interceptions through the sale of targeted advertisements to Plaintiffs on Viacom's children's websites.

185. Plaintiffs and Class Members have suffered loss by reason of these violations including, but not limited to, violation of their rights of privacy and loss of value in their Personally Identifiable Information.

186. Unless restrained and enjoined, the Defendants will continue to commit such acts.

187. Pursuant to Cal. Penal Code § 637.2, Plaintiffs and the Class Members have been injured by the violations of Cal. Penal Code § 631, and each seek damages for the greater of $5,000 or three times the amount of actual damages, whichever is greater, as well as injunctive relief.

COUNT V – NEW JERSEY COMPUTER RELATED OFFENSES ACT

U.S. Resident Children v. All Defendants

188. Plaintiffs incorporate all preceding paragraphs as if set forth herein.

189. N.J.S.A. 2A:38A-3 states that a person or enterprise is liable for:

a. The purposeful or knowing, and unauthorized altering, damaging, taking or destruction of any data, data base, computer program, computer software or computer equipment existing internally or externally to a computer, computer system or computer network;

b. The purposeful or knowing, and unauthorized altering, damaging, taking or destroying of a computer, computer system or computer network;

c. The purposeful or knowing, and unauthorized accessing or attempt to access any computer, computer system or computer network;

d. The purposeful or knowing, and unauthorized altering, accessing, tampering with, obtaining, intercepting, damaging or destroying of a financial instrument; or

e. The purposeful or knowing accessing and reckless altering, damaging, destroying or obtaining of any data, data base, computer, computer program, computer software, computer equipment, computer system or computer network.

190. Defendants did purposefully, knowingly and/or recklessly, without Plaintiffs',

Class Members' or their respective guardians' authorization, access, attempt to access, tamper with, alter, damage, take, destroy, obtain and/or intercept Plaintiffs' and Class Members' computer, computer software, data, database, computer program, computer system, computer equipment and/or computer network in violation of N.J.S.A. 2A:38A-1 et seq.

191. Many of the computers that were accessed, the terminal used in the accessing, and/or the actual damages took place in New Jersey.

192. Plaintiffs C.A.F., C.T.F., M.P. and T.P. all reside in the State of New Jersey and accessed the Viacom Children's sites from computing devices within the State of New Jersey.

193. Pursuant to N.J.S.A. 2A:38A-1 et seq., Plaintiffs and the Class Members have been injured by the violations of N.J.S.A. 2A:38A-1 et seq., and each seek damages for compensatory and punitive damages and the cost of the suit including a reasonable attorney's fee, costs of investigation and litigation, as well as injunctive relief.

COUNT VI – INTRUSION UPON SECLUSION

U.S. Resident Children v. All Defendants

194. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

195. In carrying out the scheme to track the Plaintiffs' Internet communications as described herein without the consent of the Plaintiffs or their legal guardians, the Defendants intentionally intruded upon the Plaintiffs' solitude or seclusion in that the Defendants took information from the privacy of the Plaintiffs' homes.

196. The Plaintiffs, minor children, did not, and by law could not, consent to the Defendants' intrusion.

197. The Defendants' intentional intrusion on the Plaintiffs' solitude or seclusion would be highly offensive to a reasonable person.

COUNT VII – UNJUST ENRICHMENT

U.S. Resident Children v. All Defendants

198. Plaintiffs incorporate all preceding paragraphs as if set forth herein.

199. Plaintiffs conferred a benefit on Defendants without Plaintiffs' consent or the consent of their parents or guardians, namely, access to wire or electronic communications and Plaintiffs' personal information over the Internet.

200. Upon information and belief, Defendants realized such benefits either through sales to third-parties or greater knowledge of its users' behavior without their consent.

201. Acceptance and retention of such benefit without Plaintiffs' consent is unjust and inequitable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

A. Certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure and appoint Plaintiffs as the representatives of the Class Members and their counsel as Class Counsel;

B. Award compensatory damages, including statutory damages where available, to Plaintiffs and the Class Members against Defendants for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

C. Award restitution to Plaintiffs and the Class Members against Defendants;

D. Award punitive damages in an amount that will deter Defendants and others from like conduct;

E. Permanently restrain Defendants, and their officers, agents, servants, employees, and attorneys, from tracking their users without consent or otherwise violating their policies with

users;

F. Award Plaintiffs and the Class Members their reasonable costs and expenses incurred in this action, including counsel fees and expert fees;

G. Order that Defendants delete the data they collected about users through the unlawful means described above; and

H. Grant Plaintiffs and the Class members such further relief as the Court deems appropriate.

JURY TRIAL DEMAND

Plaintiffs demand a trial by jury of all issues so triable.

Dated: October 23, 2013

Respectfully submitted,

EICHEN CRUTCHLOW ZASLOW & McELROY, LLP
Barry R. Eichen, Esq.
Evan J. Rosenberg, Esq.
40 Ethel Road
Edison, NJ 08817
Tel.: (732) 777-0100
Fax: (732) 248-8273
beichen@njadvocates.com
erosenberg@njadvocates.com

and

/s/ James P. Frickleton
BARTIMUS, FRICKLETON, ROBERTSON & GORNY P.C.
James P. Frickleton, Esq.
Edward D. Robertson III, Esq.
11150 Overbrook Road, Suite 200
Leawood, KS 66211
Tel: (913) 266 2300
Fax: (913) 266 2366
jimf@bflawfirm.com
krobertson@bflawfirm.com

Edward D. Robertson Jr. Esq.
Mary D. Winter Esq.
715 Swifts Highway
Jefferson City, MO 65109
Tel: (573) 659 4454
Fax: (573) 659 4460
chiprob@earthlink.net
marywinter@earthlink.net

Attorneys for Plaintiffs

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

IN RE NICKELODEON CONSUMER PRIVACY LITIGATION	**C.A. 12-7829 (SRC)(CLW)** **MDL No. 2443**
	Judge Stanley R. Chesler
This Document Relates to:	**SECOND CONSOLIDATED CLASS ACTION COMPLAINT**
All Actions	

I. INTRODUCTION AND OVERVIEW

1. This class action seeks damages and injunctive relief on behalf of all minor children under the age of 13 in the United States who visited Nick.com, a website owned by Defendant Viacom Inc., (hereinafter "Viacom") and which has a target audience of minor children.

2. Specifically, this case is about Defendant Viacom and Defendant Google Inc.'s (hereinafter "Google") misuse of Internet technologies ("cookies") to disclose, compile, store, and exploit the video viewing histories and Internet communications of children throughout the United States. With neither the knowledge nor the consent of their parents, the Defendants accessed, stored and utilized unique and specific electronic identifying information and content about each of these children for commercial purposes.

3. This case is brought to enforce the privacy rights of these children, and to enforce federal and state laws designed to uphold those rights.

II. NATURE OF THE ACTION

4. The named Plaintiffs are minor children under the age of 13 who were registered users of the website Nick.com.

5. The Defendants utilized Internet technologies commonly known as "cookies" to track and share the Plaintiffs' and putative class members' video-viewing histories and Internet communications on Nick.com without Plaintiffs' informed authorization or informed written consent.

6. The Defendants further utilized these technologies to track Plaintiffs' and the putative class members' Internet communications without plaintiffs' authorization or consent.

7. Plaintiffs are informed and believe the Defendants' conduct is systematic and class wide.

8. Based upon the Defendants' conduct plaintiffs assert the following statutory and common law causes-of-action:

a. Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710, et seq.;

b. Violation of the New Jersey Computer Related Offenses Act, N.J.S.A. 2A:38A-1, et seq.; and

c. Intrusion Upon Seclusion.

III. THE PARTIES

A. Plaintiffs

9. Plaintiffs C.A.F., C.T.F., M.P. and T.P. are minor children under the age of 13 who reside in the State of New Jersey. At all relevant times, they have been registered users of the website Nick.com.

10. Plaintiff T.M. is a minor child under the age of 13 who resides in the State of Illinois. At all relevant times, T.M. has been a registered user of the website Nick.com.

11. Plaintiff N.J. is a minor child under the age of 13 who resides in the State of Missouri. At all relevant times, N.J. has been a registered user of the website Nick.com.

12. Plaintiff A.V. is a minor child under the age of 13, who resides in the State of New York. At all relevant times, A.V. has been a registered user of the website Nick.com.

13. Plaintiff Johnny Doe is a minor child under the age of 13, who resides in the State of Texas. At all relevant times, he has been a registered user of the website Nick.com.

14. Plaintiff K.T. is a minor child under the age of 13, who resides in the state of Pennsylvania. At all relevant times, K.T. has been a registered user of the website Nick.com.

B. Defendant Viacom

15. Defendant Viacom, Inc. is a publicly-traded Delaware corporation with headquarters at 1515 Broadway, New York, New York 10036. Defendant Viacom does business throughout the United States and the world, deriving substantial revenue from interstate commerce within the United States.

16. Defendant Viacom publicly proclaims its Nickelodeon division to be "the number-one entertainment brand for kids."[1]

C. Defendant Google

17. Defendant Google, Inc. is a publicly traded Delaware corporation with headquarters at 1600 Amphitheatre Parkway, Mountain View, California 94043. Defendant Google does business throughout the United States and the world, deriving substantial revenue from interstate commerce within the United States.

[1] Viacom.com, Viacom Company Overview, http://www.viacom.com/brands/pages/nickelodeon.aspx (last visited October 7, 2013).

18. Google has, by design, become the global epicenter of Internet search and browsing activity. Former Google CEO and current company Executive Chairman Eric Schmidt described Google's privacy plan policy aptly in 2010. "Google's policy," Schmidt said, "is to get right up to the creepy line and not cross it." As detailed below, Google has a history of drawing a line on privacy – and then later crossing right over it.

IV. JURISDICTION AND VENUE

19. This Court has personal jurisdiction over Defendants because all Defendants have sufficient minimum contacts with this District in that they all operate businesses with worldwide reach, including but not limited to the State of New Jersey.

20. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §1331 because this action arises in part under federal statutes, namely 18 U.S.C. §2710, et seq. (the Video Privacy Protection Act). This Court further has subject matter jurisdiction pursuant to 28 U.S.C. §1332(d) (the Class Action Fairness Act) because the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and a member of the class is a citizen of a State different from any Defendant.

21. This Court has supplemental jurisdiction over the remaining state law claims pursuant to 28 U.S.C. §1367 because the state law claims form part of the same case or controversy under Article III of the United States Constitution.

22. Venue is proper in this District pursuant to 28 U.S.C. §1391 because a substantial amount of the conduct giving rise to this cause of action occurred in this District and because the United States Judicial Panel on Multidistrict Litigation transferred this case to this District for consolidated pretrial proceedings pursuant to Transfer Order in MDL No. 2443, entered on June 11, 2013.

V. FACTS COMMON TO ALL COUNTS

A. How Internet Users Access Websites

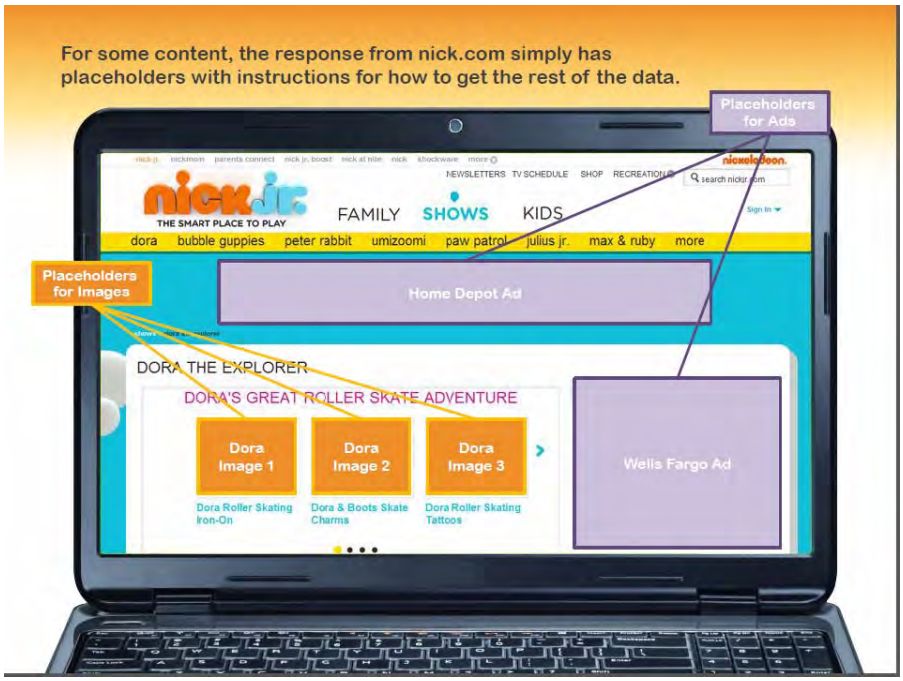
23. In order to access and communicate on the Internet, people employ web-browsers such as Apple Safari, Microsoft Internet Explorer, Google Chrome, and Mozilla Firefox.

24. Every website is hosted by a computer server, which communicates with an individual's web-browser to display the contents of webpages on the monitor or screen of their individual device.

25. The basic command web browsers use to communicate with website servers is called the "GET" command.

26. For instance, when a child types "www.nick.com" into the navigation bar of his or her web-browser and hits "Enter," the child's web browser sends a "GET" command to the Nick.com host server. The "GET" command instructs the Nick.com host server to send the information contained on Nick.com to the child's browser for display. Graphically, the concept is illustrated as follows:

27. Although a single webpage appears on the child's screen as a complete product, a single webpage is in reality an assembled collage of independent parts. Each different element of a webpage – *i.e.* the text, pictures, advertisements and sign-in box – often exist on distinct servers, which are sometimes operated by separate companies. To display each of these parts of the webpage as one complete product, the host server leaves part of its website blank.



28. Upon receiving a GET command from a child's web browser, the website host server contemporaneously instructs the child's web browser to send other GET commands to other servers responsible for filling in the blank parts of the web page.

29. Those other servers respond by sending information to fill in the blank portions of the webpage.

B. How Targeted Internet Advertising Works

30. In the Internet's formative years, advertising on websites followed the same model as traditional newspapers. Just as a sporting goods store would choose to advertise in the sports section of a traditional newspaper, advertisers on the early Internet paid for ads to be placed on specific web pages based on the type of content displayed on the web page.

31. Computer programmers eventually developed technologies commonly referred to as Internet "cookies," which are small text files that web servers can place on a person's computing device when that person's web browser interacts with the website host server.

32. Cookies can perform different functions; and some cookies were eventually designed to track and record an individual's activity on websites across the Internet.

33. In general, cookies are categorized by: (1) "time" – the length of time they remain on a user's device; and (2) "party" – describing the relationship (first or third party) between the Internet user and the party who places the cookie:

a. Cookie Classifications by *Time:*

i. "Session cookies" are placed on a person's computing device only for the time period during which the person is navigating the website that placed the cookie. The person's web browser normally deletes session cookies when he or she closes the browser; and

ii. "Persistent cookies" are designed to survive beyond a single Internet browsing session. The party creating the persistent cookie determines its lifespan. As a result, a "persistent cookie" can record a person's Internet browsing history and Internet communications for years. By virtue of their lifespan, persistent cookies can track a person's communications across the Internet. Persistent cookies are also sometimes called "tracking cookies."

b. Cookie Classifications by *Party*:

i. "First-party cookies" are set on a person's device by the website the person intends to visit. For example, Defendant Viacom sets a collection of Nick.com cookies when a child visits Nick.com. First-party cookies can be helpful to the user, server and/or website to assist with security, login and functionality; and

ii. "Third-party cookies" are set by website servers other than the server the person intends to visit. For example, the same child who visits Nick.com

will also have cookies placed on his or her device by third-party web servers, including advertising companies like Google. Unlike first-party cookies, third-party cookies are not typically helpful to the user. Instead, third-party cookies typically work in furtherance of data collection, behavioral profiling, and targeted advertising.

34. In addition to the information obtained by and stored within third-party cookies, third-party web servers can be granted access to profile and other data stored within first-party cookies.

35. Enterprising online marketers, such as Defendants, have developed ways to monetize and profit from these technologies. Specifically, third-party persistent "tracking" cookies are used to sell advertising that is customized based upon a particular person's prior Internet activity.

36. Website owners such as Viacom can now sell advertising space on their web pages to companies who desire to display ads to children that are customized based on a specific child's Internet history.

37. Moreover, many commercial websites with extensive advertising allow third-party companies such as Google to serve advertisements directly from third-party servers rather than through the first-party website's server.

38. Some websites contract with multiple third-parties to serve ads such that the website will contemporaneously instruct a user's browser to send multiple "GET" requests to multiple third-party websites.

39. To accomplish this, the host website leaves part of its webpage blank. Upon receiving a "GET" request from an individual's web browser, the website server will,

unbeknownst to that individual, immediately and contemporaneously re-direct the user's browser to send a "GET" request to the third-party company charged with serving the advertisement for that particular page.

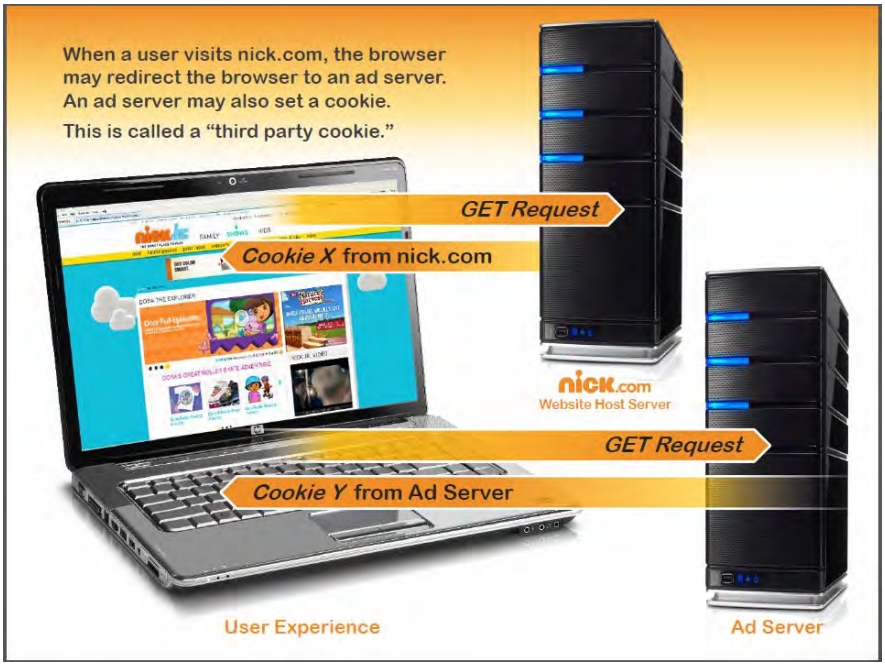
40. The transmission of such information is contemporaneous to the user's communication with the first-party website.

41. The third-party server then responds by sending the ad to the user's browser – which then displays it on the user's device.

42. In many cases, the third party receives the re-directed "GET" request and a copy of the user's request to the first-party website before the content of the initial request from the first-party webpage appears on the user's screen.

43. In the process of placing advertisements, third-party advertising companies also implant third-party cookies on individuals' computers. They further assign each specific user a unique numeric or alphanumeric identifier that is associated with that specific cookie.

44. The entire process occurs within milliseconds and the web page appears on the individual's web browser as one complete product, without the person ever knowing that multiple GET requests were executed by the browser at the direction of the web site server, and that first-party and third-party cookies were placed. Indeed, all the person has done is typed the name of a single web page into his or her browser. Graphically, the concept is illustrated as follows:



45. Because advertising companies serve advertisements on multiple sites, their cookies also allow them to monitor an individual's communications over every website and webpage on which the advertising company serves ads. And because that cookie is associated with a unique numeric or alphanumeric identifier, the data collected can be utilized to create detailed profiles on specific individuals. By observing the web activities and communications of tens of millions of Internet users, advertising companies, including Defendant Google, build digital dossiers of each individual user and tag each individual user with a unique identification number used to aggregate their web activity. This allows for the placement of "targeted" ads.

C. The Value of the Personal Information Defendants Collect

46. To the advertiser, targeted ads provided an unprecedented opportunity to reach potential consumers. The value of the information that Defendants take from people who use the Internet is well understood in the e-commerce industry. Personal information is now viewed as a form of currency. Professor Paul M. Schwartz noted in the Harvard Law Review:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and

> corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.[2]

47. Likewise, in the Wall Street Journal, privacy expert and fellow at the Open Society Institute, Christopher Soghoian, noted:

> The dirty secret of the Web is that the "free" content and services that consumers enjoy come with a hidden price: their own private data. Many of the major online advertising companies are not interested in the data that we knowingly and willingly share. Instead, these parasitic firms covertly track our web-browsing activities, search behavior and geolocation information. Once collected, this mountain of data is analyzed to build digital dossiers on millions of consumers, in some cases identifying us by name, gender, age as well as the medical conditions and political issues we have researched online.
>
> Although we now regularly trade our most private information for access to social-networking sites and free content, the terms of this exchange were never clearly communicated to consumers.[3]

48. In the behavioral advertising market, "the more information is known about a consumer, the more a company will pay to deliver a precisely-targeted advertisement to him."[4]

49. In general, behaviorally targeted advertisements based on a user's tracked internet activity sell for at least *twice* as much as non-targeted, run-of-network ads.[5]

50. Upon information and belief, most of the Defendants' advertising clients pay on a

---

[2] Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2056-57 (2004).

[3] Julia Angwin, *How Much Should People Worry About the Loss of Online Privacy?*, THE WALL STREET JOURNAL (Nov. 15, 2011).

[4] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change – A Proposed Framework for Business and Policymakers – Preliminary FTC Staff Report*, December 2010, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf at 37 (last visited October 22, 2013).

[5] NetworkAdvertising.org, *Study Finds Behaviorally-Targeted Ads More Than Twice As Valuable, Twice As Effective As Non-Targeted Online Ads*, http://www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf (last visited September 16, 2013).

cost-per-click basis.

51. The Defendants also offer cost-for-impression ads, which charge an advertising client each time the client's ad displays to a user.

52. In general, behaviorally-targeted advertisements produce 670 percent more clicks on ads per impression than run-of-network ads. Behaviorally-targeted ads are also more than twice as likely to convert users into buyers of an advertised product as compared to run-of-network ads.[6]

53. The cash value of users' personal information can be quantified. For example, in a recent study authored by Tim Morey, researchers studied the value that 180 Internet users placed on keeping personal data secure. Contact information was valued by the study participants at approximately $4.20 per year. Demographic information was valued at approximately $3.00 per year. Web browsing histories were valued at a much higher rate: $52.00 per year. The chart below summarizes the findings[7]:

[6] Howard Beales, *The Value of Behavioral Advertising*, 2010 http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf (last visited September 16, 2013).
[7] Tim Morey, *What's Your Personal Data Worth?*, January 18, 2011, http://designmind.frogdesign.com/blog/what039s-your-personal-data-worth.html (last visited September 16, 2013).

54. In 2012, Defendant Google convened a panel called "Google Screenwise Trends" through which Google paid Internet users to track their online communications through gift cards, with most valued at $5. Though it is unclear whether Google continues to operate Screenwise Trends in the United States,[8] the project remains active in the U.K., where users are paid £15 for staying with Screenwise Trends for 30 days after sign-up and an additional £5 for every 90 days users remain with the panel.[9] Google's Screenwise Trends program demonstrates conclusively that Internet industry participants, including the Defendants, recognize the enormous value in tracking users' Internet communications.

55. Targeting advertisements to children adds *more* value than targeting to adults because children are generally unable to distinguish between content and advertisements. This is especially true in the digital realm where children are less likely to identify and counteract the

[8] See Screenwisepanel.com, Sign-in Page, https://www.screenwisepanel.com/member/Index.aspx?ReturnUrl=%2fmember, (last visited Sept. 25, 2013) (plaintiffs believe this is the sign-in page for Screenwise Trend users in the United States, indicating the program is still in existence).

[9] See Screenwisetrendspanel.com, Rewards, https://www.screenwisetrendspanel.co.uk/nrg/rewards.php (last visited Sept. 25, 2013).

persuasive intent of advertising. This results in children, especially those below the age of 8, accepting advertising information contained in commercials "uncritically . . . [and as] truthful, accurate, and unbiased."[10]

56. An investigation by the Wall Street Journal revealed that "popular children's websites install more tracking technologies on personal computers than do the top websites aimed at adults."[11] In particular, Viacom disclosed substantially more information to third-party tracking companies on its children sites than typical adult websites. According to the investigation in September 2010, Viacom placed 92 tracking cookies on the Nick.com website, a total which is 144 percent more than the average number of tracking cookies placed on the 50 most popular adult websites in the United States.[12]

D. Internet Tracking is Not Anonymous

57. Though industry insiders claim publicly that tracking is anonymous, experts in the field disagree. For instance, in a widely cited blog post for The Center for Internet and Society at Stanford Law School titled "There is No Such Thing as Anonymous Online Tracking," Professor Arvind Narayanan explained:

---

[10] Report of the APA Task Force on Advertising and Children at 8 available at http://www.apa.org/pi/families/resources/advertising-children.pdf; see also, Louis J. Moses, *Research on Child Development: Implications for How Children Understand and Cope with Digital Marketing*, MEMO PREPARED FOR THE SECOND NPLAN/BMSG MEETING ON DIGITAL MEDIA AND MARKETING TO CHILDREN, June 29-30, 2009, http://digitalads.org/documents/Moses_NPLAN_BMSG_memo.pdf (last visited October 22, 2013).

[11] Steve Stecklow, *On the Web, Children Face Intensive Tracking*, THE WALL STREET JOURNAL, September 17, 2010, http://online.wsj.com/article/SB10001424052748703904304575497903523187146.html (last visited September 16, 2013).

[12] See http://blogs.wsj.com/wtk-kids/ for statistics on Nick.com and other children's sites (last visited July 30, 2014); see http://online.wsj.com/news/articles/SB10001424052748703940904575395073512989404 for tracking statistics on the most popular adult websites (last visited July 30, 2014).

> In the language of computer science, clickstreams – browsing histories that companies collect – are not anonymous at all; rather, they are pseudonymous. The latter term is not only more technically appropriate, it is much more reflective of the fact that at any point after the data has been collected, the tracking company might try to attach an identity to the pseudonym (unique ID) that your data is labeled with. Thus, identification of a user affects not only future tracking, but also retroactively affects the data that's already been collected. Identification needs to happen only once, ever, per user.
>
> Will tracking companies actually take steps to identify or deanonymize users? It's hard to tell, but there are hints that this is already happening: for example, many companies claim to be able to link online and offline activity, which is impossible without identity.[13]

58. Moreover, any company employing re-identification algorithms can precisely identify a particular consumer:

> It turns out there is a wide spectrum of human characteristics that enable re-identification: consumption preferences, commercial transactions, Web browsing, search histories, and so forth. Their two key properties are that (1) they are reasonably stable across time and contexts, and (2) the corresponding data attributes are sufficiently numerous and fine-grained that no two people are similar, except with a small probability.
>
> The versatility and power of re-identification algorithms imply that terms such as "personally identifiable" and "quasi-identifier" simply have no technical meaning. While some attributes may be uniquely identifying on their own, any attribute can be identifying in combination with others.[14]

59. The Federal Trade Commission has recognized the impossibility of keeping data derived from cookies and other tracking technologies anonymous, stating that industry, scholars, and privacy advocates have acknowledged that the traditional distinction between the two

[13] Arvind Narayanan, *There is No Such Thing as Anonymous Online Tracking*, The Center for Internet and Society Blog, July 28, 2011, http://cyberlaw.stanford.edu/blog/2011/07/there-no-such-thing-anonymous-online-tracking (last visited September 16, 2013).

[14] Arvind Narayanan, *Privacy and Security Myths of Fallacies of "Personally Identifiable Information*," Communications of the ACM, June 2010, http://www.cs.utexas.edu/users/shmat/shmat_cacm10.pdf (last visited September 16, 2013).

categories of data [personally identifiable information and anonymous information] has eroded and is losing its relevance.[15]

60. For example, in 2006, AOL released a list of 20 million web search queries connected to "anonymous" ID numbers, including one for user No. 4417749. Researchers were quickly able to identify specific persons with the so-called anonymous ID numbers. As explained by the New York Times:

> The number was assigned by the company to protect the searcher's anonymity, but it was not much of a shield.
> . . . .
> [T]he detailed records of searches conducted by Ms. Arnold and 657,000 other Americans, copies of which continue to circulate online, underscore how much people unintentionally reveal about themselves when they use search engines – and how risky it can be for companies like AOL, Google, and Yahoo to compile such data." [16]

61. Another technological innovation is the use of "browser fingerprinting," which allows websites to "gather and combine information about a consumer's web browser configuration – including the type of operating system used and installed browser plug-ins and fonts – to uniquely identify and track the consumer.[17]

62. By using browser-fingerprinting alone, the likelihood that two separate users have the same browser-fingerprint is one in 286,777 or 0.000003487 percent.[18] This accuracy is increased substantially where a tracking company also records a user's IP address and unique

---

[15] FTC.gov, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report, December 2010, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (last visited September 16, 2013).
[16] Michael Barbaro and Tom Zeller, Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. Times., Aug. 9, 2006, http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=print (last visited September 16, 2013).
[17] FTC.gov, *supra* note 15 at 36.
[18] *How Unique Is Your Web Browser?* by Peter Eckersley, available at https://panopticlick.eff.org/browser-uniqueness.pdf (last visited July 28, 2014).

device identifier.

63. Another recent innovation, as Prof. Narayanan predicted, is for companies to connect online dossiers with offline activity. As described by one industry insider:

> With every click of the mouse, every touch of the screen, and every add-to-cart, we are like Hansel and Gretel, leaving crumbs of information everywhere. With or without willingly knowing, we drop our places of residence, our relationship status, our circle of friends and even financial information. Ever wonder how sites like Amazon can suggest a new book you might like, or iTunes can match you up with an artist and even how Facebook can suggest a friend?
>
> Most tools use first-party cookies to identify users to the site on their initial and future visits based upon the settings for that particular solution. The information generated by the cookie is transmitted across the web and used to segment visitors' use of the website and to compile statistical reports on website activity. This leaves analytic vendors – companies like Adobe, Google, and IBM – *the ability to combine online with offline data*, creating detailed profiles and serving targeted ads based on users' behavior.[19]

64. On information and belief, the Defendants in this case are able to link online and offline activity and identify specific users, including the Plaintiffs and children that form the putative class. The Defendants, in fact, have marketed their ability to target individual users by connecting data obtained from first-party and third-party cookies.

a. Specifically, Defendant Viacom holds itself out to advertisers as being able to target users with "pinpoint accuracy" to reach "specific audiences on every digital platform" by "connecting the dots between first and third-party data to get at user attributes including interests, behaviors, demo, geolocation, and

[19] Tiffany Zimmerman, *Data Crumbs*, June 19, 2012, http://www.stratigent.com/community/analytics-insights-blog/data-crumbs (last visited September 16, 2013) (emphasis added).

more."[20] Viacom does this through its "Surround Sound" service powered through Adobe's Audience Manager product. Viacom Vice President for Digital Products, Josh Cogswell, has said publicly the product can be used to target "kids" and, regarding Viacom's audience, "We know who you are across our sites."

b. Defendant Google announced a new service in December 2012 called the DoubleClick Search API Conversion Service that will allow advertisers to integrate online activity with online tracking.[21]

E. Internet Service Provider and Web-Browser Privacy Policies Prohibit Unlawful and Non-Consensual Tracking of User Communications

65. Internet Service Providers (ISPs) provide connection services which allow consumers to send, and receive electronic communications on the Internet. ISPs operate under Privacy Policies that prohibit users from engaging in unlawful or non-consensual tracking of the communications of others or from utilizing the service to engage in criminal or otherwise unlawful acts. For example, major ISPs such as AT&T, Time Warner, Century Link, Verizon, and Charter all expressly prohibit unlawful acts. [22] Plaintiffs are not aware of any ISP in the United States which consents to the use of its service to engage in criminal or otherwise unlawful

[20] Viacom.com, Serving Advertisers in Surround Sound, March 26, 2012, http://blog.viacom.com/2012/03/serving-advertisers-in-surround-sound-2/ (last visited September 16, 2013) ("Kids" admission at 5:17 of video; "We know who you are across our sites," at 6:25 of video).

[21] Google.com, DS API Interface – Conversion Service Overview, https://support.google.com/ds/answer/2604604?hl=en (last visited September 16, 2013).

[22] See http://www.corp.att.com/aup/ (last visited July 28, 2014); http://help.twcable.com/twc_misp_aup.html (last visited July 28, 2014); http://www.centurylink.com/Pages/AboutUs/Legal/AcceptableUse/acceptableUsePolicy.jsp (last visited July 28, 2014); https://my.verizon.com/central/vzc.portal?_nfpb=true&_pageLabel=vzc_help_policies&id=AcceptableUse (last visited July 28, 2014); https://www.charter.com/browse/content/policies-comm-acceptable-use (last visited July 28, 2014)

acts.

66. Similarly, web-browsers are software services which allow consumers to send and receive electronic communications on the Internet. Like ISPs, web-browsing services include Terms of Use, which prohibit users from engaging in unlawful or unauthorized tracking of the communications of others or from utilizing the service to engage in criminal or otherwise unlawful acts. For example, major web-browsers such as Google Chrome, Microsoft Internet Explorer, and Apple Safari all expressly prohibit unlawful acts.[23] Plaintiffs are not aware of any major web-browser which consents to the use of its service to engage in criminal or otherwise unlawful acts.

F. How Viacom and Google Track Children's Internet Use

67. Immediately upon the Plaintiffs' first communication with Nick.com, Defendant Viacom automatically placed its own first-party cookies on the computing devices of the Plaintiffs.

68. Additionally, immediately upon the Plaintiffs' first communication with Nick.com, Viacom knowingly permitted Defendant Google to place its own third-party cookies on the computing devices of the Plaintiffs and then transmitted the Plaintiffs' subsequent communications to Google through those persistent tracking cookies and other information, or, in cases where Google's third-party cookies were already present on the Plaintiffs' computing devices, Viacom transmitted to Google the Plaintiffs' communications through the persistent tracking cookies which already existed on the user's device by virtue of Plaintiffs having visited another website affiliated with Google.

[23] See https://www.google.com/intl/en_US/chrome/browser/privacy/eula_text.html (last visited July 28, 2014); http://windows.microsoft.com/en-US/internet-explorer/products/ie-9/end-user-license-agreement (last visited July 28, 2014); and http://www.apple.com/legal/sla/docs/SafariWindows.pdf (last visited Sept. 10, 2014).

69. Viacom allowed Google to place and access cookies from its doubleclick.net domain.

70. Upon information and belief, Viacom also provided Google with access to the profile and other information contained within Viacom's first party cookies.

71. The placement and/or access of these cookies occurred before either the Plaintiffs or their legal guardians had the opportunity to consent to their placement and access to the Plaintiffs' Internet communications.

72. Google's third-party cookies tracked with a unique persistent cookie identifier, among other things, the URLs (Uniform Resource Locators) visited by the Plaintiffs, the Plaintiffs' respective IP addresses, browser settings, unique device identifiers, operating systems, screen resolutions, browser versions, detailed video viewing histories and the details of their Internet communications with Nick.com.

73. A URL is composed of several different parts.[24] For example, consider the following URL: http://www.nick.com/shows/penguins-of-madagascar/:

a. **http://**: This is the protocol identified by the web browser to the web server which sets the basic language of the interaction between browser and server. The back-slashes indicate that the browser is attempting to make contact with the server;

b. **www.nick.com**: This is the name that identifies the website and corresponding web server, with which the Internet user has initiated a communication;

[24] Microsoft.com, URL Path Length Restrictions (Sharepoint Server 2010), Aug. 5, 2010, http://technet.microsoft.com/en-us/library/ff919564(v=office.14).aspx, (last visited October 21, 2013).

c. **/shows/**: This part of the URL indicates a folder on the web server, a part of which the Internet user has requested;

d. **/penguins-of-madagascar/**: This is the name of the precise file requested; and

e. **/shows/penguins-of-madagascar/**: This combination of the folder and exact file name is called the "file path". Graphically, the concept is illustrated as follows:

74. The URLs visited by plaintiffs and putative class members contain substantive and often sensitive content. For example:

a. A Plaintiff minor child seeking information about "what to do if my parents are getting divorced" may enter that search term in the Google search engine.

b. The second result in Google's search engine is a hyperlink with the Subject Line: "How to Deal With Your Parents' Divorce: 12 Steps."

c. By clicking on the link and affirmatively indicating through the web-browser that they seek information on their parents' divorce, the browser would send a communication on the Plaintiffs' behalf to a webpage with the URL, http://www.wikihow.com/Deal-With-Your-Parents'-Divorce.

d. In response to the Plaintiffs' "GET" request communication seeking information on what to do if their parents get divorced, the website WikiHow.com returns a communication which includes an essay with 12 detailed steps a child could take if their parents were getting a divorce.

e. Google places cookies on WikiHow.com with the same unique identifiers as the cookies placed on the Viacom children's websites.

75. Similarly, for the URL, http://www.nick.com/videos/clip/digital-short-penguins-of-madagascar-shorts-skippers-nightmare.html, the URL file path contains the substance, purport and meaning of the user's communication with Nick.com, namely, it identifies the exact title of the video the user has requested and received: in particular an episode of the show Penguins of Madagascar titled "Skipper's Nightmare."

76. On Nick.com, Viacom further disclosed to Google at least the following about each Plaintiff who was a registered user of Nick.com: (1) the child's username/alias; (2) the child's gender; (3) the child's birthdate; (4) the child's IP address; (5) the child's browser settings; (6) the child's unique device identifier; (7) the child's operating system; (8) the child's screen resolution; (9) the child's browser version; (10) the child's web communications, including but not limited to detailed URL requests and video materials requested and obtained from Viacom's children's websites; and (11) the DoubleClick persistent cookie identifiers.

77. By disclosing the above information to Google, Viacom has knowingly disclosed

information which, without more, when disclosed to Google, links specific persons with their online communications and data, based on information that Google already has in its possession.

G. How Google Identifies Specific Individuals and Their Families

78. Defendant Google publicly admits that it can identify web users with Google's DoubleClick.net cookies:

> For itself, Google identifies users with cookies that belong to the doubleclick.net domain under which Google serves ads. For buyers, Google identifies users using a buyer-specific Google User ID which is an encrypted version of the doubleclick.net cookie, derived from but not equal to that cookie.[25]

79. Google has a ubiquitous presence on the Internet. In October 2012, DoubleClick cookies were present on 69 of the 100 most popular websites.[26] In July 2013, experts estimated Google accounted for 25 percent of all Internet traffic running through North American ISPs, an amount larger than the combined traffic of Facebook, Netflix, and Instagram.[27] In addition to DoubleClick, Google owns and operates:

a. The world's third most popular social network at plus.google.com,[28] for which Google claims to have over 300 million users;

b. The world's most popular search engine at Google.com, which, according to comScore, processed 12.1 billion searches in the United States in June 2014, or 68 percent of all U.S. Internet searches.[29]

---

[25] Google.com Google Developer Cookie Guide, https://developers.google.com/adexchange/rtb/cookie-guide (last visited September 16, 2013).
[26] See http://www.law.berkeley.edu/privacycensus.htm (last visited July 24, 2014).
[27] See http://www.wired.com/2013/07/google-internet-traffic/ (last visited July 29, 2014).
[28] According to Alexa, Facebook and LinkedIn have more users than Google Plus.
[29] See https://www.comscore.com/Insights/Market-Rankings/comScore-Releases-June-2014-US-Search-Engine-Rankings (last visited July 29, 2014).

c. The world's most popular email service at Gmail.com, which, as of June 2012, had more than 250 million users worldwide;[30]

d. The world's most popular video service at YouTube.com, which, according to comScore, had 153 million unique video viewers in June 2014;[31]

e. A mapping service called Google Maps at www.google.com/maps that includes applications which track the precise geo-locations of users, and which is according to some estimates, the most popular smartphone app in the world;

f. An online personal photography website called Picasa at picasa.google.com;

g. Its own electronic store called Play at play.google.com;

h. Its own web-browser called Google Chrome;

i. An online software suite called Google Apps that, as of June 2012, was used by 66 of the top 100 universities in the United States, government institutions in 45 states, and a total of 5 million businesses;[32] and

j. Android, its mobile phone platform is the most highly used platform in the United States and allows Google to track user movements, app usage, and phone calls.

80. Google collects users' IP addresses, unique device identifiers, and user account information through all of the services listed above. In addition, it tracks use of these services

[30] See http://googleblog.blogspot.com/2012/06/chrome-apps-google-io-your-web.html (last visited July 24, 2014).
[31] See http://ir.comscore.com/releasedetail.cfm?ReleaseID=860971 (last visited July 29, 2014).
[32] *Id.*

with persistent cookie identifiers. For example:

a. Google's social-network at Google Plus tracks users with cookies from DoubleClick with the same persistent identifier it uses to track at Nick.com. In addition to DoubleClick cookies, Google tracks its social network users with cookies from plus.google.com, clients6.google.com, and talkgadget.google.com.

b. Google's search engine tracks users with cookies from the main Google.com domain and from Google's social network at plus.google.com.

c. Google's email service at Gmail tracks users with cookies from mail.google.com and from Google's social network at plus.google.com.

d. Google's video service at YouTube.com tracks users with cookies from DoubleClick with the same persistent identifier that it uses to track each user at Nick.com. In addition to DoubleClick cookies, Google tracks YouTube users with cookies from its social network at plus.google.com, apis.google.com, gg.google.com, and clients6.google.com.

e. Google's map service tracks users with cookies from google.com and receives precise geo-location data from users utilizing its mapping services.

f. Google's electronic storage service called Drive tracks users with cookies from its social network at plus.google.com, and the subdomains drive.google.com and docs.google.com.

g. Google's electronic store Play tracks users with cookies from its social

networking site at plus.google.com.

81. Use of Gmail and the social network Google Plus requires registration, a process through which Google obtains a user's first and last name, hometown, email address, and other personal information about each user.

82. Other Google services collect users' first and last names, hometowns, email addresses, and other personal information when the user signs up as a member for those services.

83. Google admits that it connects persistent cookie identifiers, IP addresses, and unique device identifiers with user account information. Its current privacy policy states that:

a. It "may collect device-specific information (such as [a user's] hardware model, operating system version, unique device identifiers, and mobile network information including phone number)" and "may associate … device identifiers or phone number[s] with [a user's] Google Account."[33]

b. It may "automatically collect and store certain information in server logs. This may include: … search queries, … Internet protocol address, … device event information such as … hardware settings, browser type, browser language, the data and time of your request and referral URL," and "cookies that may uniquely identify your browser or your Google Account."[34]

84. Google's current Privacy Policy is substantially similar to the one in effect at the time the Plaintiffs' initially filed suit in this case regarding its collection of information. The policy in effect at the time Plaintiffs' filed suit provided as follows:

[33] See http://www.google.com/policies/privacy/ (last visited July 24, 2014).
[34] Id.

Device information
We may collect device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number). Google may associate your device identifiers or phone number with your Google Account.

Log information
When you use our services or view content provided by Google, we may automatically collect and store certain information in server logs. This may include:

- details of how you used our service, such as your search queries.
- telephone log information like your phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls.
- Internet protocol address.
- device event information such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL.
- cookies that may uniquely identify your browser or your Google Account.

Location information
When you use a location-enabled Google service, we may collect and process information about your actual location, like GPS signals sent by a mobile device. We may also use various technologies to determine location, such as sensor data from your device that may, for example, provide information on nearby Wi-Fi access points and cell towers.

Unique application numbers
Certain services include a unique application number. This number and information about your installation (for example, the operating system type and application version number) may be sent to Google when you install or uninstall that service or when that service periodically contacts our servers, such as for automatic updates.

Local storage
We may collect and store information (including personal information) locally on your device using mechanisms such as browser web storage (including HTML 5) and application data caches.

Cookies and anonymous identifiers
We use various technologies to collect and store information when you visit a Google service, and this may include sending one or more cookies or anonymous identifiers to your device. We also use cookies and anonymous identifiers when you interact with services we offer to our partners, such as advertising services or Google features that may appear on other sites.

85. Google's Privacy Policy in effect today differs in one key respect from the Policy

in effect at the time Plaintiff's filed suit in this case. Google's current Privacy Policy acknowledges that it has the information to connect DoubleClick cookie information with personal information collected from its other services, but promises not to. Google informs users:

> We may combine personal information from one service with information, including personal information, from other Google services – for example, to make it easier to share things with people you know. We will not combine DoubleClick cookie information with personally identifiable information unless we have your opt-in consent.

86. Google's Privacy Policy promise not to combine DoubleClick cookie information with personally identifiable information was not in place until March 1, 2012.[35] Because Plaintiffs filed suit in December 2012, Viacom's disclosures to Google were made for a significant period of time without any public commitment by Google that it would not use the information disclosed by Viacom.

87. On March 1, 2012, Google publicly announced that it would be commingling information obtained from Google users across Google accounts. In a company blog post by Alma Whitten, Google's Direct of Privacy, Product, and Engineering, the company announced:

> Our new Privacy Policy makes clear that, if you're signed in, we may combine information you've provided from one service with information from other services. In short, we'll treat you as a single user across all our products[.][36]

88. In addition to these websites and services listed above, Google advertises a "cookie matching" service for ad-buyers that permits buyers to match their own cookie with a DoubleClick persistent cookie identifier assigned to a user by Google.

89. Defendant Google admits that IP addresses and cookie information are not

[35] The changes to Google's Privacy Policy as of March 1, 2012 are highlighted here: http://www.google.com/policies/privacy/archive/20111020-20120301/ (last visited July 24, 2014).

[36] See http://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html. (last visited July 25, 2014).

anonymous to Google. In fact, Google promises users it will scrub full IP addresses and cookie information from its records after 9 or 18 months in order to "anonymize" user data:

> Like most websites, our servers automatically record the page requests made when users visit our sites. These server logs typically include your web request, IP address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser. We store this data for a number of reasons, the most important of which are to improve our services and to maintain the security of our systems. *We anonymize this log data by removing part of the IP address (after 9 months) and cookie information (after 18 months).* If you have Search History enabled, this data may also be stored in your Google Account until you delete the record of your search. *Emphasis added.*

90. Google has further admitted that IP addresses are personal information where the IP address is capable of being tied to an individual by a company. On Google's Public Policy blog in 2008, then Google software engineer Alma Whitten explained:

> [I]s an IP address personal data, or, in other words, can you figure out who someone is from an IP address? A black-and-white declaration that all IP addresses are always personal data incorrectly suggests that every IP address can be associated with a specific individual. In some contexts this is more true: if you're an ISP and you assign an IP address to a computer that connects under a particular subscriber's account, and you know the name and address of the person who holds that account, then that IP address is more like personal data, even though multiple people could still be using it. On the other hand, the IP addresses recorded by every website on the planet without additional information should not be considered personal data, because these websites usually cannot identify the human beings behind these number strings.[37]

91. Google has more information about Internet users than the ISPs identified by Whitten. Each separate Google product logs and keeps track of different categories of information about Internet users, including, but not limited to the following list:

a. first and last names,

b. home or other physical address,

c. precise current locations of users through GPS,

[37] See http://googlepublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html (last visited July 24, 2014).

d. IP addresses,

e. telephone numbers,

f. lists of contacts,

g. the content of Gmail users' Gmail messages,

h. search history at Google.com and YouTube,

i. web-surfing history,

j. Android device activity, and

k. all activity on Google's social network called Google Plus.

92. In the case of Nick.com, Google occupies the role of the ISP because it knows its users' full names, hometowns, specific geographic locations, email addresses, and more.

93. Viacom is aware of Google's ubiquitous presence on the Internet and its tracking of users across DoubleClick partner websites like Nick.com and Google's own websites at Google.com, Google Plus, YouTube.com, Gmail.com, and Play.Google.com, among others, where Google connects user IP addresses, unique device identifiers, and persistent cookie identifiers to Google account information.

94. As a result of Google's ubiquitous presence on the Internet, the information Viacom discloses to Google personally identifies the plaintiffs.

H. Google's Internal Position on Privacy.

95. Despite Google's promise not to connect DoubleClick information with Google Account information, Google reserves the right to change its Privacy Policy "from time to time" and has a history of exercising this provision. For example, its March 2012 announcement that it would commingle user information across Google accounts broke promises it had previously made with respect to Android, Google search, and Gmail.

96. Prior to March 2012, Google did not give any public indications that it was in the process of changing company policy to commingle all user data across its Search, Gmail, YouTube, Maps, Docs, Picasa, Play, Android, and other services. But this shift to share information across all Google platforms actually began at least as early as May 2010, when Google executives decided to engage in a plan it called "Emerald Sea" which involved eliminating then existing barriers between Google properties.

97. "Emerald Sea" was driven in large part by the Google's desire to better compete with Facebook to create detailed digital dossiers of its users.

98. James Whittaker, a former Google Engineering Director, described Google's motivation in a public explanation of his resignation from the company:

> It turns out that there was one place where the Google innovation machine faltered and that one place mattered a lot: competing with Facebook. … Like the proverbial hare confident enough in its lead to risk a brief nap, Google awoke from its social dreaming to find its front runner status in ads threatened. … Google could still put ads in front of more people than Facebook, but Facebook knows so much more about those people.
>
> Advertisers and publishers cherish this kind of personal information, so much so that they are willing to put the Facebook brand before their own. Exhibit A: www.facebook.com/nike, a company with the power and clout of Nike putting their own brand after Facebook's? No company has ever done that for Google and Google took it personally.

99. Unlike Facebook, prior to the commingling of information and creation of Google Plus, Google could not create nearly as total a picture of its users for advertisers.

I. Viacom Disclaims Any Control Over Use of Information It Discloses to Google

100. In its own Privacy Policy for Nickelodeon websites that Viacom filed as Exhibit D in response to Plaintiff's' First Consolidated Complaint (and which is not valid for the minor children plaintiffs in this case or for purposes of the VPPA), Viacom disavows any control over Google's practices, stating that "the use of [tracking] technology by these third parties is within

their control and not the Nickelodeon sites. Even if we have a relationship with a third party, we do not control those sites or their policies and practices regarding your information[.]"

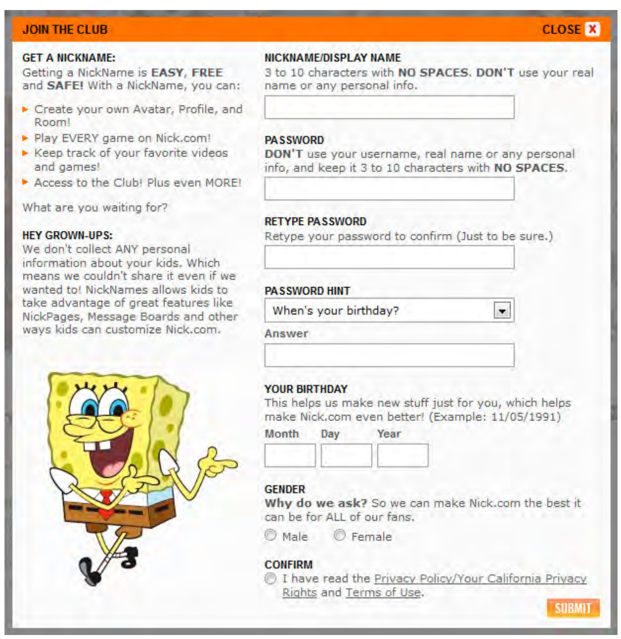
J. Viacom's Disclosures to Google are Not Necessary for Nick.com

101. Google's DoubleClick cookies are not necessary for Viacom to render any services on Nick.com. On or about August 1, 2014, Viacom revamped its Nick.com website. As of August 7, 2014, based on Plaintiffs' investigation, Defendant Viacom no longer discloses the particular video viewing or game histories of individual users of Nick.com to Google.

K. What Viacom and Google Knew About the Age and Gender of Viacom Users

102. Upon arriving at Nick.com, Viacom encouraged its users to register and establish profiles for those websites.

103. During the registration process, Viacom obtained the birthdate[38] and gender of its users, through the following sign-up form:


JOIN THE CLUB
CLOSE X
GET A NICKNAME:
Getting a NickName is **EASY**, **FREE** and **SAFE!** With a NickName, you can:
- Create your own Avatar, Profile, and Room!
- Play EVERY game on Nick.com!
- Keep track of your favorite videos and games!
- Access to the Club! Plus even MORE!

What are you waiting for?

HEY GROWN-UPS:
We don't collect ANY personal information about your kids. Which means we couldn't share it even if we wanted to! NickNames allows kids to take advantage of great features like NickPages, Message Boards and other ways kids can customize Nick.com.

NICKNAME/DISPLAY NAME
3 to 10 characters with **NO SPACES. DON'T** use your real name or any personal info.

PASSWORD
DON'T use your username, real name or any personal info, and keep it 3 to 10 characters with **NO SPACES.**

RETYPE PASSWORD
Retype your password to confirm (Just to be sure.)

PASSWORD HINT
When's your birthday?
Answer

YOUR BIRTHDAY
This helps us make new stuff just for you, which helps make Nick.com even better! (Example: 11/05/1991)
Month Day Year

GENDER
Why do we ask? So we can make Nick.com the best it can be for ALL of our fans.
Male Female

CONFIRM
I have read the Privacy Policy/Your California Privacy Rights and Terms of Use.
SUBMIT

[38] Plaintiffs note that this accurate sign-up form differs from the purported sign-up form Viacom offered as an Exhibit A attached to their previous Motion to Dismiss, which was not an accurate depiction of the sign-up process at the time the plaintiffs' filed suit. This version requires an exact birthdate for a child to create an account.

104. Viacom gave its users an internal code name based upon their answers to the gender and birth date questions. For instance, Viacom gave 6 year-old males the code name "Dil", and 12 year-old males the code name "Lou". Viacom calls this coding mechanism the "rugrat" code. When a child registered for an account, the child would also create a unique profile name that was tied to that child's profile page.

105. Viacom associated each profile name with a first-party identification cookie that had its own unique numeric or alphanumeric identifier.

106. Viacom disclosed to Google each child's profile name and the code name for the child's specific gender and age.

107. Through these disclosures and the disclosure of the persistent cookie identifiers of the DoubleClick.net cookies, and the Plaintiffs' IP address, browser settings, and other information explained above, Viacom knowingly disclosed to Google information which, without more, when disclosed to Google, itself links the actual plaintiffs to specific video materials for Defendant Google based on information Google already has in its control.

G. How Viacom Disclosed the Plaintiff Minor Children's Video Viewing Histories

108. The Viacom children's websites offer children the ability to view and interact with video materials.

109. When a child viewed a video, or played a video game on a Viacom site, an online record of the activity was made.

110. Viacom provided Google with the online records disclosing its users' video viewing activities.

111. For instance, the following video viewing activity of a Nick.com user would be provided to Google and stored within Google's doubleclick.net domain cookies:

http://ad.doubleclick.net/adi/nick.nol/atf_i_s/club/clubhouses/***penguins_of_madagascar_shorts_skippers_nightmare***[39];sec0=clbu;sec1=clubhouses;sec2=penguins_of_madagascar;cat=2;***rugrat=Dil***[40];lcategory=pom_teaser;show=pom_teaser;gametype=clubhouses;demo=D;site=nick;lcategory=nick;u= **. . .** ***[the user's unique third party cookie alphanumeric identifier appears at the end of the string])***

112. The online record Viacom provided to Google included the code name that specified the child's gender and age, which in the foregoing example is rugrat=Dil, denominating a male user, age 6. Viacom also disclosed each individual plaintiff's username to Google that was input when a child logged-in or visited his or her profile page, a process through which Google could use its unique numeric or alphanumeric identifier to associate the video materials watched by a specific child with the profile name and profile page of that specific child.

113. From this data, Google was able to compile a history of any particular child's video viewing activity.

114. At no point did Viacom or Google seek or receive the informed, written consent of any Plaintiff or their parent to disclose the video materials requested and obtained by the Plaintiffs from Viacom's children's websites to a third-party at the time such disclosure was sought and effectuated.

VI. CLASS ACTION ALLEGATIONS

115. This putative class action is brought pursuant to Federal Rule of Civil Procedure 23(b)(2) and 23(b)(3). The Plaintiffs bring this action on behalf of themselves and all similarly situated minor children under the age of 13 as representatives of a class and a subclass defined as follows:

> **U.S. Resident Class**: All children under the age of 13 in the United States who visited the website Nick.com and had Internet cookies that

[39] *Penguins of Madagascar: Skipper's Nightmare* is the name of the video requested by this user.
[40] "Dil" is the code name Viacom gives to male users, age 6.

tracked their Internet communications placed on their computing devices by Viacom and Google.

Video Subclass: All children under the age of 13 in the United States who were registered users of Nick.com and who engaged with one or more video materials on such site, and who had their video viewing histories knowingly disclosed by Viacom to Google.

116. Each Plaintiff meets the requirements of both the U.S. Resident Class and Video Subclass.

117. The particular members of the proposed Class and Subclass are capable of being described without managerial or administrative difficulties. The members of the Class and Subclass are readily identifiable from the information and records in the possession or control of the Defendants.

118. The members of the Class and Subclass are so numerous that individual joinder of all members is impractical. This allegation is based upon information and belief that Defendants intercepted the video-viewing histories and Internet communications of millions of Nick.com users.

119. There are questions of law and fact common to the Class and Subclass that predominate over any questions affecting only individual members of the Class or Subclass, and, in fact, the wrongs suffered and remedies sought by the Plaintiffs and other members of the Class and Subclass are premised upon an unlawful scheme participated in by each of the Defendants. The principal common issues include, but are not limited to, the following:

a. Whether Viacom constitutes a video tape service provider as defined in the Video Privacy Protection Act;

b. Whether the Plaintiffs constitute consumers as defined in the Video Privacy Protection Act;

c. The nature and extent to which video materials requested and obtained by Viacom website users were disclosed in violation of the Video Privacy Protection Act;

d. Whether the actions taken by the Defendants violate the New Jersey Computer Related Offenses Act;

e. Whether or not Viacom should be enjoined from further disclosing information about the video materials its minor children users watch on its sites; Whether the Defendants intruded upon the Plaintiffs' seclusion;

f. The nature and extent of all statutory penalties or damages for which the Defendants are liable to the Class and Subclass members; and

g. Whether punitive damages are appropriate.

120. The common issues predominate over any individualized issues such that the putative class is sufficiently cohesive to warrant adjudication by representation.

121. The Plaintiffs' claims are typical of those of the members of the Class and Subclass and are based on the same legal and factual theories.

122. Class treatment is superior in that the fairness and efficiency of class procedure in this action significantly outweighs any alternative methods of adjudication. In the absence of class treatment, duplicative evidence of Defendants' alleged violations would have to be provided in thousands of individual lawsuits. Moreover, class certification would further the policy underlying Rule 23 by aggregating class members possessing relatively small individual claims, thus overcoming the problem that small recoveries do not incentivize plaintiffs to sue individually.

123. The Plaintiffs, by and through their Next Friends, will fairly and adequately represent and protect the interests of the members of the Class. The Plaintiffs have suffered

injury in their own capacity from the practices complained of and are ready, willing, and able to serve as Class representatives. Moreover, Plaintiffs' counsel is experienced in handling class actions and actions involving unlawful commercial practices, including such unlawful practices on the Internet. Neither the Plaintiffs nor their counsel has any interest that might cause them not to vigorously pursue this action. The Plaintiffs' interests coincide with, and are not antagonistic to, those of the Class members they seek to represent.

124. Certification of a class under Federal Rule of Civil Procedure 23(b)(2) is appropriate because the Defendants have acted on grounds that apply generally to the Class such that final injunctive relief is appropriate respecting the Class and Subclass as a whole.

125. Certification of a class under Federal Rule of Civil Procedure 23(b)(3) is appropriate in that the Plaintiffs and the Class Members seek monetary damages, common questions predominate over any individual questions, and a plaintiff class action is superior for the fair and efficient adjudication of this controversy. A plaintiff class action will cause an orderly and expeditious administration of Class members' claims and economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured. Moreover, the individual members of the Class are likely to be unaware of their rights and not in a position (either financially or through experience) to commence individual litigation against these Defendants.

126. Alternatively, certification of a plaintiff class under Federal Rule of Civil Procedure 23(b)(1) is appropriate in that inconsistent or varying adjudications with respect to individual members of the Class would establish incompatible standards of conduct for the Defendants or adjudications with respect to individual members of the Class as a practical matter would be dispositive of the interests of the other members not parties to the adjudication or

would substantially impair or impede their ability to protect their interests.

COUNT I – VIOLATION OF THE VIDEO PRIVACY PROTECTION ACT

Children's Video Subclass v. All Defendants

127. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

128. The Video Privacy Protection Act, 18 U.S.C. § 2710, (hereinafter "VPPA") prohibits a video tape service provider from knowingly disclosing personally identifiable information concerning any consumer of such provider to a third-party without the informed written consent of the consumer given at the time such disclosure is sought.

a. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials."

b. As defined in 18 U.S.C. § 2710(a)(3), "personally identifiable information" is open-ended and "includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider."

c. As defined in U.S.C. § 2710(a)(1) a "consumer" means "any renter, purchaser or subscriber of goods or services from a video tape service provider."

d. There is no exception in the VPPA for disclosures to a third party which publicly promises not to use personally identifiable information.

e. As specified in 18 U.S.C. § 2710(b)(2)(B) at the time this action was filed, valid consent under the VPPA is the "informed, written consent of the

consumer at the time the disclosure is sought." [41]

129. As amended in December 2012, the VPPA creates an opt-out right for consumers. It requires VTSPs that disclose personally identifiable information with the "informed, written consent" of the consumer to also "provide[] an opportunity for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election." 18 U.S.C. § 2710(2)(B)(iii).

130. The Video Privacy Protection Act of 1988 was passed for the explicit purpose of protecting the privacy of individuals' and their families' video requests and viewing histories. As explained in the Senate report for the Act, "The impetus for this legislation occurred when a weekly newspaper in Washington published a profile of Robert H. Bork based on the titles of 146 files ***his family had rented*** from a video store." S.Rep. 100-599 at 6 (1988).

131. At the time of its passage, Congress was well aware of the impact of ever-changing computer technology. Upon the VPPA's introduction, the late Senator Paul Simon noted:

> There is no denying that the computer age has revolutionized the world. Over the past 20 years we have seen remarkable changes in the way each of us goes about our lives. Our children learn through computers. We bank by machine. We watch movies in our living rooms. These technological innovations are exciting and as a nation we should be proud of the accomplishments we have made. Yet, as we continue to

[41] After years of lobbying by online video service providers, Congress amended the "consent" portion of the VPPA. This action was brought under this previous definition of "consent." The new definition, also found in 18 U.S.C. § 2710 (b)(2)(B) provides that consent must be "informed, written consent (including through an electronic means using the Internet of the consumer that – (i) is in a form distinct and separate from an form setting forth other legal or financial obligations of the consumer; (ii) at the election of the consumer—(I) is given at the time the disclosure is sought; or (II) is given in advance for a set period of time, not to exceed 2 years or until consent is withdrawn by the consumer, whichever is sooner; and (iii) the video tape service provider has provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election."

> move ahead, we must protect time honored values that are so central to this society, particularly our right to privacy. *The advent of the computer means not only that we can be more efficient than ever before, but that we have the ability to be more intrusive than ever before.* Every day Americans are forced to provide to businesses and others personal information without having any control over where that information goes. These records are a window into our loves, likes, and dislikes.

S. Rep. No. 100-599 at 7-8 (1988) (emphasis added).

132. Senator Patrick Leahy also remarked at the time that new privacy protections were needed:

> It is nobody's business what Oliver North or Robert Bork or Griffin Bell or Pat Leahy watch on television or read or think about when they are home . . . . In an era of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones, all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch, who are some of the people they telephone . . . . I think that is wrong. I think that really is Big Brother, and I think it is something that we have to guard against.

S. Rep. No. 100-599 at 5-6 (1988).

133. Sen. Leahy later explained:

> It really isn't anybody's business what books or what videos somebody gets. It doesn't make any difference if somebody is up for confirmation as a Supreme Court Justice or they are running the local grocery store. It is not your business. It is not anybody else's business, whether they want to watch Disney or they want to watch something of an entirely different nature. It really is not our business."[42]

134. The sponsor of the Act, Rep. Al McCandless, also explained:

[42] GPO.gov, House Report 112-312, December 2, 2011, http://www.gpo.gov/fdsys/pkg/CRPT-112hrpt312/html/CRPT-112hrp312.htm (last visited September 16, 2013)

> There's a gut feeling that people ought to be able to read books and watch films without the whole world knowing. Books and films are the intellectual vitamins that fuel the growth of intellectual thought. The whole process of intellectual growth is one of privacy – of quiet, and reflection. This intimate process should be protected from the disruptive intrusion of a roving eye.

S. Rep. No. 100-599 at 7.

135. The legislative history of the VPPA provides that Congress understood technology would soon make tracking "relatively easy" and the intent of the VPPA was to keep up with technology:"Unlike the other definitions in [the VPPA], paragraph (a)(3) uses the word 'includes' to establish a minimum, but not exclusive definition of personally-identifiable information." S. Rep. 100-599 at 12 (1988).

136. Congress recognized the definition of PII for children's use of the Internet in the legislative history to the 2012 amendments:

> This Committee does not intend for this clarification to negate in any way existing laws, regulations, and practices designed to protect the privacy of children on the Internet. …
>
> Website operators … share in the responsibility to protect consumer privacy, particularly the privacy of children. To facilitate this goal, Congress enacted the Children's Online Privacy Protection Act effective April 21, 2000, which applies to the online collection of personal information from children under 13. Compliance with the Act is overseen by the Federal Trade Commission, which enacted rules governing web site operator compliance, including a privacy policy, when and how to seek verifiable consent from a parent, and what responsibilities an operator has to protect children's privacy and safety online.
>
> …
>
> The Act and its regulations apply to individually identifiable information about a child that is collected online, such as full name, home address, email address, telephone number or any other information that would allow someone to identify or contact the child. The Act and Rule also cover other types of information – for example, hobbies, interests, and information collected through cookies and other types of tracking mechanisms – when they are tied to individually identifiable information.

H. Rep. 112-312 at 3-4 (2011).

137. The information at issue in this case fits the current real-world definition of "personally identifiable information." For example:

a. IP addresses, unique device identifiers, persistent cookie identifiers, browser-fingerprints, and usernames/aliases can all be used to identify or contact a person – particularly when the entity to which such information is disclosed is the world's largest Internet company and tracks users' real names, addresses, geo-locations, phone numbers, contacts, and behavior across a suite of the world's most popular Internet services.

b. Both Defendants Viacom and Google are members of the Interactive Advertising Bureau and agree to comply with the IAB's Code of Conduct. In particular, Viacom and Google publicly promise through IAB membership that they will "not collect 'personal information' as defined in the Children's Online Privacy Protection Act ('COPPA'), from children they have actual knowledge are under the age of 13 or from sites directed to children under the age of 13 for Online Behavioral Advertising, or engage in Online Behavioral Advertising direct to children they have actual knowledge are under the age of 13 except as compliant with the COPPA." For children, the data tracking industry defines "personal information" as it is defined in the Children's Online Privacy Protection Act where the tracking company "has actual knowledge" that the child is under the age of 13 or where the tracking is done on a website direct to children under the age of 13.

c. The Federal Trade Commission, after extensive hearings, and in its fact-finding role regarding regulation of children's use of the Internet, found that persistent identifiers are PII:

> The Commission continues to believe that persistent identifiers permit the online contacting of a specific individual. As the Commission stated in the 2011 NPRM, it is not persuaded by arguments that persistent identifiers only permit the contacting of a device. This interpretation ignores the reality that, at any given moment, a specific individual is using that device. Indeed, the whole premise underlying behavioral advertising is to serve an advertisement based on the perceived preferences of the individual user.
>
> Nor is the commission swayed by arguments noting that multiple individuals could be using the same device. Multiple people often share the same phone number, the same home address, and the same email address, yet Congress still classified those, standing alone, as "individually identifiable information about an individual." For these reasons, and the reasons stated in the 2011 NRPM, the Commission will retain persistent identifiers within the definition of personal information.

138. Online video service providers were well-aware of the restrictions imposed by the VPPA. For instance, in 2012, online video service provider Netflix lobbied for legislation to amend the Act to no longer require consent every time it sought to disclose a video requested or viewed by a customer.

139. As stated clearly in the legislative history to the VPPA amendments of 2012:

> Since 1988, Federal law has authorized video tape service providers to share customer information with the 'informed, written consent of the consumer at the time the disclosure is sought.' This consent must be obtained each time the provider wishes to disclose.

House Report 112-312 at 4. (2012).

140. The VPPA also clearly applies to online VTSPs that show television or other video programs. As explained in the legislative history to the 2012 amendments:

> When this law was originally enacted in 1988, consumers rented movies from brick-and-mortar video stores such as Blockbuster. Today, not only are VHS

> tapes obsolete, so too are traditional video rental stores. The Internet has revolutionized how consumers rent and watch movies and television programs. Video stores have been replaced with "on-demand" cable services or Internet streaming services that allow a customer to watch a movie or TV show from their laptop or even their cell phone.
>
> H. Rep. 112-312 at 2 (2011).
>
> At the time of the VPPA's enactment, consumers rented movies from video stores. The method that Americans used to watch videos in 1988 – the VHS cassette tape – is now obsolete. In its place, the Internet has revolutionzed the way that American consumers rent and watch movies and television programs. Today, so-called "on demand" cable services and Internet streaming services allow consumers to watch movies or TV shows on televisions, laptop computers, and cell phones.
>
> S. Rep. 112-258 at 2 (2012).

141. Viacom is engaged in the business of the delivery of pre-recorded video cassette tapes or similar audio visual materials as defined by the VPPA in that the home page of Nick.com advertises it as the place to watch "2000+ FREE ONLINE VIDEOS" and "play 1000+ FREE ONLINE GAMES." The homepage prominently features a rotating section enticing users to click and watch various videos with action buttons that say "Watch now," "Check it out," or, in the case of games, "Play Now." In addition, two of the first three links in the top bar on the homepage refer to audio-visual materials as of the time Plaintiffs' originally filed this suit. *See* Nick.com (September 24, 2013).

142. Plaintiffs and members of the putative video sub-class are "consumers' under the VPPA in that they are registered users of Nick.com, and therefore, constitute subscribers to the video services Viacom provides on Nick.com.

143. Viacom disclosed to Google at least the following about each Plaintiff who was a registered user of Nick.com: (1) the child's username/alias; (2) the child's gender; (3) the child's birthdate; (4) the child's IP address; (5) the child's browser settings; (6) the child's unique device

identifier; (7) the child's operating system; (8) the child's screen resolution; (9) the child's browser version; (10) the child's web communications, including but not limited to detailed URL requests and video materials requested and obtained from Viacom's Nick.com website; and (11) the DoubleClick persistent cookie identifiers.

144. By disclosing the above information to Google, Viacom knowingly disclosed information which, without more, when disclosed to Google, links specific persons with their video requests and/or viewing histories based on information that Google already has in its possession.

145. Viacom violated the VPPA by knowingly disclosing to Google information which, without more, when disclosed to Google, links specific persons with their video requests and viewing histories based on information that Google already has in its possession.

146. Defendant Google knowingly accepted the Plaintiffs' personally identifiable information regarding video materials and services through its use of the doubleclick.net cookies and other computer technologies.

147. Viacom further violated the VPPA after passage of the amended VPPA by failing to provide plaintiffs with the opt-out right codified in the amended VPPA in 18 U.S.C. § 2710(2)(B)(iii).

148. On or about August 1, 2014, Defendant Viacom revamped its Nick.com website. As of August 7, 2014, based on Plaintiffs' investigation, Defendant Viacom no longer discloses the particular video viewing or game histories of individual users of Nick.com to Google.[43]

149. As a result of the above violations and pursuant to 18 U.S.C. § 2710, the

[43] Though Plaintiffs' investigation did not reveal the continued disclosure of information from Viacom to Google, plaintiffs' note that they have not had opportunity for discovery to determine whether disclosures between the defendants continue to occur that is not detectable from the plaintiffs' individual computers.

Defendant Viacom is liable to the Plaintiffs and the Class for "liquidated damages of not less than $2,500 per Plaintiff;" reasonable attorney's fees and other litigation costs; injunctive and declaratory relief; and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendant in the future."

COUNT II – NEW JERSEY COMPUTER RELATED OFFENSES ACT

U.S. Resident Children v. All Defendants

150. Plaintiffs incorporate all preceding paragraphs as if set forth herein.

151. N.J.S.A. 2A:38A-3 states that a person or enterprise is liable for:

a. The purposeful or knowing, and unauthorized altering, damaging, taking or destruction of any data, data base, computer program, computer software or computer equipment existing internally or externally to a computer, computer system or computer network;

b. The purposeful or knowing, and unauthorized altering, damaging, taking or destroying of a computer, computer system or computer network;

c. The purposeful or knowing, and unauthorized accessing or attempt to access any computer, computer system or computer network;

d. The purposeful or knowing, and unauthorized altering, accessing, tampering with, obtaining, intercepting, damaging or destroying of a financial instrument; or

e. The purposeful or knowing accessing and reckless altering, damaging, destroying or obtaining of any data, data base, computer, computer program, computer software, computer equipment, computer system or computer network.

152. Defendants did purposefully, knowingly and/or recklessly, without Plaintiffs', Class Members' or their respective guardians' authorization, access, attempt to access, tamper

with, alter, damage, take, destroy, obtain and/or intercept Plaintiffs' and Class Members' computer, computer software, data, database, computer program, computer system, computer equipment and/or computer network in violation of N.J.S.A. 2A:38A-1 et seq.

153. Specifically, Defendants accessed Plaintiffs' and Class Members' computers in order to illegally harvest Plaintiffs' and Class Members' personal information. Through conversion and without consent, Defendants harvested Plaintiffs' personal information for their unjust enrichment and to the financial detriment of Plaintiffs and Class Members. Had Plaintiffs, Class Members, and/or their parents and/or guardians known that Defendants were converting Plaintiffs' personal information for financial gain, Plaintiffs, Class Members, and/or their parents and/or guardians would have at least expected remuneration for their personal information at the time it was conveyed.

154. Many of the computers that were accessed, the terminal used in the accessing, and/or the actual damages took place in New Jersey.

155. Plaintiffs C.A.F., C.T.F., M.P. and T.P. all reside in the State of New Jersey and accessed the Viacom Children's sites from computing devices within the State of New Jersey.

156. Pursuant to N.J.S.A. 2A:38A-1 et seq., Plaintiffs and the Class Members have been injured by the violations of N.J.S.A. 2A:38A-1 et seq., and each seek damages for compensatory and punitive damages and the cost of the suit including a reasonable attorney's fee, costs of investigation and litigation, as well as injunctive relief.

COUNT III – INTRUSION UPON SECLUSION

U.S. Resident Children v. All Defendants

157. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

158. In carrying out the scheme to track the Plaintiffs' Internet communications as

described herein without the consent of the Plaintiffs or their legal guardians, the Defendants intentionally intruded upon the Plaintiffs' solitude or seclusion in that the Defendants took information from the privacy of the Plaintiffs' homes.

159. The Plaintiffs, minor children, did not, and by law could not, consent to the Defendants' intrusion.

160. The Defendants' intentional intrusion on the Plaintiffs' solitude or seclusion is highly offensive to a reasonable person in that Defendants' conduct violated federal and state civil and criminal statutes designed to protect individual privacy. Specifically, the Defendants' conduct violated:

a. The Video Privacy Protection Act as alleged above;

b. The Wiretap Act because they engaged in a scheme to intentionally intercept the contents of the minor Plaintiffs' electronic communications without their or their guardians' consent;

c. In the alternative to finding that Defendants' conduct violated the Wiretap Act, this Court must find that the Defendants' conduct violated the Pen Register Act, 18 U.S.C. 3121, et seq., which makes it a federal crime for any person to "install or use a pen register or trap and trace device" without the consent of the user of an electronic communication service. A "pen register" is defined as "a device or process which records or decodes dialing, routing, addressing, or signaling information." 18 U.S.C. § 3127(3). A "trap and trace device" is defined as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to

identify the source of a wire or electronic communication." 18 U.S.C. § 3127(4). Violation of the Pen Register Act is subject to imprisonment for one year.

d. The Computer Fraud and Abuse Act and corresponding computer crime laws in all 50 states because Defendants knowingly placing or facilitated the placement of third-party cookies on the computing devices of minor children who were not aware of and could not consent to their placement, thereby intentionally exceeding authorized access to the Plaintiffs' computers and obtaining information from their computers. Intentional access to a computer which exceeds authorization and results in the obtaining of information from a computer used in interstate commerce violates the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C), and corresponding computer crime statutes of all 50 states.

161. Defendants' actions in committing criminal acts which violated the privacy rights of millions of American children is highly offensive to a reasonable person.

162. Defendants' unauthorized tracking of the minor children Plaintiffs' communication on the Internet, including, as detailed above, communications on sensitive topics, such as divorce and health URLs, is highly offensive to a reasonable person.

163. The Defendants' intentional intrusion on the Plaintiffs' solitude and seclusion violated the Terms of Use of both the Internet Service Providers and the web-browsers employed by the Plaintiffs, which prohibit the use of those services in criminal activity, unlawful activity, and the tracking of Internet communications without consent.

164. In December 2012, the same month plaintiffs initially filed their respective suits,

the Center for Digital Democracy surveyed more than 2,000 adults about basic principles of children's online privacy.[44] When asked whether they agreed or disagreed with the following statements, the polled adults responded as follows:

a. "It is wrong for advertisers to collect and keep information about where a child goes online and what that child does online."

- 45 percent strongly agree
- 13 percent somewhat agree
- 12 percent somewhat disagree
- 27 percent strongly disagree
- 3 percent do not know or refused to answer

b. "It is okay for advertisers to track and keep a record of a child's behavior online if they give the child free content."

- 5 percent strongly agree
- 6 percent somewhat agree
- 16 percent somewhat disagree
- 70 percent strongly disagree
- 3 percent do not know or refused to answer

c. "As long as advertisers don't know a child's name and address, it is okay for them to collect and use information about the child's activity online."

- 4 percent strongly agree
- 14 percent somewhat agree
- 13 percent somewhat disagree
- 67 percent strongly disagree
- 2 percent do not know or refused to answer

d. "Before advertisers put tracking software on a child's computer, advertisers should receive the parent's permission."

- 82 percent strongly agree

[44] The survey is available at http://www.centerfordigitaldemocracy.org/sites/default/files/COPPA%20Executive%20Summary%20and%20Findings.pdf (last visited July 25, 2014).

- 9 percent somewhat agree
- 2 percent somewhat disagree
- 4 percent strongly disagree
- 2 percent don't know or refused to answer

e. When asked, "There is a federal law that says that online sites and companies need to ask parents' permission before they collect personal information from children under age 13. Do you think the law is a good idea or a bad idea?" 90 percent said it was a good idea, 7 percent said it was a bad idea, and 2 percent did not know or refused to answer.

f. Parents in the survey were more protective of children's privacy than non-parents.

g. In connection with an investigation of cookie tracking on children's websites, the Wall Street Journal asked readers:

"How concerned are you about advertisers and companies tracking your behavior across the web?" An overwhelming majority of respondents indicated concern.

- 59.7 percent said they were "very alarmed"
- 25 percent said they were "somewhat alarmed"
- 3.7 percent said they were "neutral"
- 7 percent said it was "not a big worry"
- 4.5 percent said they "could not care less"[45]

h. In November 2012, the Washington Post asked Americans:[46]

"How concerned are you, if at all, about the government or private companies collecting digital information from your computer or phone?"

[45] See http://blogs.wsj.com/wtk-kids/ (last visited July 30, 2014).
[46] See http://www.washingtonpost.com/page/2010-2019/WashingtonPost/2013/12/21/National-Politics/Polling/question_12669.xml?uuid=FuyJGmqMEeOZe5ITsX2slw (last visited July 30, 2014).

- 43 percent were "very concerned"
- 26 percent were "somewhat concerned"
- 18 percent were "not too concerned"
- 12 percent were "not at all concerned," and
- 1 percent had "no opinion"

How concerned are you, if at all, about the collection and use of your personal information by websites like Google, Amazon, or Ebay?

- 37 percent were "very concerned"
- 32 percent were "somewhat concerned"
- 17 percent were "not too concerned"
- 13 percent were "not at all concerned"
- 2 percent had "no opinion"

i. In Winter 2012, the Pew Research Center on the Internet and American Life asked Americans: "Which of the following statements comes closest to exactly how you, personally, feel about targeted advertising being used online – even if neither is exactly right?"

- 68 percent said, "I'm not okay with it because I don't like having my online behavior tracked and analyzed."
- 28 percent said, "I'm okay with it because it means I see ads and get information about things I'm really interested in."
- 4 percent said "neither" or "don't know."

165. Defendants' actions were highly offensive to a reasonable person for each plaintiff individually, and this offensiveness is made worse because the acts were perpetrated literally millions of times on millions of children.

166. Defendants actions were highly offensive to a reasonable person because Defendants' targeting of children was more intrusive in that the defendants placed significantly more tracking technologies on children's websites than adult websites to take advantage of the Plaintiffs' vulnerability as children.

167. Defendants' actions were highly offensive to reasonable people because they

violated the online advertising industry and their own standards for respecting the personal information of children.

168. As a result of the above, the Defendants are liable to the Plaintiffs and the Class for general damages to the Plaintiffs' interest in privacy resulting from the invasions, compensatory and punitive damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

A. Certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure and appoint Plaintiffs as the representatives of the Class Members and their counsel as Class Counsel;

B. Award compensatory damages, including statutory damages where available, to Plaintiffs and the Class Members against Defendants for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

C. Award restitution to Plaintiffs and the Class Members against Defendants;

D. Award punitive damages in an amount that will deter Defendants and others from like conduct;

E. Permanently restrain Defendants, and their officers, agents, servants, employees, and attorneys, from tracking their users without consent or otherwise violating their policies with users;

F. Award Plaintiffs and the Class Members their reasonable costs and expenses incurred in this action, including counsel fees and expert fees;

G. Order that Defendants delete the data they collected about users through the unlawful means described above; and

H. Grant Plaintiffs and the Class members such further relief as the Court deems appropriate.

JURY TRIAL DEMAND

Plaintiffs demand a trial by jury of all issues so triable.

Dated: September 11, 2014

Respectfully submitted,

EICHEN CRUTCHLOW ZASLOW & McELROY, LLP
Barry R. Eichen, Esq.
Evan J. Rosenberg, Esq.
40 Ethel Road
Edison, NJ 08817
Tel.: (732) 777-0100
Fax: (732) 248-8273
beichen@njadvocates.com
erosenberg@njadvocates.com

and

BARTIMUS, FRICKLETON, ROBERTSON & GOZA P.C.
James P. Frickleton, Esq.
Edward D. Robertson III, Esq.
11150 Overbrook Road, Suite 200
Leawood, KS 66211
Tel: (913) 266 2300
Fax: (913) 266 2366
jimf@bflawfirm.com
krobertson@bflawfirm.com

Edward D. Robertson Jr. Esq.
Mary D. Winter Esq.
715 Swifts Highway
Jefferson City, MO 65109
Tel: (573) 659 4454
Fax: (573) 659 4460
chiprob@earthlink.net
marywinter@earthlink.net
Attorneys for Plaintiffs

~~TOP SECRET//COMINT//ORCON,NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

[redacted]

Docket Number: PR/TT [redacted]

MEMORANDUM OPINION

This matter is before the Court upon the government's application to re-initiate in expanded form a pen register/trap and trace (PR/TT) authorization for the National Security Agency (NSA) to engage in bulk acquisition of metadata[1] about Internet communications. The government's application also seeks Court authorization to query and use information previously obtained by NSA, regardless of whether the information was authorized to be acquired under

[1] When used in reference to a communication, "metadata" is information "about the communication, not the actual communication itself," including "numbers dialed, the length of a call, internet protocol addresses, e-mail addresses, and similar information concerning the delivery of the communication rather than the message between two parties." 2 Wayne R. LaFave, Jerold H. Israel, Nancy J. King & Orin S. Kerr, Criminal Procedure § 4.6(b) at 476 (3d ed. 2007).

prior bulk PR/TT orders of the Foreign Intelligence Surveillance Court (FISC or "Court") or exceeded the scope of previously authorized acquisition. For the reasons explained herein, the government's application will be granted in part and denied in part.

I. History of Bulk PR/TT Acquisitions Under the Foreign Intelligence Surveillance Act

From [redacted], NSA was authorized, under a series of FISC orders under the PR/TT provisions of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1841-1846, to engage in the bulk acquisition of specified categories of metadata about Internet communications. Although the specific terms of authorization under those orders varied over time, there were important constants. Notably, each order limited the authorized acquisition to [redacted] categories of metadata.[2] As detailed herein, the government acknowledges that

[redacted]

NSA exceeded the scope of authorized acquisition continuously during the more than [redacted] years of acquisition under these orders.

In addition, each order authorized NSA analysts to access the acquired metadata only through queries based on validated "seed" accounts, i.e., Internet accounts for which there was a reasonable articulable suspicion ("RAS") that they were associated with a targeted international terrorist group; for accounts used by U.S. persons, RAS could not be based solely on activities protected by the First Amendment.[3] The results of such queries provided analysts with information about the [redacted] of contacts and usage for a seed account, as reflected in the collected metadata, which in turn could help analysts identify previously unknown accounts or persons affiliated with a targeted terrorist group. See [redacted] Opinion at 41-45. Finally, each bulk PR/TT order included a requirement that NSA could disseminate U.S. person information to other agencies only upon a determination by a designated NSA official that it is related to counterterrorism information and is necessary to understand the counterterrorism information or to assess its importance.[4]

---

[2](continued)

[redacted]

The current application relies on this prior framework, but also seeks to expand authorization in ways that test the limits of what the applicable FISA provisions will bear. It also raises issues that are closely related to serious compliance problems that have characterized the government's implementation of prior FISC orders. It is therefore helpful at the outset to summarize both the underlying rationale of the prior authorizations and the government's frequent failures to comply with their terms.

A. Initial Approval

The first application for a bulk PR/TT authorization was granted by the Honorable Colleen Kollar-Kotelly in [redacted] Judge Kollar-Kotelly authorized PR/TT surveillance [redacted] See [redacted] Opinion at 72-80.[5] When known, the particular customers [redacted] were identified in the Court's order pursuant to 50 U.S.C. § 1842(d)(2)(A)(ii). See [redacted] Opinion at 22-23.

The [redacted] Opinion authorized the acquisition of [redacted] categories of metadata:

[redacted]

[redacted]

The government proposed to collect these categories of metadata from [redacted]

[redacted]

[redacted]

[redacted]

Judge Kollar-Kotelly found that the proposed collection of information within Categories [redacted] comported with the applicable statutory definitions of "pen register" and "trap and trace device,"[7] id. at 13-17, and with the Fourth Amendment, id. at 58-61. [redacted]

[redacted]

The [redacted] Opinion stated the Court's understanding that the application sought authority to obtain only [redacted] categories of information and specified that it authorized "only the collection of information in Categories [redacted] Id. at 11 (emphasis in original). Each subsequent bulk PR/TT order adopted as its rationale the analysis and conclusions set out in the [redacted] Opinion.[8]

---

[7] See 18 U.S.C. § 3127(3), (4). These definitions are more fully discussed at pages 25-26, infra.

[8] See e.g., Docket No. PR/TT [redacted] Primary Order issued on [redacted] at 5; Docket (continued...)

It was anticipated that the authorized PR/TT surveillance would "encompass [redacted] Opinion at 39-40 (internal quotations omitted).

Pursuant to 50 U.S.C. § 1842(c)(2), the initial application included a certification that the information likely to be obtained was relevant to an ongoing investigation to protect against international terrorism, which was not being conducted solely upon the basis of activities protected by the First Amendment. Docket No. PR/TT [redacted] Application filed [redacted]

[redacted]

[9] Bulk PR/TT surveillance was first approved in support of investigations of [redacted] and the collected metadata could only be accessed through queries based on seed accounts for which there was RAS that the account was associated with [redacted] July [redacted] Opinion at 72, 83. The range of terrorist organizations for which a RAS determination could support querying the metadata was [redacted] The present description of these Foreign Powers is contained in the Declaration of Michael E. Leiter, Director of the National Counterterrorism Center (NCTC), filed in docket number [redacted] which is incorporated by reference in the current application. See Docket No. PR/TT [redacted] Application filed [redacted] at 2.

([redacted] Application"), at 26.[10] Judge Kollar-Kotelly found that the sweeping and non-targeted scope of the proposed acquisition was consistent with this certification of relevance. [redacted] Opinion at 49. In making this finding, the Court relied on several factors, including NSA's efforts "to build a meta data archive that will be, in relative terms, richly populated with [redacted] communications," at least as compared with the entire universe of Internet communications, [redacted] Opinion at 47,[11] and the presence of "safeguards" proposed by the government "to ensure that the information collected will not be used for unrelated purposes," id. at 27, thereby protecting "the continued validity of the certification of relevance," id. at 70. These safeguards importantly included both the limitation that NSA

[10] The government argued that "FISA prohibits the Court from engaging in any substantive review of this certification," and that "the Court's exclusive function" was "to verify that it contains the words required" by the statute. [redacted] Opinion at 26. The Court did not find such arguments persuasive. Id. However, because the government had in fact provided a detailed explanation of the basis for the certification, the Court did not "decide whether it would be obliged to accept the applicant's certification without any explanation of its basis" and instead "assume[d] for purposes of this case that it may and should consider the basis" of the certification of relevance. Id. at 27-28.

[redacted]

analysts could access the bulk metadata only on the basis of RAS-approved queries, id. at 42-43, 56-58, and the rule governing dissemination of U.S. person information outside of NSA, id. at 85.

However, the finding of relevance most crucially depended on the conclusion that "the proposed bulk collection . . . is necessary for NSA to employ . . . analytic tools [that] are likely to generate useful investigative leads for ongoing efforts by the [Federal Bureau of Investigation (FBI)] (and other agencies) to identify and track [redacted] Id. at 48. Consequently, "the collection of both a huge volume and high percentage of unrelated communications . . . is necessary to identify the much smaller number of [redacted] such that the entire mass of collected metadata is relevant to investigating [redacted] affiliated persons. Id. at 48-49; see also id. at 53-54 (relying on government's explanation why bulk collection is "necessary to identify and monitor [redacted] operatives whose Internet communications would otherwise go undetected in the huge streams of [redacted] communications").

B. First Disclosure of Overcollection

During the initial period of authorization, the government disclosed that NSA's acquisitions had exceeded the scope of what the government had requested and the FISC had approved. Insofar as it is instructive regarding the separate form of overcollection that has led directly to the current application, this prior episode is summarized here.

On [redacted] the government provided written notice to the FISC that it had exceeded the scope of authorized collection [redacted] Docket No. PR/TT [redacted] Notice of Compliance Incidents, filed on [redacted] On the same day, Judge Kollar-Kotelly ordered the government to provide additional information about this non-compliance, including a "full description of the scope, nature, and circumstances of any unauthorized collection" [redacted] Docket No. PR/TT [redacted] Order Regarding Disclosed Violations Involving [redacted] issued on [redacted] Order"), at 6. The government made an interim response to the [redacted] Order in the form of a Declaration of [redacted] filed in Docket No. PR/TT [redacted] on [redacted] ("[redacted] Decl."), and a fuller response in the form of a Declaration of [redacted] filed in Docket No. PR/TT [redacted] on [redacted] ("[redacted] Decl.").

As described by the government, the unauthorized collection resulted from failures to [redacted] in the manner required. [redacted] Decl. at 8-11.[12] By the government's account, the lack of required [redacted] did not result from technical difficulty or malfunction, but rather from a failure of "those NSA officials who understood in detail the requirements of the [redacted] Opinion] . . . to communicate those requirements effectively

[redacted]

to the [redacted] . . . who were directly responsible" for implementation. Id. at 5. The government assessed the violations to have been caused by "poor management, lack of involvement by compliance officials, and lack of internal verification procedures – not by bad faith." Id. at 7.

The Court had specifically directed the government to explain whether this unauthorized collection involved the acquisition of information other than the approved Categories [redacted] Order at 7. In response, the Deputy Secretary of Defense stated that the "Director of NSA has informed me that at no time did NSA collect any category of information . . . other than the [redacted] categories of meta data" approved in the [redacted] Opinion, but also noted that the NSA's Inspector General had not completed his assessment of this issue. [redacted] Decl. at 21.[13] As discussed below, this assurance turned out to be untrue.

Regarding the information obtained through unauthorized collection, the Court ordered the government to describe whether it "has been, or can be, segregated from information that NSA was authorized to collect," "how the government proposes to dispose of" it, and "how the government proposes to ensure that [it] is not included . . . in applications presented to this Court." [redacted] Order at 7-8. In response, the government stated that, while it was not

[13] At a hearing on [redacted] Judge Kollar-Kotelly referred to this portion of the Deputy Secretary's declaration and asked: "[C]an we conclude that there wasn't content here?" [redacted] of NSA, replied: "There is not the physical possibility of our having [redacted] Docket Nos. [redacted] Transcript of Hearing Conducted [redacted] at 16-17.

feasible to segregate authorized collection from unauthorized collection on an item-by-item basis, NSA had eliminated access to the database that contained the entire set of metadata, and repopulated the databases used by analysts to run queries so that they only contained information [redacted] that had not been involved in the unauthorized collection. [redacted] [redacted] Decl. at 25-26. The government asserted that, after taking these actions, NSA was "making queries against a database that contain[ed] only meta data that NSA was authorized to collect." Id. at 26. As to information disseminated outside of NSA, the government reported that it had reviewed disseminated NSA reports and concluded that just one report was potentially based on improperly collected information. [redacted] Decl. at 9-10. NSA cancelled this report and confirmed that the recipient agencies had purged it from their records. Id. at 11.

The initial bulk PR/TT authorization granted by the [redacted] Opinion was set to expire on [redacted] shortly after the government had disclosed this unauthorized collection. On that date, Judge Kollar-Kotelly granted an application for continued bulk PR/TT acquisition; however, in that application, the government only requested authorization for acquisition [redacted] that had not been subject to the [redacted] See Docket No. PR/TT [redacted] Application filed on [redacted] ("[redacted] Application"), at 9-15; Primary Order issued on [redacted] at 2-5.[14] The government represented that the PR/TT [redacted] had "fully complied with the orders of the Court."

[14] Subsequent applications and orders followed the same approach. See, e.g., Docket No. PR/TT [redacted] Application filed on [redacted] at 9-13; Primary Order issued on [redacted] at 2-5.

Declaration of [redacted] at 2-3 (Exhibit C to [redacted] Application). The government also described in that application new oversight mechanisms to ensure against future overcollection. [redacted] Application at 8-9. These included a requirement that, "at least twice during the 90-day authorized period of surveillance," NSA's Office of General Counsel (NSA OGC) "will conduct random spot checks [redacted] to ensure that [redacted] functioning as authorized by the Court. Such spot checks will require an examination of a sample of data." Id. at 9. The Court adopted this requirement in its orders granting the application, as well as in subsequent orders for bulk PR/TT surveillance.[15]

C. Overcollection Disclosed in [redacted]

In December [redacted] the government reported to the FISC a separate case of unauthorized collection, which it attributed to a typographical error in how a prior application and resulting orders had described communications [redacted] See Docket No. PR/TT [redacted] Verified Motion for an Amended Order filed on [redacted] at 4-6. The government sought a nunc pro tunc correction of the typographical error in the prior orders, which would have effectively approved two months of unauthorized collection. Id. at 7. The government represented that, with regard to prior collection [redacted] it could not

[15] See [redacted]

"accurately segregate" information that fell within the scope of the prior orders from those that did not. Id.

The FISC approved prospective collection [redacted] on the terms requested by the government when it granted a renewal application [redacted] See Docket No. PR/TT [redacted] Primary Order issued on [redacted] at 5-6. However, the FISC withheld nunc pro tunc relief for the previously collected information, and NSA removed from its systems all data collected [redacted] under the prior order. See Docket [redacted] at 18.

D. Non-Compliance Disclosed [redacted]

The next relevant compliance problems surfaced in [redacted] and involved three general subjects: (1) accessing of metadata; (2) disclosure of query results and information derived therefrom; and (3) overcollection. These compliance disclosures generally coincided with revelations about similar problems under a separate line of FISC orders providing for NSA's bulk acquisition of metadata for telephone communications pursuant to 50 U.S.C. § 1861.[16]

1. Accessing Metadata

On January [redacted] the government disclosed that NSA had regularly accessed the bulk telephone metadata using a form of automated querying based on telephone numbers that had not been approved under the RAS standard. See Docket No. BR 08-13, Order Regarding

[16] The Section 1861 orders, like the bulk PR/TT orders, permit NSA analysts to access the bulk telephone metadata only through queries based on RAS-approved telephone numbers. See, e.g., Docket No. [redacted], at 7-10.

Preliminary Notice of Compliance Incident Dated [redacted] issued on [redacted] at 2-3. The Honorable Reggie B. Walton of this Court ordered the government to verify that access to the bulk PR/TT metadata complied with comparable restrictions, noting "the similarity between the querying practices and requirements employed" in both contexts. See Docket No. PR/TT [redacted] Order issued on [redacted] at 1.

In response, the government reported that it had identified, and discontinued, a non-automated querying practice for PR/TT metadata that it had concluded was non-compliant with the required RAS approval process. See Docket No. PR/TT [redacted] Government's Response to the Court's Order Dated [redacted] filed on [redacted] at 2-6 ([redacted] Response").[17] The government's [redacted] Response also described additional oversight and

[17] This practice involved an analyst running a query using as a seed "a U.S.-based e-mail account" that had been in direct contact with a properly validated seed account, but had not itself been properly validated under the RAS approval process. [redacted] Response at 2-3. When he granted renewed authorization for bulk PR/TT surveillance on [redacted], Judge Walton ordered the government not to resume this practice without prior Court approval. See Docket No. PR/TT [redacted] Primary Order issued [redacted] at 10.

In its response, the government also described an automated means of querying, which it regarded as consistent with the applicable PR/TT orders. This form of querying involved the determination that an e-mail address satisfied the RAS standard, but for the lack of a connection to one of the Foreign Powers (e.g, there were sufficient indicia that the user of the e-mail address was involved in terrorist activities, but the user's affiliation with a particular group was unknown). See Declaration of Lt. Gen. Keith B. Alexander, Director of NSA, at 8 (attached at Tab 1 to [redacted] Response) ([redacted] Alexander Decl."). In the event that such an e-mail address was in contact with a RAS-approved seed account on an NSA "Alert List," that e-mail address would itself be used as a seed for automatic querying, on the theory that the requisite nexus to one of the Foreign Powers had been established. Id. at 8-9. The government later reported that it had discontinued this practice, see Docket No. PR/TT [redacted] NSA 90-Day

(continued...)

compliance measures being taken with regard to the bulk PR/TT program, see [redacted] Response at 6-7, which Judge Walton adopted as requirements in his order authorizing continued bulk PR/TT surveillance on [redacted]. See Docket No. PR/TT [redacted] Primary Order issued [redacted] at 13-14. Finally, the government's response noted the commencement by NSA of a "complete ongoing end-to-end system engineering and process review (technical and operational) of NSA's handling of PR/TT metadata to ensure that the material is handled in strict compliance with the terms of the PR/TT Orders and the NSA's descriptions to the Court." [redacted] Alexander Decl. at 16.[18]

---

[17](...continued)
Report filed [redacted] at 8 (Exhibit B to Application), and the Court ordered the government not to resume it without prior Court approval. See Docket No. PR/TT [redacted] Primary Order issued [redacted] at 10.

[18] On [redacted] the government provided written notice of a separate form of unauthorized access relating to the use by NSA technical personnel of bulk PR/TT metadata to identify [redacted] which they then employed for "metadata reduction and management activities" in other data repositories. See Docket No. PR/TT [redacted] Preliminary Notice of Compliance Incident filed on [redacted] at 2-3. The government assessed this practice to be inconsistent with restrictions on accessing and using bulk PR/TT metadata. Id. at 3. On [redacted] Judge Walton issued a supplemental order which, inter alia, directed the government to discontinue such use or show cause why continued use was necessary and appropriate. See Docket No. PR/TT [redacted] Supplemental Order issued on [redacted] Order"), at 4. In response, the government described the deleterious effects that would likely result from discontinuing the use of [redacted] derived from the bulk PR/TT metadata. See Docket No. PR/TT [redacted] Declaration of [redacted] NSA, filed on [redacted] at 1-3, 6 [redacted] Decl."). On [redacted] Judge Walton approved the continuation of NSA's use of [redacted] Docket No. PR/TT [redacted] Supplemental Order issued on [redacted] at 2-3. In addition, with regard to a then-recent misstatement by the government concerning when NSA had terminated automatic querying of the bulk PR/TT metadata, see [redacted]
(continued...)

2. Disclosure of Query Results and Information Derived Therefrom

Also in the [redacted] Order, the Court noted recent disclosure of the extent to which NSA analysts who were not authorized to access the PR/TT metadata directly nonetheless received unminimized query results. [redacted] Order at 2. The Court permitted the continuance of this practice for a 20-day period, but provided that such sharing shall not continue thereafter "unless the government has satisfied the Court, by written submission, that [it] is necessary and appropriate." Id. at 4. In response, the government stated that "NSA's collective expertise in [the targeted] Foreign Powers resides in more than one thousand intelligence analysts," less than ten percent of whom were authorized to query the PR/TT metadata. [redacted], [redacted] Declaration at 7-8. Therefore, the government posited that sharing "unminimized query results with non-PR/TT-cleared analysts is critical to the success of NSA's counterterrorism mission." Id. at 8. Judge Walton authorized the continued sharing of such information within NSA, subject to the training requirement discussed at pages 18-19, infra. See Docket Nos. PR/TT [redacted] & BR 09-06, Order issued on [redacted] Order"), at 7.

On [redacted] the government submitted a notice of non-compliance regarding dissemination of information outside of NSA that resulted from NSA's placing of query results into a database accessible by other agencies' personnel without the determination, required for

---

[18](...continued)
[redacted] Order at 2, the Court ordered NSA not to "resume automated querying of the PR/TT metadata without the prior approval of the Court." Id. at 3.

any U.S. person information, that it related to counterterrorism information and was necessary to understand the counterterrorism information or assess its importance. See Docket No. PR/TT [redacted] Preliminary Notice of Compliance Incident filed on [redacted] Between [redacted] and [redacted] approximately 47 analysts from the FBI, the Central Intelligence Agency (CIA), and the National Counterterrorism Center (NCTC) queried this database in the course of their responsibilities and accessed unminimized U.S. person information. See Docket No. PR/TT [redacted] Report of the United States filed on [redacted] Report"), Exhibit A, Declaration of Lt. Gen. Keith B. Alexander, Director, NSA, at 11-13. NSA terminated access to this database for other agencies' personnel by [redacted] Id. at 12. Based on its end-to-end review, NSA concluded that NSA personnel "failed to make the connection between continued use of the database and the new dissemination procedures required by the Court's Orders." Id. at 15.

The government further disclosed that, apart from this shared database, NSA analysts made it a general practice to disseminate to other agencies NSA intelligence reports containing U.S. person information extracted from the PR/TT metadata without obtaining the required determination. See Docket No. PR/TT [redacted] Government's Response to the Court's Supplemental Order Entered on [redacted], filed on [redacted] at 2. The large majority of disseminated reports had been written by analysts cleared to directly query the PR/TT metadata. See Docket No. PR/TT [redacted] Declaration of [redacted] NSA, filed on [redacted], at 2. In response to these disclosures, Judge Walton ordered that, prior to receiving query

results, any NSA analyst must first have received "appropriate and adequate training and guidance regarding all rules and restrictions governing the use, storage, and dissemination of such information." [redacted] Order at 7. He also required the government to submit weekly reports on dissemination, including a certification that the required determination had been made for any dissemination of U.S. person information, and to include "in its submissions regarding the results of the end-to-end review[] a full explanation" of why this dissemination rule had been disregarded. Id. at 7-8.

Subsequently, in response to the latter requirement, the government merely stated: "Although NSA now understands the fact that only a limited set of individuals were authorized to approve these releases under the Court's authorization, it seemed appropriate at the time" to delegate approval authority to others. [redacted] Report, Exhibit A, at 17. The government's explanation speaks only to the identity of the approving official, but a substantive determination regarding the counterterrorism nature of the information and the necessity of including U.S. person information was also required under the Court's orders. See page 3, supra. It appears that, for the period preceding the adoption of the weekly reporting requirement, there is no record of the required determination being made by any NSA official for any dissemination. As far as can be ascertained, the requirement was simply ignored. See [redacted] Report, Exhibit A, at 18-19.

NSA completed its "end-to-end review" of the PR/TT metadata program on [redacted], [redacted]. See [redacted] Report, Exhibit B. On [redacted], Judge Walton granted an

application for continued bulk PR/TT authorization. In that application, the government represented that "**all the technologies used by NSA to implement the authorizations granted by docket number PR/TT [redacted] and previous docket numbers only collect, or collected, authorized metadata.**" Docket No. PR/TT [redacted] Application filed on [redacted] Application"), at 11 n.6 (emphasis in original).

3. Overcollection

Notwithstanding this and many similar prior representations, there in fact had been systemic overcollection since [redacted] On [redacted] the government provided written notice of yet another form of substantial non-compliance discovered by NSA OGC on [redacted][19] this time involving the acquisition of information beyond the [redacted] authorized categories. See Docket No. PR/TT [redacted] Preliminary Notice of Compliance Incident filed on [redacted] at 2. This overcollection, which had occurred continuously since the initial authorization in [redacted] id. at 3, included the acquisition of [redacted] id. at 2. The government reported that NSA had ceased querying PR/TT metadata and suspended receipt of metadata [redacted] Id. The government later advised that this continuous overcollection acquired

[19] Since [redacted] NSA OGC had been obligated to conduct periodic checks of the metadata obtained at [redacted] to ensure that [redacted] were functioning in an authorized manner. See page 13, supra.

many other types of data[20] and that "[v]irtually every PR/TT record" generated by this program included some data that had not been authorized for collection. [redacted] application, Exhibit D, NSA Response to FISA Court Questions dated [redacted] ("[redacted] Response"), at 18.

The government has provided no comprehensive explanation of how so substantial an overcollection occurred, only the conclusion that, [redacted] there was a failure to translate the technical requirements" [redacted] "into accurate and precise technical descriptions for the Court." [redacted] Report, Exhibit A, at 31. The government has said nothing about how the systemic overcollection was permitted to continue, [redacted] On the record before the Court, the most charitable interpretation possible is that the same factors identified by the government [redacted] remained unabated and in full effect: non-communication with the technical personnel directly responsible [redacted] resulting from poor management. However, given the duration of this problem, the oversight measures ostensibly taken since [redacted] to detect overcollection, and the extraordinary

[redacted]

fact that NSA's end-to-end review overlooked unauthorized acquisitions that were documented in virtually every record of what was acquired, it must be added that those responsible for conducting oversight at NSA failed to do so effectively. The government has expressed a belief that "the stand-up of NSA's Office of the Director of Compliance in July 2009" will help avoid similar failures in the future, both with respect to explaining to the FISC what NSA actually intends to do and in conforming NSA's actions to the terms of FISC authorizations. Id. at 31-32.

E. Expiration of Bulk PR/TT Authorities

The PR/TT authorization granted in Docket No. PR/TT [redacted] was set to expire on [redacted] On [redacted] the government submitted a proposed renewal application, which acknowledged [redacted] information that may not have been contemplated under prior orders. See Docket No. PR/TT [redacted] Supplemental Order issued on [redacted] Order"), at 2. The proposed application sought approval [redacted] subject to the restrictions that NSA analysts would not query the PR/TT metadata previously received by NSA[21] and that information prospectively obtained [redacted] would be stored [redacted] and not [redacted] o access or use. Id. at 2. After Judge Walton expressed concern about the merits of the

[21] The government requested in its proposed application that, if "immediate access to the metadata repository is necessary in order to protect against an imminent threat to human life," the government would "first notify the Court." [redacted] Order at 3. Instead, Judge Walton permitted access to protect against an imminent threat as long as the government provided a report.

proposed application,[22] the government elected not to submit a final application. Id. at 3. As a result, the authorization for bulk PR/TT surveillance expired on [redacted] Judge Walton directed that the government "shall not access the information [previously] obtained . . . for any analytic or investigative purpose" and shall not "transfer to any other NSA facility information . . . currently stored [redacted] Id. at 4-5. He also provided that, "[i]n the extraordinary event that the government determines immediate access to the [PR/TT metadata] is necessary in order to protect against an imminent threat to human life, the government may access the information," and shall thereafter "provide a written report to the Court describing the circumstances and results of the access." Id. at 5.[23]

F. The Current Application

On [redacted] the government submitted another proposed application, which in most substantive respects is very similar to the final application now before the Court. Thereafter, on [redacted] the undersigned judge met with representatives of the executive branch to explore a number of factual and legal questions presented. The government responded to the Court's questions in three written submissions,

---

[22] The proposed application did not purport to specify the types of data acquired [redacted] or, importantly, to provide a legal justification for such acquisition under a PR/TT order.

[23] In compliance with this requirement, the government has reported that, under this emergency exception, NSA has run queries of the bulk metadata in response to threats stemming from (i) [redacted] See, e.g., Docket No. PR/TT [redacted] Reports filed on [redacted] and various reports filed from [redacted]

filed on [redacted]. The government then submitted its revised, final application on [redacted], with those prior written responses attached as Exhibit D.

To enter the PR/TT order requested in the current application, or a modified PR/TT order, the Court must find that the application meets all of the requirements of Section 1842. See 50 U.S.C. § 1842(d)(1). Some of these requirements are plainly met: the government has submitted to a judge of the FISC a written application that has been approved by the Attorney General (who is also the applicant). See [redacted] Application at 1, 20; 50 U.S.C. § 1842(a)(1), (b)(1), (c). The application identifies the Federal officer seeking to use the PR/TT devices covered by it as General Keith B. Alexander, the Director of NSA, who has also verified the application pursuant to 28 U.S.C. § 1746 in lieu of an oath or affirmation. See [redacted] pplication at 5, 18; 50 U.S.C. § 1842(b), (c)(1).

In other respects, however, the Court's review of this application is not nearly so straightforward. As a crucial threshold matter, there are substantial questions about whether some aspects of the proposed collection are properly regarded as involving the use of PR/TT devices. There are also noteworthy issues regarding the certification of relevance pursuant to Section 1842(c)(2) and the specifications that the order must include under Section 1842(d)(2)(A), as well as post-acquisition concerns regarding the procedures for handling the metadata. The Court's resolution of these issues is set out below.

In the remainder of this Opinion, the Court will first consider whether the proposed collection involves the use of a PR/TT device within the meaning of the applicable statutory definitions, and whether the data that the government seeks to collect consists of information that may properly be acquired by such a device. Next, the Court will consider whether the application satisfies the statutory relevance standard and contains all the necessary elements. The Court will then address the procedures and restrictions proposed by the government for the retention, use, and dissemination of the information that is collected. Finally, the Court will consider the government's request for permission to use all previously-collected data, including information falling outside the scope of the Court's prior authorizations.

II. The Proposed Collection, as Modified Herein, Involves the Installation and Use of PR/TT Devices

A. The Applicable Statutory Definitions

For purposes of 50 U.S.C. §§ 1841-1846, FISA adopts the definitions of "pen register" and "trap and trace device" set out in 18 U.S.C. § 3127. See 50 U.S.C. § 1841(2). Section 3127 provides the following definitions:

> (3) the term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication . . . ;[24]

[24] The definition excludes any device or process used by communications providers or customers for certain billing-related purposes or "for cost accounting or other like purposes in the ordinary course of business." § 3127(3). These exclusions are not pertinent to this case.

> (4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

These definitions employ three other terms – "electronic communication," "wire communication," and "contents" – that are themselves governed by statutory definitions "set forth for such terms in section 2510" of title 18. 18 U.S.C. § 3127(1). Section 2510 defines these terms as follows:

> (1) "Electronic communication" is defined as:
>
> any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include – (A) any wire or oral communication.[25]

18 U.S.C. § 2510(12).

> (2) "Wire communication" is defined as:
>
> any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception . . . furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.

18 U.S.C. § 2510(1).

---

[25] The other exclusions to this definition at Section 2510(12)(B)-(D) are not relevant to this case.

(3) "Contents" is defined to "include[] any information concerning the substance, purport, or meaning" of a "wire, oral, or electronic communication." 18 U.S.C. § 2510(8).[26]

Together, these definitions set bounds on the Court's authority to issue the requested order because the devices or processes to be employed must meet the definition of "pen register" or "trap and trace device."

[redacted]

As explained by the government, the proposed collection [redacted] Declaration of Gen. Keith B. Alexander, Director of NSA, at 23-24 (attached as Exhibit A to [redacted] Application) ([redacted] Alexander Decl."). [redacted]

[26] Different definitions of "wire communication" and "contents" are set forth at 50 U.S.C. § 1801(l) & (n). The definitions in Section 1801, however, apply to terms "[a]s used in this subchapter" – i.e., in 50 U.S.C. §§ 1801-1812 (FISA subchapter on electronic surveillance) – and thus are not applicable to the terms "wire communication" and "contents" as used in the definition of "pen register" and "trap and trace device" applicable to Sections 1841-1846 (FISA subchapter on pen registers and trap and trace devices).

[redacted] See id., Tab 2, at 1-2 n.2.[27]

Subject to the following discussion of what types of information may properly be regarded as non-content addressing, routing or signaling information, the Court concludes that this [redacted] is consistent with the statutory definitions of "pen register" and, insofar as information about the source of a communication is obtained, "trap and trace device." Each communication subject to collection is either a wire communication or an electronic

[redacted]

communication under the definitions set forth above.[28] The end-result of the collection process[29] is that only metadata authorized by the Court for collection is forwarded to NSA for retention and use. [redacted] Finally, and again subject to the discussion below regarding what types of information may properly be acquired, the Court concludes that the automated processes resulting in the transmission to NSA of information

[28] Many of the communications for which information will be acquired will fall within the broad definition of "electronic communication" at 18 U.S.C. § 2510(12). If, however, a covered communication consists of an "aural transfer," i.e., "a transfer containing the human voice at any point between and including the point of origin and the point of reception," id. § 2510(18), then it could constitute a "wire communication" under the meaning of Section 2510(1). In either case, the communications subject to collection are "wire or electronic communication[s]," as required in Sections 3127(3) & (4).

[29] The term "process," as used in the definitions of "pen register" and "trap and trace device", has its "generally understood" meaning of "a series of actions or operations conducing to an end" and "covers software and hardware operations used to collect information." In re Application of the United States for an Order Authorizing the Installation and Use of a PR/TT Device on E-Mail Account, 416 F. Supp.2d 13, 16 n.5 (D.D.C. 2006) (Hogan, District Judge) (internal quotations and citations omitted).

[30] Accord [redacted] Opinion at 12-13; In re Application of the United States for an Order Authorizing the Use of Two PR/TT Devices, 2008 WL 5082506 at *1 (E.D.N.Y. Nov. 26, 2008) (Garaufis, District Judge) (recording and transmitting contents permissible under PR/TT order where government computers were configured to immediately delete all contents). But see In re Application of the United States for an Order Authorizing the Use of a PR/TT Device On Wireless Telephone, 2008 WL 5255815 at *3 (E.D.N.Y. Dec. 16, 2008) (Orenstein, Magistrate Judge) (any recording of contents impermissible under PR/TT order, even if deleted before information is provided to investigators).

resulting from [redacted] about communications is a form of "record[ing]" or "decod[ing]" permissible under the definition of "pen register."

C. The Requested Information

The application seeks to expand considerably the types of information authorized for acquisition. Although the government provides new descriptions for the categories of information sought, see [redacted] Alexander Decl., Tab 2, they encompass all the types of information that were actually collected (to include unauthorized collection) under color of the prior orders. Memorandum of Law and Fact in Support of Application for Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes ("Memorandum of Law") at 3, submitted as Exhibit B to the [redacted] Application.

1. The Proper Understanding of DRAS Information and Contents

The government contends that all of the data requested in this application may properly be collected by a PR/TT device because all of it is dialing, routing, addressing or signaling ("DRAS") information, and none constitutes contents. Id. at 22. In support of that contention, the government advances several propositions concerning the meaning of "dialing, routing, addressing, or signaling information" and "contents," as those terms are used in the definitions of "pen register" and "trap and trace device." While it is not necessary to address all of the government's assertions, a brief discussion of the government's proposed statutory construction will be useful in explaining the Court's decision to approve most, but not all, of the proposed collection.

The government argues that DRAS information and contents are "mutually exclusive categories," and that Congress intended for DRAS information "to be synonymous with 'non-content.'" Id. at 23, 51. The Court is not persuaded that the government's proposed construction can be squared with the statutory text. The definition of pen register covers "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility . . ., provided, however, that such information shall not include the contents of any communication." § 3127(3). The structure of the sentence – an affirmative description of the information to be recorded or decoded, followed by a proviso that "such information shall not include the contents of any communication" – does not suggest an intention by Congress to create two mutually exclusive categories of information. Instead, the sentence is more naturally read as conveying two independent requirements – the information to be recorded or decoded must be DRAS information and, whether or not it is DRAS, it must not be contents. The same observations apply to the similarly-structured definition of "trap and trace device." See 18 U.S.C. § 3127(4) ("a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication").

The breadth of the terms used by Congress to identify the categories of information subject to collection and to define "contents" reinforces the conclusion that DRAS and contents are not mutually exclusive categories. As the government observes, see Memorandum of Law at

37, the ordinary meanings of the terms "dialing," "routing," addressing," and "signaling" – which are not defined by the statute – are relatively broad. Moreover, as noted above, the term "contents" is broadly defined to include "any information concerning the substance, purport, or meaning of [an electronic] communication." 18 U.S.C. § 2510(8) (emphasis added). And "electronic communication," too, is defined broadly to mean "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system . . . ." 18 U.S.C. § 2510(12) (emphasis added).

Given the breadth of the terms used in the statute, it is not surprising that courts have identified forms of information that constitute both DRAS and contents. In the context of Internet communications, a Uniform Resource Locator (URL) – "an address that can lead you to a file on any computer connected to the Internet"[31] – constitutes a form of "addressing information" under the ordinary meaning of that term. Yet, in some circumstances a URL can also include "contents" as defined in Section 2510(8). In particular, if a user runs a search using an Internet search engine, the "search phrase would appear in the URL after the first forward slash" as part of the addressing information, but would also reveal contents, i.e., the "'substance' and 'meaning' of the communication . . . that the user is conducting a search for information on a particular topic." In re Application of the United States for an Order Authorizing the Use of a Pen Register and Trap, 396 F. Supp.2d 45, 49 (D. Mass. 2005) (Collins, Magistrate Judge); see

[31] See Newton's Telecom Dictionary 971 (24th ed. 2008).

also In re Pharmatrak, Inc., 329 F.3d 9, 16, 18 (1st Cir. 2003) (URLs including search terms are "contents" under Section 2510(8)).[32] In the context of telephone communications, the term "dialing information" can naturally be understood to encompass all digits dialed by a caller. However, some digits dialed after a call has been connected, or "cut through," can constitute "contents" – for example, if the caller is inputting digits in response to prompts from an automated prescription refill system, the digits may convey substantive instructions such as the prescription number and desired pickup time for a refill. Courts accordingly have described post-cut-through digits as dialing information, some of which also constitutes contents. See In re Application of the United States for an Order (1) Authorizing the Installation and Use of a PR/TT Device and (2) Authorizing Release of Subscriber and Other Information, 622 F. Supp.2d 411, 412 n.1, 413 (S.D. Tex. 2007) (Rosenthal, District Judge); In re Application, 396 F. Supp.2d at 48.

In light of the foregoing, the Court rejects the government's contention that DRAS information and contents are mutually exclusive categories. Instead, the Court will, in accordance with the language and structure of Section 3127(3) and (4), apply a two-part test to

[32] But see H.R. Rep. No. 107-236(I), at 53 (2001) (stating that the portion of a URL "specifying Web search terms or the name of a requested file or article" is not DRAS information and therefore could not be collected by a PR/TT device).

the information that the government seeks to acquire and use in this case: (1) is the information DRAS information?; and (2) is it contents?[33]

In determining whether or not the types of information sought by the government constitute DRAS information, the Court is guided by the ordinary meanings of the terms "addressing," "routing," and "signaling," and by the context in which the terms are used.[34] As the government asserts, "addressing information" may generally be understood to be "information that identifies recipients of communications or participants in a communication" and "may refer to people [or] devices." Memorandum of Law at 37.[35] The Court also agrees with the government that "routing information" can generally be understood to include information regarding "the path or means by which information travels." Memorandum of Law at 37. As will be explained more fully in the discussion of "communications actions" below, the Court adopts a somewhat narrower definition of "signaling information" than the government. In summary, the Court concludes that signaling information includes information that is utilized in

---

[33] To decide the issues presented by the application, the Court need not reach the government's contention that Congress intended DRAS information to include all information that is not contents, or its alternative argument that, if there is a third category consisting of non-DRAS, non-content information, a PR/TT device may properly collect such information. See Memorandum of Law at 49-51.

[34] The government does not contend that any of the information sought constitutes only "dialing information," which it asserts "presumptively relates to telephones." Memorandum of Law at 37 n.19.

[35] See Newton's Telecom Dictionary at 89 ("An address comprises the characters identifying the recipient or originator of transmitted data.").

or pertains to (1) logging into or out of an account or (2) processing or transmitting an e-mail or IM communication. See pages 50-56, infra.[36]

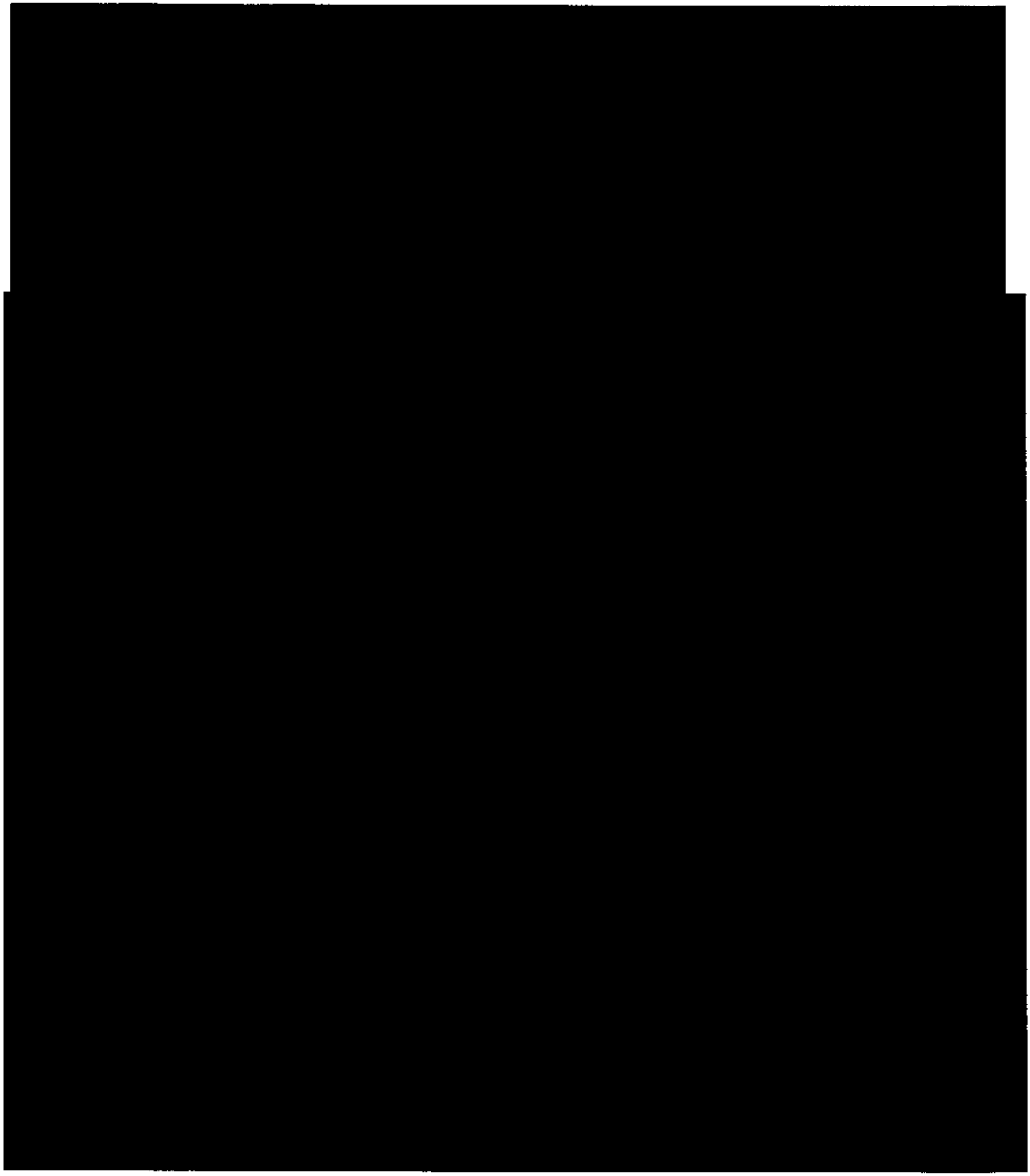
With regard to "contents," the Court is, of course, bound by the definition set forth in Section 2510(8), which, as noted, covers "any information concerning the substance, purport, or meaning" of the wire or electronic communication to which the information relates. When the communication at issue is between or among end users, application of the definition of "contents" can be relatively straightforward. For an e-mail communication, for example, the contents would most obviously include the text of the message, the attachments, and the subject-line information. In the context of person-to-computer communications like the interactions between a user and a web-mail service provider, however, determining what constitutes contents can become "hazy." See 2 LaFave, et al. Criminal Procedure § 4.6(b) at 476 ("[W]hen a person sends a message to a machine, the meaning of 'contents' is unclear."). Particularly in the user-to-provider context, the broad statutory definition of contents includes some information beyond what might, in ordinary parlance, be considered the contents of a communication.

2. The Categories of Metadata Sought for Acquisition

The government requests authority to [redacted] categories of [redacted]

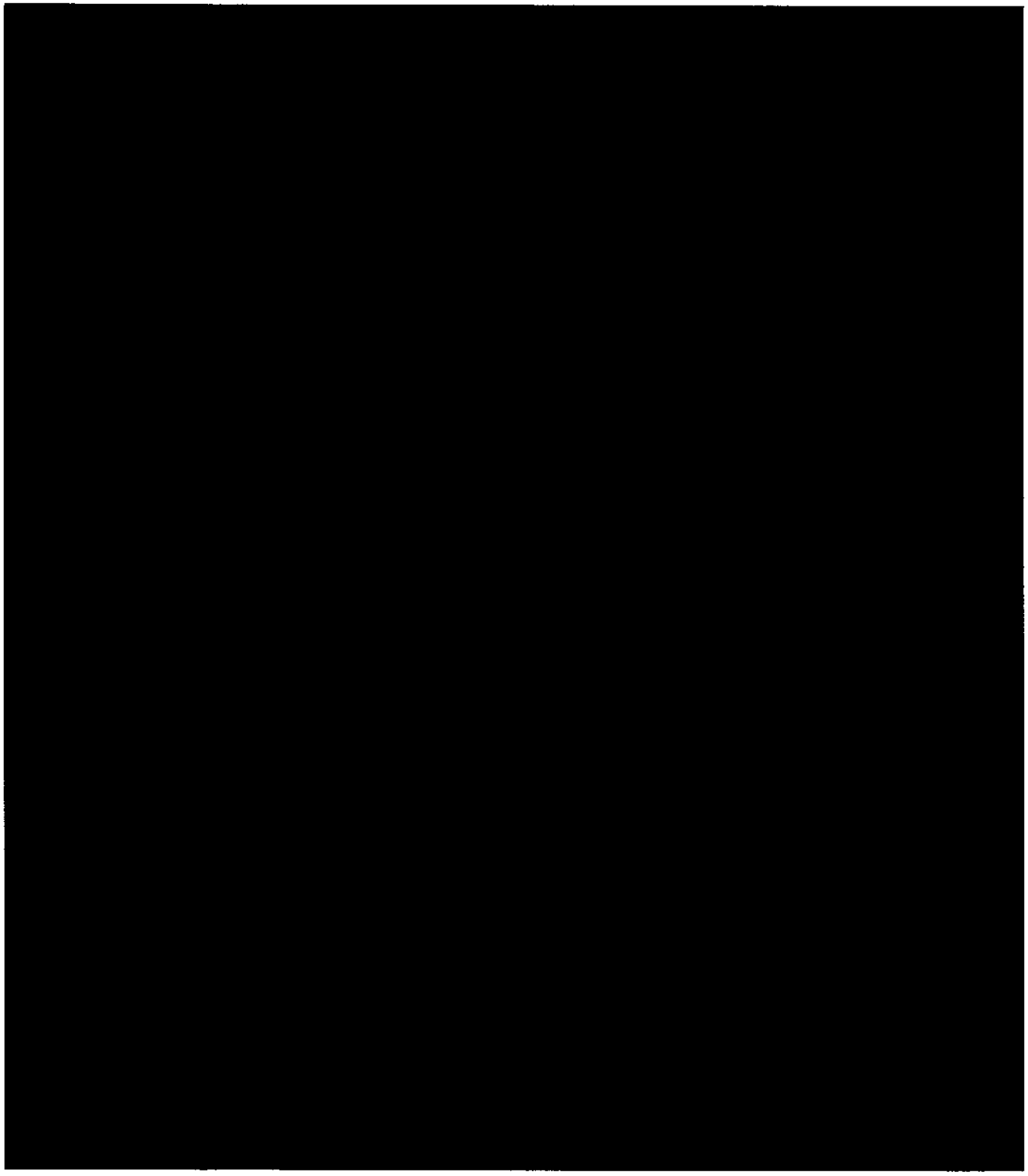
[36] For purposes of this Opinion, the term "e-mail communications" refers to e-mail messages sent between e-mail users [redacted]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

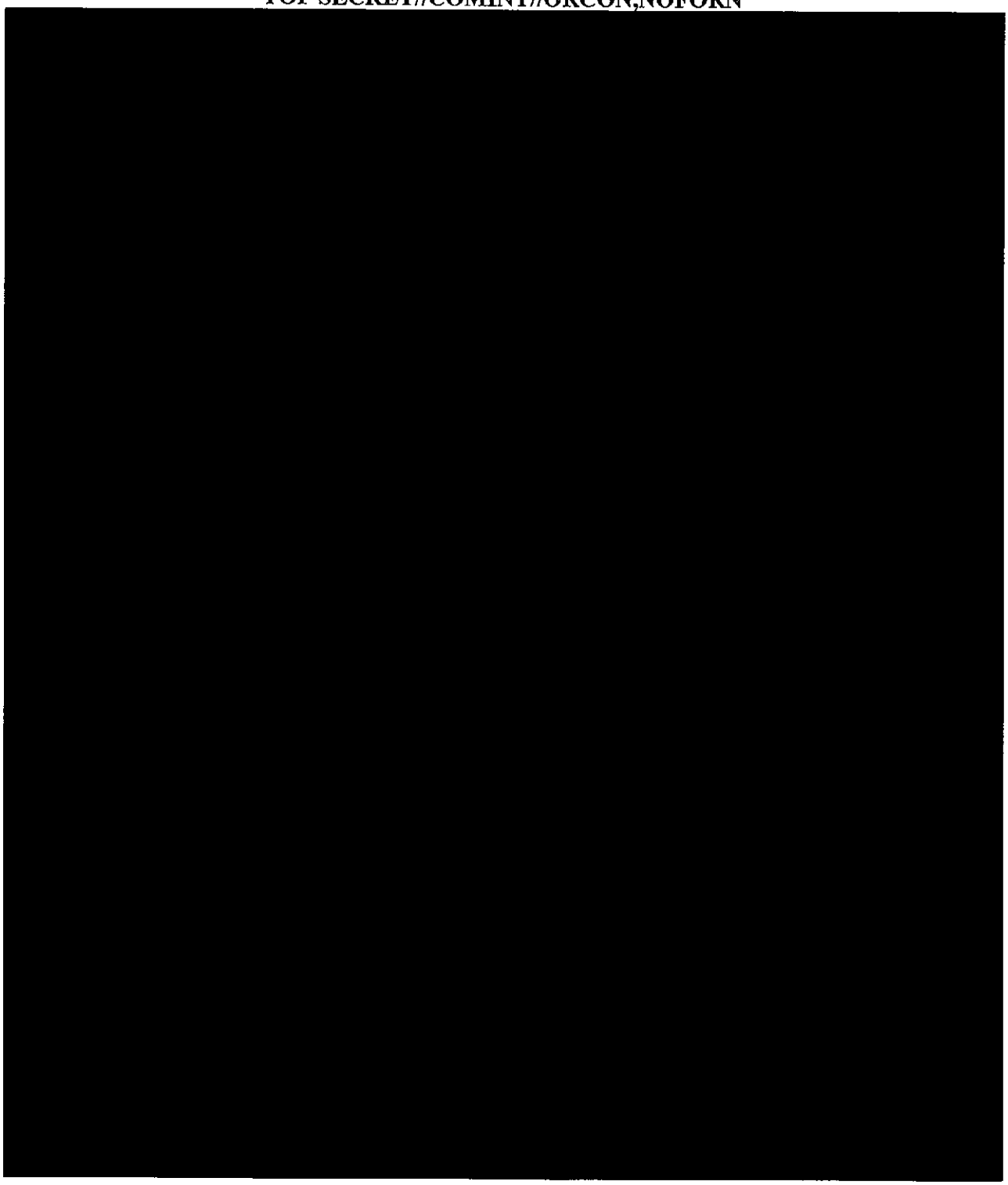


~~TOP SECRET//COMINT//ORCON,NOFORN~~

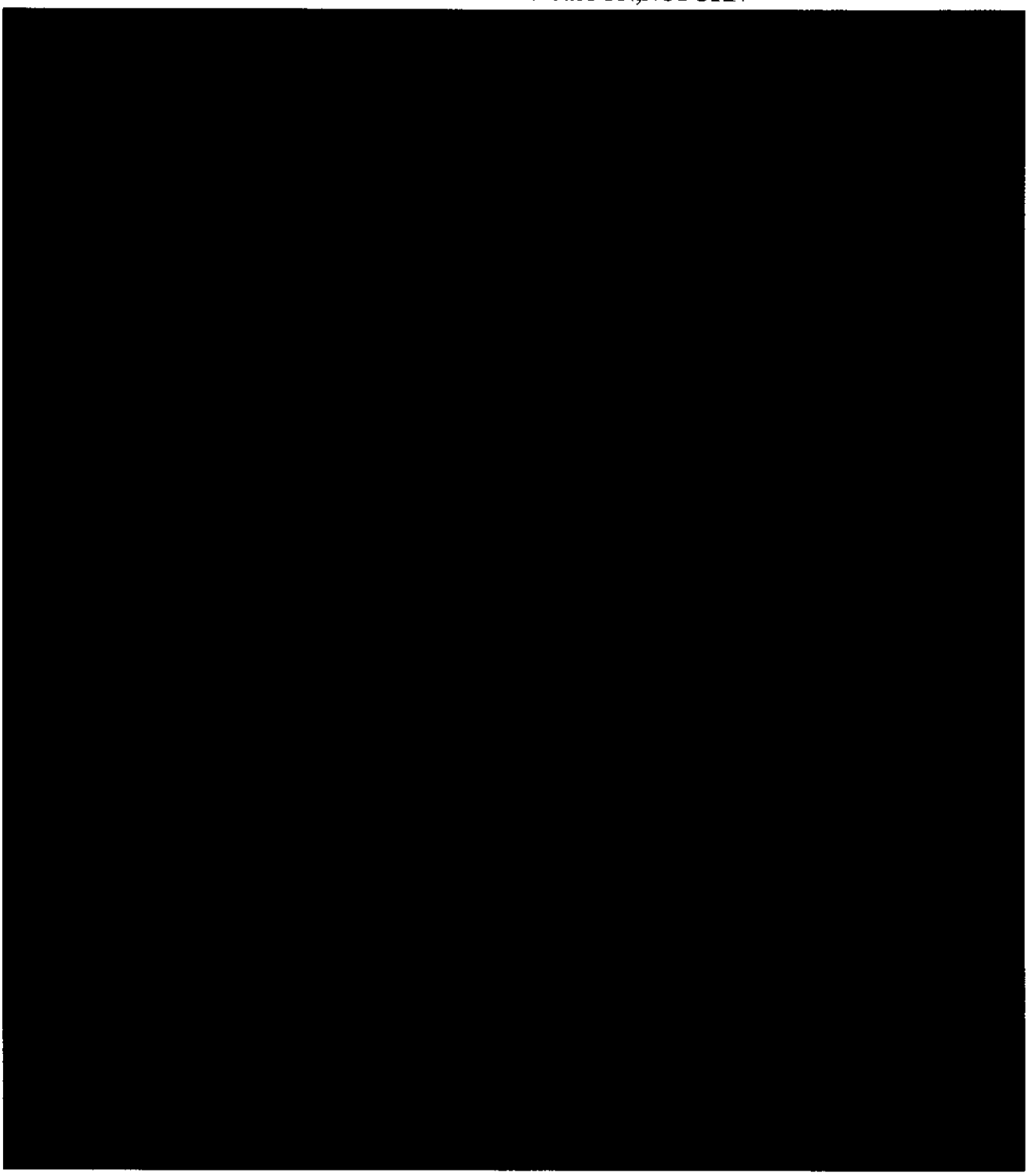
~~TOP SECRET//COMINT//ORCON,NOFORN~~



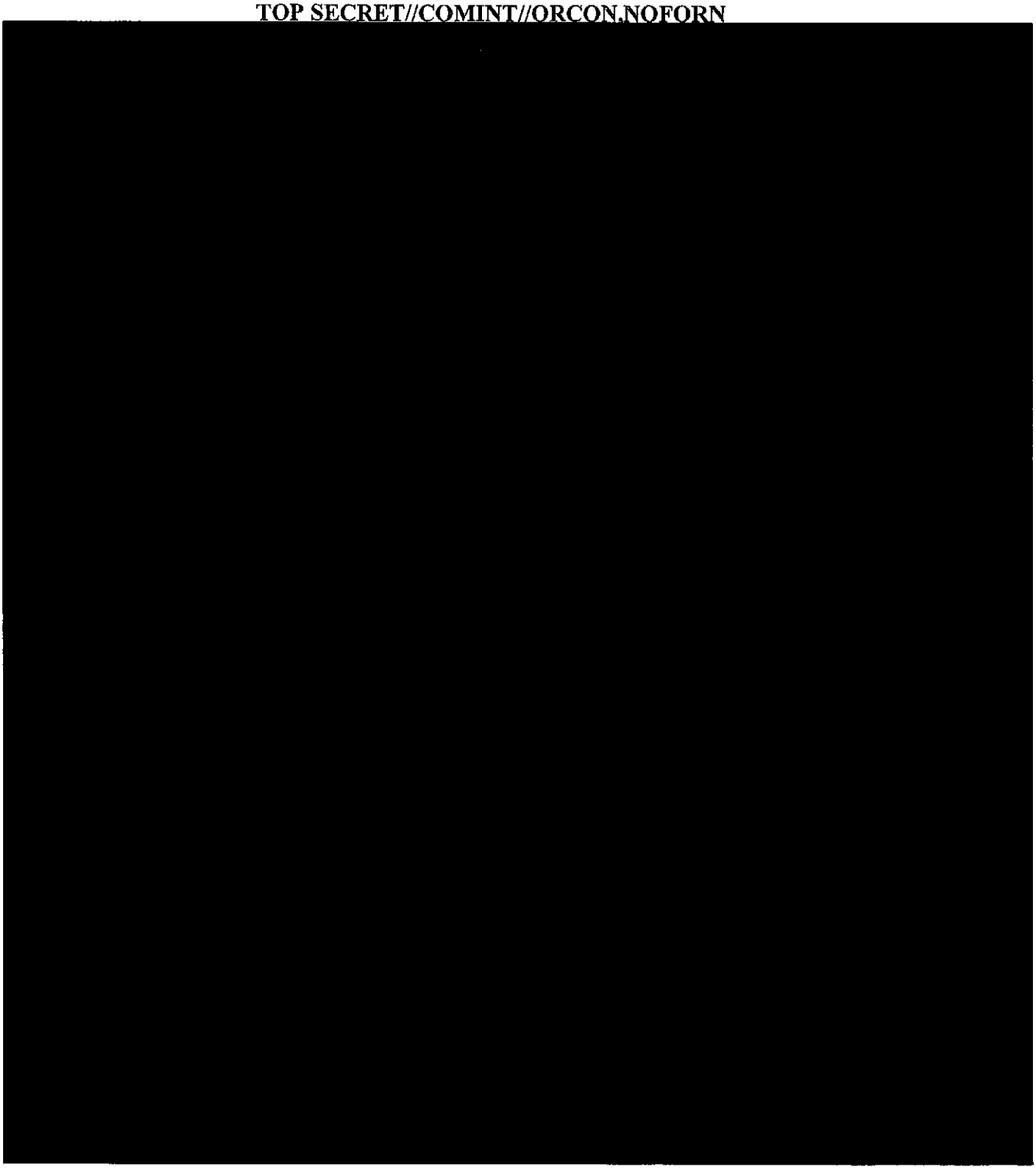
~~TOP SECRET//COMINT//ORCON,NOFORN~~



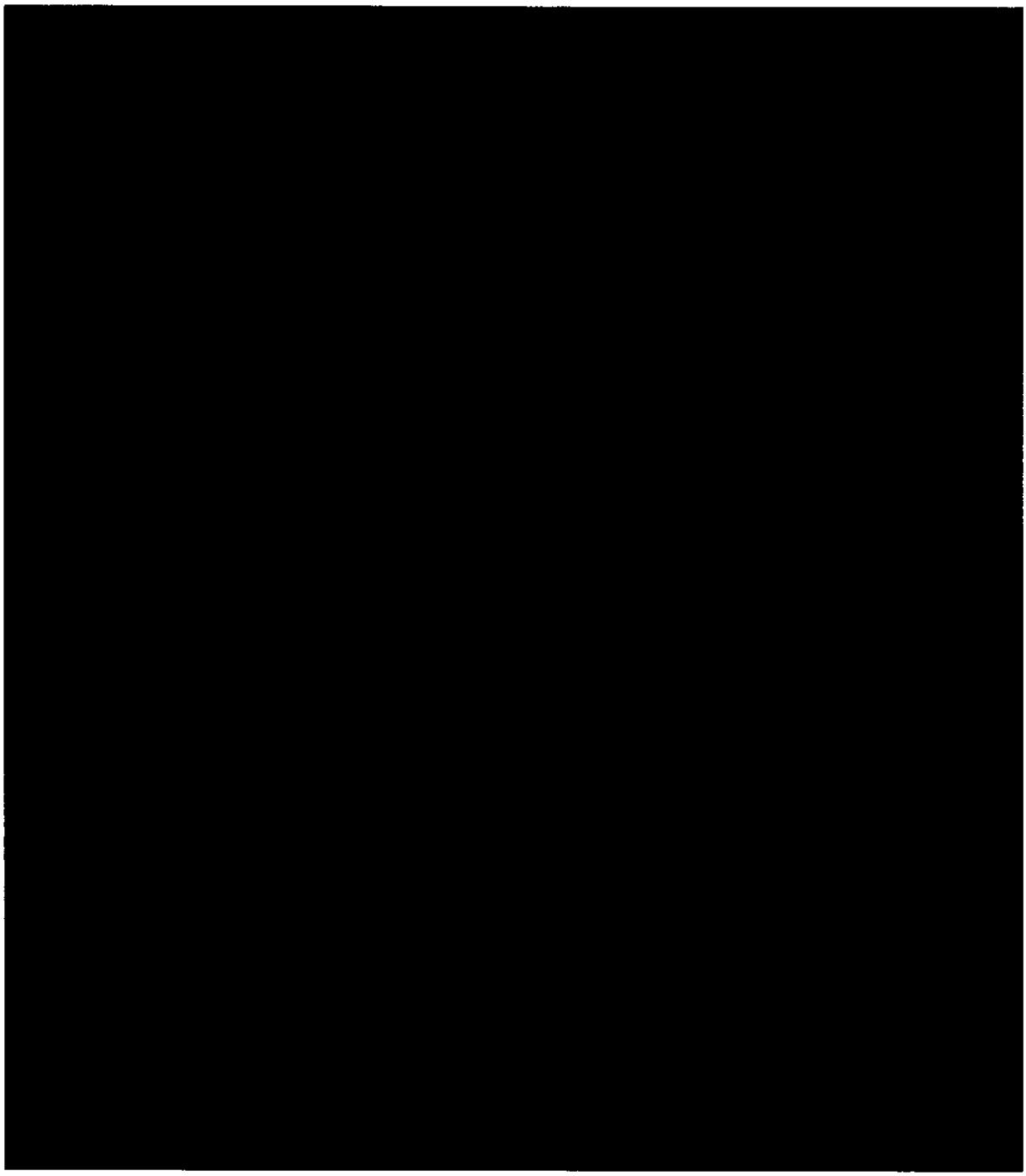
~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

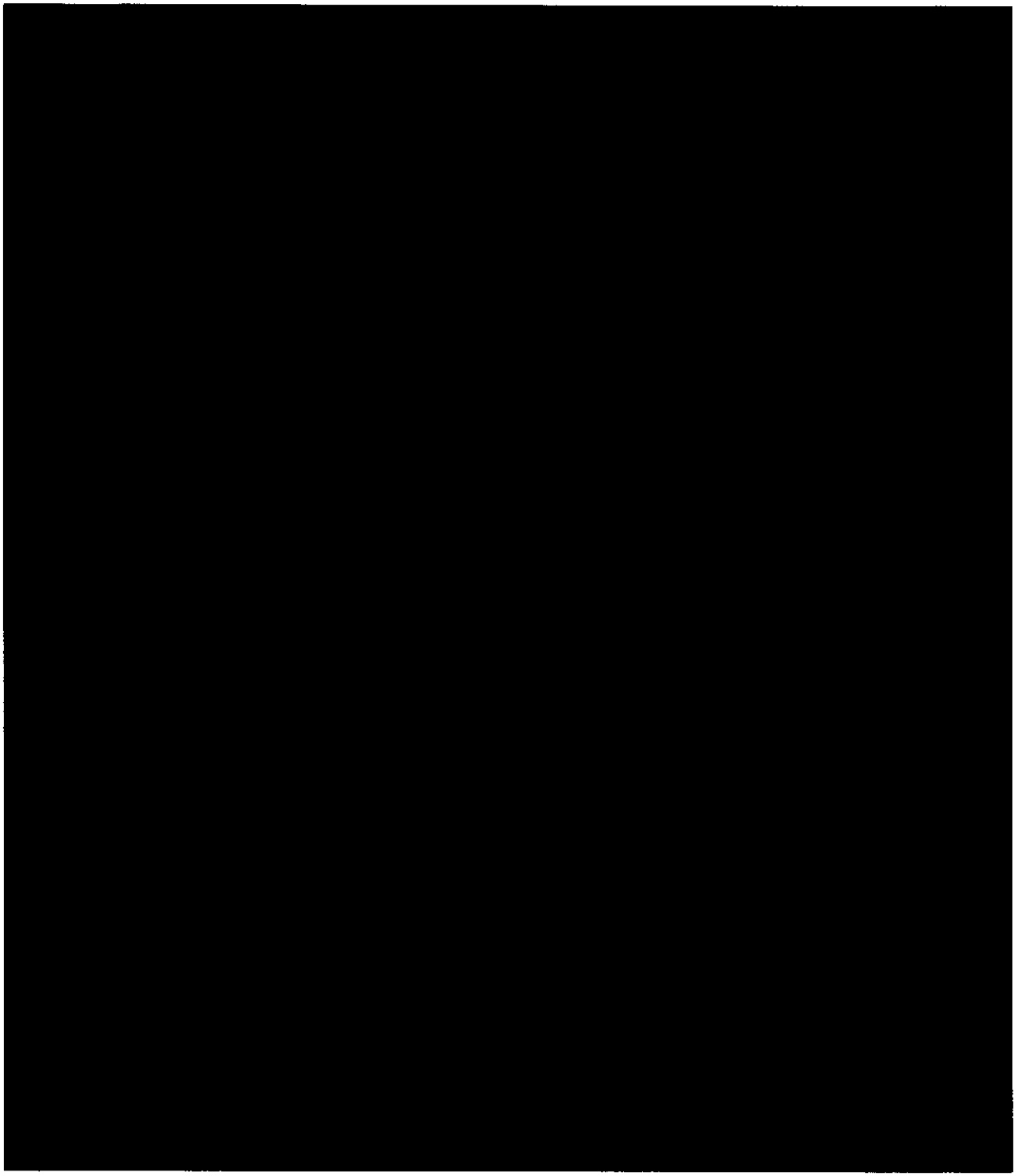


~~TOP SECRET//COMINT//ORCON,NOFORN~~

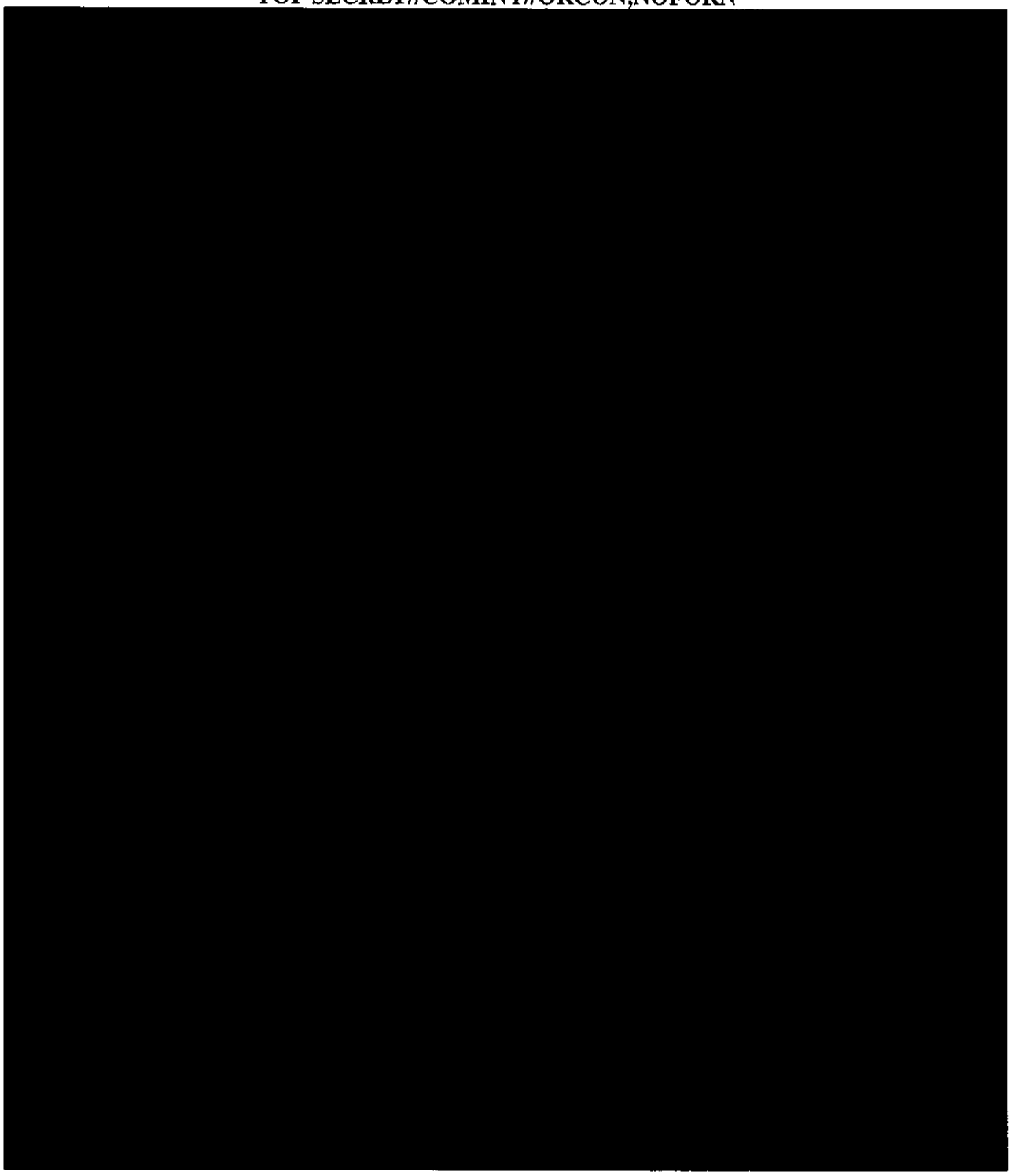


~~TOP SECRET//COMINT//ORCON,NOFORN~~

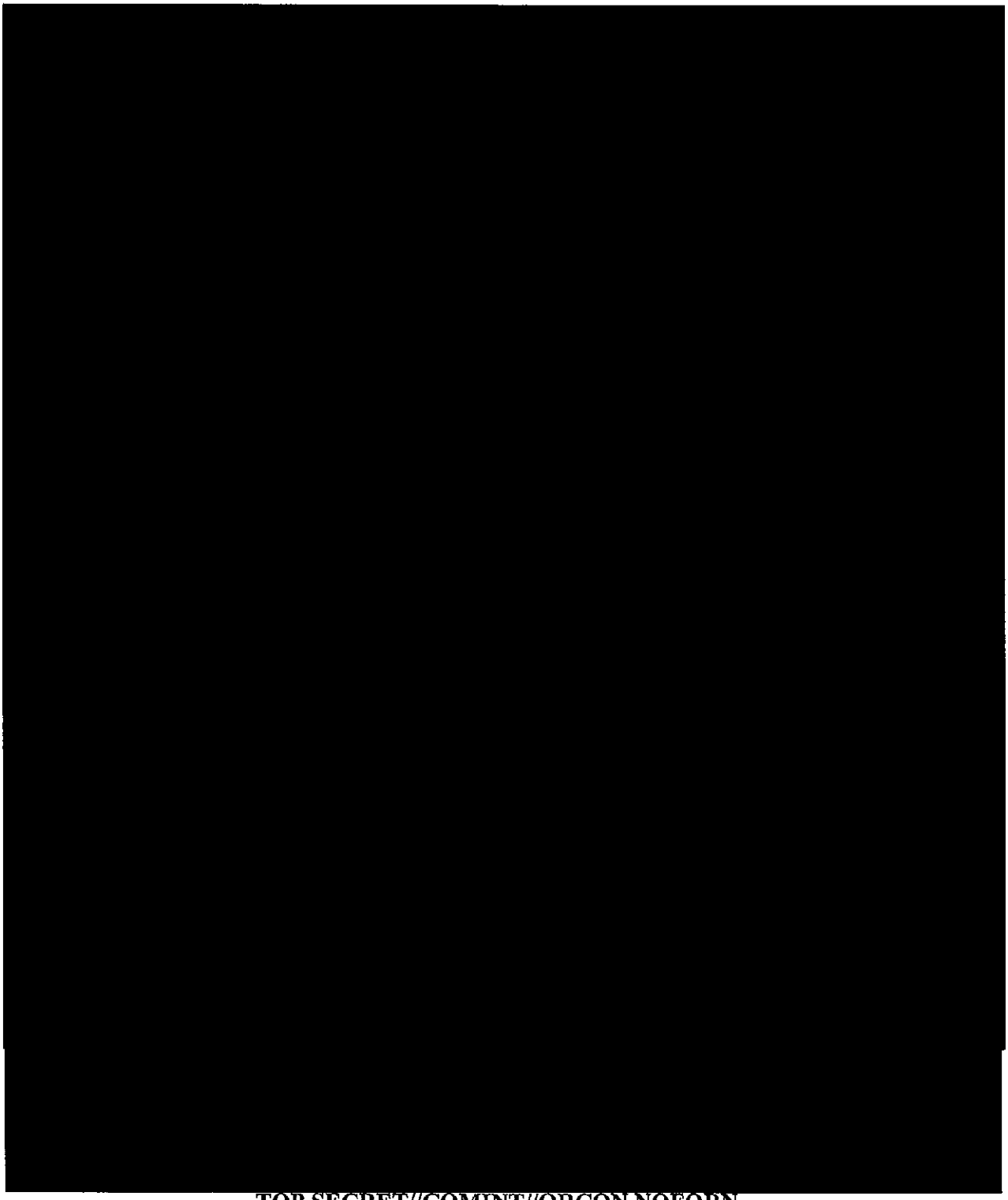
~~TOP SECRET//COMINT//ORCON,NOFORN~~



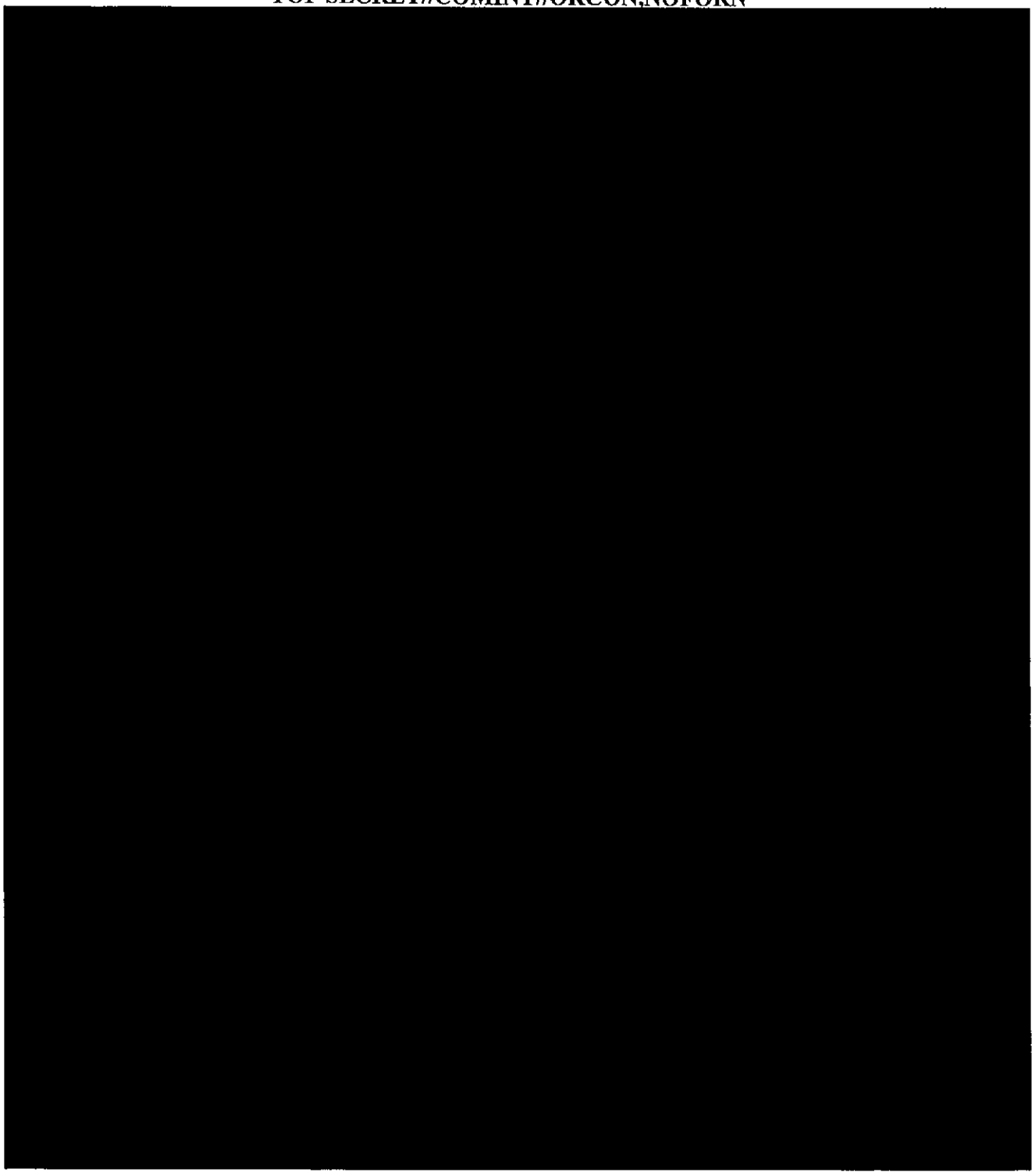
~~TOP SECRET//COMINT//ORCON,NOFORN~~



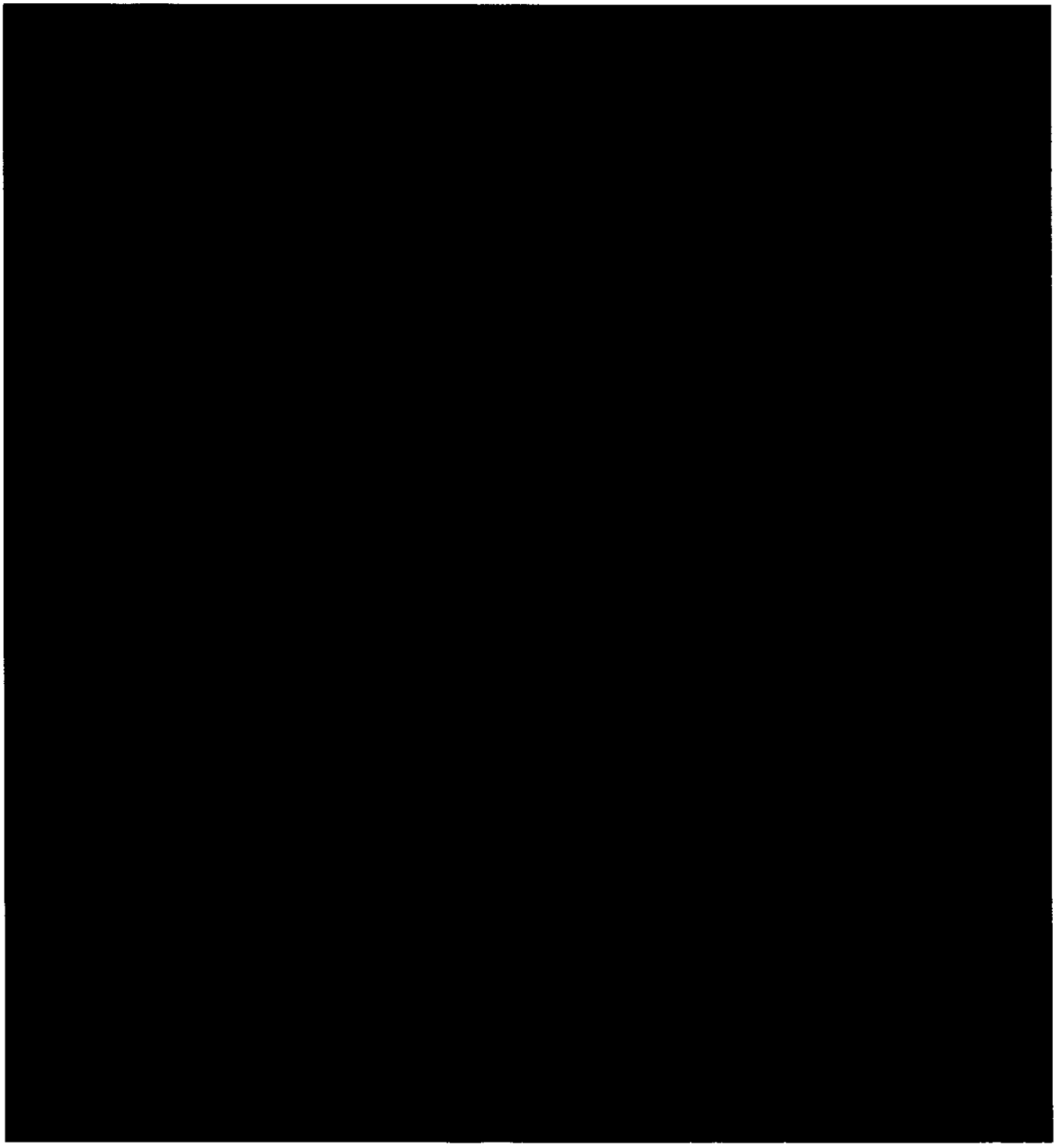
~~TOP SECRET//COMINT//ORCON,NOFORN~~



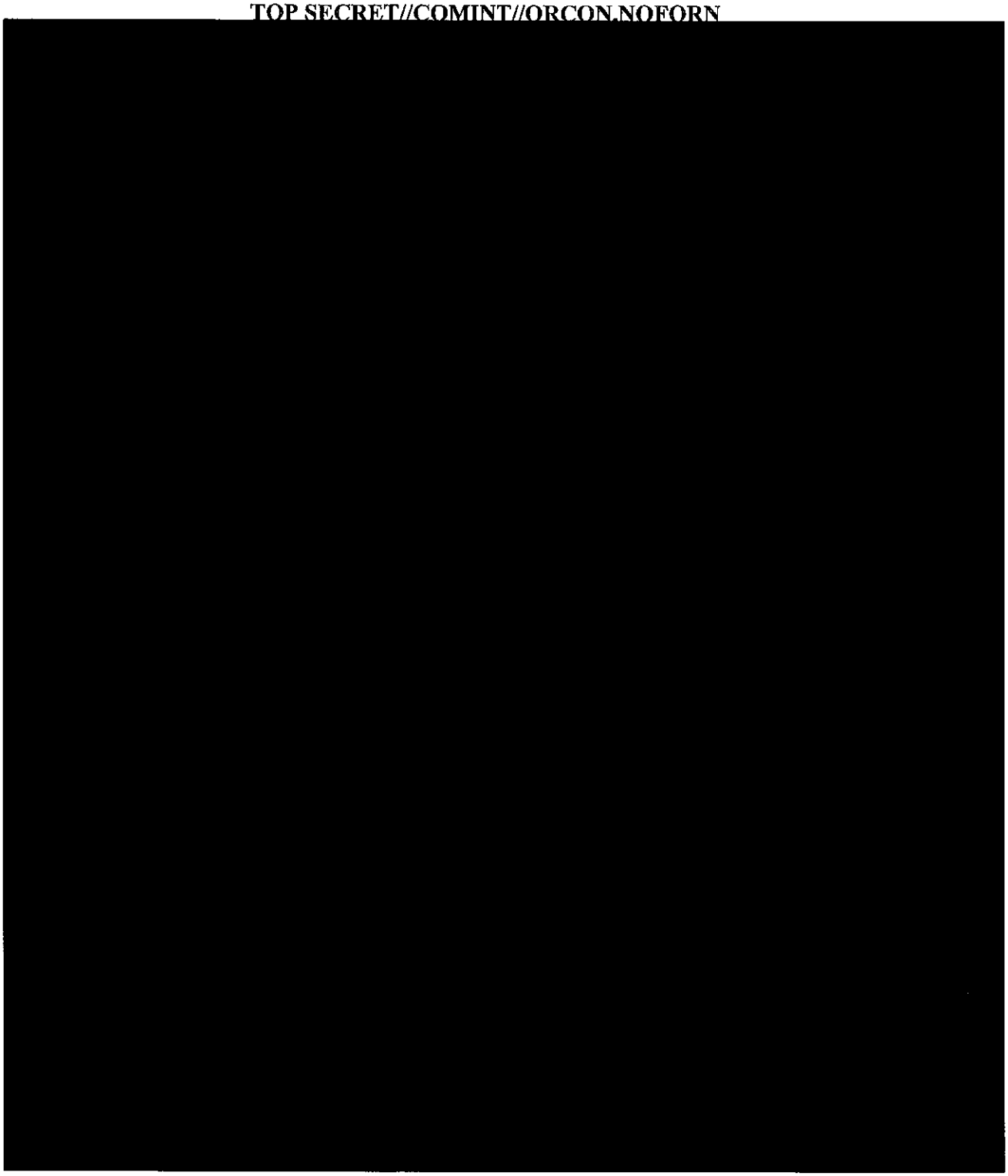
~~TOP SECRET//COMINT//ORCON,NOFORN~~



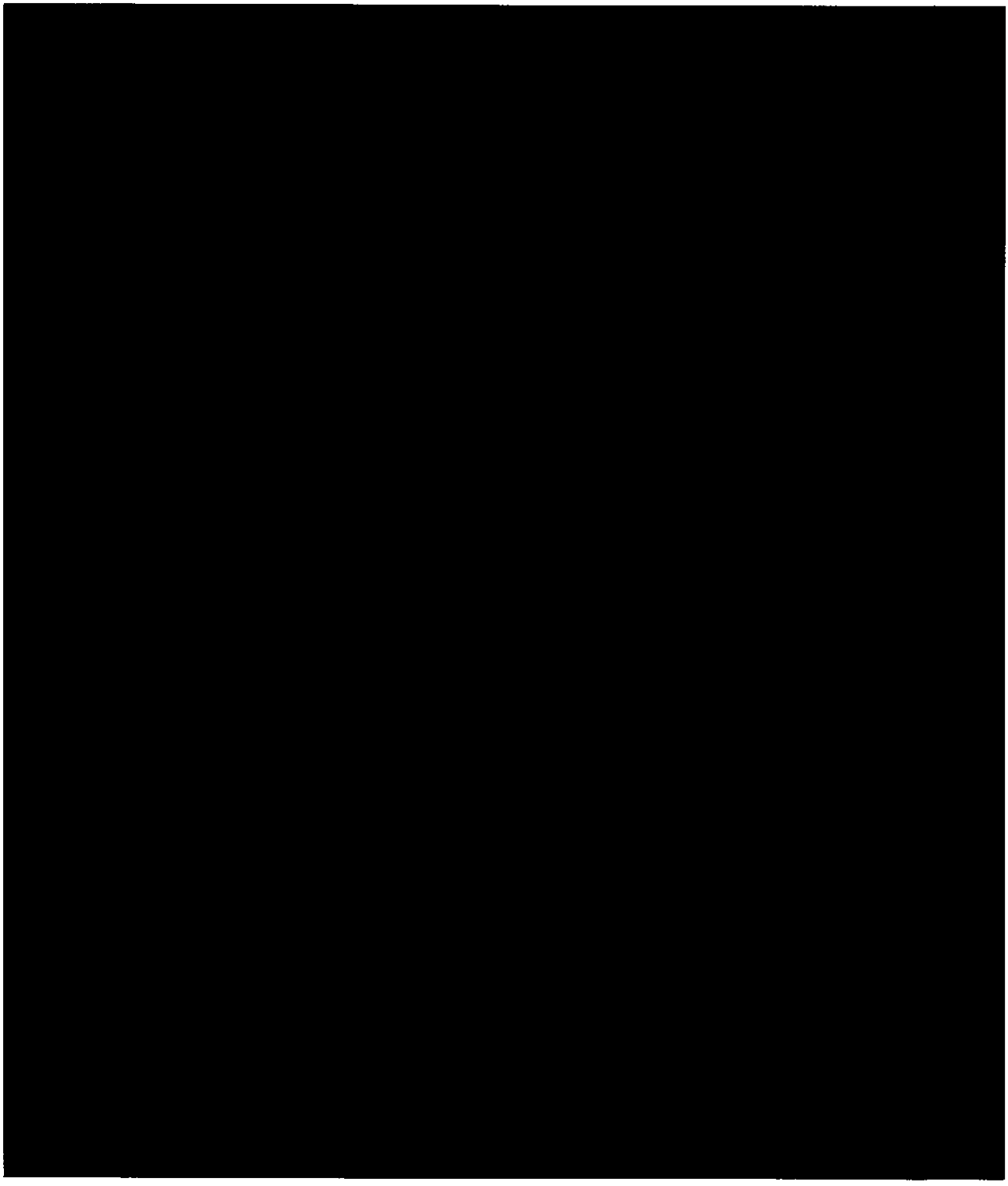
~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

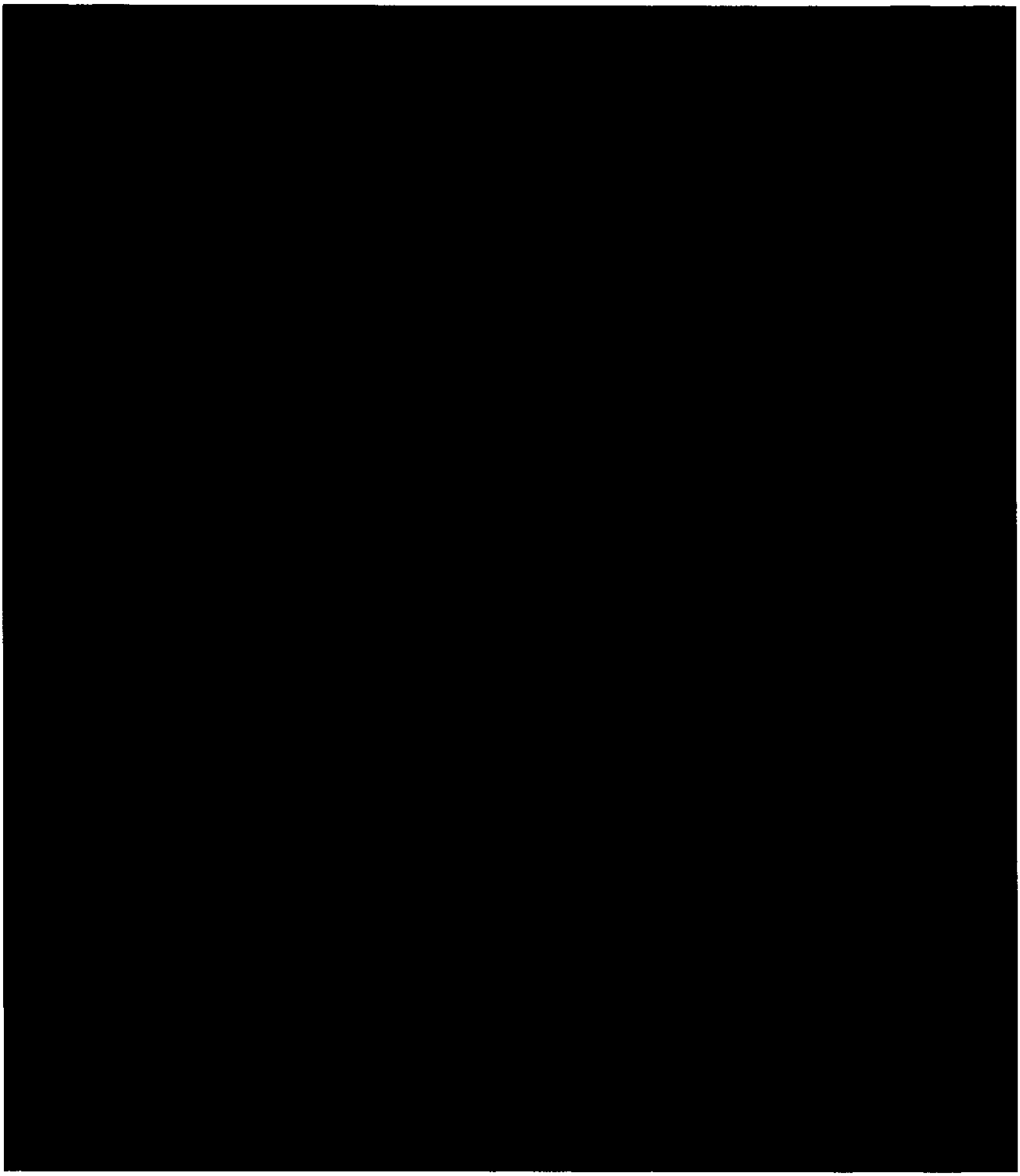


~~TOP SECRET//COMINT//ORCON,NOFORN~~



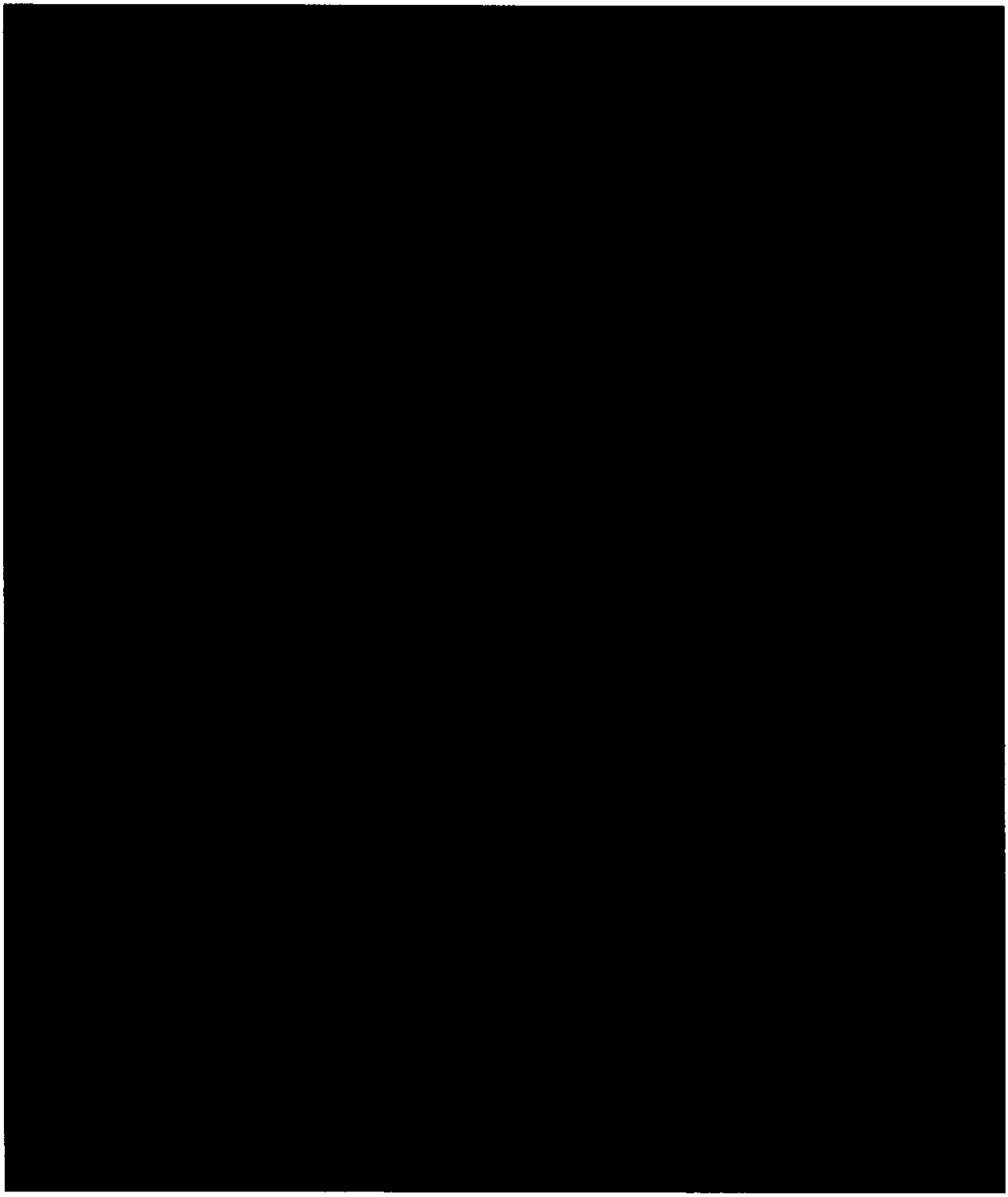
~~TOP SECRET//COMINT//ORCON,NOFORN~~

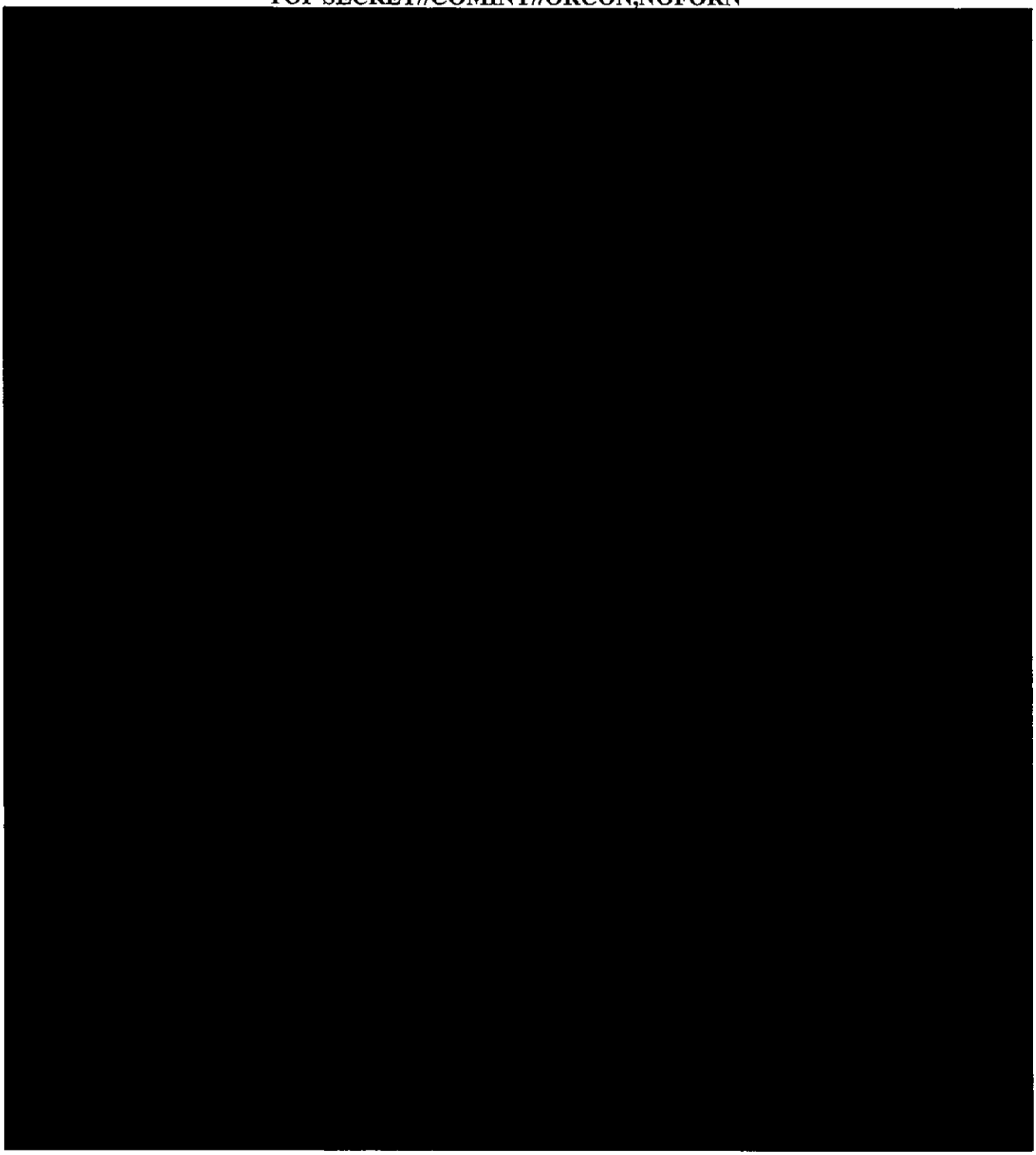
~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~





[redacted]

Within the definitions of "pen register" and "trap and trace device," "signaling information" appears as the fourth and final item in a list of undefined terms that all modify "information": "dialing, routing, addressing, [and/or] signaling information." 18 U.S.C. § 3127(3), (4). It is well-established in statutory interpretation that one term appearing within a list may take its meaning from the character of the other listed terms.[47] Here, the other three terms modifying "information" are not merely "associated with" a communication. Rather, dialing, routing, and addressing information are all types of information that, in the context of a

[redacted]

[47] See, e.g., Dolan v. United States Postal Serv., 546 U.S. 481, 486-87 (2006) ("'[A] word is known by the company it keeps' – a rule that 'is often wisely applied where a word is capable of many meanings in order to avoid the giving of unintended breadth to the Acts of Congress.'") (quoting Jarecki v. G.D. Searle & Co., 367 U.S. 303, 307 (1961)); Schreiber v. Burlington Northern, Inc., 472 U.S. 1, 8 (1985) (recognizing the "'familiar principle of statutory construction that words grouped in a list should be given related meaning'") (quoting Securities Indus. Ass'n v. Board of Governors, 468 U.S. 207, 218 (1984)).

communication, particularly relate to the transmission of the communication to its intended party. By placing "signaling" within the same list of types of communication-related information, Congress presumably intended "signaling information" likewise to relate to the transmission of a communication.

The wording of a related provision lends further support to this interpretation:

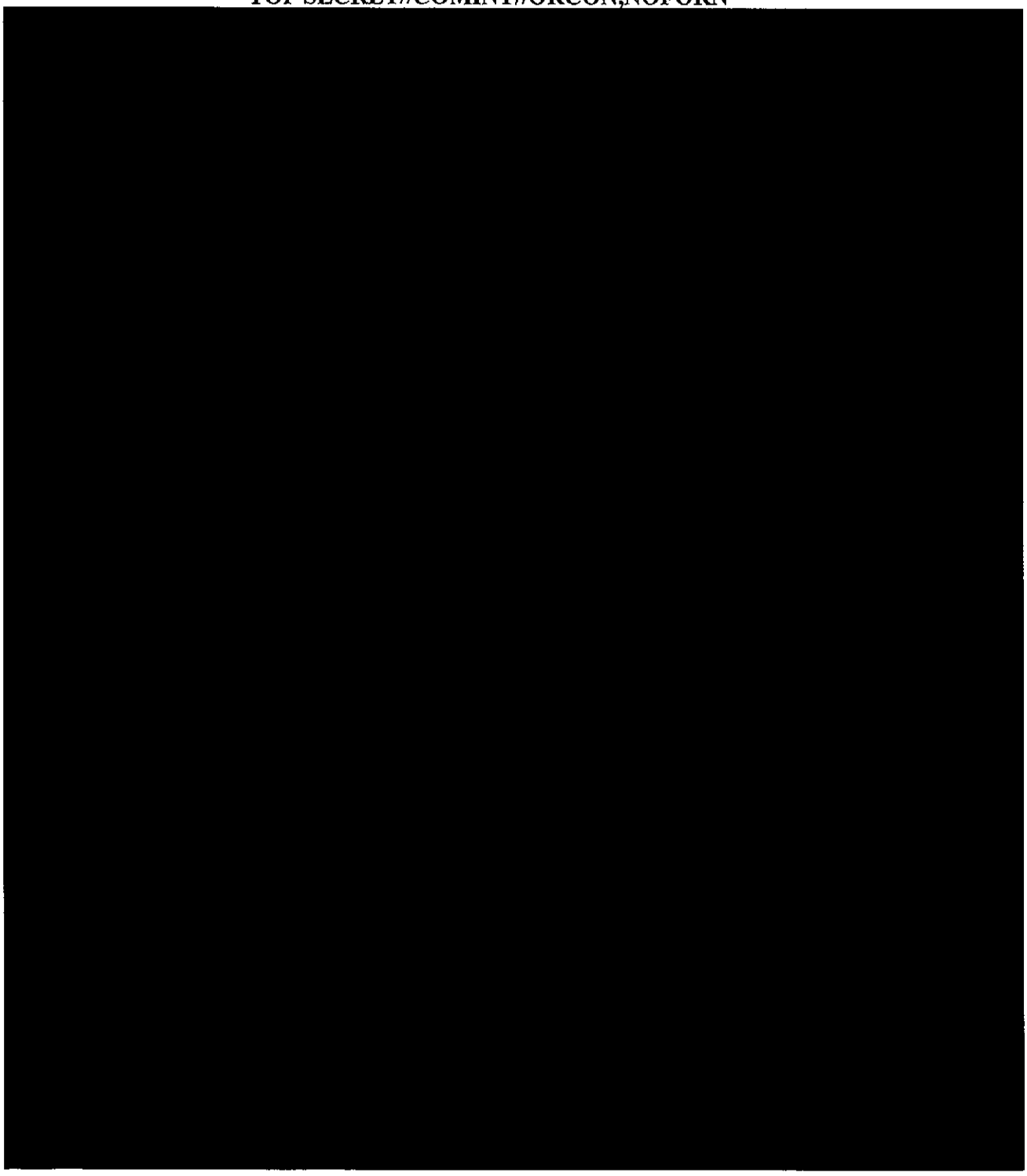
> A government agency authorized to install and use a pen register or trap and trace device . . . shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.

18 U.S.C. § 3121(c) (emphasis added). Questions of available technology aside, there is no reason to think Congress intended to compel an agency deploying a PR/TT device to try to avoid acquiring data that would constitute DRAS information under the definitions of "pen register" and "trap and trace device." For this reason, Section 3121(c) strongly suggests that the intended scope of acquisition under a PR/TT device is DRAS information utilized in the processing and transmitting of a communication.[48]

[redacted]

The legislative history relied on by the government, see Memorandum of Law at 52, actually points to a similar conclusion about the intended scope of signaling information to be acquired by a PR/TT device. It states that "orders for the installation of [PR/TT] devices may obtain any non-content information – 'dialing, routing, addressing, and signaling information' – utilized in the processing or transmitting of wire and electronic communications." H.R. Rep. No. 107-236(I), at 53 (emphasis added; footnote omitted). Moreover, the particular types of information mentioned in the legislative history as DRAS information that may be collected by a PR/TT device all pertain to the processing or transmitting of a communication. See, e.g., id. (referencing "attempted connections," including "busy signals" and "packets that merely request a telnet connection in the Internet context"). The House report states that "non-content information contained in the 'options field' of a network packet header constitutes 'signaling' information and is properly obtained by an authorized pen register or trap and trace device." Id. at 53 n.1. [redacted]

~~TOP SECRET//COMINT//ORCON,NOFORN~~



[redacted]

b. Contents

As noted above, "contents," "when used with respect to any . . . electronic communication, includes any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added). "Electronic communication" is also defined broadly, so that it encompasses the exchanges of information between account user and provider that are described by communications actions. And of course, the definitions of "pen register" and "trap and trace device" provide that the information acquired "shall not include the contents of any communication," Section 3127(3) & (4) (emphasis added) – unqualified language that certainly seems to include electronic communications between account users and providers. The combined literal effect of these provisions appears to be that PR/TT devices may not obtain any information concerning the substance, purport, or meaning of any communication, including those between account users and providers, and that communications actions that divulge any such information would be impermissible "contents" for purposes of a PR/TT authorization.

The government does not directly confront the statutory text on this point. It does argue, however, that an expansive, literal understanding of the prohibition on acquiring "contents" would lead to an absurd and unintended restriction on what PR/TT devices can do. Specifically, the government notes that the electronic impulses transmitted by dialing digits on a telephone

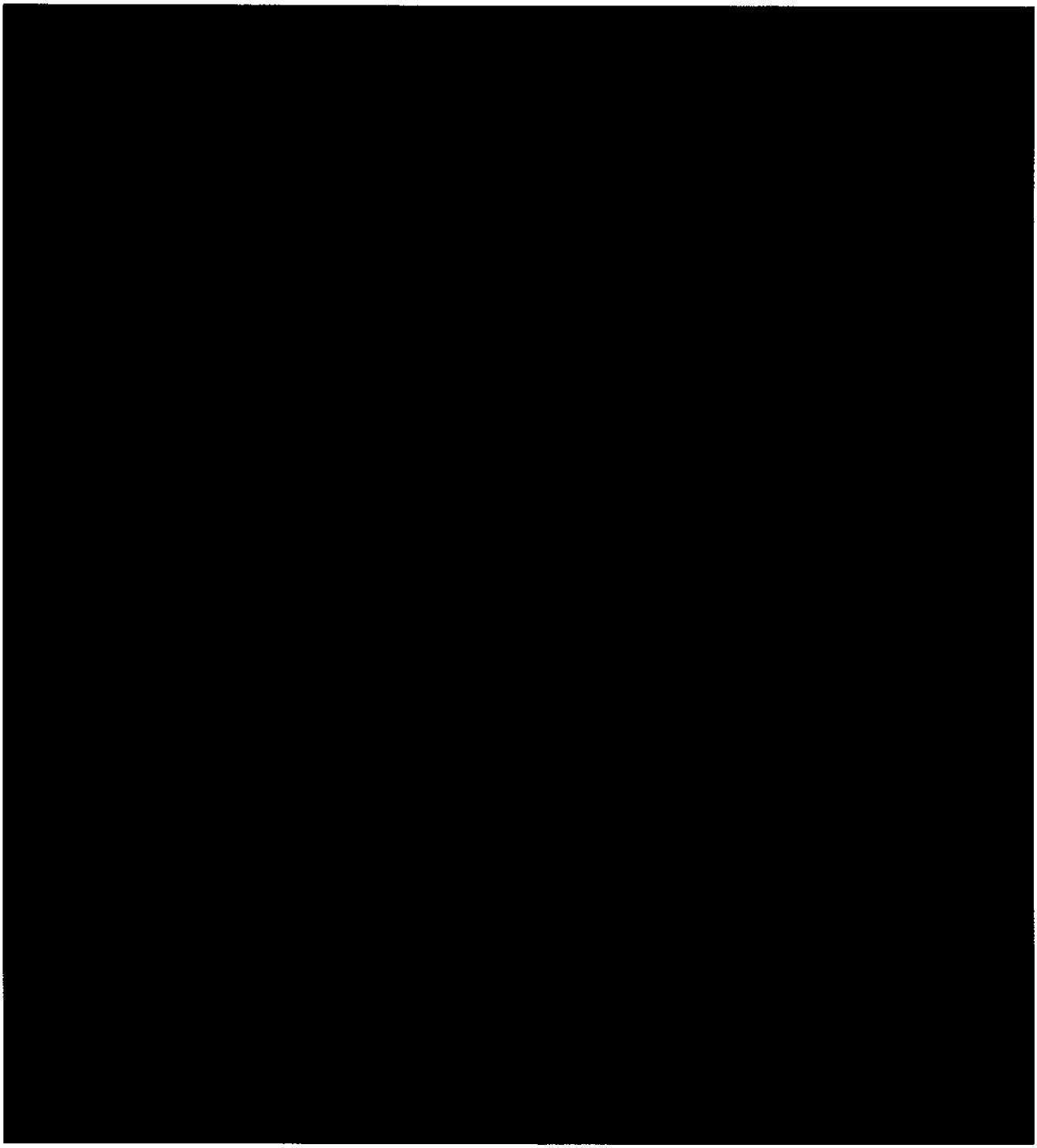
[49] The Court's understanding of "processing" and "transmitting" e-mail [redacted] is set forth below. See pages 63-64, infra.

literally qualify as an "electronic communication" under Section 2510(12), but the "import" of that communication – i.e., "place a call from this telephone to the one whose number has been dialed" – has never been understood to be impermissible "contents" under the PR/TT statute. See [redacted] Response at 7.

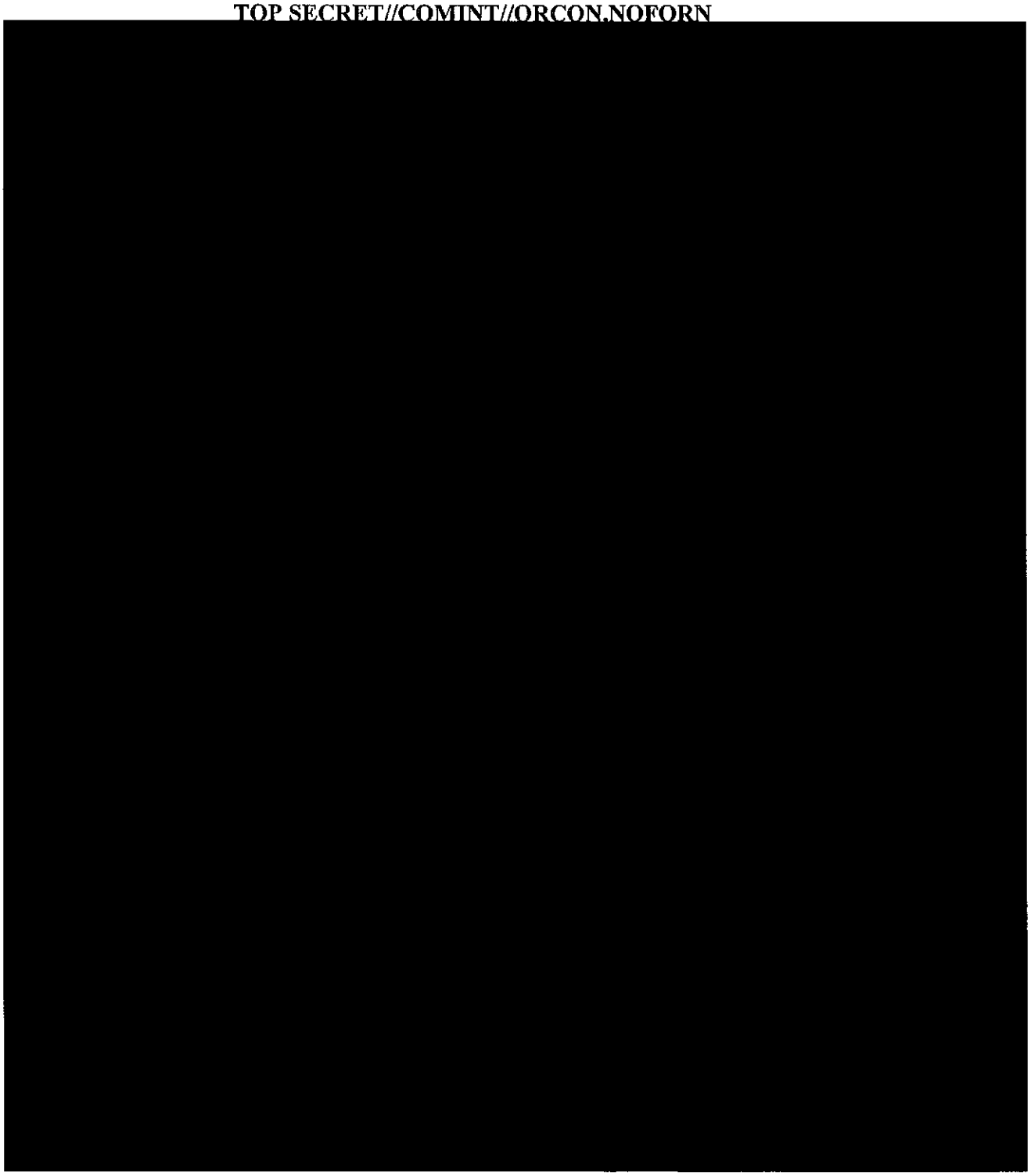
[redacted]

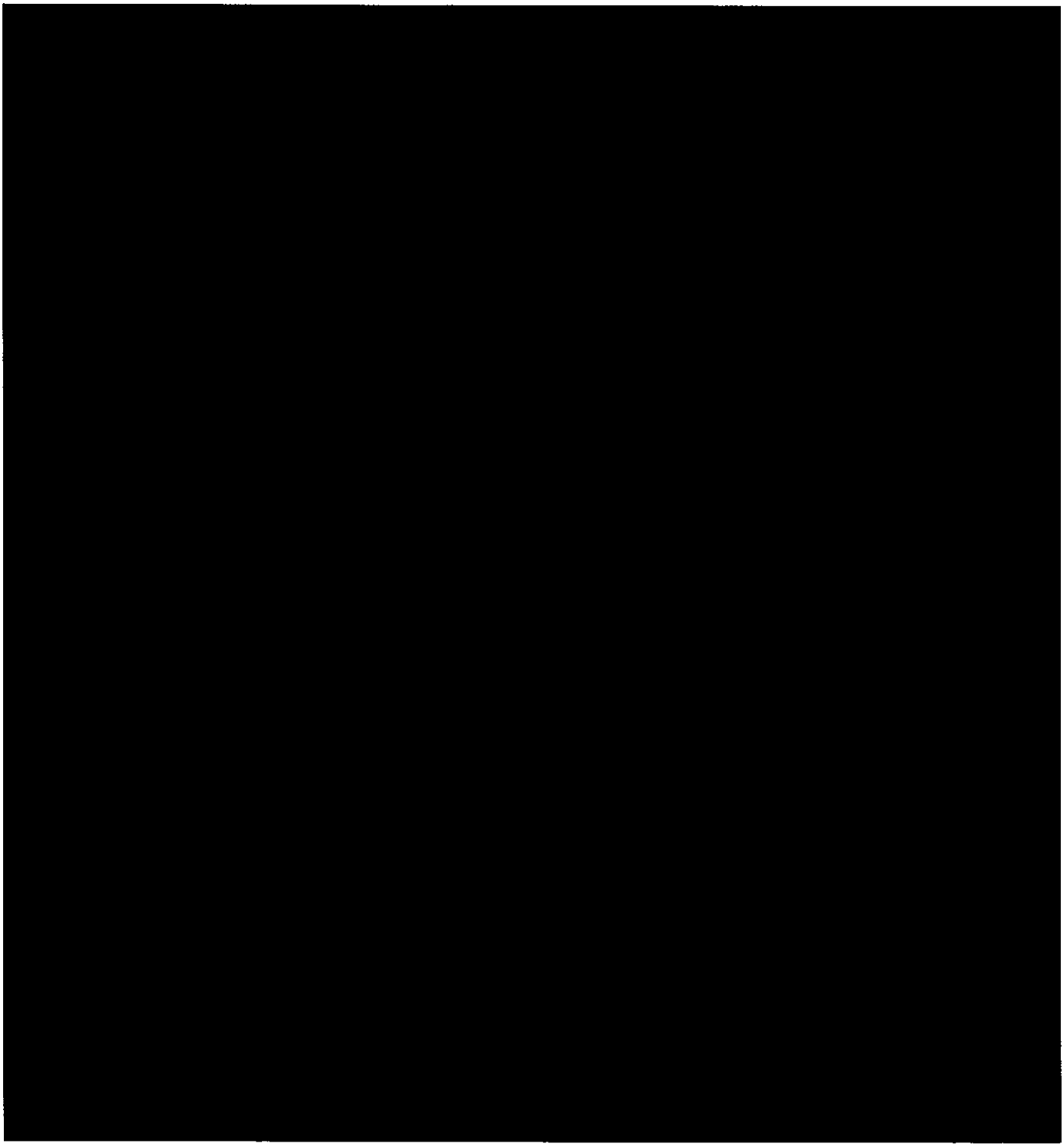
[50] While Congress sought, in the relevant statutory definitions, to reinforce "a line identical to the constitutional distinction" between contents and non-contents "drawn by the . . . Supreme Court in Smith v. Maryland, 442 U.S. 735, 741-43 (1979)," H.R. Rep. No. 107-236(I), at 53, it also expanded the "pen register" and "trap and trace" definitions to a broad range of Internet communications for which the scope of Fourth Amendment protections is unclear, see, e.g., 2 LaFave, et al. Criminal Procedure § 4.4(a) at 456-57 (the law is "highly unsettled," with "a range of different ways that courts plausibly could apply the Fourth Amendment to Internet communications").

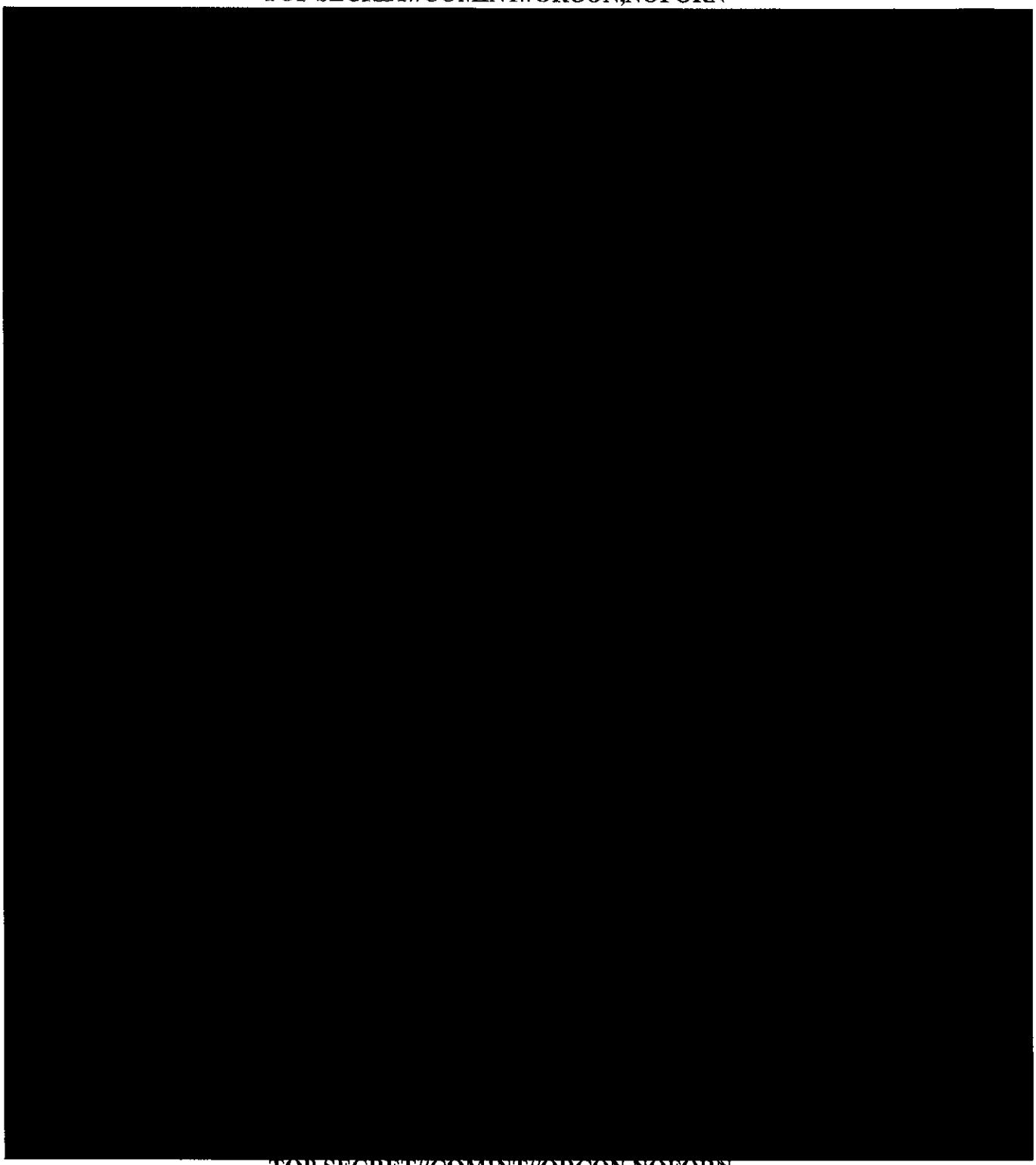
~~TOP SECRET//COMINT//ORCON,NOFORN~~



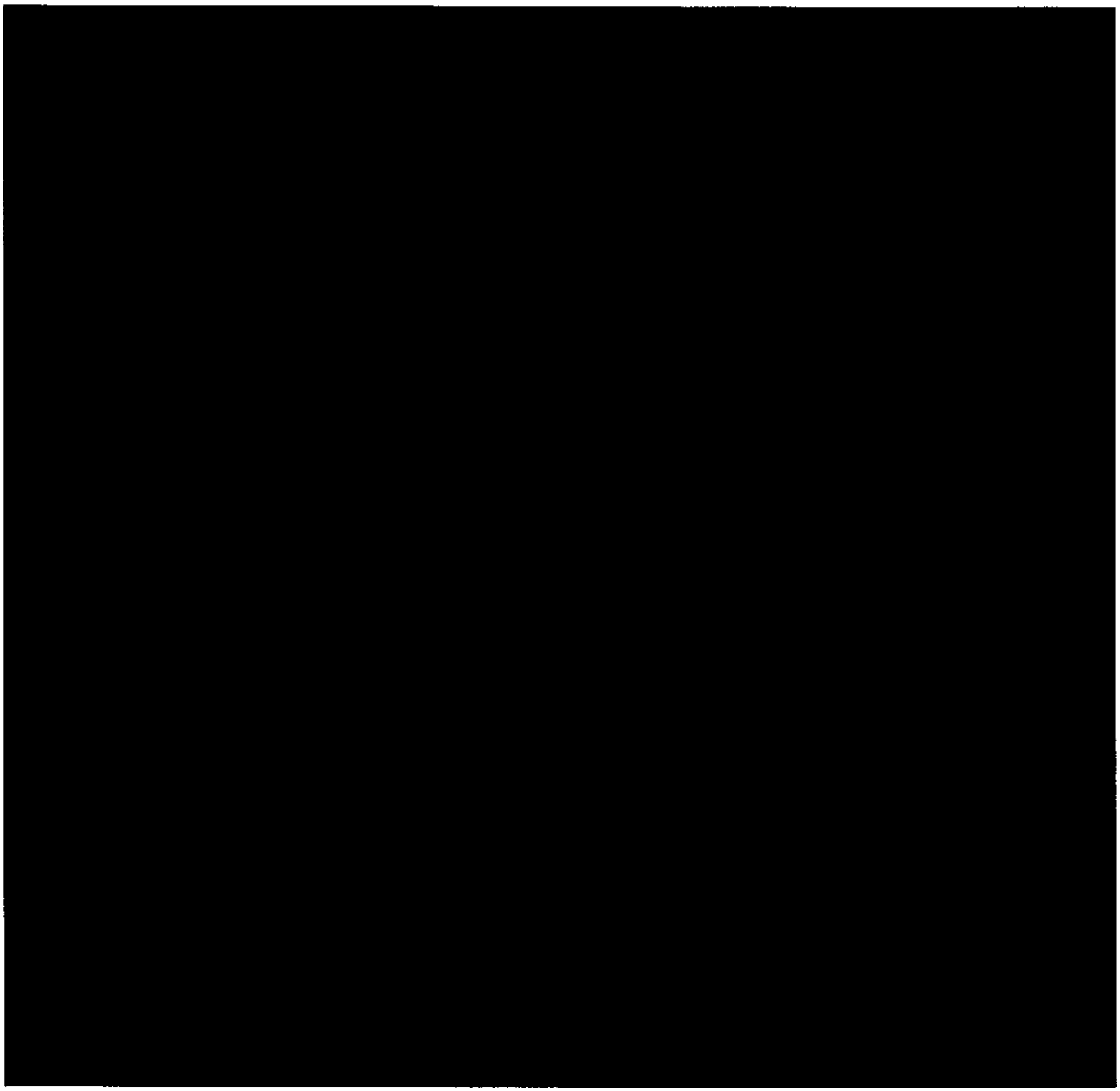
~~TOP SECRET//COMINT//ORCON,NOFORN~~





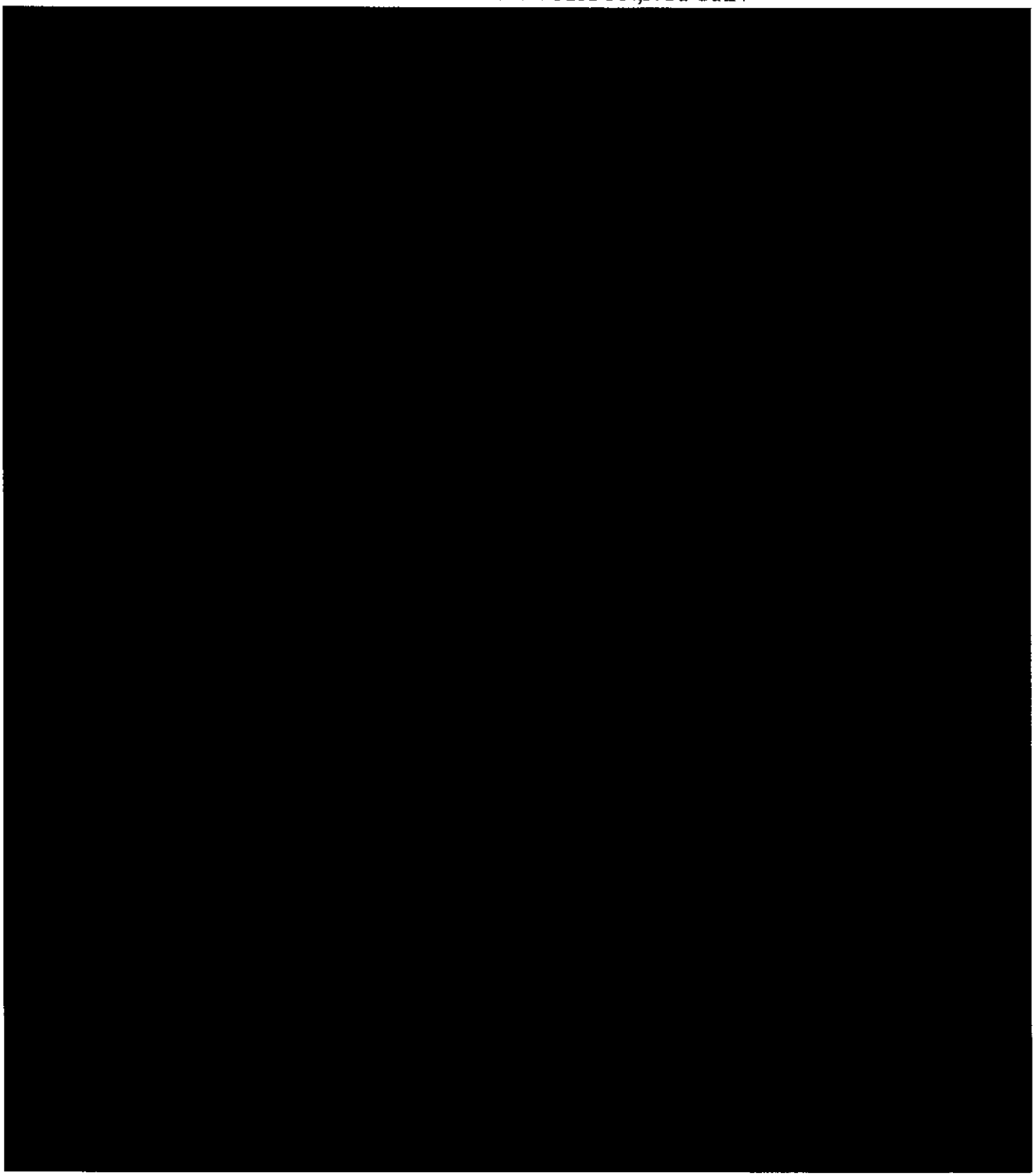


~~TOP SECRET//COMINT//ORCON,NOFORN~~



[53] See, e.g., TRW Inc. v. Andrews, 534 US. 19, 31 (2001) ("It is our duty to give effect, if possible, to every clause and word of a statute.") (citation and internal quotations omitted); accord Duncan v. Walker, 533 U.S. 167, 174 (2001).

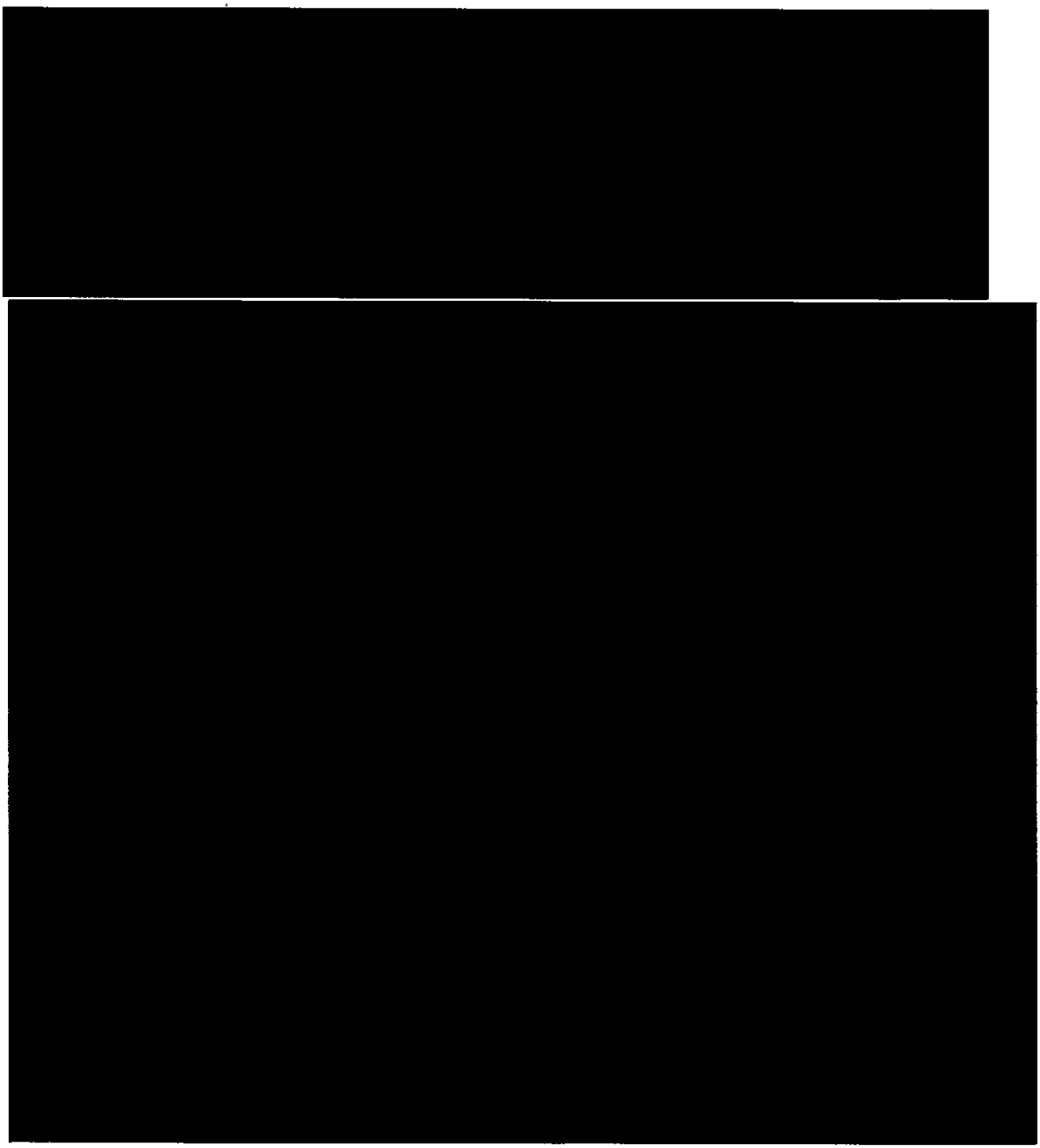
~~TOP SECRET//COMINT//ORCON,NOFORN~~



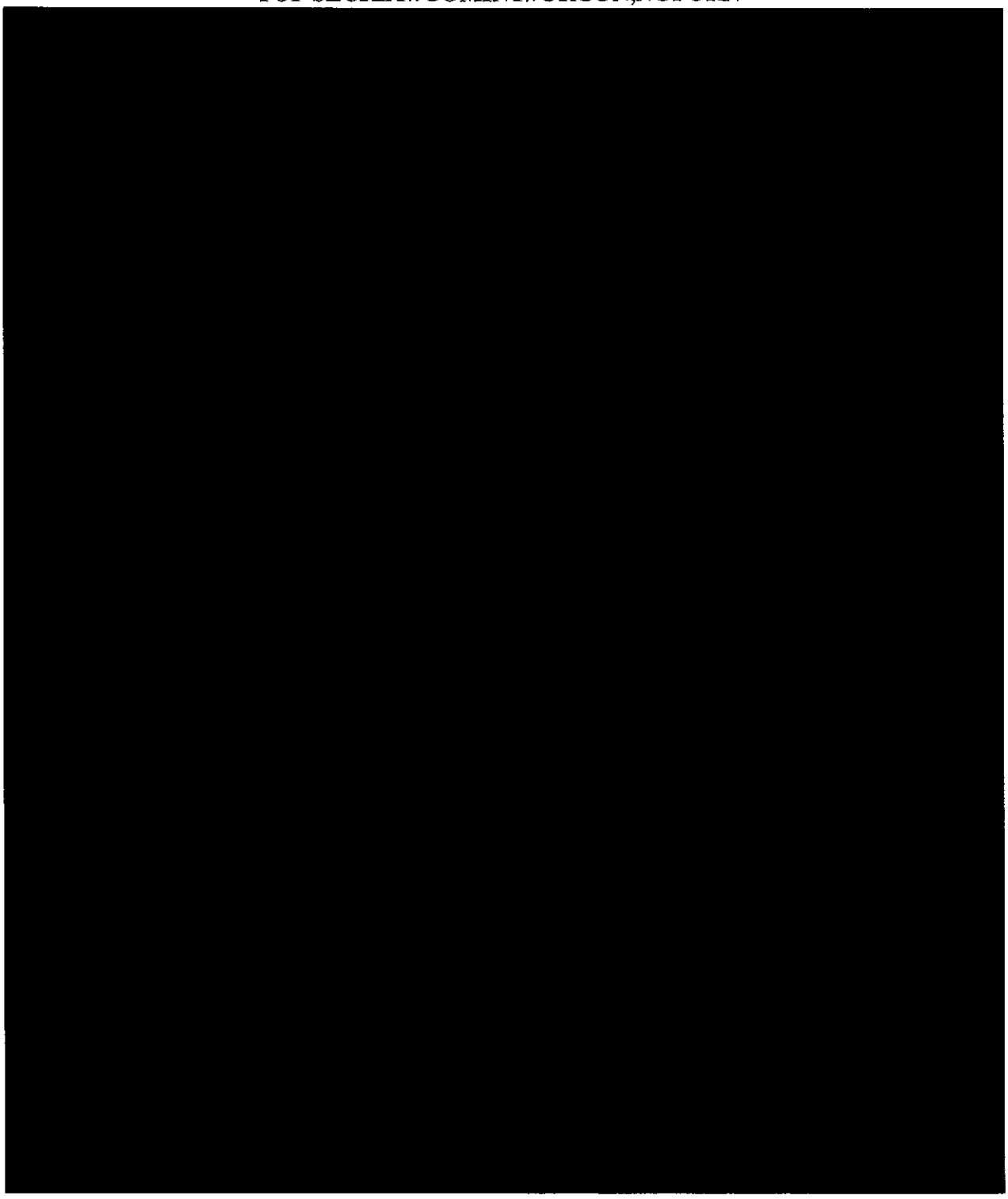
~~TOP SECRET//COMINT//ORCON,NOFORN~~

[redacted]

~~TOP SECRET//COMINT//ORCON,NOFORN~~

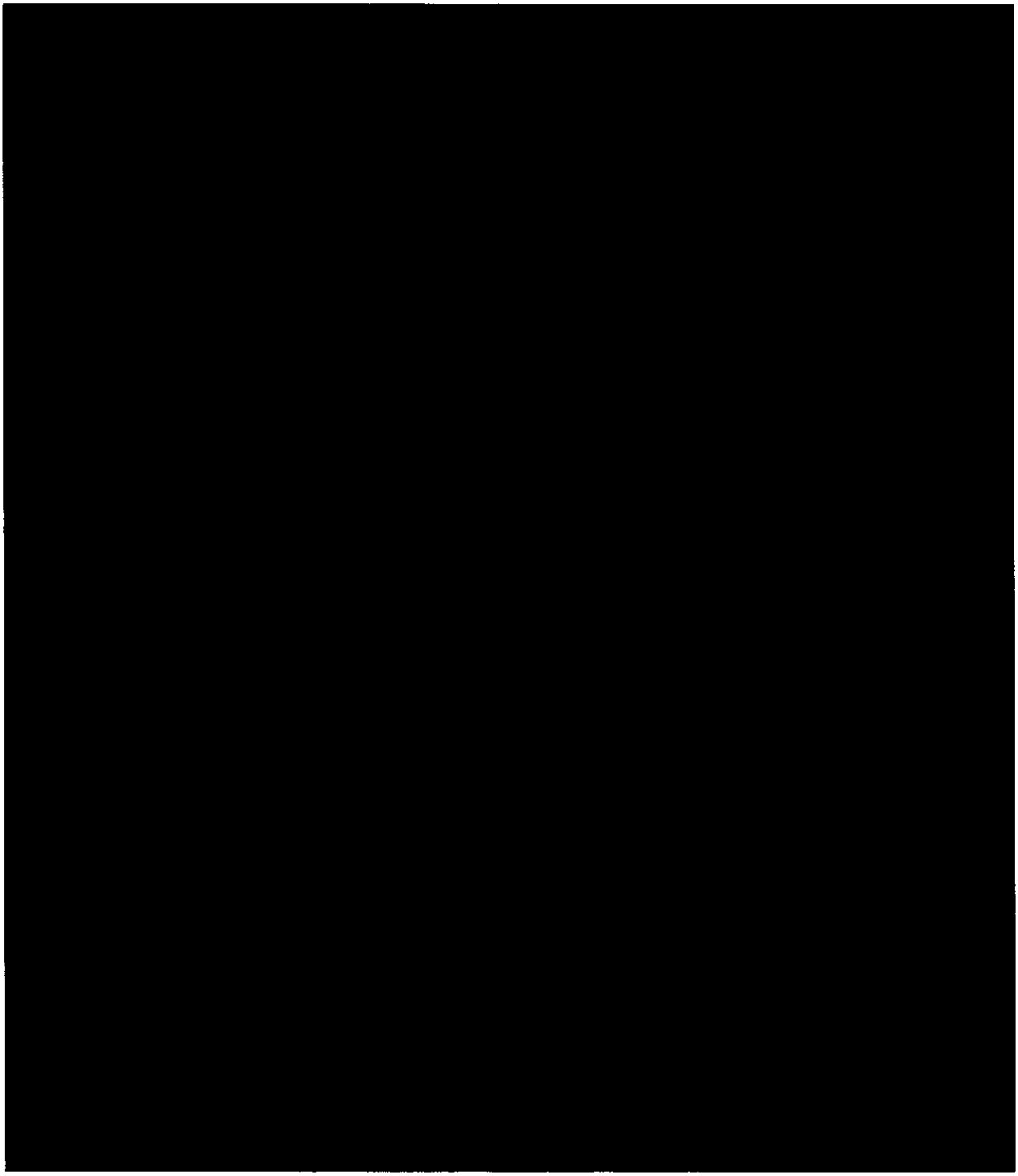


~~TOP SECRET//COMINT//ORCON,NOFORN~~



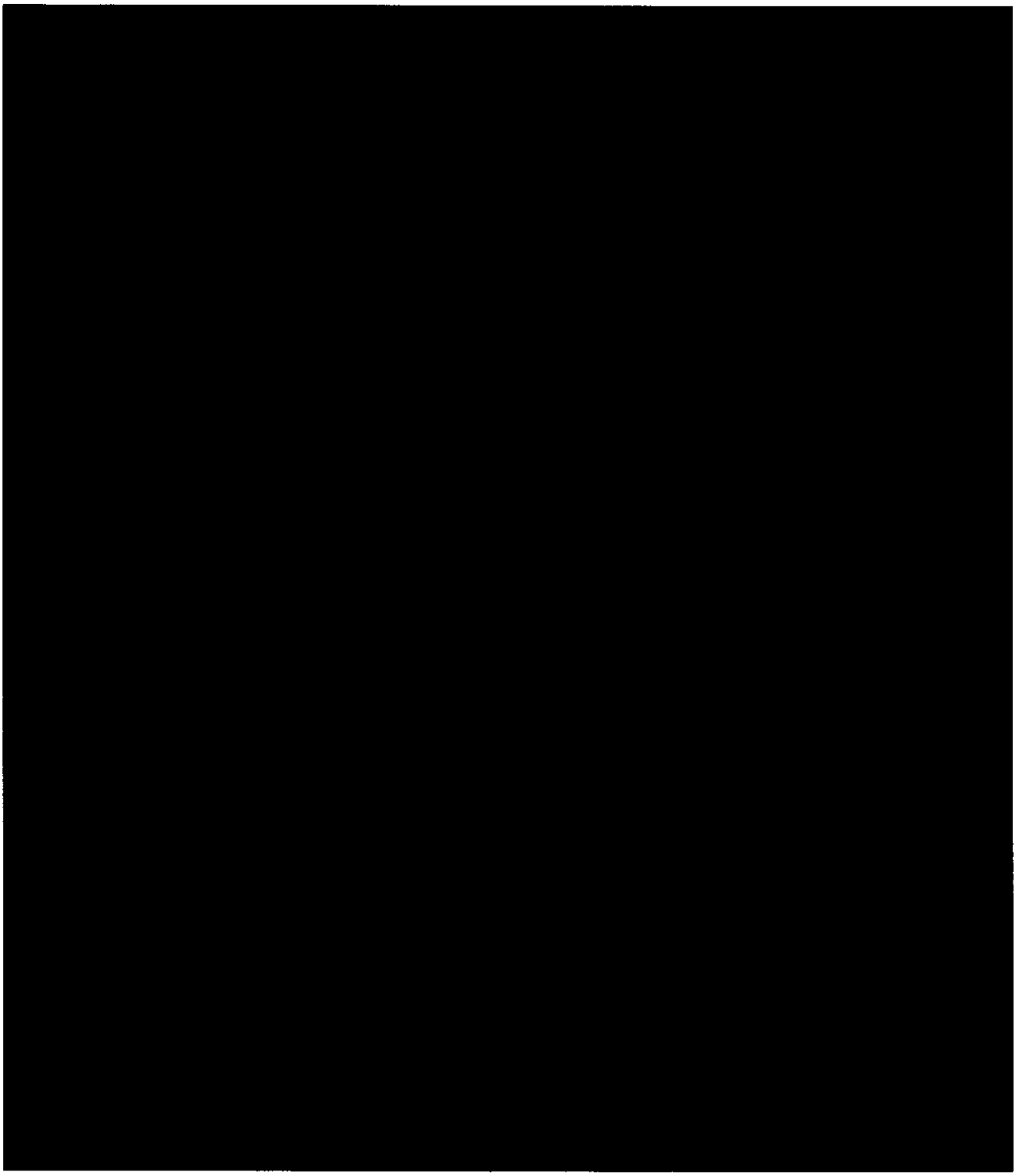
~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~



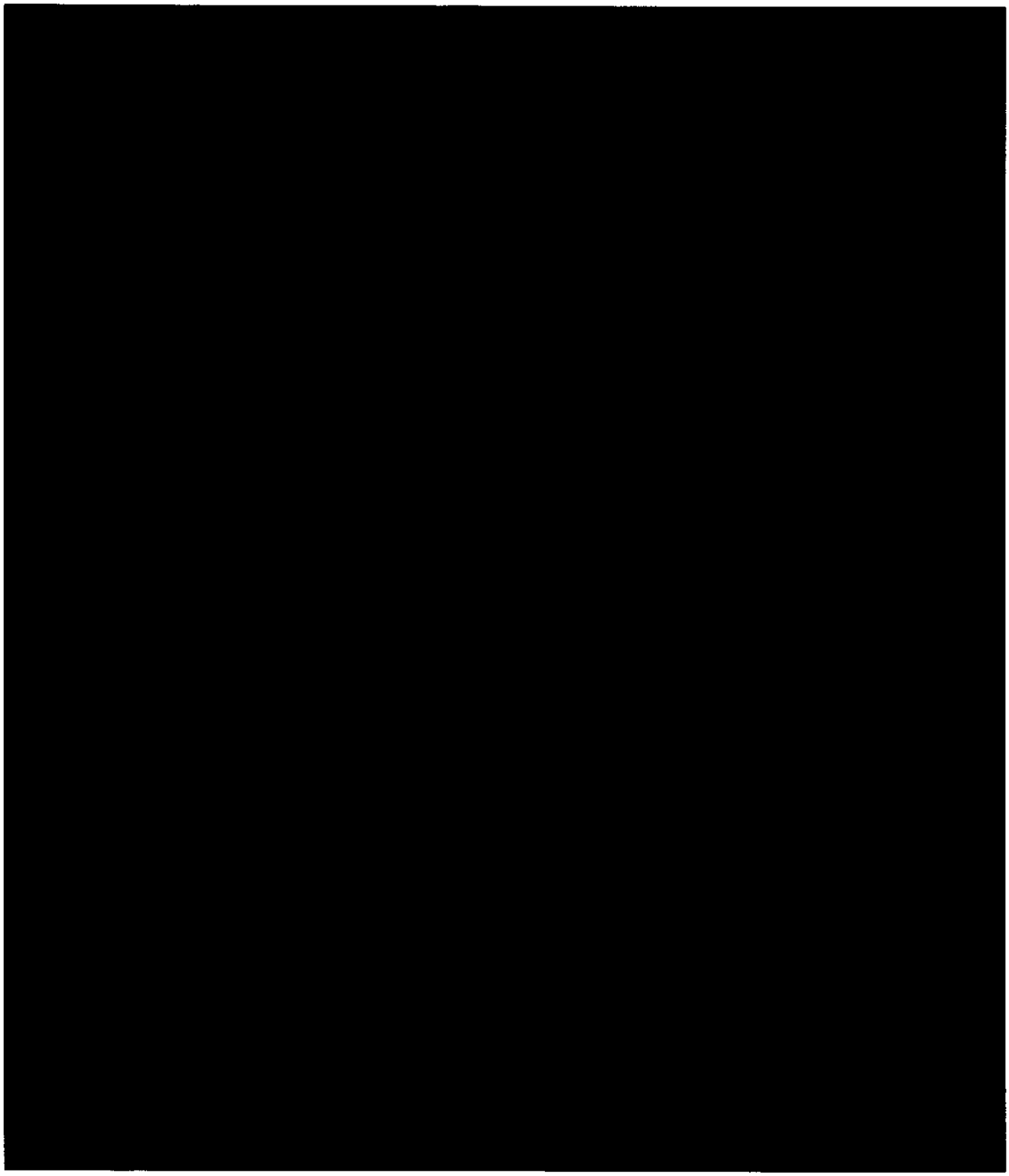
~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~



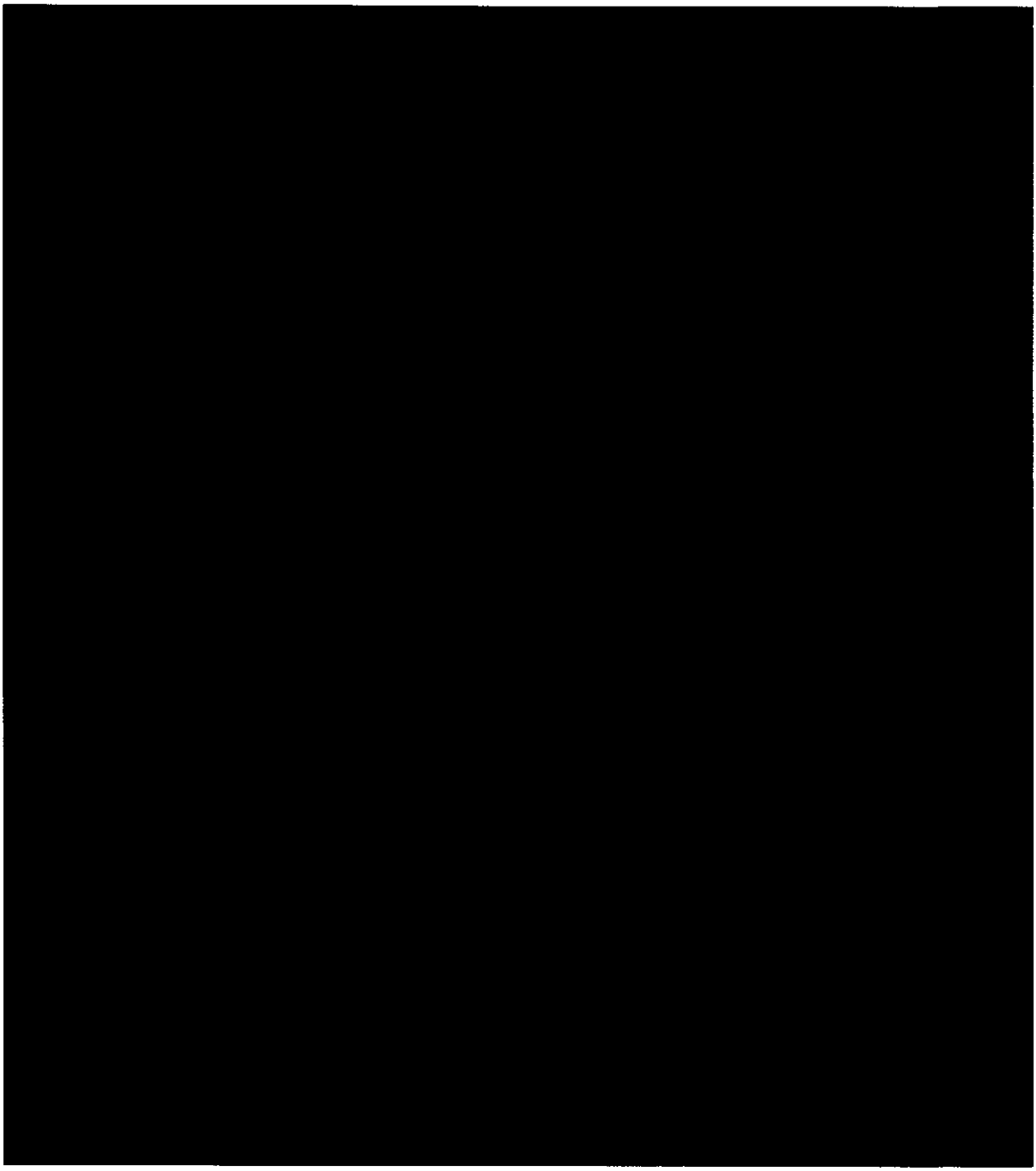
~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

~~TOP SECRET//COMINT//ORCON,NOFORN~~



The foregoing analysis has involved difficult line-drawing. But the end-results correspond well with the evident legislative purpose of permitting the acquisition of DRAS information for e-mail [redacted] while avoiding the acquisition of the contents of electronic communications, [redacted] The Court believes that this approach is necessary to ensure that the authority sought by the government [redacted] is limited to non-content signaling information properly subject to collection by a PR/TT device. Given the challenges presented by this category of metadata, the Court's authorization will be limited to the [redacted] approved above. [redacted]

III. The Application Satisfies the Applicable Statutory Requirements

A. Request to Re-Initiate and Expand Collection

The current application, in comparison with prior dockets, seeks authority to acquire a much larger volume of metadata at a greatly expanded range of facilities,[56] while also modifying

[redacted]

– and in some ways relaxing – the rules governing the handling of metadata. In the foreseeable future, NSA does not expect to implement the full scope of the requested authorization because of processing limitations. [redacted] Response at 1. Even so, NSA projects the creation of [redacted] metadata records per day during the period of the requested order, compared with the norm under prior orders of approximately [redacted] records per day. Id. That is roughly an 11- to 24-fold increase in volume.

The history of material misstatements in prior applications and non-compliance with prior orders gives the Court pause before approving such an expanded collection. The government's poor track record with bulk PR/TT acquisition, see pages 9-22, supra, presents threshold concerns about whether implementation will conform with, or exceed, what the government represents and the Court may approve. However, after reviewing the government's submissions and engaging in thorough discussions with knowledgeable representatives, the Court believes that the government has now provided an accurate description of the functioning of the [redacted] and the types of information they obtain. In addition, the Court is approving proposed modifications of the rules for NSA's handling of acquired information only insofar as they do not detract from effective implementation of protections regarding U.S. person information.

B. Relevance

The current application includes a certification by the Attorney General "that the

[redacted]

information likely to be obtained from the pen registers and trap and trace devices requested in this Application . . . is relevant to ongoing investigations to protect against international terrorism that are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution." [redacted] Application at 19. In its wording, this certification complies with the statute's requirement of a certification of relevance.[57] As explained below, the Court also finds that there is an adequate basis for regarding the information to be acquired as relevant to the terrorist-affiliated Foreign Powers that are the subject of the investigations underlying the application. See note 9, supra.[58]

As summarized above, the [redacted] Opinion's finding of relevance most crucially depended on the conclusion that bulk collection is necessary for NSA to employ analytic tools that are likely to generate useful investigative leads to help identify and track terrorist operatives. See page 9, supra. However, in finding relevance, the [redacted] Opinion also relied on

---

[57] Under FISA, a PR/TT application requires

> a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution.

50 U.S.C. § 1842(c)(2).

[58] The government again argues that the Court should conduct no substantive review of the certification of relevance. See Memorandum of Law at 29. This opinion follows Judge Kollar-Kotelly's [redacted] Opinion in assuming, without conclusively deciding, that substantive review is warranted. See note 10, supra.

NSA's efforts to acquire metadata that [redacted] See page 8, supra.[59] For purposes of assessing relevance, the primary difference between the current application and prior bulk PR/TT authorizations is that the current application encompasses a much larger volume of communications, without limiting the requested authorization to streams of data with a relatively high concentration of Foreign Power communications.[60]

There is precedent, however, for concluding that a wholly non-targeted bulk production of metadata under Section 1861 can be relevant to international terrorism investigations. In those cases, the FISC has found that the ongoing production by major telephone service providers of call detail records for all domestic, United States-to-foreign, and foreign-to-United States calls, in order to facilitate comparable forms of NSA analysis and with similar restrictions on handling and dissemination, is relevant to investigations of the Foreign Powers. See, e.g., Docket No. [redacted]

[59] As part of the relevance analysis, the [redacted] Opinion also relied on the presence of "safeguards" governing the handling and dissemination of the bulk metadata and information derived from it. The safeguards proposed in the current application are discussed below, and, as modified, the Court finds them to be adequate. See Part IV, infra.

[60] The current application also seeks to expand the categories of metadata to be acquired for each communication. The Court is satisfied that the categories of metadata described in the current application constitute directly relevant information, insofar as they relate to communications of a Foreign Power. See, e.g., [redacted] Alexander Decl. at 19-22. The metadata for other communications is relevant to the investigations of the Foreign Powers for the reasons discussed herein.

[redacted] Primary Order issued on [redacted], at 2-19.[61]

The current application similarly supports a finding of relevance for this non-targeted form of bulk acquisition of Internet metadata because it "will substantially increase NSA's ability to detect and identify the Foreign Powers and those individuals affiliated with them." [redacted] Alexander Decl. at 18. There is credible testimony that terrorists affiliated with the Foreign Powers attempt to conceal operational communications by [redacted] See id. at 9, 11. Terrorist efforts to evade surveillance, in combination with the inability to know the full range of ongoing terrorist activity at a given time, make it "impossible to determine in advance what metadata will turn out to be valuable in tracking, identifying, characterizing and exploiting a terrorist." Id. at 17-18. Analysts know that terrorists' communications are traversing Internet facilities within the United States, but "they cannot know ahead of time . . . exactly where." Id. at 18. And, if not captured at the time of transmission, Internet metadata may be "lost forever." Id. For these reasons, bulk collection of metadata is necessary to enable retrospective analysis, which can uncover new terrorists, as well

[61] The current application further resembles the bulk productions of metadata under Section 1861 in that it proposes to capture metadata for a larger volume of U.S. person communications. See [redacted] Response at 3. The Court is satisfied that the increase in U.S. person communications does not undermine the basis for relevance, particularly in view of the specific safeguards for accessing and disseminating U.S. person information.

as e-mail accounts used by known terrorists that otherwise would be missed. Id. at 21-22.[62]

As the [redacted] Opinion recognizes, the relevance standard does not require "a statistical 'tight fit' between the volume of proposed collection and the much smaller proportion of information" that pertains directly to a Foreign Power. [redacted] Opinion at 49-50. Nor, in the Court's view, does the relevance standard necessarily require a PR/TT authorization to limit collection to [redacted] of Foreign Power communications. The circumstances that make bulk metadata relevant include [redacted] Alexander Decl. at 18. It follows that some Foreign Power communications [redacted]

[redacted]

C. Specifications of the Order

Section 1842(d)(2)(A) requires a PR/TT order to

specify–

> (i) the identity, if known, of the person who is the subject of the investigation;
>
> (ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied; and
>
> (iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied.[65]

[redacted]

In this case, the subjects of the relevant investigations are sufficiently identified, to the extent known, as the enumerated Foreign Powers "and unknown persons in the United States and abroad affiliated with the Foreign Powers." [redacted] Primary Order at 2-3.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[67] See, e.g., Docket No. PR/TT [redacted] Application at 26 n.15, Primary Order issued on [redacted] at 3 [redacted]

[redacted]

At this pre-collection stage, it is uncertain to which facilities PR/TT devices will be attached or applied during the pendency of the initial order. See pages 76-77, supra; [redacted] Response at 1-2. For this reason, and because the Court is satisfied that other specifications in the order will adequately demarcate the scope of authorized collection, the Court will issue an order that does not identify persons pursuant to Section 1842(d)(2)(A)(ii). However, once this surveillance is implemented, the government's state of knowledge may well change. Accordingly, the Court expects the government in any future application to identify persons (as described in Section 1842(d)(2)(A)(ii)) who are known to the government for any facility that the government knows will be subjected to PR/TT surveillance during the period covered by the requested order.

Section 1842(d)(2)(A)(iii) requires the order to specify "the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied." The order specifies the location of each facility. The Court is also satisfied that "the attributes of the communications to which the order applies" are

appropriately specified. Acquisition of particular forms of metadata (described in Part II, supra) is authorized for all e-mail [redacted] communications traversing any of the communications facilities at the specified locations. This form of specification is consistent with the language of Section 1842(d)(2)(A)(iii) and is sufficient to delineate the scope of authorized acquisition from that which is not authorized.[68]

IV. The Court Approves, Subject to Modifications, the Restrictions and Procedures Proposed by the Government For the Retention, Use, and Dissemination of the PR/TTMetadata

Unlike other provisions of FISA, the PR/TT provisions of the statute do not expressly require the adoption and use of minimization procedures. Compare 50 U.S.C. §§ 1805(c)(2)(A) & 1824(c)(2)(A) (providing that orders authorizing electronic surveillance or physical search must direct that minimization procedures be followed). Accordingly, routine FISA PR/TT orders do not require that minimization procedures be followed. The government acknowledges, however, that the application now before the Court is not routine. As discussed above, the government seeks to acquire information concerning [redacted] electronic communications, the vast majority of which, viewed individually, are not relevant to the counterterrorism purpose of the collection, and many of which involve United States persons. In light of the sweeping and non-targeted nature of the collection for which authority is sought, the government proposes a

[redacted]

number of restrictions on retention, use, and dissemination, some of which the government refers to as "minimization" procedures. See, e.g., Memorandum of Law at 4, 17. The restrictions now proposed by the government are similar, but not identical, to the rules that were adopted by the Court in its [redacted] Order in Docket Number PR/TT [redacted] Order"), the most recent order authorizing bulk PR/TT collection by NSA.

Absent any suggestion by the government that a different standard should apply, the Court is guided in assessing the proposed restrictions by the definition of minimization procedures in 50 U.S.C. § 1801(h).[69] Because procedures satisfying that definition are sufficient

---

[69] Section 1801(h) defines "minimization procedures" in pertinent part as follows:

> (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
>
> (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in [50 U.S.C. § 1801(e)(1)], shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; [and]
>
> (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes[.]
>
> . . .

50 U.S.C. § 1801(h).

under FISA to protect the privacy interests of United States persons with respect to the acquisition, use, and dissemination of the contents of communications, restrictions meeting the same standard are also at least adequate in the context of the collection and use of non-content metadata. Guided by the Section 1801(h) standard, the Court concludes, for the reasons stated below, that the procedures proposed by the government, subject to the modifications described below, are reasonably designed in light of the nature and purpose of the bulk PR/TT collection to protect United States person information, and to ensure that the information acquired is used and disseminated in furtherance of the counterterrorism purpose of the collection.

A. Storage and Traceability

NSA will continue to store the PR/TT data that it retains in repositories within secure networks under NSA's control. [redacted]lexander Decl. at 24. As was the case under the [redacted] Order, the data collected pursuant to the authority now sought by the government will carry unique markings that render it distinguishable from information collected by NSA pursuant to other authorities. [redacted] Response at 15; see also Declaration of [redacted] NSA, filed on [redacted] in Docket No. PR/TT [redacted] ([redacted] Decl.") at 14 n.8. The markings, which are applied to the data before it is made available for analytic querying and remain attached to the information as it is stored in metadata repositories, see [redacted] Response at 15, are designed to ensure that software and other controls (such as user authentication tools) can restrict access to the PR/TT data solely to authorized personnel who have received appropriate training regarding the special rules for using

and disseminating such information. See [redacted] Alexander Decl. at 24-25; [redacted] Decl. at 14 n.8. After PR/TT metadata is queried in accordance with the procedures described below, the query results (including analytic output based on query results)[70] will remain identifiable as bulk PR/TT-derived information. See [redacted] Response at 15. Such traceability enables NSA personnel to adhere to the special rules for disseminating PR/TT-derived information that are described below.

B. Access to the Metadata by Technical Personnel for Non-Analytic Purposes

Under the approach proposed by the government, "[t]rained and authorized technical personnel" will be permitted to access the metadata to ensure that it is "usable for intelligence analysis." Id. at 25. For example, such personnel may access the metadata to perform processes designed to prevent the collection, processing, or analysis of metadata associated with [redacted] to create and maintain records necessary to demonstrate compliance with the terms of authority granted; or to develop and test technologies for possible use with the metadata. Id.[71] Similar non-analytic

[70] The government has explained that "[q]uery results could include information provided orally or in writing, and could include a tip or a lead (e.g., 'A query on RAS-approved identifier A revealed a direct contact with identifier Z'), a written or electronic depiction of a chain or pattern, a compilation or summary of direct or indirect contacts of a RAS-approved seed, a draft or finished report, or any other information that would be returned following a properly predicated PR/TT query." [redacted] Response at 15 n.6.

[71] An authorized NSA technician may query the metadata with a non-RAS-approved identifier for the limited purpose of determining whether such identifier is an unwanted [redacted] Alexander Decl. at 25. After recognizing a [redacted]

(continued...)

access by appropriately trained and authorized technical personnel was permitted under the [redacted] Order. See [redacted] Order at 10.

C. Access by Analysts

NSA analysts will query the metadata that is collected only with RAS-approved "seed" identifiers, in accordance with the same basic framework that was approved by the Court in the [redacted] Order. See [redacted] Alexander Decl. at 26-27; [redacted] Order at 7-9. An identifier may be approved for use as a querying seed in one of two ways. First, an identifier may be used as a seed after a designated "approving official" (i.e., the Chief or Deputy Chief of NSA's Homeland Analysis Center, or one of 20 authorized Homeland Mission Coordinators[72]) determines that the available facts give rise to a reasonable articulable suspicion that the identifier is associated with one of the targeted Foreign Powers. [redacted] Alexander Decl. at 26-27. Before querying can be performed using an identifier that is reasonably believed to be used by a United States person, NSA's Office of General Counsel (OGC) must determine that the identifier is not regarded as associated with a Foreign Power solely based on activities that are

---

[71](...continued)
[redacted] through such a query, the NSA technician could share the query results – i.e., the identifier and the fact that it is a [redacted] – with other NSA personnel responsible for the removal of unwanted metadata from NSA's repositories, but would not be permitted to share any other information from the query. Id. at 25-26.

[72] The [redacted] Order identified one approving official in addition to the 22 officials listed here. See [redacted] Order at 8 (listing the Chief, Special FISA Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate as one of the 23 approving officials).

protected by the First Amendment. Id. at 27. Second, an identifier that is the subject of electronic surveillance or physical search pursuant to 50 U.S.C. § 1805 or § 1824 based on this Court's finding of probable cause that such identifier is used by an agent of a Foreign Power may be deemed RAS-approved without review by an NSA designated approving official. Id.

As was the case under the Court's [redacted] Order and prior orders in this matter, RAS-approved queries of the collected data will take the form of "contact chaining." Id. at 18. Such queries yield data for all communications within two "hops" of the RAS-approved seed. Id. The first hop acquires data regarding all identifiers that have been in contact with the seed, and the second hop yields data for all identifiers in contact with identifiers that were revealed by the first hop. Id. at 18 n.12. The government asserts, and the Court has previously accepted, that "[g]oing out to the second 'hop' enhances NSA's ability to find, detect and identify the Foreign Powers and those affiliated with them by greatly increasing the chances that previously unknown Foreign Power-associated identifiers may be uncovered." Id. at 18-19 n.12; [redacted] Opinion and Order at 48.[73]

---

[73] NSA also intends to perform [redacted] The government has clarified in connection with this application, however, that [redacted] is not used as a means for querying the metadata, but instead is applied only to the results of RAS-approved contact-chaining queries. See [redacted] Response at 16.

The government's proposed RAS-approval and querying process differs in two noteworthy respects from the approach previously approved by the Court. First, unlike RAS approvals made pursuant to the [redacted] Order and prior orders in this matter,[74] RAS approvals made under the approach now proposed by the government will expire after a specified time. A determination by a designated approving official for an identifier reasonably believed to be used by a United States person would be effective for 180 days, while such a determination for any other identifier would last for one year. [redacted] Alexander Decl. at 27. An identifier deemed approved based on FISC-authorized electronic surveillance or physical search will be subject to use as a seed for the duration of the FISC authorization. Id. The adoption of fixed durations for RAS approvals will require the government at regular intervals to renew its RAS assessments for identifiers that it wishes to continue to use as querying "seeds." The re-evaluations that will be required under the proposed approach can be expected to increase the likelihood that query results are relevant to the counterterrorism purpose of the bulk metadata collection and to reduce the amount of irrelevant query results (including information regarding

[74] Previously, approved identifiers remained eligible for querying until they were affirmatively removed from the list of approved "seed" accounts. The government's practice was to remove identifiers from the list only "[w]hen NSA receive[d] information that suggest[ed] that a RAS-approved e-mail address [was] no longer associated with one of the Foreign Powers"; implicitly, the mere passage of time without new information did not obligate the government to revoke a RAS approval. See Docket No. PR/TT [redacted] NSA 90-Day Report to the Foreign Intelligence Surveillance Court filed on [redacted] at 6. The government had informed the Court on [redacted] that it was "developing a framework within which to revalidate, and when appropriate, reverse . . . RAS approvals," id. at 6, but it does not appear that the new framework had been implemented before the expiration of the Court's [redacted] Order on [redacted].

United States persons) that is yielded.

The second proposed change to the process involves the number of NSA personnel permitted to perform RAS-approved queries. Unlike the [redacted] Order and prior orders in this matter, which limited the number of analysts permitted to run such queries, the re-initiation proposed by the government has no such limitation. See Id. at 26 n.18; [redacted] Order at 7. The government instead proposes the use of "technical controls" to "block any analytic query of the metadata with a non-RAS-approved seed." [redacted] Alexander Decl. at 26 n.18. The government further notes that all analytic queries will continue to be logged, and that the creation and maintenance of auditable records will "continue to serve as a compliance measure." Id.; see also [redacted] Order at 7. In light of the safeguards noted by the government, and the additional fact that no identifier will be eligible for use as a querying seed without having first been approved for querying by a designated approving official (or deemed approved by virtue of a FISC order), the Court is satisfied that it is unnecessary to limit the number of NSA analysts eligible to conduct RAS-approved queries.

D. Sharing of Query Results Within NSA

The government's proposal for sharing query results within NSA is similar to the approach approved by the Court last year. The [redacted] Order provided, subject to a proviso that is discussed below, that the unminimized results of RAS-approved queries could be "shared with other NSA personnel, including those who are not authorized to access the PR/TT metadata." [redacted] Order at 11. The basis for such widespread sharing of query results

within NSA was the government's assertion that analysts throughout the agency address counterterrorism issues as part of their missions and, therefore, have a need for the information.[75] Presumably for the same reason, the government proposes in the application now before the Court that the results of RAS-approved queries be available to all NSA analysts for intelligence purposes, and that such analysts be allowed to apply "the full range of SIGINT analytical tradecraft" to the query results. [redacted] Alexander Decl. at 28 n.19.[76] The Court is satisfied

---

[75] In a declaration filed in Docket Number PR/TT [redacted] late last year, the Director of NSA explained that:

> NSA's collective expertise in the[] Foreign Powers resides in more than [redacted] intelligence analysts, who sit, not only in the NSA's Counterterrorism Analytic Enterprise, but also in other NSA organizations or product lines. Analysts from other product lines also address counterterrorism issues specific to their analytic missions and expertise. For example, the International Security Issues product line pursues foreign intelligence information on [redacted] including [redacted] The mission of the Combating Proliferation product line includes identifying connections between proliferators of weapons of mass destruction and terrorists, including those associated with the Foreign Powers. The International Crime and Narcotics product line identifies connections between terrorism and human or nuclear smuggling or other forms of international crime. . . . Each of the NSA's ten product lines has some role in protecting the Homeland from terrorists, including the Foreign Powers. Because so many analysts touch upon terrorism information, it is impossible to estimate how many analysts might be served by access to the PR/TT results.

[redacted] Report, Exhibit A at 5-6.

[76] The [redacted] Order did not explicitly authorize NSA analysts to apply the "full range of SIGINT tools" to PR/TT query results, but, at the same time it placed no limit on the analytical tools or techniques that could be applied by the trained analysts who were entitled to have access to query results. Accordingly, the Court views the express reference to "the full range of analytic tools" in the government's proposal as a clarification of prior practice that the Court, in any event, approves.

that such internal sharing remains appropriate, subject to the training requirement that is discussed below.

E. Dissemination Outside NSA

The government's proposed rules for disseminating PR/TT-derived information outside of NSA are slightly different from the procedures that were previously in place. Under the [redacted] Order, NSA was required to "treat information from queries of the PR/TT metadata in accordance with United States Signals Intelligence Directive 18 (USSID 18)" – NSA's standard procedures for handling Signals Intelligence collection – and to "apply USSID 18 to minimize information concerning U.S. persons obtained from the pen registers and trap and trace devices authorized herein." [redacted] Order at 12. In addition,

> before NSA disseminate[d] any U.S. person identifying information outside of NSA, the Chief of Information Sharing Services in the Signals Intelligence Directorate, the Senior Operations Officer at NSA's National Security Operations Center, the Signals Intelligence Directorate Director, the Deputy Director of NSA, or the Director of NSA [was required to] determine that the information identifying the U.S. person [was] in fact related to counterterrorism information and that it [was] necessary to understand the counterterrorism information or assess its importance.

Id.

The government's proposal has the same two basic elements, although they are worded slightly differently. First, NSA "will apply the minimization and dissemination procedures of Section 7 of [USSID 18] to any results from queries of the metadata disseminated outside of NSA in any form." [redacted] Alexander Decl. at 28. Second,

> prior to disseminating any U.S. person information outside NSA, one of the officials listed in Section 7.3(c) of USSID 18 (i.e., the Director of NSA, the Deputy Director of

> NSA, the Director of the Signals Intelligence Directorate (SID), the Deputy Director of the SID, the Chief of the Information Services (ISS) office, the Deputy Chief of the ISS office, and the Senior Operation Officer of the National Security Operations Center) must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.

Id.

The differences are not material. Although the proposal refers specifically to "the minimization and dissemination procedures of Section 7 of [USSID 18]" rather than to USSID 18 generally, the Court does not understand any difference in meaning to be intended; indeed, Section 7 is the portion of USSID 18 that specifically covers disseminations outside NSA. See [redacted] Application, Tab C (USSID 18), at 8-10. With regard to the application of the counterterrorism purpose requirement, the proposal adds two high-ranking NSA officials (the Deputy Director of the SID and the Deputy Chief of the ISS office) to the list of five officials who were previously designated to make the required determination. The Court is aware of no reason to think that the two additional officials are less suited than the other five to make the required determination, or that their designation as approving officials will undermine the internal check that is provided by having high-ranking NSA officials approve disseminations that include United States person identifying information.[77]

---

[77] Like the [redacted] Order, the government's proposal would also permit NSA to "share results derived from intelligence analysis queries of the metadata, including U.S. person identifying information, with Executive Branch personnel . . . in order to enable them to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings." [redacted] Alexander Decl. 28-29; see also [redacted]
(continued...)

The government's proposal contains one additional element that was not part of the framework approved by the Court in the [redacted] Order. Specifically, the government proposes that "[i]n the extraordinary event that NSA determines that there is a need to disseminate information identifying a U.S. person that is related to foreign intelligence information, as defined by 50 U.S.C. § 1801(e), other than counterterrorism information and that is necessary to understand the foreign intelligence information or assess its importance, the Government will seek prior approval from the Court." [redacted] Alexander Decl. at 28 n.20. Insofar as the government's proposal invites the Court to review and pre-approve individual disseminations of information based upon the Court's own assessments of foreign intelligence value, the Court declines the invitation. The judiciary is ill-equipped to make such assessments, which involve matters on which the courts generally defer to the Executive Branch.[78] In the

---

[77](...continued)
[redacted] Order at 12-13. The government's current proposal also permits such sharing with Executive Branch personnel "to facilitate their lawful oversight functions." [redacted] Alexander Decl. at 29. Although the [redacted] order did not contain an explicit provision to this effect, sharing for such purposes was plainly contemplated. See, e.g., [redacted] Order at 16 (providing for NSD review of RAS querying justifications).

[78] See, e.g., Holder v. Humanitarian Law Project, — U.S. —, 2010 WL 2471055, *22 (June 21, 2010) ("[W]hen it comes to collecting evidence and drawing factual inferences in [the national security] area, the lack of competence on the part of the courts is marked.") (citation and internal quotation marks omitted); Reno v. American-Arab Anti-Discrimination Comm., 525 U.S. 471, 491 (1999) ("a court would be ill-equipped to determine [the] authenticity and utterly unable to assess [the] adequacy" of the executive's security or foreign policy reasons for treating certain foreign nationals as a "special threat"); Regan v. Wald, 468 U.S. 222, 243 (1984) (giving the "traditional deference to executive judgment" in foreign affairs in sustaining President's decision to restrict travel to Cuba against a due process challenge).

event, however, that NSA encounters circumstances that it believes necessitate alteration of the dissemination procedures that have been approved by the Court, the government may obtain prospectively-applicable modifications to those requirements upon a determination by the Court that such modifications are appropriate under the circumstances and in light of the sweeping and non-targeted nature of the PR/TT collection. Cf. Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search § I.D (on file with the Court in Docket No. 08-1833).

F. Retention

Under the [redacted] Order, the PR/TT metadata was available for querying for four and one-half years, after which it had to be destroyed. [redacted] Order at 13. The four-and-one-half-year retention period was originally set based upon NSA's assessment of how long collected metadata is likely to have operational value. See [redacted] Opinion at 70-71. Pursuant to the government's proposal, the retention period would be extended to five years. [redacted] Application at 13. The government asserts that the purpose of the change is to "develop and maintain consistency" with the retention period for NSA's bulk telephony metadata collection, which is authorized by this Court under the FISA business records provision, 50 U.S.C. § 1861. [redacted] Response at 24. The Court is satisfied that the relatively small extension of the retention period that is sought by the government is justified by the administrative benefits that would result.

G. Oversight

The government proposes to employ an internal oversight regime that closely tracks the oversight provisions adopted by the Court in the [redacted] Order, requiring, among other things, that NSA OGC and NSD take various steps to ensure that the data is collected and handled in accordance with the scope of the authorization. Compare [redacted] Order at 13-16, with [redacted] Alexander Decl. at 29-30. There is, however, one significant difference. The [redacted] Order required NSA OGC to ensure that all NSA personnel permitted to access the metadata or receive query results were first "provided the appropriate and adequate training and guidance regarding the procedures and restrictions for storage, access, and dissemination of the PR/TT metadata and/or PR/TT metadata-derived information, i.e., query results." [redacted] Order at 13-14. The analogous oversight provision in the government's current proposal, by contrast, directs NSA OGC and the Office of the Director of Oversight and Compliance (ODOC) to ensure that adequate training and guidance is provided to NSA personnel having access to the metadata, but not to those receiving query results. See [redacted] Alexander Decl. at 29. As discussed above, the government has proposed special rules and restrictions on the handling and dissemination of query results. Most notably, PR/TT query results must remain identifiable as bulk PR/TT-derived information, see [redacted] Response at 15, and may not be disseminated outside NSA without the prior determination by a designated official that any United States person information relates to counterterrorism information and that it is necessary to understand the counterterrorism information or to assess its importance. [redacted]

[redacted] Alexander Decl. at 28. To follow those rules, NSA personnel must know and understand them.

As noted above, NSA's record of compliance with these rules has been poor. Most notably, NSA generally disregarded the special rules for disseminating United States person information outside of NSA until it was ordered to report such disseminations and certify to the FISC that the required approval had been obtained. See pages 18-19, supra. The government has provided no meaningful explanation why these violations occurred, but it seems likely that widespread ignorance of the rules was a contributing factor.

Accordingly, the Court will order NSA OGC and ODOC to ensure that all NSA personnel who receive PR/TT query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information.

H. Reporting

The reporting requirements proposed by the government are similar to the reporting requirements adopted by the Court in the [redacted] Order. Compare [redacted] Alexander Decl. at 31, with [redacted] Order at 16-18. As was previously the case, the government will submit reports to the Court approximately every 30 days and upon requesting any renewal of the authority sought. S[redacted] Alexander Dec. at 31. The 30-day reports will include "a discussion of the queries made since the last report and NSA's application of the RAS standard." Id. Because NSA will not apply the requested authority to particular

[redacted] however, the 30-day reports will no longer include a discussion of "changes in the description of the [redacted] . . . or in the nature of the communications carried thereon." See [redacted] Order at 16. Like the [redacted] Order, the government's proposal will also require it, upon seeking renewal of the requested authority, to file a report describing "any new facility proposed to be added" and "any changes proposed in the collection methods." [redacted] Alexander Decl. at 31.

The [redacted] Order also directed the government to submit weekly reports listing each instance in which "NSA has shared, in any form, information obtained or derived from the PR/TT metadata with anyone outside NSA," including a certification that the requirements for disseminating United States person information (i.e., that a designated official had determined that any such information related to counterterrorism information and was necessary to understand courterterrorism information or to assess its importance) had been followed. See [redacted] Order at 17. The government's proposal does not include such a requirement. In light of NSA's historical problems complying with the requirements for disseminating PR/TT-derived information, the Court is not prepared to eliminate this reporting requirement altogether. At the same time, the Court does not believe that weekly reports are still necessary to ensure compliance. Accordingly, the Court will order that the 30-day reports described in the preceding paragraph include a statement of the number of instances since the preceding report in which NSA has shared, in any form, information obtained or derived from the PR/TT metadata with anyone outside NSA. For each such instance in which United States person information has been

shared, the report must also include NSA's attestation that one of the officials authorized to approve such disseminations determined, prior to dissemination, that the information was related to counterterrorism information and necessary to understand the counterterrorism information or to assess its importance.

V. The Government's Request for Authority to Access and Use All Previously Collected Data

The government seeks authority to access and use all previously acquired bulk PR/TT data, including information not authorized for collection under the Court's prior orders, subject to the same restrictions and procedures that will apply to newly-acquired PR/TT collection. See [redacted] Application at 16. For the following reasons, the Court will grant the government's request in part and deny it in part.

A. The [redacted] Order

As discussed above, after the government disclosed the continuous and widespread collection of data exceeding the scope of the Court's prior orders dating back to [redacted] it elected not to seek renewal of the authority granted in the [redacted] Order. The government was unable, before the expiration of that authority on [redacted], to determine the extent to which the previously-acquired information exceeded the scope of the Court's orders or to rule out the possibility that some of the information fell outside the scope of the pen register statute. See [redacted] Order at 2-4. Accordingly, as an interim measure, Judge Walton entered an order on [redacted] directing the government not to access the information previously

obtained "for any analytic or investigative purpose," except when such access is "necessary to protect against an imminent threat to human life." See [redacted] Order at 4-5; see also page 23, supra.

The application now before the Court includes a request to lift the [redacted] Order. See [redacted] Application at 16. Since [redacted], both the Court and the government have had the opportunity to make a thorough assessment of the scope and circumstances of the overcollection and to consider the pertinent legal issues. Based on that assessment, the Court believes that it is now appropriate to rescind the [redacted] Order, which, as noted, was intended to be an interim measure, and to refine the rules for handling the prior bulk PR/TT collection.

B. The Court Lacks Authority to Grant the Government's Request in its Entirety

The Court concludes that it has only limited authority to grant the government's request for permission to resume accessing and using previously-collected information. As discussed in more detail below, the Court concludes that it possesses authority to permit the government to query data collected within the scope of the Court's prior orders, and that it is appropriate under the circumstances to grant such approval. But for information falling outside the scope of the prior orders, the Court lacks authority to approve any use or disclosure that would be prohibited under 50 U.S.C. § 1809(a)(2). Accordingly, the Court will deny the government's request with respect to those portions of the unauthorized collection that are covered by Section 1809(a)(2). To the extent that other portions of the unauthorized prior collection may fall outside the reach of

Section 1809(a)(2), the Court concludes that it has authority to grant the government's request and that it is appropriate under the circumstances to do so.

1. Information Authorized for Acquisition Under the Court's Prior Orders

The government argues that the FISA PR/TT statute, 50 U.S.C. § 1842, empowers the Court to authorize NSA to resume querying the prior collection in its entirety. See Memorandum of Law at 72-73. As discussed above, the Court continues to be satisfied that it may, pursuant to Section 1842 and subject to appropriate restrictions, authorize NSA to acquire, in bulk, the metadata associated with Internet communications transiting the United States. Further, although Section 1842 does not explicitly require the application of minimization procedures to PR/TT-acquired information, the Court also agrees that in light of the sweeping and non-targeted nature of this bulk collection, it has authority to impose limitations on access to and use of the metadata that NSA has accumulated.

The Court is satisfied that it may invoke the same authority to permit NSA to resume querying the PR/TT information that was collected in accordance with the Court's prior orders. The Court is further persuaded that, in light of the government's assertion of national security need,[79] it is appropriate to exercise that authority. Accordingly, the Court hereby orders that the government may access, use, and disseminate bulk PR/TT information that was collected in

[79] See [redacted] Alexander Decl. at 10 n.6 ("The ability of NSA to access the information collected under docket number PR/TT [redacted] and previous dockets is vital to NSA's ability to carry out its counterterrorism intelligence mission. If NSA is not able to combine the information it collects prospectively with the information it collected [previously], there will be a substantial gap in the information available to NSA.").

accordance with the terms of the Court's prior orders, subject to the procedures and restrictions discussed herein that will apply to newly-acquired metadata.

2. Information Not Authorized for Acquisition Under the Court's Prior Orders

By contrast, the Court is not persuaded that it has authority to grant the government's request with respect to all information collected outside the scope of its prior orders. FISA itself precludes the Court from granting that request in full.

a. 50 U.S.C. § 1809(a)(2) Precludes the Court from Granting the Government's Request with Respect to Some of the Prior Unauthorized Collection

The crucial provision of FISA, 50 U.S.C. § 1809, provides, in pertinent part, as follows:

> (a) Prohibited Activities
>
> A person is guilty of an offense if he intentionally –
>
> . . .
>
> (2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by this chapter, chapter 119, 121, or 206 of Title 18 or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 1812 of this title.

50 U.S.C. § 1809(a)(2).

Section 1809(a)(2) has three essential elements: (1) the intentional disclosure or use of information (2) obtained under color of law through electronic surveillance (3) by a person knowing or having reason to know that the information was obtained through electronic surveillance not authorized by one of the enumerated (or similar) statutory provisions. The

government's request to access, use, and disseminate the fruits of the prior unauthorized collection implicates all three elements of Section 1809(a)(2)'s criminal prohibition.

Application of the first two elements is straightforward. Plainly, conducting contact chaining inquiries of stored data and sharing the query results both within and outside NSA would constitute the intentional use and disclosure of information.[80] It is also clear that the data previously collected by the government – which was acquired through the use of orders issued by this Court pursuant to FISA – was obtained "under color of law." See West v. Atkins, 487 U.S. 42, 49-50 (1988) (explaining that the misuse of authority possessed by virtue of law is action "under color of law").[81]

The third element requires lengthier discussion, but, in summary, the Court concludes that some of the prior bulk PR/TT collection is information that the responsible government officials know or have reason to know was obtained through electronic surveillance not authorized by one of the statutory provisions referred to in Section 1809(a)(2). To begin with,

---

[80] Insofar as the government contends that Section 1809(a)(2) reaches only "intentional violations of the Court's orders," or "willful" as opposed to intentional conduct, see Memorandum of Law at 74 n. 37, the Court disagrees. The plain language of the statute requires proof that the person in question "intentionally" disclosed or used information "knowing or with reason to know" the information was obtained in the manner described.

[81] The phrase "a person" in Section 1809 is certainly intended to cover government officials. In addition to requiring conduct "under color of law," the statute provides an affirmative defense to prosecution for a "law enforcement or investigative officer engaged in the course of his official duties" in connection with electronic surveillance "authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction." See 50 U.S.C. § 1809(b).

the language of Section 1809(a)(2) demonstrates that Congress intended at least some unauthorized PR/TT acquisitions to be covered by the criminal prohibition. The statute expressly reaches, among other things, information obtained through "electronic surveillance not authorized by this chapter, [or] chapter 119, 121, or 206 of Title 18." Section 1809 is part of Chapter 36 of Title 50 of the U.S. Code. Chapter 36, in turn, encompasses all of FISA, as codified in Title 50, including FISA's PR/TT provisions found at 50 U.S.C. §§ 1841-1846. Accordingly, "this chapter" in Section 1809(a)(2) refers in part to the FISA PR/TT provisions. Moreover, Chapter 206 of Title 18, which is also referenced in Section 1809(a)(2), consists exclusively of the PR/TT provisions of the criminal code, 18 U.S.C. §§ 3121-3127, key portions of which are incorporated by reference into FISA. See 50 U.S.C. § 1841(2) (incorporating the definitions of "pen register" and "trap and trace device" found at 18 U.S.C. § 3127). Because Chapter 206 of Title 18 authorizes no means of acquiring information other than through the use of PR/TT devices, Section 1809(a)(2)'s reference to "electronic surveillance" must be understood to include at least some information acquired through the use of PR/TT authority.

That conclusion is reinforced by examination of FISA's definition of "electronic surveillance," which applies to Section 1809, see 50 U.S.C. § 1801 ("As used in this subchapter: . . ."), and which is broad enough to include some (but not necessarily all) information acquired through the use of PR/TT devices.[82] "Electronic surveillance" is defined, in

[82] See also H.R. Rep. 95-1283, pt. 1, at 51 (1978) ("The surveillance covered by [Section 1801(f)(2)] is not limited to the acquisition of the oral or verbal contents of a communication . . . (continued...)

pertinent part, as "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States." 50 U.S.C. § 1801(f)(2).[83] For purposes of this definition of "electronic surveillance," "contents" is defined in Section 1801(n) to include, among other things, "any information concerning the identity of the parties" to a communication "or the existence . . . of that communication."[84] "Wire communication" is defined as "any communication while it is being carried by a wire, cable, or other like connection

---

[82](...continued)
[and] includes any form of 'pen register' or 'touch-tone decoder' device which is used to acquire, from the contents of a voice communication, the identities or locations of the parties to the communication.").

[83] Section 1801(f) includes three additional definitions of "electronic surveillance," only one of which appears to have any possible application with regard to the prior bulk PR/TT collection. Subsections (f)(1) ("the acquisition . . . of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person") and (f)(3) ("the intentional acquisition . . . of any radio communication") are flatly inapplicable. Subsection (f)(4) could apply to the extent the prior collection included non-wire communications acquired under "circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." The Court's analysis of Section 1809(a)(2) would, of course, apply identically to prior unauthorized collection constituting "electronic surveillance" under any of the definitions set forth in Section 1801(f).

[84] As noted above, the definition of "contents" in Section 1801(n) is different than the definition of "contents" in 18 U.S.C. § 2510(8) – the latter definition does not include information concerning the identity of the parties to or the existence of the communication. See page 27, supra; [redacted] Opinion at 6 n.6. Accordingly, information constituting "contents" as used in Section 1801(f) can be acquired through the use of a PR/TT device, provided that it does not also constitute "contents" under Section 2510(8) and that it otherwise satisfies the statutory requirements for acquisition by PR/TT collection.

furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign commerce." 50 U.S.C. § 1801(*l*). Reading those definitions together, then, "electronic surveillance" includes, among other things, the acquisition (1) by an electronic, mechanical, or other surveillance device (2) of information concerning the identity of the parties to or the existence of any communication to or from a person in the United States, (3) when such information is acquired in the United States (4) while the communication is being carried on a wire, cable, or other like connection furnished or operated by a common carrier.

The unauthorized portion of the prior PR/TT collection includes some information that meets all four of these criteria. First, there is no question that the prior collection was acquired through the use of "electronic, mechanical, or other surveillance devices." See, e.g., [redacted] Decl. at 9 (describing the use of "NSA-controlled equipment or devices" to "extract metadata for subsequent forwarding to NSA's repositories").

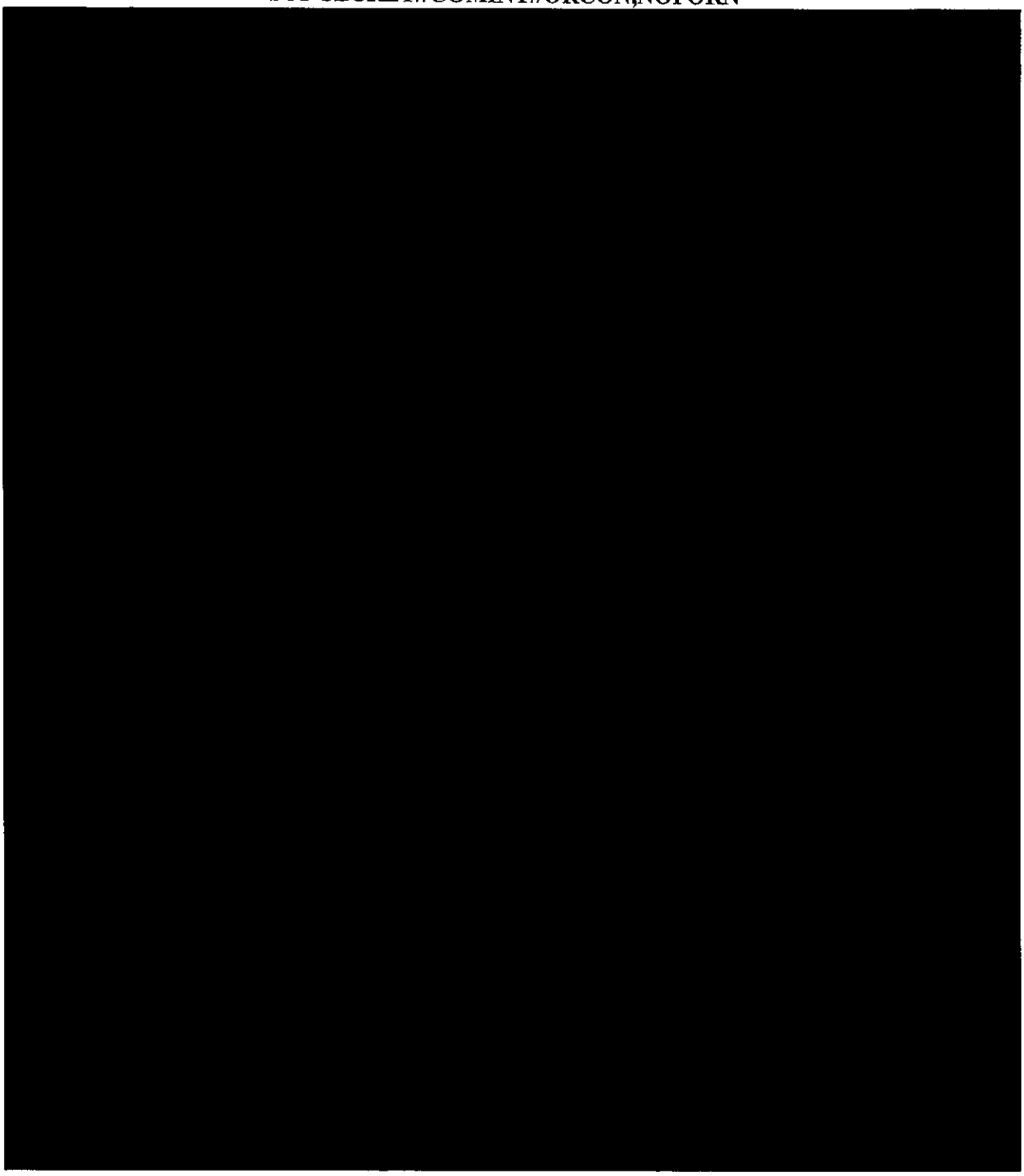
Second, the overcollection included information concerning the identity of the parties to and the existence of communications to or from persons in the United States. Persons in the United States were parties to some of the communications for which data was acquired. See, e.g., [redacted] Application at 5-6 (stating that the collection will include metadata pertaining to persons within the United States); id. at 9 (stating that the "collection activity . . . will collect metadata from electronic communications that are: (1) between the United States and abroad; (2) between overseas locations; and (3) wholly within the United States"). And, as discussed above,

the unauthorized collection included: [redacted] All of these forms of information concern the existence of an associated communication, and many of them could also concern the identities of the communicants.

Third, the data previously collected, both authorized and unauthorized, was acquired in the United States. See, e.g., [redacted] Application at 9 ("All of the collection activity described above will occur in the United States . . . ."); [redacted] Opinion at 72-80 [redacted]

Fourth, it appears that much, and perhaps all, of the information previously collected was acquired while the associated communication was "being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign commerce." See 50 U.S.C. § 1801(*l*). [redacted]

~~TOP SECRET//COMINT//ORCON,NOFORN~~



~~TOP SECRET//COMINT//ORCON,NOFORN~~

[redacted]

For the foregoing reasons, the Court concludes that at least some of the data previously collected, including portions of the data that was not authorized by the Court's prior orders, constitutes unauthorized "electronic surveillance" under Section 1809(a)(2). But that does not complete the analysis. Section 1809 does not prohibit all disclosures or uses of unauthorized electronic surveillance; rather, it reaches disclosure or use only by "a person knowing or having reason to know" that the information was obtained through unauthorized electronic surveillance.

The Court concludes that the knowledge requirement is satisfied for some of the prior unauthorized collection constituting electronic surveillance. The government has acknowledged that particular portions of the prior collection fell outside the scope of the Court's prior

[redacted]

authorizations. See generally [redacted] Report. Further, some of that unauthorized collection is identifiable as electronic surveillance – i.e., as information concerning the identity of the parties to or the existence of any communication to or from a person in the United States that was acquired in the United States while the communication was being carried on a wire, cable, or other like connection furnished or operated by a common carrier. As demonstrated above, the government's filings dating back to [redacted] demonstrate that most, if not all, of the information previously collected was acquired in the United States [redacted] The government's descriptions of the overcollected information make clear that the information concerns the identity of the parties, the existence of the communication, or both. Finally, the information available to the government – e.g., e-mail identifiers [redacted] – is likely to make some of the data collected identifiable as concerning communications to or from a person in the United States. Accordingly, the Court concludes that the government officials responsible for using and making disclosures of bulk PR/TT-derived information know or have reason to know that portions of the prior collection constitute unauthorized electronic surveillance.[86]

---

[86] In the law enforcement context, courts have held that there is no statutory prohibition on the use – specifically, the evidentiary use – of the results of unlawful PR/TT surveillance. See, e.g., Forrester, supra, 512 F.3d at 512-13 (citing cases). Those decisions, however, do not address the potential application of Section 1809(a)(2), and so provide no basis for departing from the clear terms of that statutory prohibition. Indeed, Forrester recognized that suppression would be warranted if it were "clearly contemplated by [a] relevant statute" and stressed that the party seeking suppression had failed to "point to any statutory language requiring suppression." (continued...)

b. Section 1809(a)(2) Applies to the Prior Collection

The government does not contest that portions of the prior collection contain information that the responsible officials know or have reason to know constitutes "electronic surveillance" that was collected without the necessary authority. Instead, the government offers several reasons why it believes Section 1809(a)(2) presents no bar to Court approval of use of the prior collection. The Court finds the government's contentions unpersuasive.

The government argues that the opening phrase of 50 U.S.C. § 1842(a) vests the Court with authority to enter an order rendering Section 1809(a)(2) inapplicable. See Memorandum of Law at 74 n. 37. The Court disagrees. Section 1842(a), which is entitled "Application for authorization or approval," provides in pertinent part as follows:

> Notwithstanding any other provision of law, the Attorney General or a designated attorney for the government may make an application for an order or an extension of an order authorizing or approving the installation or use of a pen register or trap and trace device for any investigation to obtain foreign intelligence information . . . .

As the context makes clear, the opening phrase "[n]othwithstanding any other provision of law" in Section 1842 relates to the circumstances in which the government may apply for an order permitting it to install and use a PR/TT device for foreign intelligence purposes. It does not speak to the Court's authority to grant a request for permission to use and disclose information

---

[86](...continued)
Id. at 512; see also Nardone v. United States, 302 U.S. 379, 382-84 (1937) (statute prohibiting any person from divulging the substance of interstate wire communications precluded testimony by law enforcement agents about such communications).

obtained in violation of prior orders authorizing the installation of PR/TT devices. Indeed, the Court finds nothing in the text of Section 1842 or the other provisions of FISA that can be read to confer such authority, particularly in the face of the clear prohibition set forth in Section 1809(a)(2).

The government next contends that because the Court has, in its prior orders, regulated access to and use of previously accumulated metadata, it follows that the Court may now authorize NSA to access and use all previously collected information, including information that was acquired outside the scope of prior authorizations, so long as the information "is within the scope of the [PR/TT] statute and the Constitution." Memorandum of Law at 73. But the government overstates the precedential significance of the Court's past practice. The fact that the Court has, at the government's invitation, exercised authority to limit the use of properly-acquired bulk PR/TT data does not support the conclusion that it also has authority to permit the use of improperly-acquired PR/TT information, especially when such use is criminally prohibited by Section 1809(a)(2).

The Court has limited the access to and use of information collected in accordance with prior authorizations, in view of the sweeping and non-targeted nature of that collection. The Court has done so within a statutory framework that generally permits the government to make comparatively liberal use, for foreign intelligence purposes, of information acquired pursuant to PR/TT orders, and in which the Court generally has a relatively small role beyond the acquisition

stage.[87] Thus, the Court's prior orders in this matter are notable not because they permitted the use of PR/TT-acquired data – again, the statute itself generally allows the use and dissemination of properly-acquired PR/TT information for foreign intelligence purposes – but because they imposed restrictions on such use to account for the bulk and non-targeted nature of the collection.[88] The Court has never authorized the government to access and use information collected outside the scope of its prior orders in this matter. Indeed, in the prior instances in which the Court learned of overcollections, it has carefully monitored the disposition of the improperly-acquired information to ensure that it was not used or disseminated by the government. See pages 11-12, 14, supra.

The government further contends that Rule 10(c) of the Rules of this Court gives the Court discretion to authorize access to and use of the overcollected information. Memorandum of Law at 73. The Court disagrees. Rule 10(c) requires the government, upon discovering that

---

[87] As discussed above, unlike the provisions for electronic surveillance and physical search, see 50 U.S.C. §§ 1801-1812, 1821-1829, the FISA PR/TT provisions do not require the application of Court-approved minimization procedures. In the context of Court-authorized electronic surveillance and physical searches, such procedures govern not only the acquisition of information, but also its retention and dissemination. See 50 U.S.C. §§ 1801(h), 1821(4). Like the electronic surveillance and physical search provisions, the FISA PR/TT provisions limit the use and disclosure of information acquired for law enforcement and other non-foreign intelligence-related purposes. Compare 50 U.S.C. § 1845 with 50 U.S.C. § 1806.

[88] Contrary to the government's assertion, the imposition of restrictions on the use and dissemination of the data collected is not "unique" to the bulk PR/TT. Indeed, the Court restricts the government's use of [redacted] See, e.g., Docket No. PR/TT [redacted] Primary Order at 4.

"any authority granted by the Court has been implemented in a manner that did not comply with the Court's authorization," to notify the Court of the incident and to explain, among other things, "how the government proposes to dispose of or treat any information obtained as a result of the non-compliance." FISC Rule 10(c). Rule 10 does not explicitly give the Court the authority to do anything. To be sure, the rule implicitly recognizes the Court's authority, subject to FISA and other applicable law, to ensure compliance with its orders and with applicable Court-approved procedures. It does not, however, state or suggest that the Court is free in the event of an overcollection to dictate any disposition of the overcollected material that it wishes, without regard to other provisions of law, such as Section 1809(a)(2).[89]

Finally, insofar as the government suggests that the Court has inherent authority to permit the use and disclosure of all unauthorized collection without regard to Section 1809, see Memorandum of Law at 73-74 & n.37, the Court again must disagree. To be sure, this Court, like all other Article III courts, was vested upon its creation with certain inherent powers. See In

[redacted]

re Motion for Release of Court Records, 526 F. Supp. 2d 484, 486 (FISA Ct. 2007); see also Chambers v. NASCO, Inc., 501 U.S. 32, 43 (1991) ("It has long been understood that [c]ertain implied powers must necessarily result to our Courts of justice from the nature of their institution . . . ."). It is well settled, however, that the exercise of such authority "is invalid if it conflicts with constitutional or statutory provisions." Thomas v. Arn, 474 U.S. 140, 148 (1985). And defining crimes is not among the inherent powers of the federal courts; rather, federal crimes are defined by Congress and are solely creatures of statute. Bousley v. United States, 523 U.S. 614, 620-21 (1998); United States v. Hudson, 11 U.S. (7 Cranch) 32, 34 (1812). Accordingly, when Congress has spoken clearly, a court assessing the reach of a criminal statute must heed Congress's intent as reflected in the statutory text. See, e.g., Huddleston v. United States, 415 U.S. 814, 831 (1974). The plain language of Section 1809(a)(2) makes it a crime for any person, acting under color of law, intentionally to use or disclose information with knowledge or reason to know that the information was obtained through unauthorized electronic surveillance. The Court simply lacks the power, inherent or otherwise, to authorize the government to engage in conduct that Congress has unambiguously prohibited.[90]

---

[90] In its [redacted] Response at page 4 n.1, the government added an alternative request for the Court to amend all prior bulk PR/TT orders nunc pro tunc to permit acquisition of the overcollected information. The Court denies that request. Nunc pro tunc relief is appropriate to conform the record to a court's original intent but is not a means to alter what was originally intended or what actually transpired. See, e.g., U.S. Philips Corp. v. KBC Bank N.V., 590 F.3d 1091, 1094 (9th Cir. 2010) (citing cases). Here, the prior bulk PR/TT orders make clear that the Court intended to authorize the government to acquire only information [redacted]

(continued...)

For the foregoing reasons, the Court will deny the government's request for authority to access and use portions of the accumulated prior PR/TT collection constituting information that the government knows or has reason to know was obtained through electronic surveillance not authorized by the Court's prior orders.

c. Portions of the Unauthorized Collection Falling Outside the Scope of Section 1809(a)(2)

There is one additional category of information to consider – overcollected information that is not subject to Section 1809(a)(2). The Court is not well positioned to attempt a comprehensive description of the particular types of information that are subject (or not) to Section 1809(a)(2)'s prohibition, but it appears that some of the overcollected data is likely to fall outside its reach. For example, NSA may have no way to determine based on the available information whether a particular piece of data relates to a communication obtained from the [redacted] Similarly, it may not be apparent from available information whether the communication to which a piece of data relates is to or from a person in the United States, such that acquisition constituted electronic surveillance as defined at Section 1801(f)(2).

---

[90](...continued)
[redacted] categories. Nunc pro tunc relief would thus be inappropriate here. See page 14, supra (discussing an instance in which the Court declined to grant a comparable request for nunc pro tunc relief).

When it is not known, and there is no reason to know, that a piece of information was acquired through electronic surveillance that was not authorized by the Court's prior orders, the information is not subject to the criminal prohibition in Section 1809(a)(2). Of course, government officials may not avoid the strictures of Section 1809(a)(2) by cultivating a state of deliberate ignorance when reasonable inquiry would likely establish that information was indeed obtained through unauthorized electronic surveillance. See, e.g., United States v. Whitehill, 532 F.3d 746, 751 (8th Cir.) (where "failure to investigate is equivalent to 'burying one's head in the sand,'" willful blindness may constitute knowledge), cert. denied, 129 S. Ct. 610 (2008). However, when it is not known, and there is genuinely no reason to know, that a piece of information was acquired through electronic surveillance that was not authorized by the Court's prior orders, the information is not subject to the criminal prohibition in Section 1809(a)(2).

The Court is satisfied that neither Section 1809(a)(2) nor any other provision of law precludes it from authorizing the government to access and use this category of information. The bigger question here is whether the Court should grant such authority. Given NSA's longstanding and pervasive violations of the prior orders in this matter, the Court believes that it would be acting well within its discretion in precluding the government from accessing or using such information. Barring any use of the information would provide a strong incentive for the exercise of greater care in this massive collection by the executive branch officials responsible for ensuring compliance with the Court's orders and other applicable requirements. On the other hand, the government has asserted that it has a strong national security interest in accessing and

using the overcollected information. The Court has no basis to question that assertion. Furthermore, high-level officials at the Department of Justice and NSA have personally assured the Court that they will closely monitor the acquisition and use of the bulk PR/TT collection to ensure that the law, as reflected in the Court's orders, is carefully followed by all responsible officials and employees. In light of the government's assertions of need, and in heavy reliance on the assurances of the responsible officials, the Court is prepared – albeit reluctantly – to grant the government's request with respect to information that is not subject to Section 1809(a)(2)'s prohibition. Hence, the government may access, use, and disseminate such information subject to the restrictions and procedures described above that will apply to future collection.

The Court expects the responsible executive branch officials to act with care and in good faith in determining which portions of the prior collection are subject to Section 1809(a)(2)'s prohibition. The authorization to use overcollected information falling outside the scope of the criminal prohibition should not be understood as an invitation to disregard information that, if pursued, would create a reason to know that data was obtained by unauthorized electronic surveillance within the meaning of Section 1809(a)(2). The Court also expects the government to keep it reasonably apprised with regard to efforts to segregate those portions of the prior collection that it intends to use from the portions it is prohibited from using. Accordingly, the Court will order that each of the 30-day reports described above include a description of those efforts.

VI. Conclusion

For all the reasons set forth herein, the government's application will be granted in part and denied in part. Accompanying Primary and Secondary Orders are being issued contemporaneously with this Memorandum Opinion.

Signed [redacted] P02:37 _____ E.T.
Date Time

JOHN D. BATES
Judge, United States Foreign
Intelligence Surveillance Court

[redacted]

All redacted information exempt under b(1) and/ or b(3) except where otherwise noted.

~~TOP SECRET//HCS/COMINT//ORCON,NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COU[redacted] PM 1:43

WASHINGTON, D.C.

[redacted]

[redacted]: Docket Number: PR/TT

MEMORANDUM OF LAW AND FACT IN SUPPORT OF APPLICATION FOR PEN REGISTERS AND TRAP AND TRACE DEVICES FOR FOREIGN INTELLIGENCE PURPOSES

~~TOP SECRET//HCS/COMINT//ORCON,NOFORN~~

Classified by: David S. Kris, Assistant Attorney General, NSD, DOJ
Reason: 1.4(c)
Declassify on: [redacted]

INTRODUCTION (U)

The nature of the Internet allows terrorists to conceal their communications within plain sight – commingled with the voluminous quantity of legitimate, non-terrorist related communications that occur every day. Analytic tools used in ongoing investigations enable the Government to sift through and identify terrorist communications. Use of such tools requires the collection of and access to bulk quantities of metadata associated with Internet communications (not including the substance, meaning, or purport of any communications).[1] The pen register and trap and trace provisions of Title IV of the Foreign Intelligence Surveillance Act of 1978, as amended, authorize the Government to obtain such access.[2] ~~(TS//SI//NF)~~

In a series of authorization orders issued between July 2004 and [redacted] this Court authorized bulk pen register collection under FISA. On [redacted] that authority expired, and the Court issued an order generally barring access to stored metadata that was collected during the preceding 4½ years. The current Application seeks authority to reinitiate bulk pen register collection on terms similar, but not identical, to those authorized in the prior orders, and to access the previously collected metadata. ~~(TS//SI//NF)~~

[redacted]

[2] For simplicity, we use the term "pen register" in this document to include both pen registers and trap and trace devices. (U)

1. Facilities. The Court's prior orders allowed NSA to conduct surveillance on [redacted] The attached Application for Use of Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes ("Application") seeks authority to conduct pen register surveillance on [redacted] This issue is discussed in more detail in Part I.C.2. of this Memorandum. ~~(TS//SI//NF)~~

2. Metadata. The prior authorization orders allowed NSA to acquire certain types of metadata from e-mail [redacted] although as described in the Report of the United States in docket number PR/TT [redacted], filed on [redacted] ("Compliance Report"), NSA was also collecting other types of metadata outside the scope of the prior orders. The new Application seeks authority to acquire all of the metadata NSA was previously acquiring, including metadata from [redacted] The Application also seeks access to all previously collected metadata now residing in NSA's databases, because that metadata, some of which was obtained in violation of the Court's prior orders, is nonetheless within the scope of the pen register statutes, the Fourth Amendment, and the current proposed authorization order, and is essential to the proper functioning of the pen register surveillance program. This issue is discussed in more detail in Parts I, II, and III of this Memorandum. ~~(TS//SI//NF)~~

3. Minimization. The prior authorization orders required adherence to certain minimization procedures, particularly with respect to the handling of query results that have been simplified or eliminated in the Application. We believe that certain of these procedures are unnecessary because query results represent a relatively small amount of information that is most relevant to foreign intelligence needs. In light of the requirement that analysts may query the bulk metadata only with an identifier[3] as to which there is reasonable, articulable suspicion ("RAS") that it is used by one of the identified targets, query results are effectively needles drawn from the haystack. Accordingly, this Application proposes adherence to the standards set out in United States Signals Intelligence Directive No. SP0018 (1993) ("USSID 18") to any results from queries of the metadata disseminated outside of NSA in any form. In addition, prior to disseminating any U.S. person information outside NSA, certain NSA officials must determine that the information identifying the U.S. person is in fact related to counterterrorism information and is necessary to understand the counterterrorism information or assess its importance. This issue is discussed in more detail in Part III.C.3. of this Memorandum.

~~(TS//SI//NF)~~

* * *

This memorandum has two main parts. It begins with a background discussion of [redacted] ("Foreign Powers") targeted in the Application, the threat they pose, their use of the Internet, and the relevance and value to U.S. national security of metadata collection in bulk. The background discussion also summarizes how the bulk data is analyzed and some of the

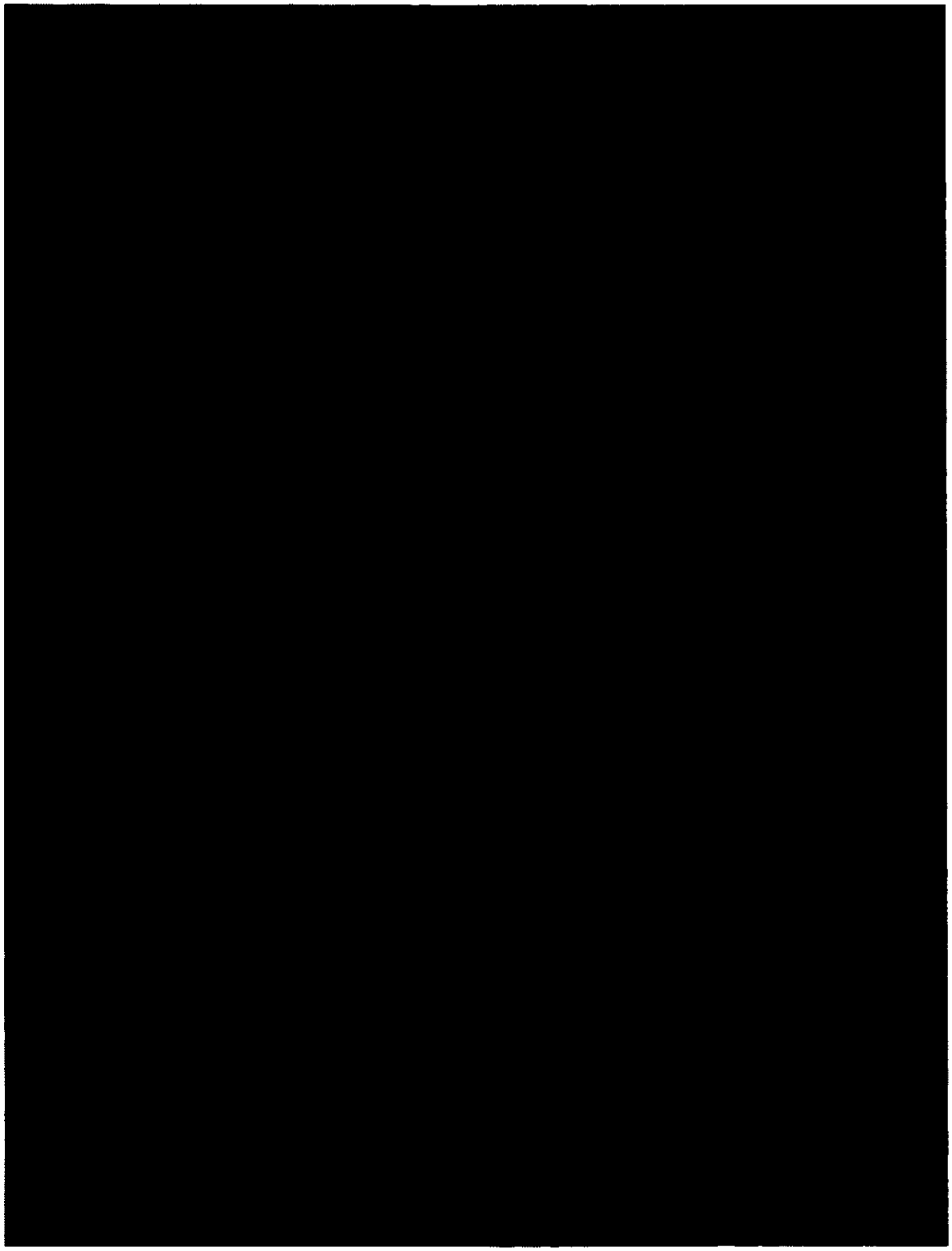
[redacted]

oversight mechanisms that apply to that analysis. The memorandum then sets out a legal analysis of the bulk metadata collection proposed in the Application, including a summary of argument and a detailed legal argument. The legal argument addresses, among other things, the scope of the applicable pen register statutes, the relevance of the data collected, the nature of the metadata proposed to be collected under those statutes, the constitutionality of such collection under the Fourth Amendment, and the issue of access to previously collected metadata that now resides in Government databases. ~~(TS//SI//NF)~~

BACKGROUND

I. Foreign Powers Threat (U)

As demonstrated in previous filings by the Government in matters before this Court, the Foreign Powers targeted in the attached Application present persistent, lethal, and long-term threats to the United States and its interests abroad. A document recovered from [redacted] Declaration of Michael E. Leiter, Director of the National Counterterrorism Center ("NCTC") (filed at docket number [redacted] ("NCTC Declaration"), at 6. At the same time, according to the U.S. Intelligence Community (IC), [redacted] *Id.* at 89. [redacted] *Id.* The following summary of the threats posed by these Foreign Powers is supported by the NCTC Declaration, which provides greater detail on the targeted Foreign Powers' terrorist activities. ~~(TS//HCS//NF)~~



[redacted]

II. Foreign Powers' Use of the Internet ~~(S)~~

As explained in detail in the Declaration of General Keith B. Alexander, U.S. Army, Director of the NSA ("DIRNSA") in support of the Application (the "DIRNSA Declaration"), terrorists use Internet communications for many of the same reasons as the average person: [redacted]

[redacted]

[redacted] *Id.* Use by terrorists of the specific techniques noted above and detailed in the DIRNSA Declaration demonstrates why it is necessary for NSA to collect and maintain access to a repository of bulk metadata associated with Internet communications in order to best protect against acts of international terrorism against the United States and its interests. ~~(S//SI)~~

While all Internet communications are potentially the source of valuable foreign intelligence information, NSA believes that metadata associated with [redacted] is of particular importance. *Id.* ¶ 14 n.9. [redacted] *See* Declaration of Lieutenant General Keith B. Alexander, U.S. Army, Director of the NSA, Ex. A to the Compliance Report, at 20-23. ~~(TS//SI//NF)~~

NSA's experience has shown that terrorists use [redacted] DIRNSA Decl. ¶ 14 n. 9.

A. Discovering the Enemy: Metadata Analysis ~~(TS//SI//NF)~~

While the Foreign Powers' exploitation of the Internet poses a daunting challenge to the IC, it also presents a great opportunity. As summarized above and described in greater detail in the DIRNSA Declaration, [redacted]

Analysis of the metadata from this Internet traffic can be a powerful tool for discovering enemy communications. However, Foreign Powers take affirmative and intentional steps to [redacted]

[redacted] *Id.* ¶ 21. Identifying these enemy communications in the billions of bits of Internet traffic, however, is like finding a needle in a haystack. For analysts to have the best chance at finding the terrorists, they need a mechanism to convert the Internet stream of communications traffic into something that can be searched in a targeted way. The mechanism for accomplishing that is the extraction of the metadata from the stream of Internet communications (without collecting the content of the communications) and storing it in a database for later analysis. Collecting metadata is the best avenue for solving this fundamental problem: although investigators do not know exactly where the terrorists' communications are hiding in the billions of bits of data flowing through the United States today, we do know that they are there, and if we place the metadata in a repository now, we will be able to use it in a targeted way to find the terrorists tomorrow. *See id.* ¶¶ 21-23. ~~(TS//SI//NF)~~

Collecting metadata from that stream creates invaluable capabilities for analysts that are otherwise unavailable. Most significantly, it allows for retrospective "contact chaining." *See id.* ¶ 26. [redacted] By examining metadata that has been collected over a period of time, analysts can search to find the contacts associated with that "seed" identifier. The ability to see who communicates with whom may lead to the discovery of other terrorist operatives, or it may help to identify hubs or common contacts between targets of interest whose relationships were previously unknown. Indeed, NSA's systems would automatically identify not only the first tier of contacts made by the seed, but also the contacts associated with the first tier identifiers. *Id.* ¶¶ 22-25, n.12. Going

out to the "second hop" enhances the ability of analysts to find additional terrorist connections. A seed e-mail address, for example, may be in touch with several e-mail addresses previously unknown to analysts. Following the contact chain out to the second hop to examine the contacts made by those e-mail addresses may reveal a contact that connects back to a different terrorist-associated e-mail address already known to the analyst. *Id.* ¶ 24 n.12. ~~(TS//SI//NF)~~

The capabilities offered by such searching of collected metadata are vastly more powerful than chaining that might be performed through prospective pen registers targeted at individual e-mail accounts. If investigators find a new identifier when [redacted] ability to trace terrorist connections by chaining two steps out from the original target. Instead, to find that second tier of contacts, a new individual pen register would have to be targeted at each e-mail account identified in the first tier. The time it would take to acquire the new pen registers would necessarily mean losing valuable data. And the data loss in the most critical cases would only be increased by terrorists' propensity for frequently changing their e-mail addresses. *Id.* ¶ 27. ~~(TS//SI//NF)~~

As proposed in the Application, analysts would query the bulk data with e-mail addresses or other identifiers as to which there is reasonable, articulable suspicion ("RAS") that the

identifier is associated with one of the targeted Foreign Powers or individuals. *Id.* ¶¶ 24, 31. [redacted] Successful exploitation of the Internet communications of the Foreign Powers requires that NSA is in a constant state of development and discovery, as the terrorists [redacted] Metadata analysis contributes to this critical target monitoring, development and discovery by providing information that an analyst can use to determine various intelligence information, including but not limited to [redacted] *Id.* ¶ 25. Thus, the collected metadata provides an invaluable capability that could not be reproduced through any other mechanism because it allows analysts to bridge the gap between a known identifier and an unknown identifier, even where a terrorist has practiced strict operations security. ~~(TS//SI//NF)~~

B. Targeting the Relevant Data for Collection ~~(S)~~

Performing the metadata analysis described above necessarily requires collecting data in bulk. In other words, it entails collecting data on a significant number of communications that will not ever be found to have a connection with terrorists. The breadth of the collection, however, is necessary. The very reason for collecting the data to preserve it for later analysis is that it is [redacted]

~~TOP SECRET//HCS/COMINT//ORCON,NOFORN~~

[redacted] Effective metadata analysis requires broad collection and archiving of metadata. *See id.* ¶¶ 21-22. ~~(TS//SI//NF)~~

NSA will [redacted]

As discussed in more detail in Part II of this memorandum, that is consistent with the pen register statutes, which require specification of the "location" of relevant facilities, "if known." 50 U.S.C. § 1842(d)(2)(A)(iii). ~~(TS//SI//NF)~~

Under the Application, NSA's extraction of metadata would focus upon certain categories of data that are present [redacted] In particular, the NSA's current metadata collection efforts are focused on [redacted] types of data that fit in [redacted] categories. *Id.* Tab 2. Those [redacted] categories are communications addressing information, [redacted] The [redacted] types of metadata are [redacted] *Id.* These

~~TOP SECRET//HCS/COMINT//ORCON,NOFORN~~

types of metadata are useful in the investigation and analysis regarding the Foreign Powers through contact chain queries, a sophisticated means of identifying associations among individuals through exploitation of Internet communications metadata. *Id.* ¶¶ 23-24. ~~(TS//SI//NF)~~

All of the information collected by NSA's collection and retention systems would be subject to validation at collection and some of it would be subjected to multi-level validation before being stored in the NSA's repositories. An example of these validation checks are [redacted]

The ability of NSA analysts to access the information collected under docket number PR/TT [redacted] and previous dockets is vital to NSA's ability to fully carry out its counterterrorism intelligence mission. *Id.* ¶ 13 n.6. Without access to that data, there would be [redacted] *Id.* ~~(TS//SI//NF)~~

C. Searching the Metadata ~~(S)~~

[redacted]

[redacted]

[redacted] *Id.* ¶ 17. [redacted]

Id. ¶ 17. [redacted]

Id. ¶ 18. [redacted]

Id. ¶ 17. ~~(TS//SI//NF)~~

After the NSA has collected and retained the metadata, the use of that data will be subject to strict procedures and safeguards. First, NSA will store and process the collected metadata in repositories within secure networks under NSA's control. *Id.* ¶ 29. The metadata will carry unique markings such that software and other controls (including user authentication services) can restrict access to it to only authorized personnel. *Id.* NSA analytic personnel will query the metadata repository solely with RAS-approved identifiers (such as an e-mail address). *Id.* ¶¶ 24, 31.

The repositories will store, and the queries will address, metadata from the prospective collection proposed in the Application, as well as data obtained from the authority in docket number PR/TT [redacted] and previous dockets. The ability of NSA analysts to access the information collected under docket number PR/TT [redacted] and previous dockets is vital to NSA's ability to fully carry out its counterterrorism intelligence mission. *Id.* ¶ 13 n.6. Without access to that data, there will be a substantial gap in the information available to NSA. *Id.* ~~(TS//SI//NF)~~

Second, NSA will apply the procedures to ensure appropriate dissemination of the metadata. NSA will apply the minimization and dissemination requirements and procedures of Section 7 of USSID 18 to any results from queries of the metadata disseminated outside of NSA in any form. *Id.* ¶ 32. In addition, prior to disseminating any U.S. person information outside NSA, one of the officials listed in Section 7.3(c) of USSID 18 (*i.e.*, the Director of NSA, the Deputy Director of NSA, the Director of the Signals Intelligence Directorate (SID), the Deputy Director of the SID, the Chief of the Information Sharing Services (ISS) office, the Deputy Chief of the ISS office, and the Senior Operation Officer of the National Security Operations Center) must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance. *Id.* ~~(TS//SI//NF)~~

Third, NSA's collection, access, and dissemination of information obtained pursuant to the authority requested in the Application will be subject to rigorous internal and external oversight. At NSA, the Office of the Director of Compliance (ODOC), the Office of the General Counsel (OGC), and the Inspector General (IG) will conduct oversight of the activities described in the Application and Declaration; oversight will also be conducted by the National Security Division (NSD) of the Department of Justice (DOJ). In addition, the Office of the Director of National Intelligence (ODNI) has independent responsibility over the IC and must ensure that NSA's intelligence activities are conducted in compliance with the law. Accordingly, ODNI personnel may participate in the oversight activities described below. Specifically:

(i) NSA's OGC and Office of the Director of Compliance (ODOC) will ensure that personnel with access to the metadata receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and retention of the metadata and the results of queries of the metadata and will maintain records of such training. OGC will provide NSD/DoJ with

copies of all formal briefing and/or training materials (including all revisions thereto) used to brief/train NSA personnel concerning this authority.

(ii) NSA's ODOC will monitor the implementation and use of the software and other controls (including user authentication services) and the logging of auditable information referenced above.

(iii) NSA's OGC will consult with NSD/DoJ on all significant legal opinions that relate to the interpretation, scope, and/or implementation of this authority. When operationally practicable, such consultation shall occur in advance; otherwise NSD will be notified as soon as practicable.

(iv) At least once during the authorization period, NSA's OGC, ODOC, NSD/DoJ, and any other appropriate NSA representatives will meet for the purpose of assessing compliance with this Court's orders. Included in this meeting will be a review of the metadata collected to ensure that only those categories or types of information described in Tab 2 are being collected. The results of this meeting will be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authority requested herein.

(v) At least once during the authorization period, NSD/DoJ will meet with NSA's Office of the Inspector General to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders.

(vi) At least once during the authorization period, NSA's OGC and NSD/DoJ will review a sample of the justifications for RAS approvals for identifiers used to query the metadata.

(vii) Prior to implementation, all proposed automated query processes will be reviewed and approved by NSA's OGC, NSD/DoJ, and the Court.

DIRNSA Decl. ¶ 34. ~~(TS//SI//NF)~~

Finally, approximately every thirty days, NSA shall file with the Court a report that includes a discussion of the queries made since the last report and NSA's application of the RAS standard. In addition, should the Government seek renewal of the requested authority, NSA shall also include in its report detailed information regarding any new facility proposed to be added to such authority and a description of any changes proposed in the collection methods, to include functioning and control of the pen registers and trap and trace devices. *Id.* ¶ 35. ~~(TS//SI//NF)~~

SUMMARY OF ARGUMENT

1. The pen register provisions in FISA authorize the Government to apply to the Court "for an order . . . authorizing or approving the installation or use of a pen register or trap and trace device" where two essential requirements are met. 50 U.S.C. § 1842(a)(1).[5] (U)

The first requirement is that the pen register be installed or used for certain specified investigations. *Id.* In particular, a pen register may be sought "for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution which is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order." *Id.* (U)

In this case, as explained in more detail in the Application, DIRNSA Declaration, and NCTC Declaration, the pen register order is sought for investigations to protect against international terrorism by [redacted] as well as other unknown persons in the United States and abroad who are affiliated with them. These investigations are being conducted by the FBI pursuant to guidelines approved by the Attorney General pursuant to Executive Order 12333, as amended, and to the extent the subjects of investigation are United States persons, the investigations are not being conducted solely on the basis of activities protected by the First Amendment. *See* 50 U.S.C. § 1842(a)(1). Thus, the

[5] The argument Section contains a more complete discussion of all requirements for issuance of a pen register order. This summary focuses only on the most significant requirements. (U)

first requirement in the statute is met. In this respect, the current Application is no different from Applications previously granted by this Court. ~~(TS//SI//NF)~~

The second requirement is that the pen register Application include a "certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1842(c)(2). In this case, as explained in more detail in the DIRNSA Declaration and elsewhere in the Application, the information sought by the pen register is "foreign intelligence information" which is relevant to ongoing investigations to protect against international terrorism that are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution. Thus, the second requirement is met. The essential theory of relevance advanced in the current Application remains what it was in prior Applications granted by the Court – *i.e.*, that data collected in bulk is relevant to the ongoing investigations because of the analysis that bulk collection permits, even if the vast majority of the collected metadata does not in fact pertain to any terrorist. ~~(TS//SI//NF)~~

Where the requirements are met, the statute provides that a judge of this Court "shall enter an ex parte order as requested, or as modified, approving the installation and use of a pen register or trap and trace device." 50 U.S.C. § 1842(d)(1). The Court's order itself must satisfy three main requirements that are set forth in the statute. (U)

First, the order "shall specify" the "identity, if known, of the person who is the subject of the investigation." 50 U.S.C. § 1842(d)(2)(A)(i). In this case, as discussed above and in the DIRNSA Declaration and elsewhere, the "persons" who are the subjects of the investigations are the Foreign Powers and unknown persons in the United States and abroad who are affiliated with

them. *See* 50 U.S.C. §§ 1801(a), (m), 1841(1) (definition of "person" includes foreign powers, such as international terrorist groups and foreign governments). Again, in this respect the current Application is no different than other Applications previously granted by the Court. ~~(TS//SI//NF)~~

Second, the Court's order must also specify "the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied." 50 U.S.C. § 1842(d)(2)(a)(ii). In this case, as discussed in the DIRNSA Declaration, those persons are certain providers of telecommunications and related services, [redacted] *See* 50 U.S.C. §§ 1801(m), 1841(1) (definition of "person" includes corporations). Prior Applications likewise applied to telecommunications providers. ~~(TS//SI//NF)~~

Third and finally, the Court's order must specify the "attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order." 50 U.S.C. § 1842(d)(2)(a)(iii). The current Application proposes a different approach to this third and final element of the Court's order. ~~(TS//SI//NF)~~

a. At the outset, the current Application would expand the list of "attributes" of communications that may be collected. Prior orders authorized collection of [redacted] categories of metadata from e-mail [redacted] communications, and the current Application refers to [redacted] categories composed of [redacted] types. By way of illustration, [redacted] As

explained in Tab 2 to the DIRNSA Declaration, NSA will not collect any [redacted] without the Court's prior approval. ~~(TS//SI//NF)~~

As explained in Part I.C. of this Memorandum, all of the metadata to be collected under the current Application – including metadata types not previously authorized for collection – are within the scope of the pen register statutes, because all are "dialing, routing, addressing, and signaling information" and none is "contents."[6] Congress did not define the terms "dialing, routing, addressing, or signaling information," and these terms should be read in accordance with their broad ordinary meaning. Even if some of the metadata that is the subject of the Application is not "dialing, routing, addressing, or signaling" information, it may still be collected under the pen register statutes, because the statutes may be read to permit a pen register to acquire all communications information other than the "contents" of communications. That interpretation follows from the text of the statute and the legislative history of the USA PATRIOT Act. Pub. L. No. 107-56, § 206, 115 Stat. 272, 282 (2001). ~~(TS//SI//NF)~~

[6] As the Court is aware, the terms "pen register" and "trap and trace device" as used in FISA are defined in 18 U.S.C. § 3127, part of the U.S. Code chapter governing pen register surveillance in criminal cases. 50 U.S.C. § 1841(2). Under Section 3127(3), a "pen register" is a device or process which "records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication." Similarly, a trap and trace device is a device or process which "captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." 18 U.S.C. § 3127(4). ~~(TS//SI//NF)~~

It is difficult to provide a one-to-one comparison between what was collected in the past pen register program and in the current Application because the types of data have been re-organized in this Application to provide a better organizational framework. That said, the general description of data that is sought under this Application that was not the subject of any of the previous orders are metadata [redacted] *See* DIRNSA Decl. Tab 2. The Compliance Report filed in docket PR/TT [redacted] provides an exhaustive account of the specific types of metadata that were collected outside the authority of the previous pen register Orders. The authority sought in this Application includes the authority to collect that metadata, which the Government submits may be lawfully collected under the authority of the pen register statute. ~~(TS//SI//NF)~~

Congress intended the USA PATRIOT Act's amendments to "reinforce the statutorily prescribed line between a communication's contents and non-content information" – a line that it characterized as "identical to the constitutional distinction drawn by the U.S. Supreme Court in *Smith v. Maryland*, 442 U.S. 735, 741-43 (1979)." H.R. Rep. No. 107-236, at 53 (2001). In other words, "dialing, routing, addressing, and signaling information" and "contents" may be read as mutually exclusive categories that together define the universe of information that might be acquired (with the appropriate authorization) from a wire or electronic communication. Accordingly, a pen register may collect all non-content information from the communications passing through the transmission facility to which it is attached or applied, where "content" is defined as "any information concerning the substance, purport, or meaning of" a wire or electronic communication. 18 U.S.C. §§ 2510(8), 3127(1).[7] ~~(TS//SI//NF)~~

[redacted]

[7] Even if the Court were to disagree with this conclusion, and identify some intermediate data that are neither "contents" nor "dialing, routing, addressing, or signaling information," a pen register may collect that intermediate data. To qualify as a pen register, a device or process must capture, record or decode dialing, routing, addressing, and signaling information, but nothing in the statutory definition forbids the additional acquisition of other information transmitted by a wire or electronic communications facility, as long as that other information is not content or billing information. (U)

[redacted] Information that is both located in the appropriate field and is in the appropriate format for addressing is by definition "addressing information." ~~(TS//SI//NF)~~

Nothing in the pen register statutes requires "addressing information" to be used for the functional or technical purposes of addressing at the time of collection. The statute defines a pen register as a device or process that records or decodes addressing information "transmitted by an instrument or facility from which a wire or electronic communication is transmitted," as long as the information is not "contents," 18 U.S.C. § 3127(3). As proposed in the Application, NSA's pen registers will record and decode metadata only from Internet communications that are transmitted on the facilities identified in Tab 1 to the DIRNSA Declaration, including [redacted] sent e-mail [redacted]

b. The current Application also differs from its predecessors with respect to the "facilities" from which metadata will be collected. The Court's prior orders allowed NSA to conduct surveillance on [redacted]

[redacted] As explained in Tab 1 to the DIRNSA Declaration, the current Application treats [redacted] The statute requires nothing more. ~~(TS//SI//NF)~~

2. The collection and use of the bulk metadata sought in the Application is consistent with the Fourth Amendment. *See Smith v. Maryland*, 442 U.S. 735 (1979). In *Smith*, the Court held that "the installation and use of a pen register" was not a "search" under the Fourth Amendment. *Id.* at 736. Like the pen register in *Smith*, the pen register in this matter will acquire only the non-content attributes of communications indistinguishable from addressing information voluntarily conveyed to third parties. It therefore does not implicate the Fourth Amendment. ~~(TS//SI//NF)~~

Even if the Fourth Amendment protected some of the collected information [redacted] collection of that information would be reasonable, and therefore constitutional, in light of the unique protections governing the pen register bulk collection program, and under the "special needs" doctrine recognized by the Supreme Court and the Foreign Intelligence Surveillance Court of Review. *See, e.g., Griffin v. Wisconsin*, 483 U.S. 868,

[9] Even if the Court disagreed with that assertion, and concluded that there are [redacted] it would not affect the analysis, because FISA does not require specification of individual facilities for pen register surveillance, but only the "*location* of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied," and even then only if the location "is known." 50 U.S.C. § 1842(d)(2)(A)(iii) (emphasis added). In this respect, FISA's pen register provisions (Title IV) differ significantly from its provisions governing full-content collection (Title I), which require the Court to find probable cause that a foreign power or agent of a foreign power is using or about to use each of the facilities at which the surveillance will be directed, and the Court's orders to specify the nature as well as the location of each such facility. 50 U.S.C. § 1805(a)(2)(B), (c)(1)(B). ~~(TS//SI//NF)~~

873 (1987); *In re Sealed Case*, 310 F.3d 717, 742 (FISA Ct. Rev. 2002); *In re Directives*, 551 F.3d 1004, 1007 (FISA Ct. Rev. 2008). ~~(TS//SI//NF)~~

3. In addition to granting the Application for prospective collection, the Court should grant commensurate and continuing authority to query metadata previously collected. That is the case even though, as discussed in the Compliance Report, the prior pen register collection in certain ways exceeded the scope of the Court's orders. As detailed in the DIRNSA Declaration, without access to the previously collected information, the value of the pen register will be dramatically reduced. *See* DIRNSA Decl. ¶ 13 n.6. ~~(TS//SI//NF)~~

From the beginning, this Court has asserted a continuing jurisdiction over the bulk pen register program that is both prospective and retroactive, regulating in each authorization order the collection and querying of all data collected under all prior orders. The Government supported that assertion of jurisdiction in 2004, and continues to do so today in light of the unique nature of the bulk pen register program. That expansive jurisdiction, however, gives the Court authority to grant access to the stored metadata even though some of it exceeded the scope of the Court's prior orders. Indeed, the Court's rules give it discretion in this area, *see* FISC R. 10(c)(iv), and the Court should exercise that discretion to permit retention and querying of data that, although collected in violation of the Court's prior orders, is within the scope of the statute, Constitution, and the current proposed order, and is critical to the proper functioning of the bulk pen register surveillance program. The Court should not require destruction of the overcollected data, and should lift its [redacted] order generally barring access to the stored data. Additionally, NSA asserts that [redacted]

[redacted]

[redacted] DIRNSA Decl. ¶ 20 n.11. ~~(TS//SI//NF)~~

I. The Application Fully Complies with All Statutory Requirements. (U)

FISA provides a mechanism for the Government to obtain the metadata that is necessary to perform the type of contact chaining analysis described above that is vital for counterterrorism and foreign intelligence investigations. As this Court has previously ruled in docket number PR/TT [redacted] and subsequent orders renewing and modifying that authority, such data may lawfully be obtained using a pen register obtained pursuant to 50 U.S.C. § 1842.[10] The Government's Application satisfies all four statutory requirements of Section 1842(a)-(c), which are: (1) the device or process used to effect the surveillance must qualify as a "pen register"

---

[10] In docket number PR/TT [redacted] and subsequent applications renewing and modifying that authority, this Court authorized installation and use of pen registers similar to those described above. Those orders allowed NSA to collect, in bulk, metadata associated with e-mail [redacted] communications that traversed [redacted] In reliance on representations made by the Government since submission of the initial pen register application in 2004, the Court approved NSA's pen register collection as part of an effort to develop foreign intelligence on the activities of [redacted] The Court's [redacted] Order in docket number PR/TT [redacted] and preceding docket numbers extended authorization to target [redacted] The Court's [redacted] Order in docket number PR/TT [redacted] and preceding docket numbers extended authorization to target [redacted] (TS//SI//NF)

On [redacted] the Government orally notified the Court of a potential compliance problem. The compliance problem involved the collection of data that possibly fell outside the scope of the order, which permitted bulk collection of specified categories of information for e-mail [redacted] associated with investigations of the targeted Foreign Powers. A formal written notification to this Court followed on [redacted] On [redacted] this Court was informed of the Government's decision not to seek renewal at that time of the pen register collection in PR/TT [redacted] On [redacted] when the existing order expired, the Court entered an order directing that the Government not access for analytic or investigative purposes the information collected under the prior pen register orders unless the access was necessary to protect against an imminent threat to human life. Supplemental Order and Opinion, docket number PR/TT [redacted] at 5. This Court did authorize the Government to access the previously collected metadata for purposes of conducting non-analytic technical reviews. ~~(TS//SI//NF)~~

As detailed in the Compliance Report, the information collected included data that was not within the categories specified by the pen register orders. For the reasons stated herein, the data could lawfully have been collected under the pen register statute and the Fourth Amendment and indeed proposed for collection in the current Application. ~~(TS//SI//NF)~~

and/or "trap and trace device," 50 U.S.C. §§ 1841(2), 1842(a)(1); (2) the Application must have been approved by the Attorney General or a designated government attorney, 50 U.S.C. § 1842(c); (3) the Application must include the identity of the U.S. Government official seeking to use the pen register covered by the Application, 50 U.S.C. § 1842(c)(1); and (4) the Applicant must certify that the information "likely to be obtained" is foreign intelligence or is "relevant to an ongoing investigation to protect against international terrorism." 50 U.S.C. § 1842(c)(2). ~~(TS//SI//NF)~~

The second and third statutory requirements are clearly met. The Attorney General has approved the Application, and the Application specifies that the Director of the NSA is the government official seeking to use the pen register devices covered by the Application. The only requirements that merit further discussion are that the devices or processes used to effectuate the surveillance must qualify as pen registers and trap and trace devices and that the Application must contain a certification of relevance. This Court has previously found that bulk collection of metadata from e-mail [redacted] met the requirements of Section 1842, and should do so again here. ~~(S)~~

A. Scope of Review (U)

Section 1842(d) of FISA expressly limits the Court's discretion to consider an Application for a pen register. It states

> [u]pon an application made pursuant to this Section, the judge shall enter an ex parte order as requested, or as modified, approving the installation and use of a pen register or trap and trace device if the judge finds that the application satisfies the requirements of this Section. (U)

In keeping with the plain language of this provision, as the Government has argued to the Court in the past, judicial review of an Application for a pen register is limited.[11] In her Opinion and Order in docket number PR/TT [redacted] did not accept these arguments. *See* Opinion and Order, docket number PR/TT [redacted], at 26-27. Instead, Judge Kollar-Kotelly conducted an independent evaluation of the basis of the Certification of relevance, found it persuasive, and granted the Government's Application in docket number PR/TT [redacted]. The Government continues to believe that the language of the Certification should be determinative of this issue and incorporates those previously advanced arguments as if set forth more fully herein. However, acknowledging the Court's Opinion and Order in docket number PR/TT [redacted], this Memorandum of Law and Fact also discusses the relevance of the information sought to these ongoing investigations to protect against international terrorism. ~~(TS//SI//NF)~~

B. The Information Sought Through the Application is Relevant to an Ongoing Investigation to Protect Against International Terrorism. ~~(S)~~

The metadata sought through the Application is unquestionably relevant to an ongoing investigation to protect against international terrorism because it seeks to obtain non-content information relating to the Foreign Powers and those unknown individuals associated with them who may be plotting terrorist attacks and discover [redacted] as to how, and with whom, these Foreign Powers communicate while engaged in these terrorist conspiracies. The nature and volume of worldwide Internet communications provides a ready-made realm within which

[11] Section 1842(d)(1) directs that an order "shall" be entered by the judge if the Court finds that the Application satisfies Section 1842's requirements, one of which is that the Application contain a certification about the information likely to be obtained. 50 U.S.C. § 1842(c)(2). Like the criminal pen register provision upon which it is modeled (18 U.S.C. §§ 3121-27), FISA's pen register provisions limit judicial review to ensuring that the statutory requirements for an Application have been satisfied – *e.g.*, that the Application contains the required certification. *See United States v. Hallmark*, 911 F.2d 399 (10th Cir. 1990); *In re Application for an Order Authorizing Installation and Use of a Pen Register and Trap and Trace Device*, 846 F. Supp. 1555 (M.D. Fla. 1994). The statute does not call for the Court to look behind the Certification or to conduct an independent review of the information likely to be acquired. ~~(S)~~

terrorists conceal their activities ostensibly within plain sight – through communications metadata processed through the same communications pathways as legitimate, non-terrorist related communications. That the majority of metadata collected previously, and that is proposed to be collected now, through this program will not be terrorist-related does not lessen the relevance of the information to these ongoing international terrorism investigations. Rather, when viewed in the context of the time span over which these terrorist groups conceptualize, plan, and carry out their terrorist attacks, the fact that the metadata relating to terrorist communications hides within the vast stream of otherwise legitimate Internet metadata only heightens the relevance of and necessity to collect the metadata sought in the Application. DIRNSA Decl. ¶¶ 14, 21-23. ~~(S)~~

Relevance here is not properly measured through scientific metrics or the number of reports issued over the course of a year and it does not require a statistical "tight fit" between the volume of proposed collection and the much smaller proportion of information that will be directly "relevant" to investigations of the Foreign Powers to protect against international terrorism. *See* Opinion and Order, docket number PR/TT [redacted], at 49-50. Rather, relevance here properly is measured in packets of metadata that, over an extended period of time, can help to fill in information that provides a more complete picture of the communications practices of these Foreign Powers and their agents. ~~(TS//SI//NF)~~

The metadata that has been and would be acquired through this collection is pertinent to the FBI's investigations into the Foreign Powers because, when collected and analyzed, the metadata provides assistance to investigators in putting together the complete picture of how these Foreign Powers and their agents communicate over extended periods of time. *See, e.g.*, 13 Oxford English Dictionary 561 (2d ed. 1989) ("relevant" means "[b]earing upon, connected

with, pertinent to, the matter in hand"); Webster's Third New Int'l Dictionary 1917 (1993) ("relevant" means "bearing upon or properly applying to the matter at hand . . . pertinent"); *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 351 (1978) (noting that the phrase "relevant to the subject matter involved in the pending action" in Fed. R. Civ. Proc. 26(b)(1) has been "construed broadly to encompass any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case"); Fed. R. Evid. 401 ("'Relevant evidence' means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence."). ~~(TS//SI//NF)~~

Here, a substantial portion of the metadata that has been and will be collected does not relate to these Foreign Powers and their agents. That does not weigh against a determination that the information sought is relevant to an ongoing investigation to protect against international terrorism. To the contrary, as explained in the DIRNSA Declaration, this intelligence tool – one of many used by the Government in its efforts to counter the threat posed by these Foreign Powers – inherently requires collecting and storing large volumes of the metadata to enable later analysis -- analysis that may continue for years for it to be truly effective. Unless metadata is stored at the time of transmittal, it will be lost forever. DIRNSA Decl. ¶ 22. Therefore, all of the metadata collected is relevant because it is necessary for the success of the investigative tool. ~~(TS//SI//NF)~~

C. The Relevant Pen Register Statutes Are Satisfied. (U)

The collection devices[12] [redacted] will record, decode, and capture data that is exchanged between Internet users [redacted] The communications to be collected would fall into [redacted] categories: [redacted] sections I.C.3. and II.A. of this memorandum. ~~(TS//SI//NF)~~

1. The Proposed Collection Will Use "Pen Registers" and "Trap and Trace Devices" As Those Terms Are Defined By Statute. (U)

The devices described in the Application that will be used to accomplish the proposed collection satisfy the statutory definitions of "pen registers" and "trap and trace devices" in 18 U.S.C. §§ 3127(3) and (4) and incorporated into FISA by 50 U.S.C. § 1841(2). Title IV of FISA

[12] The pen register in the Application [redacted] (TS//SI//NF)

authorizes the Attorney General or a designated attorney for the Government to apply to this Court

> for an order or an extension of an order authorizing or approving the installation and use of a pen register or trap and trace device for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution which is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order.

50 U.S.C. § 1842(a)(1). ~~(S)~~

Title IV of FISA expressly incorporates the definitions of the terms "pen register" and "trap and trace device" from 18 U.S.C. § 3127 for use under FISA's pen register provisions. 50 U.S.C. § 1841(2). That Section provides that a "pen register" is

> a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication.[13]

18 U.S.C. § 3127(3).[14] Similarly, a "trap and trace device" is defined as

---

[13] The definition also states that devices or processes used for billing or recording as an incident to billing are not "pen registers." The devices the Government proposes using in its Application do not perform such billing services or collected related information. (U)

[14] "[W]ire communication" for purposes of this provision is defined as

> any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station).

18 U.S.C. § 2510(1). "[E]lectronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system . . . but does not include . . . any wire or oral communication." 18 U.S.C. § 2510(12). The term "[c]ontents" includes "any information concerning the substance, purport, or meaning of [a particular] communication." 18 U.S.C. § 2510(8). These terms are incorporated into the chapter governing the use of pen registers and trap and trace devices. 18 U.S.C. § 3127(1). E-mail [redacted] "electronic communications" within the scope of the pen register statute. See S. Rep. 99-541 at 14 (1986) ("This term [electronic communications] includes electronic mail, digitized transmissions, and video teleconferences"); *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457, 461-62 (5th Cir. 1994). (U)

> a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

18 U.S.C. § 3127(4). (U)

Pen registers historically were used to record the metadata associated with a particular telephone number. With the evolution in communications technology, some courts began to approve the installation and use of pen registers to collect metadata associated with an e-mail account. The USA PATRIOT Act amended Section 3127(3) and (4) of Title 18 to clarify that use of these devices was not limited to telephones[15] and could also be used on computers and cell phones.[16] Pub. L. No. 107-56, § 206, 115 Stat. 272, 282 (2001). Today, orders for use and installation of such devices for Internet communications are routinely granted by federal courts under 18 U.S.C. § 3123 (albeit not for bulk collection). Indeed, this Court has authorized the installation and use of devices substantially similar to the proposed collection devices here and did so after concluding that the collection devices satisfied the pen register statute. Opinion and Order, docket number PR/TT [redacted] at 13-17. ~~(TS//SI//NF)~~

2. The Pen Register Devices Will Collect Specified Attributes of Communications From Facilities [redacted] (U)

The Application explains how [redacted] devices will record, decode, and capture metadata in bulk for e-mail [redacted] communications transmitted by certain facilities. The Government is

[15] Prior to the amendment, a pen register was defined as "a device which records or decodes electronic or other impulses which identify the number dialed or otherwise transmitted on the telephone line to which such device is attached." 18 U.S.C. § 3127(3). Similarly, a trap and trace device was defined as "a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted." 18 U.S.C. § 3127(4). Thus, a pen register was generally used to record outgoing telephone numbers, and a trap and trace device was used to record incoming numbers. (U)

[16] *See* H.R. Rep. No. 107-236, pt. 1 at 53. (U)

not *required* to plead anything in its Application about the facility under Section 1842(c). However, Section 1842(d)(2) requires the Court's order approving the use of a pen register to specify the "identity, if known of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied" and, "if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied." 50 U.S.C. § 1842(d)(2)(A)(ii) & (iii). ~~(TS//SI//NF)~~

In the attached Application, the Government provides this Court with information sufficient to satisfy the statutory requirements for the issuance of an Order. Tabs 1 and 2 of the DIRNSA Declaration include: (1) [redacted] the facilities to which the pen registers and trap and trace devices are to be attached or applied – *e.g.*, [redacted] (2) the attributes of the communications to which the order applies, – *e.g.*, message addresses, such as badguy@[redacted] and (3) [redacted] facilities to which the pen registers and trap and trace devices are to be attached or applied. That level of specificity is ample for the type of collection conducted with a pen register. Use of a pen register does not constitute a search within the meaning of the Fourth Amendment. *Smith v. Maryland*, 442 U.S. 220 (1979). Consequently, the Fourth Amendment's particularity requirement does not apply.[17] *Maryland v. Garrison*, 480 U.S. 79 (1987) (Warrant Clause of the Fourth Amendment

[17] Notably, the facilities requirement for Title IV is less substantial than for Title I of FISA. In contrast to Title IV, orders under Title I of FISA must specify, among other requirements, the "nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known." 50 U.S.C. § 1805(c)(1)(B) (emphasis added). Orders under Title IV of FISA require only "the location of the ... facility" to which the pen register or trap and trace device is to be attached or applied and even that information only "if known." 50 U.S.C. § 1842(d)(2). Thus, the plain text of the requirements for orders under the two FISA provisions require differing degrees of descriptive detail for the facilities to which they apply, and the requirements of Title IV are less stringent than those required of Title I. ~~(S)~~

requires particularity describing the place to be search and the persons or things to be seized.).

~~(TS//SI//NF)~~

3. The Data That Would Be Collected Are Dialing, Routing, Addressing, or Signaling Information Properly Collected Under Section 1842. (U)

All of the data that would be obtained by the collection devices should be considered "dialing, routing, addressing, and signaling information" under a broad interpretation of those terms. That said, even under a narrow interpretation, the vast majority of the data that would be collected under the Application would properly be considered dialing, routing, addressing, and signaling information (and as discussed in the next part of this memorandum, all of the data would be properly collected because they are not the "contents" of a communication).

~~(TS//SI//NF)~~

No case law specifically addresses application of the terms "dialing, routing, addressing, or signaling" to all of the particular types of data that would be collected as proposed in the Application. But this Court has previously authorized the collection of most of the types of data in docket PR/TT [redacted] and previous dockets.[18] Some of these data, such as forms of message addresses like IP address and to/from information, have been found to be lawfully collected by a pen register. *See, e.g., United States v. Forrester*, 512 F.3d 500, 509-11 (9th Cir. 2008) (upholding pen register collection of to/from information, IP address, and total volume of data transmitted for e-mail messages). The remaining data should generally be viewed as the type of

[18] It is difficult to provide a one-to-one comparison between what was collected in the past pen register program and in the current Application because the types of data have been re-categorized in this Application to provide a better organizational framework. The data that are sought under this Application that was not the subject of any of the previous orders are metadata related to [redacted] *See, e.g.*, DIRNSA Decl. Tab 2. These are discussed at *infra*, 39-44. The Compliance Report provides an exhaustive account of the specific types of metadata that were collected outside the authority of the previous pen register Orders. The authority sought in this Application includes the authority to collect that metadata, which the Government submits may be lawfully collected under the authority of the pen register statute. ~~(TS//SI//NF)~~

[redacted] information transmitted in association with electronic communications that pen registers have traditionally collected. ~~(TS)~~

The terms "routing," "addressing," and "signaling" are not defined by Section 3127 and should be interpreted in light of their broad plain meanings.[19] "Routing" is technically defined as "the process of selecting the circuit path for a message." *Newton's Telecom Dict.* 786 (2006, 22nd Ed.). The term "route" is more generally defined as "an established or selected course of travel or action." *Webster's Collegiate Dict.* 1021 (1998, 10th Edition). Thus, "routing information" encompasses the path or means by which information travels or information about the path and means by which information travels. (U)

Similarly, "addressing information" is susceptible to broad interpretation. Newton's Telecom Dictionary describes an "address" as follows: "An address comprises the characters identifying the recipient or originator of transmitted data." *Newton's Telecom Dict.* 87. Webster's Collegiate Dictionary provides a similar definition of "address": "to identify (as a peripheral or memory location) by an address or a name for information transfer." *Webster's Collegiate Dict.* 13. Thus, "addressing information" may be understood to be information that identifies recipients of communications or participants in a communication. Moreover, addressing information may refer to people and/or devices. (U)

Lastly, "signaling information" also potentially has a broad meaning. "Signaling" information is generally understood to represent information transmitted by telephone systems to commence or terminate calls and to register the presence of a cell phone. *Newton's Telecom Dict.* 823. However, the meaning of that term should not be cabined to telephony and should be

[19] "Dialing" is much less ambiguous than the other terms. It presumptively relates to telephones, since the original version of the pen register provisions used that term since it was originally enacted to cover telephony. Accordingly, the Government does not believe that most of the data that would be collected could properly be considered "dialing information." ~~(TS)~~

given broader application, because Congress intended each of these terms to apply to all forms of communications. H.R. Rep. No. 107-236 at 53 (terms were meant to apply "across the board to all communications, media, and to actual connections as well as attempted connections"). The less technical meaning of "signal" is "something that incites to action" or "conveys notice or warning." *Webster's Collegiate Dict.* at 1091. Thus, signaling information should be understood to include transmissions between communications devices (*e.g.*, the user's computer and an ISP's web server) that prompt certain actions or responses associated with a communication or register the presence of a device.[20] ~~(TS//SI//NF)~~

The legislative history suggests that Congress intended these undefined terms to be given broad effect, even beyond their conventional technical meanings. For example, the House Report states that "non-content information contained in the 'options field' of a network packet header constitutes 'signaling' information and is properly obtained by an authorized pen register or trap and trace device." H.R. Rep. No. 107-236 at 53 n.1. The options field of Internet packet header information does not conduct "signaling" in the conventional sense. Rather, it carries data used in the transmission of the packet such as time stamp, security, and routing information. Yet Congress made clear its intent in the legislative history that options field information is subject to collection as part of a pen register order. Accordingly, the Government submits that this Court should not rely on a narrow reading of these statutory terms and that all [redacted] of the attributes or data types specified in the DIRNSA Declaration are one or more of "routing," "addressing," or "signaling" information. ~~(TS//SI//NF)~~

[20] [redacted]

[redacted]

21 [redacted]

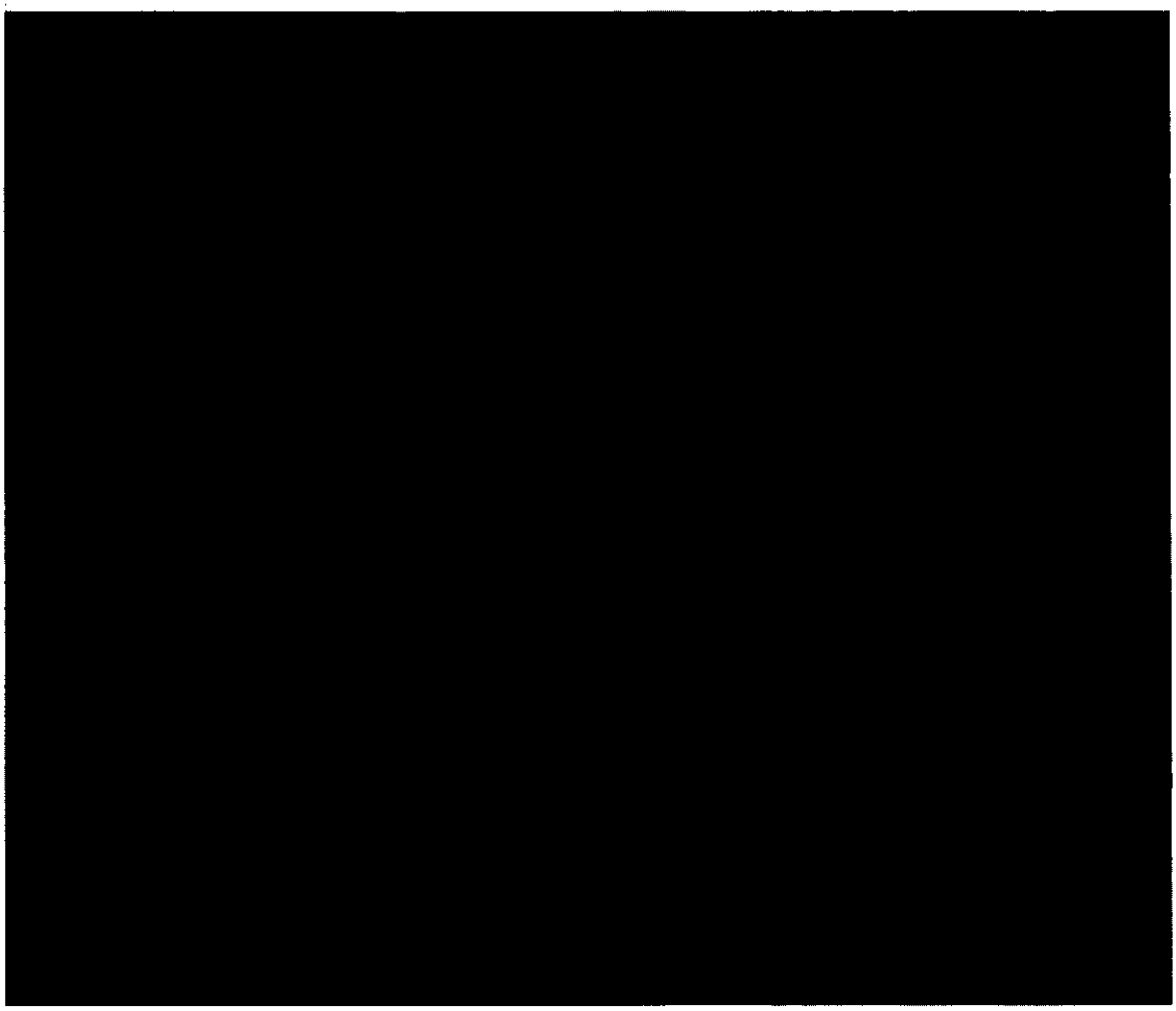
[redacted]

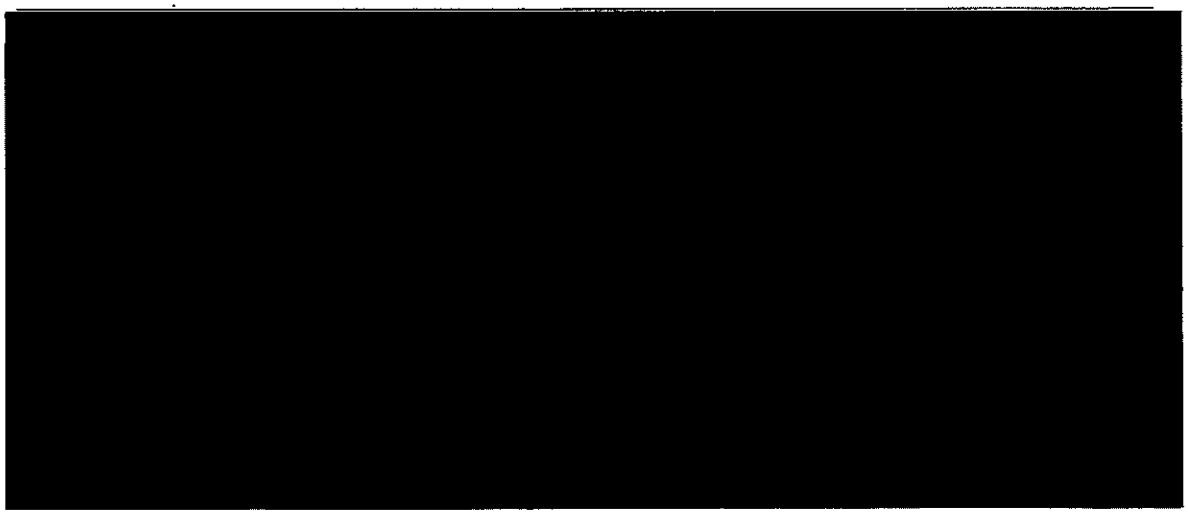
[redacted]

[redacted]

23 [redacted]

24 [redacted]





[redacted]

4. **None of the data That Would Be Collected by the Proposed Collection Devices Is Content.** ~~(TS//SI//NF)~~

None of the data that would be collected under the Application are "contents," as defined by 18 U.S.C. § 2510(8). As this Court determined in docket number PR/TT [redacted], Section 2510(8) of Title 18, rather than Title I of FISA, supplies the operative definition of "contents" for purposes of FISA's pen register provision, 50 U.S.C. § 1842. When Congress added Section 1842 to FISA, it incorporated Title 18's definition of "contents" into FISA's pen register provision (Title IV) by expressly incorporating the Title 18 definitions of "pen register" and "trap and trace device," *see* 50 U.S.C. § 1841(2), which in turn rely on the definitions of "contents" in Title 18, *see* 18 U.S.C. § 3127. *See also* 50 U.S.C. 1801 (specifying the meanings of certain words, including "contents," "[a]s used in this title" – *i.e.*, title I of FISA).

~~(TS//SI//NF)~~

Section 2510(8) defines content to "include[] any information concerning the substance, meaning, or purport of the communication." The Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508 (1986), amended the definition of content under 18 U.S.C. § 2510(8) resulting in a narrower definition of content than under Title I of FISA. The FISA definition of content "includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication." 50 U.S.C. § 1801(n). Section 2510(8)'s amended definition omits any reference to "the identity of

the parties" or "the existence" of the communication. Thus, Section 2510(8)'s definition of content focuses only on information that reveals the meaning of a particular communication and specifically does not include information that identifies the parties to that communication. *See Jessup-Morgan v. Am. Online, Inc.*, 20 F. Supp. 2d 1105, 1108 (E.D. Mich. 1998) (holding that identifying information, such as identification of an account customer, is not content within Section 2510(8)); *see also Hill v. MCI WorldCom Commc'n, Inc.*, 120 F. Supp. 2d 1194 (S.D. Iowa 2000) (billing/invoice information and names, addresses and phone numbers of persons she called are not "contents" under Section 2510(8)). Further, Congress did not intend for transactional records to be considered content. S. Rep. No. 99-541 at 13 ("[T]he amended definition thus distinguishes between the substance, purport or meaning of the communication and the existence of the communication or transactional records about it.").[25] (U)

The data identified in Tab 2 of the DIRNSA Declaration are the type of [redacted] information that should not be considered "content," since they do not reveal the substance, purport, or meaning of the underlying communications. [redacted]

[redacted]

[25] The legislative history of the USA PATRIOT Act indicates that once pen registers were expressly made applicable to Internet communications, Congress had concerns about their potential to collect content information. H.R. Rep. No. 107-23 at 53. However, those concerns were focused on particular types of information that are [redacted]

[redacted]

Thus, the configuration of the pen register devices will help avoid concerns that have been identified by courts in other contexts about the collection of "content" information by devices that the Government has sought to install and use under Title 18's pen register provisions. For instance, in *Brown v. Waddell*, 50 F.3d 285 (4th Cir. 1995), the Court of Appeals found that a clone pager that collected phone numbers pursuant to the criminal pen register provision (18 U.S.C. §§ 3121-27) was not a "pen register device" because it intercepted alphanumeric characters that could constitute content. The court's concern was that such pagers could be used to capture sequences of numbers that went beyond the length of ordinary phone numbers and therefore were more likely to have a coded substantive meaning. *See, e.g.*, *id.* at 293 ("[T]he numbers capable of being so re-transmitted surely would have to be limited to raw telephone numbers to retain pen register status."). Here, however, [redacted] DIRNSA Decl. ¶ 18-19. [redacted] *Id.* at 19 n.10. [redacted]

The validation scheme also helps avoid concerns that have been raised about the use of a pen register to collect [redacted] which have been the subject of several district court opinions. [redacted]

[redacted] Nevertheless, [redacted] Moreover, the validation scheme is consistent with 18 U.S.C. § 3121(c), which mandates that the Government "use technology reasonably available to it" to prevent the capture of the contents of communications. ~~(TS//SI//NF)~~

Cases discussing the distinction between metadata and the content of communications are scarce.[26] Yet, the Court of Appeals' discussion of content in the Fourth Amendment context in *United States v. Forrester* is instructive on the issue of content for Internet communications. The Court of Appeals made an analogy between Internet communications and letters:

> [W]hen the government obtains the to/from addresses of a person's emails or the IP addresses of websites visited, it does not find out the contents of the messages or know the particular pages on the websites the person viewed. At best, the government may make educated guesses about what was said in the messages or viewed on the websites based on its knowledge of the email to/from addresses and IP addresses-but this is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed. Like IP addresses, certain phone numbers may strongly indicate the underlying contents of the communication; for example, the government would know that a person who dialed the phone number of a chemicals company or a gun shop was likely seeking information about chemicals or firearms. Further, when an individual dials a pre-recorded information or subject-specific line, such as sports scores, lottery results or phone sex lines, the phone number may even show that the caller had access to specific content information. Nonetheless, the Court in [*Smith v. Maryland*] and [*Katz v. United States*] drew a clear line between unprotected addressing information and protected content information that the government did not cross here.

812 F.3d at 503, *citing* 495 F.3d 1041, 1049 (9th Cir. 2007). (U)

---

[26] In one case a magistrate held that information from the subject lines of e-mails, application commands, search queries, requested file names, and file paths were content. *In re Application of the United States of America for an Order Authorizing the Use of a Pen Register and Trap on [xxx] Internet Service Account/User Name [xxxxxxx@xxx.com]*, 396 F. Supp. 2d 45, 49 (D. Mass 2005). (U)

To extend this analogy to the physical world using the [redacted] types of data in Tab 2 of the DIRNSA Declaration, the metadata collected by the devices could be likened to information concerning a [redacted] It is information regarding [redacted]. While these pieces of information provide details about [redacted] they reveal nothing about *what* it actually says. ~~(TS//SI//NF)~~

The applicability of this reasoning to certain categories of metadata sought to be collected is uncontroversial. However, the [redacted] metadata discussed in detail above – [redacted] – also warrant in depth treatment here. ~~(TS//SI//NF)~~

[redacted] This metadata does not reveal the substance, meaning, or purport of the communication between user and provider. Rather, it consists of [redacted] ~~(TS//SI//NF)~~

Second, as previously discussed, [redacted] Accordingly, it also should not be considered content. ~~(TS//SI//NF)~~

Lastly, the "to," "from," "cc," and "bcc" information that would be collected is similarly not content of those communications. That information is indistinguishable from other addressing information used for purposes of identifying the parties to a communication; identifying information was removed from the definition of content by ECPA. S. Rep. No. 99-541 at 13. Moreover, as explained above, this information is obtained from [redacted] and should not be regarded as the "substance, purport, or meaning" of the communication [redacted] (TS//SI//NF)

Thus, considering the technical precautions that will be taken and the manner in which the definition of "contents" provided by Section 2510(8) as amended by ECPA has been interpreted, the metadata that would be collected would constitute non-content information permissibly obtained using a pen register device. ~~(TS//SI//NF)~~

5. Pen Registers May Collect Any Non-Content Data Associated With The Transmission of Electronic Communications, Regardless of Whether It Is Dialing, Routing, Addressing, and Signaling Information. (U)

Even if certain types of data that the Government proposes to collect under this Application are not dialing, routing, addressing, or signaling information, they still may lawfully

be collected by a pen register authorized under FISA because they are not "content." The text and legislative history of the pen register statute may be interpreted to permit a pen register to collect *any* non-content data, so long as the device or process used to collect it also records or decodes "dialing, routing, addressing, and signaling information and does not collect the content of any communications." In other words, to the extent that some communications data are neither dialing, routing, addressing, and signaling information nor "contents," a pen register can obtain them if it also records, decodes, or captures dialing, routing, addressing, and signaling information. ~~(TS//SI//NF)~~

The text of Sections 3127(3) and (4) do not limit pen register collection to dialing, routing, addressing, and signaling information.[27] Rather, Sections 3127(3) states that a pen register is a "device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communications is transmitted, provided however, that such information shall not include the contents of any communication." The definition of a trap and trace device in Section 3127(4) is similar. While a pen register must perform those functions to qualify as a pen register, neither the definitions of a pen register or trap and trace device in 18 U.S.C. § 3127, nor Section 1842 of FISA, limits the information they may collect to dialing, routing, addressing, and signaling information. The only express limitation imposed on the type of information these devices may collect is the prohibition on the collection of the content of communications.[28] ~~(TS//SI//NF)~~

[27] This conclusion is not foreclosed by any other statute that might limit the Government's ability to collect information. Section 1842 of FISA provides that pen register may be obtained "[n]otwithstanding any other provision of law." Such language evidences Congress' intent to override any law that impeded that authority to obtain such a pen register. *See Liberty Maritime Corp. v. United States*, 928 F.2d 413, 416-17 and n.4 (D.C. Cir. 1991). (U)

[28] Section 3127(3) of Title 18 is also drafted to state that devices or processes used for billing or recording as an incident to billing are not "pen registers." [redacted] devices will not serve those purposes, so that provision is not germane to this analysis. ~~(TS)~~

The legislative history to the USA PATRIOT Act amendments to the pen register definition offers some support for this interpretation. As discussed above, in 2001, Congress amended the pen register statute to provide that a pen register is a "device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication. *See* Pub. L. No. 107-56, § 216(c) (2001) (codified at 18 U.S.C. § 3127(3)). The definition of "pen register" previously had provided that a "pen register" is "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached." 18 U.S.C. § 3127(3) (2000).[29] One significant purpose of those amendments was to make the statute expressly applicable to computers and cell phone communications, as well as standard public switch telephone networks.[30] *Id.* at 47. In doing so, Congress broadened not only the nature of the device that may qualify as a pen register, but also the categories of information collected by a "pen register." (U)

The USA PATRIOT Act amendments used the term "dialing, routing, addressing, and signaling information" to cabin the information that a pen register must decode or record. While Congress used this term rather than "non-content," the legislative history suggests that Congress intended for "dialing, routing, addressing, and signaling information" to be synonymous with "non-content." The House Report states

---

[29] The USA PATRIOT Act similarly amended the definition of a trap and trace device to refer to "dialing, routing, addressing, and signaling information." Pub. L. No. 107-56, § 216(c). (U)

[30] The USA PATRIOT Act modified the definition of pen registers to explicitly apply to non-telephonic technology. Whereas the definition of a pen register device under Section 3127(3) previously only referred to "numbers dialed or otherwise transmitted through a telephone line," amended Section 3127(3) referred to "dialing, routing, addressing, and signaling information transmitted by an instrument or facility." Likewise, the definition of a trap and trace device was amended to refer to "dialing, routing, addressing, and signaling information." 18 U.S.C. § 3127(4). (U)

> [T]he section clarifies that orders for the installation of pen register and trap and trace devices may obtain *any non-content information* –"dialing, routing, addressing, and signaling information" – utilized in the processing or transmitting of wire and electronic communications. Just as today, such an order could not be used to intercept the contents of communications protected by the wiretap statute. The amendments reinforce the statutorily prescribed line between a communication's contents and non-content information, a line identical to the constitutional distinction drawn by the U.S. Supreme Court in *Smith v. Maryland*, 442 U.S. 735, 741-43 (1979). Thus, for example, an order under the statute could not authorize the collection of email subject lines, which are clearly content. Further, an order under the statute could not be used to collect information other than 'dialing, routing, addressing, and signaling' information, such as the portion of a URL (Uniform Resource Locator) specifying Web search terms or the name of a requested file or article. This concept, that the information properly obtained by using a pen register or trap and trace device is non-content information, applies across the board to all communications media.[31]

H.R. Rep. No. 107-236, at 53 (emphasis added). (U)

Here, regardless of whether the modified pen register provision was intended to permit the collection of all non-content – as the plain text of the statute appears to permit and the legislative history arguably supports – or only a subset of non-content that is dialing, routing, addressing, and signaling information, the Government submits that the non-content data identified in Tab 2 of the DIRNSA Declaration may be lawfully collected in either case under the authority of a pen register. All of the information to be collected is "dialing, routing, addressing, and signaling information" and, even if it is not, it may be collected because none of it is "content." ~~(TS//SI//NF)~~

[31] We acknowledge the existence of certain counter-arguments concerning the legislative history. The House Report quoted above, for instance, might arguably demonstrate that the reference in Sections 3127(3) and 3127(4) to "dialing, routing, addressing, or signaling information" was intended to specify the types of non-content information the collection of which had been approved in *Smith v. Maryland*. Similarly, the reference to particular types of content information – e-mail subject lines and URLs – might simply reflect Congress's attempt to underscore that pen registers may not collect content information. (U)

II. Operation of the Proposed Collection Devices Would Not Violate the Fourth Amendment. (U)

As argued above, all data that would be collected by the NSA's devices are non-content information constituting dialing, routing, addressing, and signaling information. It is well-established that information traditionally understood to be "dialing, routing, signaling, and addressing information" is not subject to the Fourth Amendment's protection. This was essentially the holding of *Smith v. Maryland* and the underpinning of the current pen register provisions, as modified by the USA PATRIOT Act: there is no legitimate expectation of privacy for such information. ~~(TS//SI//NF)~~

The information proposed to be collected under this Application falls within the phrase "dialing, routing, addressing, and signaling information," and in any event is non-content information voluntarily shared with a third party. Therefore, the information is not subject to a reasonable expectation of privacy. Moreover, even if certain categories of data are subject to a reasonable expectation of privacy, the collection program as a whole – particularly in light of the strict access and use limitations on the data once collected – would be reasonable under the Fourth Amendment in light of the "special needs" doctrine. ~~(TS//SI//NF)~~

A. The Proposed Collection Devices Would Be Consistent with *Smith v. Maryland*. (U)

Smith v. Maryland, the seminal case on the Fourth Amendment's application to use of pen registers for telephones, found that such devices could be operated without violating the Fourth Amendment to obtain non-content information that was given to a provider for purposes of completing a telephone call. In *Smith*, the Court rejected the argument that an individual can have a Fourth Amendment-protected "legitimate expectation of privacy regarding the numbers he dialed on his phone." 442 U.S. at 742 (internal quotation marks omitted). The Court

concluded that telephone subscribers know that they must convey the numbers they wish to call to the telephone company (because such conveyance is necessary for the company to complete their calls). Thus, the Court concluded, they cannot claim "any general expectation that the numbers they dial will remain secret." *Id.* at 743. Even if a subscriber could somehow claim a subjective intention to keep the numbers he dialed secret, the Court found that this was not an expectation that society would recognize as reasonable. To the contrary, the situation fell squarely into the line of cases in which the Court had ruled that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743-44. ~~(S)~~

The Supreme Court has not addressed the use of pen registers in the context of computer networks, but lower courts have reached the same conclusion about non-content information voluntarily provided for use in transmission of communications. *See, e.g.*, *Forrester*, 512 F.3d at 509. Indeed, this Court also arrived at that conclusion when it approved the Application for the previous bulk pen register collection in docket PR/TT [redacted]. This Court ruled, "[T]here is no reasonable expectation of privacy under the Fourth Amendment in the metadata to be collected ...." Opinion and Order, docket number PR/TT [redacted], at 59. ~~(TS//SI//NF)~~

The core of *Smith* and its progeny is the principle that non-content information that is voluntarily and knowingly provided to third parties is not protected by the Fourth Amendment. Users of communications systems understand that they are voluntarily exposing that information to third parties when they engage in communications requiring such disclosure. Therefore, that information is no longer subject to a legitimate expectation of privacy. *Smith* at 743-44, *citing United States v. Miller*, 425 U.S. 435, 442-44 (1976); *United States v. White*, 401 U.S. 745, 752 (1971). That is the case, moreover, regardless of whether the third party (*e.g.*, an ISP) records

the information. *See Smith*, 442 U.S. at 745 ("The fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not in our view, make any constitutional difference"). (U)

As argued *supra*, 44-49, all of the data that would be collected by the proposed devices are not the content of communications. They are information about and related to the transmission of communications. Consistent with this fact, the data would be collected from the portions of communications in which non-content information is generally found. DIRNSA Decl. ¶¶ 17-19. The e-mail validation scheme that ensures that [redacted] also prevents the unintended collection of content as analogous to PCTDD information. Moreover, the [redacted] information [redacted] of e-mail [redacted] – essentially, all of the dialing, routing, addressing, and signaling information – are data that fall under *Smith* and are not protected by the Fourth Amendment. ~~(TS//SI//NF)~~

The users of Internet communications such as e-mail [redacted] should be cognizant of the fact that they are conveying their information to a third-party provider. Indeed, the convenience [redacted] (TS//SI//NF)

[redacted]

[redacted] *See* DIRNSA Decl. ¶ 14 n.9. Nevertheless, the Government submits that under the circumstances relevant to this collection, such information is not subject to a legitimate expectation of privacy. It is non-content information knowingly exposed to the provider and collected in a manner consistent with addressing information. ~~(TS//SI//NF)~~

Smith rests on the notion that a legitimate expectation of privacy is lost when one voluntarily exposes transmission (non-content) information to the third party communication provider; it should not be understood to be limited to information that is surrendered be used for purposes of actually transmitting the data. Instead, it merely requires that the information be surrendered knowing that the information is transmitted to the ISP. Furthermore, the non-content information that would be collected from [redacted]

Case law governing the use of mail covers is instructive on the issue of an expectation of privacy for such information. It is well established that the Fourth Amendment is not implicated by "mail covers," through which postal officials monitor and report for regular letter mail the same type of information contained in e-mail meta data – *i.e.*, information on the face of the envelope, including the name of the addressee, the postmark, the name and address of the sender (if it appears), and the class of mail. *See, e.g., United States v. Choate*, 576 F.2d 165, 174-77 (9th Cir. 1978); *cf. United States v. Charbonneau*, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997) ("Email is almost equivalent to sending a letter via the mails."); *United States v. Maxwell*, 45

M.J. 406, 418 (C.A.A.F. 1996) ("In a sense, email is like a letter."). Courts have reasoned that "[s]enders knowingly expose[] the outsides of the mail to postal employees and others," *Choate*, 576 F.2d at 177, and therefore have "no reasonable expectation that such information will remain unobserved," id. at 175; *see also Vreeken v. Davis*, 718 F.2d 343, 347-48 (10th Cir. 1983) (concluding the "mail cover at issue in the instant case is indistinguishable in any important respect from the pen register at issue in *Smith*"); *United States v. DePoli*, 628 F.2d 779, 786 (2d Cir. 1980) ("[T]here is no reasonable expectation of privacy with regard to the outside of a letter . . . ."); *United States v. Huie*, 593 F.2d 14, 15 (5th Cir. 1979) (per curiam) ("There is no reasonable expectation of privacy in information placed on the exterior of mailed items . . . ."). ~~(TS//SI//NF)~~

B. Use of the Proposed Collection for the Devices to Protect Against Terrorist and Foreign Intelligence Threats Would Not Violate the Fourth Amendment Because Their Use Is Reasonable Under the "Special Needs" Doctrine.[32] (U)

The overarching Government effort to collect non-content information, for which there is no reasonable expectation of privacy, in support of vital national security objectives, does not implicate the Fourth Amendment. Even assuming, however, that Fourth Amendment protections applied to some of the collected information [redacted] collection of that information is consistent with the Fourth Amendment. The Fourth Amendment requires no warrant here, only that the collection be reasonable. ~~(TS//SI//NF)~~

The collection of data arguably protected by the Fourth Amendment does not require a warrant because the collection program as a whole – in light of the strict restrictions on accessing

[32] The discussion of the Fourth Amendment assumes that the collection of metadata would occur lawfully under the pen register statute. We believe that even if that statute allows collection beyond what is described in *Smith*, such that the Fourth Amendment is implicated, it is still permissible under the Fourth Amendment's "special needs" doctrine, at least under the totality of circumstances surrounding the collection proposed in the Application. ~~(S)~~

and querying the database and disseminating collected information; the governmental interest; and the limited nature of the intrusion on privacy – is reasonable under the Fourth Amendment. The "nature and immediacy of the governments concerns," which are to identify and track foreign power operatives and thwart terrorist attacks, implicates governmental concerns that are at their most extreme. *Board of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie County v. Earls,* 536 U.S. 822, 833 (1976). The Supreme Court has recognized exceptions to the Fourth Amendment's warrant requirement "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987) (internal citations omitted); *see also Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995). The Government's foreign intelligence collection through use of the devices is just such a special need, justifying an exception to the warrant requirement. *See In re Sealed Case*, 310 F.3d at 742 ("[A]ll the . . . courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information."). *See also In re Directives*, 551 F.3d at 1007 ("[W]e hold that a foreign intelligence exception to the Fourth Amendment's warrant requirement exists when the surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States."). ~~(TS//SI//NF)~~

Equally clearly, "the imposition of a warrant requirement [would] be a disproportionate and perhaps even disabling burden" on the Government's ability to obtain foreign intelligence information effectively. *Cf. United States v. Bin Laden*, 126 F. Supp. 2d 264, 273 (S.D.N.Y. 2000), *aff'd on other grounds*, 552 F.3d 157, 171 (2d Cir. 2008)(discussing activity abroad). The Government's foreign intelligence purposes for the overall effort to identify, track, and thwart

agents of Foreign Powers require that the devices collect metadata in bulk; such collection is necessary to make connections between terrorists and their associates. An individualized warrant requirement is a threshold, disabling requirement for such a collection. In terms of process alone, because the Government cannot identify the persons whose communications the devices will collect, it could not apply for a warrant. Furthermore, as the Fourth Circuit has explained, "attempts to counter foreign threats to the national security require the utmost stealth, speed, and secrecy"; accordingly, "[a] warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, in some cases delay executive response to foreign intelligence threats, and increase the chance of leaks regarding sensitive executive operations." *United States v. Truong Dinh Hung*, 629 F.2d 908, 913 (4th Cir. 1980) *quoted in In re Directives*, 551 F.3d at 1011-12. ~~(TS//SI//NF)~~

To the extent there is a reasonable expectation of privacy in some information, collection of such information complies with the Fourth Amendment's reasonableness requirement. In evaluating the constitutional reasonableness of a government search, a court must look to the totality of the circumstances, *United States v. Knights*, 534 U.S. 112, 118 (2001), "balancing [the individual's] Fourth Amendment interests against [the search's] promotion of legitimate governmental interests," *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 619 (1989) (citations and internal quotation marks omitted). (U)

The Government has a compelling interest in obtaining foreign intelligence information to protect national security. "[I]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." *Haig v. Agee*, 453 U.S. 280, 307 (1981) (internal citations omitted). The overall collection effort aims to protect the nation from terrorist threats, which is a "governmental interest . . . of the highest order of magnitude." *In re*

Directives, 551 F.3d at 1012. *See also In re Sealed Case*, 310 F.3d at 746 (holding terrorist threats "may well involve the most serious threat our country faces."). ~~(TS//SI//NF)~~

The privacy interests at stake are limited. Most of the information collected by the devices is the type of information that clearly enjoys no Fourth Amendment protection under *Smith*. Insofar as certain categories of information might arguably be subject to a reasonable expectation of privacy, that expectation may well be diminished in light of the nature of e-mail communications and the need to share the information with the service provider for purposes of transmitting the communication. *Cf. United States v. Bach*, 310 F.3d 1063, 1066 (8th Cir. 2002); Orin S. Kerr, *Internet Surveillance After the USA PATRIOT Act: The Big Brother that Isn't*, 97 NW. U.L.R. 607, 628-29 (2003) ("[B]ecause the contents of Internet communications are mixed together with envelope information and disclosed to the ISP, it is at least possible that courts will find that Internet users cannot have a reasonable expectation of privacy in Internet content information, much like postcards or cordless phone calls."). In addition, the Government's Application proposes numerous safeguards and procedures that reasonably protect the interests of United States persons. Access to the metadata requires a particularized showing that there is a reasonable, articulable suspicion that the seed identifier is associated with a Foreign Power. RAS determinations, moreover, are made by supervisors and are reviewed periodically by the Department of Justice's National Security Division and NSA's OGC. The supervisor and oversight reviews are a sufficient internal check against arbitrary action. ~~(TS//SI//NF)~~

The protections extend to the use and dissemination of the results of metadata queries. The Government's minimization procedures are incorporated from USSID 18 and FISA and require, among other things, that the identity of U.S. persons be redacted from intelligence reports prior to dissemination unless the information is in fact related to counterterrorism

information and is necessary to understand the counterterrorism information or assess its importance. This dissemination standard is virtually identical to that used by the Court in approving applications for electronic surveillance, and to the minimization procedures that were an important factor in the Court of Review's decision holding traditional FISA surveillance to be reasonable under the Fourth Amendment. *In re Sealed Case*, 310 F.3d at 740. ~~(TS//SI//NF)~~

C. The Proposed Collection Is Reasonable Because It is Appropriately Tailored to Balance the Overwhelming National Security Interest with the Minimal Intrusion to Privacy Interests. (U)

All of the metadata collected is properly collected under the Fourth Amendment because all of it is relevant to the FBI's investigations into these Foreign Powers, in the sense that full collection of all the metadata is vital for the use of the analytic tools the NSA will bring to bear to find the communications of these Foreign Powers. Neither the Fourth Amendment nor Title IV of FISA expressly imposes any requirement to tailor collection precisely to obtain solely communications that are strictly relevant to the investigation. While it is true that the overwhelming majority of communications from which metadata have been and will be collected will not be associated with these Foreign Powers, this does not present any infirmity under the Fourth Amendment or Section 1842. The collection program here is and has been appropriately tailored to balance the overwhelming national security interest at stake here and the minimal intrusion into privacy interests that will be implicated by collecting metadata, much of which will never be seen by a human being unless a connection to a terrorist-associated identifier is found. It is, therefore, reasonable under the Fourth Amendment. ~~(TS//SI//NF)~~

1. FISA Does Not Require Pen Registers or Trap and Trace Devices to Collect Only Narrowly Tailored Information and Any Application of Fourth Amendment Balancing Factors Demonstrates that the Collection is Reasonable. (U)

Title IV of FISA does not require that pen registers acquire only narrowly tailored information. The only statutory requirement is that "the information likely to be obtained" be "relevant to an investigation to protect against international terrorism." 50 U.S.C. § 1842(c). That standard does not require that all of the information likely to be obtained by a pen or trap be directly connected with the underlying investigation. The Government could never make such an absolute certification. Even in FISA pen register cases targeting individuals, many communication events are recorded that do not directly bear upon the investigation at issue.[33] ~~(S)~~

The Government cannot identify precisely which communications from the stream of billions are carrying the messages of these Foreign Powers, a challenge that may remain relatively constant given the worldwide nature of Internet communications. The Government therefore seeks to collect solely the e-mail metadata from these Internet communications – not their contents – so that it can use the metadata over an extended period of time to trace or determine connections between known terrorist identifiers and other identifiers (such as e-mails [redacted]). (TS//SI//NF)

[33] The same is true in cases where greater privacy interests are at stake and where the terms of the statute reflect a concern for tailoring the collection. For example, in cases where this Court authorizes electronic surveillance of Foreign Powers or agents of Foreign Powers pursuant to Title I of FISA, 50 U.S.C. §§ 1801-1812, [redacted] Instead, communications of that nature are minimized in accord with minimization procedures that the agencies conducting the electronic surveillance are ordered to follow by the Court. Here, although Title IV of FISA does not impose a requirement for minimization procedures, the Government has (as discussed in the Application and proposed orders) tailored this collection program and the Court has imposed processes and controls on it that the Government believes will limit the already minimal intrusion to privacy interests. ~~(TS//SI//NF)~~

Although the Government is not required by Title IV of FISA to tailor this collection to limit the intrusion to privacy interests, the Government's structuring of this collection program has and will limit any such intrusion. Thus, the collection clearly is appropriate and meets any examination that the Court would conduct by balancing Government's interests in conducting the collection against the potential intrusion into individual privacy interests. The collection therefore is consistent with one of the principal objectives of the entire statutory scheme under FISA – to achieve the appropriate balance between those interests. *See, e.g.*, H.R. Rep. No. 95-1283, pt. 1, at 47 (1978) ("The primary thrust of [FISA] is to protect Americans both from improper activities by our intelligence agencies as well as from hostile acts by Foreign Powers and their agents."); *id.* (discussing circumstances where "the countervailing privacy considerations militating against seeking [foreign intelligence] information through electronic surveillance are outweighed by the need for the information"); *id.* at 70 (discussing the "balance between security and civil liberties" to explain a particular provision in FISA). ~~(S)~~

The use of a balancing analysis, moreover, is supported by analogy to the method of analysis used to assess the reasonableness of a search under the Fourth Amendment – an approach that Judge Kollar-Kotelly explored and found persuasive in her Opinion and Order in docket number PR/TT [redacted] *See, e.g.*, Opinion and Order, docket number PR/TT [redacted], at 50-54. The reasons underlying Judge Kollar-Kotelly's discussion in her Opinion and Order have not changed in the past five years, for there is no Fourth Amendment-protected interest in the metadata at issue here. *See supra* at 53-57. As a result, the standards applied under Fourth Amendment balancing are far more rigorous than any that the Court should read into the statutory requirement that collection under Section 1842 be likely to obtain "relevant" information. Nevertheless, the balancing methodology applied under the Fourth Amendment –

balancing the Government's interest against the privacy interest at stake – demonstrates the reasonableness of the collection. ~~(TS//SI//NF)~~

It is well-established that determining the reasonableness of a search or seizure under the Fourth Amendment requires "balancing the nature of the intrusion on the individual's privacy against the promotion of legitimate governmental interests." *Board of Educ. v. Earls*, 536 U.S. at 829. Even where constitutionally protected interests are at stake (and they are not at stake here), the Fourth Amendment does not require the "least intrusive" or most "narrowly tailored" means for obtaining information. *See, e.g., id.* at 837 ("[T]his Court has repeatedly stated that reasonableness under the Fourth Amendment does not require employing the least intrusive means, because the logic of such elaborate less-restrictive-alternative arguments could raise insuperable barriers to the exercise of virtually all search-and-seizure powers.") (internal citation and quotation marks omitted); *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. at 663 ("We have repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment."). Instead, the Supreme Court has indicated that any tailoring of the search should be considered as part of the reasonableness analysis in considering the "efficacy of [the] means for addressing the problem." *Id.* (U)

Even under the more exacting standards imposed by the Fourth Amendment, if the Government's interest is great and the intrusion into privacy is relatively minimal, the measure of efficacy required to make a search "reasonable" is not a numerically demanding success rate for the search. For example, in considering the use of warrantless and suspicionless roadblocks to temporarily seize automobiles and screen for drunken drivers, the Supreme Court found that an arrest rate of only 1.6 percent of drivers passing through drunk driving roadblocks established sufficient "efficacy" to sustain the constitutionality of the practice. *See Michigan Dep't of State*

Police v. Sitz, 496 U.S. 444, 454-55 (1990). Similarly, the Court has approved the use of suspicionless roadblocks near the border to find illegal aliens even when the roadblocks successfully detected illegal immigrants in only 0.12 percent of the vehicles passing through the checkpoint. *See United States v. Martinez-Fuerte*, 428 U.S. 543, 554 (1976). In sum, "[t]he effectiveness of the [state's] plan, in terms of percentage, need not be high where the objective is significant and the privacy intrusion limited." *Jones v. Murray*, 962 F.2d 302, 308 (4th Cir. 1992). (U)

Here, the Government's interest is at its zenith. As the Supreme Court has recognized, "[i]t is obvious and unarguable that no governmental interest is more compelling than the security of the Nation." *Haig*, 453 U.S. at 307 (citations and internal quotation marks omitted). Tracking down agents of these Foreign Powers remains essential to safeguarding the Nation from the grave threat of further terrorist attacks that these Foreign Powers continue to plan and make efforts to carry out. Acquiring bulk metadata is an important step among several in the process of locating terrorists. Archiving the metadata has and will continue to enable historical chaining [redacted] of Internet communications. Those methods of analysis (among others) are invaluable tools in efforts to identify the broad scope of the terrorist activities of these Foreign Powers and their agents. The Government cannot rely solely on targeted metadata collection because it cannot know [redacted] exactly which communications will show the connections among terrorists. *Cf. Martinez-Fuerte*, 428 U.S. at 557 (upholding suspicionless roadblocks to search for illegal aliens in part because a "requirement that stops on major routes inland always be based on reasonable suspicion would be impractical because the flow of traffic tends to be too heavy to allow the particularized study

of a given car that would enable it to be identified as a possible carrier of illegal aliens"). ~~(TS//SI//NF)~~

Balanced against this extraordinarily strong governmental interest is the minor intrusion into the privacy interests of innocent Internet users in the metadata associated with their electronic communications. There is, of course, no constitutionally protected privacy interest in such metadata. Rather, it is analogous to the dialed-number information for telephone calls considered by the Supreme Court in *Smith v. Maryland*, 442 U.S. 735 (1979) (discussed above). In *Smith*, the Court squarely rejected the view that an individual can have a Fourth Amendment protected "legitimate expectation of privacy regarding the numbers he dialed on his phone." *Smith*, 442 U.S. at 742 (internal quotation marks omitted). Just as telephone users who "voluntarily convey[]" information to the phone company "in the ordinary course" of making a call "assum[e] the risk" that this information will be passed on to the government or others, *Smith*, 442 U.S. at 744 (internal quotation marks omitted), so too do e-mail [redacted] users assume the risk that the addressing information on their communications may be shared. ~~(S)~~

2. The Application of the RAS Standard Has and Will Function to Significantly Limit the Actual Amount of Metadata that is Viewed by the NSA. ~~(TS//SI//NF)~~

In weighing the intrusion into privacy that the proposed collection would involve, it is also significant that, while the Government will collect a large volume of metadata, only a tiny fraction of that information has been and will ever be seen by any human being, and then only on the basis of a targeted inquiry. As described herein, the Government will search the metadata only in prescribed ways designed to uncover communications identifiers associated with these Foreign Powers. Metadata concerning an individual's communications that is collected will be [redacted] but the information pertaining to that individual's

communications will never be presented to a human being unless the computer program identifies a terrorist connection in the form of contact with a terrorist-associated identifier that has been determined to satisfy the RAS standard. The fact that no person will ever view the overwhelming majority of the information collected here reduces even further the weight to be accorded any intrusion into privacy. ~~(TS//SI//NF)~~

Here, as in the predecessor collections to the attached Application that this Court has granted, the actual amount of raw metadata that will ever be seen by an NSA analyst is substantially less than the total amount of metadata collected. That is because any search or analysis of the collected data will occur only after the Government has identified a particular Internet communications identifier (*e.g.*, an address that is associated with these Foreign Powers or their or affiliated terrorist organizations). In identifying such identifiers, the Government will consider an identifier to be terrorist-associated only when "based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion" that the identifier is associated with agents of [redacted] DIRNSA Decl. ¶¶ 24, 31. For example, [redacted] This is, in effect, the standard applied in the criminal law context for a "Terry" stop. *See Terry v. Ohio*, 392 U.S. 1, 21, 30 (1968); *see also Illinois v. Wardlow*, 528 U.S. 119, 123 (2000) (police officer may conduct a brief, investigatory Terry stop "when the officer has a reasonable, articulable suspicion that criminal activity is afoot"). The determination that an identifier satisfies that standard must be approved by one of the following people: the Chief or Deputy Chief, Homeland Security

Analysis Center; or one of the twenty specially-authorized Homeland Mission Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate. DIRNSA Decl. ¶ 31. In sum, the application of this standard further reinforces the reasonableness of the collection as it, in effect, significantly reduces the total amount of metadata that will ever be analyzed by NSA. ~~(TS//SI//NF)~~

When the Government's need for the metadata collection at issue is balanced against the minimal intrusion on the privacy interests of those innocent users of the Internet whose metadata would be collected, the balance tips overwhelmingly in favor of the Government. If, as the Supreme Court concluded in *Martinez-Fuerte*, the Government's interest in stemming the flow of illegal immigration is sufficient to sustain suspicionless seizures of motorists as constitutionally reasonable even when the seizures yield a success rate of only 0.12 percent in finding illegal aliens, then the Government's interest in finding a terrorist plotting the deaths of thousands should easily sustain a collection program that implicates no constitutionally protected interests even if its success rate in identifying terrorists is substantially lower than that. The statutory standard of relevance certainly cannot be construed to impose a more demanding tailoring requirement than the Fourth Amendment.[34] ~~(S)~~

[redacted]

The exploitation of the metadata information described in the attached Application is appropriate under these circumstances. It involves solely information in which there is no constitutionally protected privacy interest (as opposed to the contents of communications), and application of the reasonably articulable suspicion standard will substantially limit the amount of metadata that actually is seen by one of only a limited number of NSA analysts. There is no attempt to censor the communications from which metadata will be acquired.[35] Thus, the collection the Government proposes here –collection that will take place under the FISA statute and with judicial oversight – does not strike any more aggressive balance between the Government's interest in intelligence and individual privacy than the overall balance that Congress itself struck in the statute with respect to non-content metadata that is appropriately collected through a pen register. ~~(TS//SI//NF)~~

3. The Government's Use of the Collected Metadata Will Be Strictly Circumscribed, and the Government Will Apply Procedures To Protect U.S. Person Information. ~~(S)~~

The Government represents to this Court that, although the data collected under the attached Application will necessarily be broad in order to achieve the critical intelligence

[35] The First Amendment similarly presents no concerns regarding the proposed collection, as this Court previously has found. *See* Opinion and Order, docket number PR/TT [redacted] at 66-69. As Judge Kollar-Kotelly acknowledged in her Opinion and Order, "[t]he weight of authority supports the conclusion that Government information-gathering that does not constitute a Fourth Amendment search or seizure will also comply with the First Amendment when conducted as a part of a good-faith criminal investigation." *Id.* at 66. Here, the proposed collection will not be for ordinary law enforcement purposes, but rather for the extraordinarily compelling purposes of protecting against the terrorist activities of the Foreign Powers. This interest clearly satisfies any "good faith" standard that would be applicable. *See United States v. Aguilar*, 883 F.2d 662, 705 (9th Cir. 1989); *Reporters Comm. For Freedom of the Press v. AT&T*, 593 F.2d 1030, 1051 (D.C. Cir. 1978); *see also* Opinion and Order, docket number PR/TT [redacted] at 66-67. Further, the Government has certified that the investigations are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution, and the proposed Primary Order further directs, as to any seed identifiers reasonably believed to be used by or associated with a United States person, *that NSA's Office of General Counsel (OGC) shall first determine that any identifier so believed is not regarded as associated with a Foreign Power solely on the basis of activities that are protected by the First Amendment to the Constitution.* As such, the proposed collection poses no First Amendment concern here. ~~(TS//SI//NF)~~

objectives of metadata analysis, the use of that information for analysis will be strictly tailored to identifying terrorist communications and will occur solely according to stringent procedures, including minimization procedures designed to protect U.S. person information. ~~(TS//SI//NF)~~

When such a communication is identified, as outlined above, the NSA may perform several types of analysis with the metadata it has collected. For example, it may perform contact-chaining – that is, it may search the metadata to determine what other identifiers the target identifier has been in contact with. In addition, the results of such a query may be subjected to other forms of SIGINT analysis. DIRNSA Decl. ¶ 25. It bears emphasis that, given the types of analysis the NSA will perform, no information about an identifier will ever be accessed by or presented in an intelligible form to any person unless that identifier has been in direct contact (within two hops) of an identifier for which NSA has satisfied the RAS standard. ~~(TS//SI//NF)~~

Second, the Government will follow strict procedures ensuring the limited use of the metadata and protecting U.S. person information. These procedures will include ensuring adherence to the requirements that access to the data generate auditable records; analytic queries of the data are limited to RAS-approved seed identifiers; and that the underlying metadata is destroyed within five years of collection. DIRNSA Decl. ¶¶ 31, 33. In particular, NSA will apply the minimization and dissemination requirements and procedures of Section 7 of USSID 18 to any results from queries of the metadata disseminated outside of NSA in any form. *Id.* ¶ 32. In addition, prior to disseminating any U.S. person information outside NSA, one of the officials listed in Section 7.3(c) of USSID 18 (*i.e.*, the Director of NSA, the Deputy Director of NSA, the Director of the SID, the Deputy Director of the SID, the Chief of the ISS office, the Deputy Chief of the ISS office, and the Senior Operation Officer of the National Security

Operations Center) must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance. *Id.* In this regard, the procedures the Government proposes to use are more exacting than is required by statute. In contrast to other provisions in FISA, Title IV does not require any minimization procedures to be followed when the Government obtains approval for pen registers or trap and trace devices, and indeed applications under Title IV of FISA do not normally stipulate that minimization procedures will be followed. *Cf.* 50 U.S.C. § 1805(c)(2) (FISA order approving electronic surveillance must direct that minimization procedures be followed). ~~(TS//SI//NF)~~

Finally, to ensure that the Court can understand the way the above-described standards and procedures are applied, and the way the Government is accessing the information collected under the attached Application, when and if the Government seeks a reauthorization of the pen registers and trap and trace devices in the Application, it will provide the Court with a report about the searches that have been conducted of the acquired bulk metadata. DIRNSA Decl. ¶ 35. ~~(S)~~

III. The Government Requests Authorization under 50 U.S.C. § 1842 to Access, Process, and Use Metadata Previously Obtained [redacted] (S)

As discussed above, the attached Application seeks authorization from the Court to install and use pen registers on a prospective basis. In addition, and in accord with that request, the Court also should grant commensurate and continuing authority to query metadata previously collected. That is the case even though, as discussed in the Compliance Report, the prior pen register collection in certain ways exceeded the scope of the Court's orders. For the reasons set forth above, however, such collection did not exceed *the scope of the pen register statute, the*

Constitution, or the current proposed order. As detailed in the DIRNSA Declaration, without access to the previously collected information, the value of the pen register will be reduced. *See* DIRNSA Decl. 13 n.6. ~~(TS//SI//NF)~~

Beginning in its first order in July 2004, the Court has recognized the unique nature of bulk pen register and has regulated it at two critical stages: a collection stage, in which metadata is extracted from the Internet and stored in NSA databases; and at the querying stage, in which the metadata is extracted from the databases if responsive to a identifier as to which there is reasonable articulable suspicion that it is used by one of the Foreign Powers specified in the Court's orders. This regulatory framework differentiates the bulk pen register orders from traditional FISA pen register orders in two important ways. ~~(TS//SI//NF)~~

First, the bulk orders have regulated both collection and use, where a traditional pen register order regulates collection only. *Cf.* 50 U.S.C. § 1845(a)(2) (requiring that pen register information be used lawfully). Second, each bulk pen register order has regulated not only querying of the information acquired during the 90 days following entry of the order, but also the information acquired pursuant to all of its predecessor orders.[36] In that sense, the Court has asserted a continuing jurisdiction over the bulk pen register program that is both prospective and retroactive. The Government supported that assertion of jurisdiction in 2004, and continues to do so today in light of the unique nature of the bulk pen register program. ~~(TS//SI//NF)~~

[36] In a way, this difference in the bulk pen register orders is similar to the Government's obligations pursuant to minimization procedures that the Government is ordered to follow where this Court authorizes electronic surveillance of Foreign Powers or their agents pursuant to 50 U.S.C. §§ 1801-1812. *See also* note 34, *supra* (discussing how tailoring of this collection through the regulation of queries minimizes the already minimal potential intrusion to privacy interests). In those cases, the Government affirmatively pleads and is ordered to follow those minimization procedures "as to all information acquired through the authorities" requested in those Applications -- a limitation on how the Government deals with that information even well after the effective period of surveillance ends. Here, even though the pen register statute does not require minimization procedures for pen registers, in this Application and in the prior Applications and orders in the bulk pen register collection, similar controls on the Government's querying of the information are imposed. ~~(TS//SI//NF)~~

The Court's continuing jurisdiction under Section 1842 justifies an order granting access to the stored metadata, even though some of that metadata exceeded the scope of the Court's prior orders. In effect, the Court has treated the "installation and use" of the bulk pen register as embracing not only current collection but also querying and related actions, whether the data being queried are newly collected or old. *See generally In the Matter of Application of the United States*, 416 F. Supp. 2d 13, 16 & n.5 (D.D.C. 2006). As such, it is within the Court's Section 1842 authority to permit querying of all accumulated metadata, as long as that metadata is within the scope of the statute and the Constitution, as it is for reasons discussed above. And as noted above, the value of the bulk pen register would be dramatically reduced without access to the years of accumulated data that resides in the NSA's databases pursuant to the prior orders. ~~(TS//SI//NF)~~

There is no independent limitation that would prohibit the Court's authorization of access to the stored metadata under Section 1842. The Court's rules give it discretion to enter this requested order lifting the current embargo on the NSA's ability to query this data, *see* FISC R. 10(c)(iv), and there is precedent for similar actions, although in light of the unique nature of the bulk pen register it should not be surprising that there are no cases directly on point. *See, e.g.*, *In re* [redacted] docket numbers [redacted] (seeking authority to index and log a communication that was previously indexed and logged in violation of the known or extended absence provision of the FBI's Standard Electronic Surveillance Minimization Procedures); *In re* [redacted] docket number [redacted] (authorizing retention of information previously obtained from pen register surveillance of a location not specified in the Court's authorization order because of the government's "good-faith implementation" of the pen

register order concerning the correct telephone numbers used by the correct target).[37] For these reasons, we believe the Court may affirmatively authorize access to and use of the stored metadata under Section 1842. ~~(TS//SI//NF)~~

--- *Remainder of page intentionally left blank* ---

[37] Section 1809 of Title 50, the criminal provision of FISA, is not to the contrary. Section 1809 is a provision that penalizes certain intentional violations of the Court's orders. That is consistent with Section 1809's requirement of an intentional violation of a known legal duty and its inclusion of an affirmative defense for officers who act in any manner authorized by court order. Here, of course, we are seeking an order expressly authorizing access to the previously collected data. If indeed the Court enjoys authority to issue such an order, as we argue it does, then Section 1809 should not be read to restrict that authority, given that FISA's pen register provisions apply "[n]otwithstanding any other provision of law," including Section 1809. 50 U.S.C. § 1842(a)(1). In light of that proviso and the requirement that the conduct be willful, the existence of the order would of course preclude any criminal penalty for conduct in conformity with it. ~~(TS//SI//NF)~~

IV. Conclusion (U)

For the foregoing reasons, the Government submits that this Court should authorize the Government to use and install pen registers and trap and trace devices as proposed in the Application and be permitted to access and prospectively use the data that is the subject to Supplemental Order and Opinion in PRTT [redacted] (TS//SI//NF)

Respectfully submitted,

Eric H. Holder, Jr.
Attorney General of the United States

David S. Kris
Assistant Attorney General
for National Security
U.S. Department of Justice

AUDIO TRANSCRIPTION

UNITED STATES COURT OF APPEALS
THIRD CIRCUIT

IN RE:
GOOGLE, INC. COOKIE PLACEMENT CONSUMER PRIVACY LITIGATION — NO. 13-4300

AUDIO TRANSCRIPTION OF
HEARING

THE ALBERT BRANSON MARIS COURTROOM

19TH FLOOR

THURSDAY, DECEMBER 11, 2014

9:30 A.M.

BEFORE JUDGES FUENTES, FISHER and KRAUSE

Due to the quality of the recorded media, portions were unable to be transcribed. The transcript may also include misinterpreted words. The transcriber was not present at the time of the recording; therefore, this transcript should not be considered verbatim.

AUDIO RECORDING WAS TRANSCRIBED BY:
Sherri L. Jolley
Midwest Litigation Services
711 North Eleventh Street
St. Louis, Missouri 63101
(314) 644-2191

T R A N S C R I P T I O N

THE CLERK: Please rise. The court is now in session. Please be seated.

JUDGE FUENTES: I'll call the next matter, in re Google Cookie Placement Consumer Privacy Litigation.

Mr. Barnes.

MR. BARNES: Thank you, Your Honors. Jay Barnes on behalf of the appellants. I'd like to reserve four minutes for rebuttal, Your Honors.

JUDGE FUENTES: Yes.

MR. BARNES: May it please the Court. Your Honors, this is a case about Internet privacy. In fact, it's a case about the biggest Internet hacking and tracking scheme in history, a scheme which led to the largest fine in the history of the FTC, and the largest multi-state settlement of its kind with state attorneys general in history.

JUDGE FISHER: We noticed you're new counsel as of this morning. Which firm are you from?

MR. BARNES: I'm from Barnes & Associates in Missouri.

JUDGE FISHER: From where?

MR. BARNES: Missouri.

JUDGE FISHER: What firm?

MR. BARNES: Barnes & Associates.

JUDGE FISHER: Okay.

MR. BARNES: All right.

JUDGE FISHER: I didn't see you -- I didn't see you on the original brief.

MR. BARNES: There was a little mix-up there, Your Honor.

JUDGE FISHER: Huh?

MR. BARNES: There was a little mix-up there, Your Honor. It was my understanding that I had been entered six weeks ago and --

JUDGE FISHER: That's okay. I was just curious.

MR. BARNES: All right.

JUDGE KRAUSE: We're glad you didn't get notice last night.

JUDGE FISHER: We don't usually get somebody to jump in a case like this at the last minute.

MR. BARNES: All right. Well, I've been here for a while, Your Honor.

What the defendants did in this case was employ sophisticated computer coding schemes to hack their way around the plaintiffs' chosen privacy settings on the web browsers they used to send and receive communications on the Internet -- in

particular, Apple Safari and Microsoft Internet Explorer.

And by engaging in these hacks, what the defendants were able to do was track, intercept, and access the contents of communications that the plaintiffs had just made or were in the process of making with websites on the Internet. And they did this without the consent of the plaintiffs or the knowledge of the plaintiffs, without the consent or knowledge of the websites or of the web browsers.

The plaintiffs made nine total claims, and we stand by each of them, but because we have only limited time here today, we'd like to focus on the Wire Tap Act, intrusion upon seclusion, and the Stored Communications Act.

JUDGE KRAUSE: Can you address first on standing, where -- where do you allege that you have incurred any costs or that the -- that the PII information has lost value in the marketplace or there's been a lost opportunity to sell? Where do we find that quantifiable loss?

MR. BARNES: Your Honors, that's in Paragraph 49, 56 through 66, and Paragraph 193. And you asked about standing, so I'll skip ahead to intrusion upon seclusion because I think that's where the standing

argument is most pressing.

JUDGE FUENTES: Where is that, Mr. Barnes?

MR. BARNES: The intrusion upon seclusion claim. We made a claim for intrusion upon seclusion -- common law intrusion upon seclusion, and invasion of privacy under the California Constitution.

JUDGE FUENTES: Could you also comment -- you know, Judge Robinson, in her opinion, stated that plaintiffs have not alleged injury and facts sufficient to confer Article 3 standing.

MR. BARNES: And, Your Honor, that's --

JUDGE FUENTES: That's a very wide, you know -- sweeps widely, the statement.

MR. BARNES: And that's what I want to get to. First, there's the allegations of economic harm, which I just referenced in those paragraphs.

JUDGE KRAUSE: But what's referenced there suggests that this information has economic value to the defendants, that there is a nascent market and some polls where people are beginning to put some value on how they would -- how they would value the protection of this data. But where do you allege that the class members' data actually lost value just because the defendants have a copy of it?

MR. BARNES: Well, Your Honors, they took something that was the property of the plaintiffs and absconded it as their own. An analogous situation could be a misappropriation of trade secrets claim, which we have not made in this case, but for which there are damages from taking information, even if there's not a diminution in value to the plaintiff in that type of case. And then there's available damages for a reasonable royalty value.

But for intrusion claims, plaintiffs can

just -- can state the invasion of privacy at -- to assert standing.

JUDGE KRAUSE: But we have some statutes where we need to find economic loss, so if -- if you could focus on that. Where do we see some concrete loss of opportunity or loss of economic value? Where is there an allegation that any of the class members ever sought to sell their data --

MR. BARNES: There's --

JUDGE KRAUSE: -- or that when they did, it was valued at less than it would've been otherwise?

MR. BARNES: There's not an allegation for seeking to sell the data by the plaintiffs, Your Honor, but this is information that has a value that was

taken from them that diminishes its value in the market.

JUDGE FUENTES: But there's no actual sale, no actual --

MR. BARNES: There's no sale --

JUDGE FUENTES: -- transaction?

MR. BARNES: -- from the -- from the plaintiff. No, Your Honor. But if -- for intrusion claims -- we have statutory standing if we talk about the elements of those torts.

JUDGE FUENTES: It sounds like you want to focus on the privacy claims --

MR. BARNES: Well, I want to --

JUDGE FUENTES: -- rather than those that involve economic loss.

MR. BARNES: Well, I want to focus on the Wire Tap Act, which -- for which we have statutory --

JUDGE FUENTES: Yeah. Yeah.

MR. BARNES: -- standing; intrusion, which is the common law claim that's a century old; and then the Stored Communications Act for which we also have statutory standing.

JUDGE FISHER: All right. On the Wire Tap Act, since you want to focus on that, let's go to the Wire Tap Act.

MR. BARNES: Thank you, Your Honor.

JUDGE FISHER: Okay. Now, the Wire Tap Act only -- you know, only requires one-party consent, correct?

MR. BARNES: Under the federal law, it's --

JUDGE FISHER: Under the federal law, that's the Wire Tap Act --

MR. BARNES: That's right. And under --

JUDGE FISHER: -- we're talking about.

MR. BARNES: -- California law, it is all parties to the communication.

JUDGE FISHER: Let's stick with the federal law for a second.

MR. BARNES: Yes, Your Honor.

JUDGE FISHER: One-party consent. The other side argues that at the minimum there's at least one-party -- there's at least one-party consent because the website consented.

MR. BARNES: Well, Your Honors, that turns the well-pleaded facts of the plaintiffs' complaint upside down. I think it's in Paragraph 125 of the complaint where the plaintiffs quote statements from the websites at issue. If you look at the response when this hack was revealed, the websites didn't know it was

happening.

There's a -- Safari didn't know it was happening -- or at least said publicly they didn't know it was happening; they wanted it to stop. Internet Explorer said they wanted it to stop. But if you look at the plaintiff's complaint, the websites did not know, either. That's -- I'm sorry, it's Paragraph 126, Your Honors, with the quotes from the websites.

And consent, Your Honors, so -- is a factual issue, and they have to show that the websites did in fact consent to this when the plaintiff's complaint shows that at least some of these websites publicly said they did not consent to this. And the reason they didn't consent or didn't know is because of the highly secretive nature of how the defendants carried out this hacking scheme. It involved an invisible i-frame, an invisible form, an invisible submission.

JUDGE FUENTES: You're not referring to the blocker that was on the Safari --

MR. BARNES: That is -- that is --

JUDGE FUENTES: -- browser?

MR. BARNES: -- Safari. It was to work -- it was a scheme to work their way around the blocker in the Safari browser.

JUDGE KRAUSE: Can you focus for us --

what is the "this"? Don't we need to be clear about what -- what is the communication we are talking about?

MR. BARNES: Yes, Your Honors, and that comes under the Wire Tap Act claim, and that is the question about whether we've (unintelligible) alleged contents. We allege contents -- the interception of contents in three forms: Detailed URLs, filled-in forms on websites on the Internet, and search queries.

And under the Wire Tap Act, contents is defined as any information relating to the substance, purport or meaning of an electronic communication, and it protects both the sending and the receiving of communications. So the question is whether those three things contain information relating to the substance, purport or meaning of any communication, whether they're being sent by the plaintiffs somewhere or being received in return.

JUDGE FISHER: But if we find it's one-party consent, we don't need to get the content?

MR. BARNES: Well, but the -- there's a fact issue there.

JUDGE FISHER: That's a big issue for you. That's a big issue for you.

MR. BARNES: There's a fact issue there, Judge, and --

JUDGE FISHER: Yes, but that -- to -- you want us to get to content, and I understand why, but if we conclude there's one-party consent, that the websites consented, the content issue becomes irrelevant under the Wire Tap Act.

MR. BARNES: There's two issues there: One, it's a fact issue; two, to the extent it's not a fact issue, we prevailed in the District Court and the defendants failed to cross-appeal. And then there's the fact that it turns the complaint upside down, which is the complaint shows that these websites did not consent to this type of activity.

JUDGE KRAUSE: I need to go back, please, to what is the type of activity we're talking about? Because if it's -- if the communication in question is transmission of URLs, for example, can you identify for us, what URLs are being transmitted as a result of the cookie that wouldn't otherwise be transmitted?

MR. BARNES: Well, Your Honors, we're talking about a difference in kind, here. If there was consent at all from those websites, it was only to the fact that, here, we need an advertisement here. In this case, that's not what happened. It was -- it's the difference, I would say, between consent to a picture from

-- with robe on from the neck down to consent with a picture with robe off with face revealed. They are completely different items, Your Honor, and this is the difference between the two.

JUDGE FUENTES: Could you help me with the functioning of cookies, what exactly they're doing? I see that there are different portrayals of exactly what they do and how much information they accumulate. And in one instance they function largely as passive and somewhat benign, placing identifying markers on communications between, in this case, plaintiffs and the defendants' server. In other instances they behave like spyware -- or, at least, that's the allegations -- and I get that impression from the complaint -- tracking the plaintiffs' Internet histories and so forth.

MR. BARNES: Well, Your Honor --

JUDGE FUENTES: Which of those models or portrayals is the one that you're --

MR. BARNES: This is a case about the non-consensual use of cookies. And --

JUDGE FUENTES: Cookies generally?

MR. BARNES: Cookies -- in particular, the defendants' cookies that were used to track all of the plaintiffs' communications on the Internet without their consent by hacking their way around the privacy

settings on these web browsers.

JUDGE FUENTES: But do they all behave the same way? I think that's really what I'm trying to get at. Which is the model that you're pursuing?

MR. BARNES: Well, an ordinary cookie, a consensual cookie, does not require a company to put an invisible i-frame on a web page followed by an invisible form, and then have an invisible submission to that form, and then have an invisible -- you know, have the plaintiffs hit enter button, unbeknownst to them, in order to then track the communication.

JUDGE KRAUSE: But this very -- this very cookie where there's a different default setting on browsers is being put on millions of people's computers regularly, right?

MR. BARNES: Well, to the extent it's placed on browsers that don't have that default setting -- they don't have to jump through this hacking scheme in order to get the cookie to track where there's a web browser that's configured not to block it.

JUDGE KRAUSE: That may go to the consent, but I think Judge Fuentes' question is going back to a different issue, which is really, what is it that you are alleging is being transmitted here?

Because if it's -- if the only thing

you're pointing to is that the cookie is now providing identifying information for that browser, some unique identifier to a company, the substantive communication -- and let's assume it's that for a moment -- that is otherwise being transmitted in the ordinary course, then aren't we left with record information?

MR. BARNES: No, Your Honors, and the reason why is it's a difference in kind and not a difference in degree. It is then connected. There's -- the value in that -- and, Your Honors, I'm going to try to jump back to the -- and this goes to the original standing question on intrusion upon seclusion, which is a common law tort, which has existed for a century.

And the Supreme Court in Doe vs. Chao explained that these -- for these common law privacy torts they provide for general damages which are presumed. The Supreme Court didn't just come up with that. It got it from a century of case law.

JUDGE KRAUSE: Let's focus on the Wire Tap Acts.

MR. BARNES: Okay.

JUDGE KRAUSE: And so the communication that you're asking us to look at here as creating liability under the Wire Tap Act, what is that communication?

MR. BARNES: The interception includes the URL, it includes the cookie ID, and it includes their browser -- a browser fingerprint, and it includes other information. It is -- but it is the totality of that information which makes it a wire tap.

JUDGE FUENTES: You know, I wanted to pursue that, also. I wonder if a cookie is -- is it something that's going to work like a behavioral sort of monitor? In other words, it's going to send somewhere my history -- my browsing history, perhaps a number of URLs, et cetera. What does it do? Or is it --

MR. BARNES: It --

JUDGE FUENTES: Or it just sends information about what -- where I'm clicking on the computer?

MR. BARNES: Well, it's part of the process of compiling just what you're talking about. And this summer, in Riley vs. California, the Supreme Court held unanimously that that type of data is protected --

JUDGE FUENTES: But do you know --

MR. BARNES: -- by the Fourth Amendment.

JUDGE FUENTES: Do you know if it does that, or is that just a theory for your case? I mean, do you know that it compiles the history of where I've been on the computer?

MR. BARNES: Well, it's --

JUDGE FUENTES: Does it know more about me than I want it to know?

MR. BARNES: It's included in the -- I believe it's included within the plaintiffs' petition. And that's the way these defendants' business models work, is to track all of the different places you're going on the Internet and to track your search and browsing history.

JUDGE FISHER: Let me make sure I understand. Obviously, you're here because you -- the District Court granted the motion to dismiss. You want us to decide something different than that. But what do you want us to do?

MR. BARNES: Well, we --

JUDGE FISHER: What do you want us to do? Tell us -- tell us -- you really didn't answer fully the standing question. You know, how do you get standing under the California -- under the CIPA?

MR. BARNES: Well, under the California Wire Tap Act --

JUDGE FISHER: Yes.

MR. BARNES: -- it's a statutory standing, Your Honors. And, again, that's an issue we prevailed on in the District Court -- not proper on appeal

-- but it's also an issue in which this District has -- the Circuit has found statutory standing exists where a plaintiff has adequately alleged all of the elements of a statutory standing -- statutory claim.

JUDGE FISHER: Let's suppose we didn't conclude that you had any standing under the federal statutes. Can we find that you have standing statutorily under the state statutes --

MR. BARNES: Yes, you --

JUDGE FISHER: -- when in -- when -- let me finish my question -- when, in effect, that would be allowing the states to statutorily provide standing under Article 3?

MR. BARNES: Yes, you can, Your Honors. And I think you can -- the right rule on the intrusion upon seclusion claim and the invasion of privacy claim is that the plaintiffs adequately allege standing because there is a violation of their rights to privacy, which was highly offensive and a serious invasion of privacy, as evidenced by the fact that Congress and every single state has made this activity illegal, as evidenced by the largest fine in the history of the Federal Trade Commission, as evidenced by the largest multi-state privacy settlement that piqued the ire of nearly 40 separate state attorneys general, and as evidenced by the

wire tap claim that we've stated that in California and every other state has held that that gives rise to the tort of intrusion upon seclusion or invasion of privacy.

And even if this court were to hold -- which we disagree with -- that there's no Wire Tap claim, at the very least, the defendants have violated the Pen Register Act, which is another federal statute protecting privacy and for which there are criminal penalties.

JUDGE KRAUSE: Sorry. Did you raise that claim?

MR. BARNES: We raised it within the context of the intrusion upon seclusion claim, alleging --

JUDGE KRAUSE: Alleging a violation of federal Pen Register statute?

MR. BARNES: No. We've alleged violations of their right to privacy in general. And part of the invasion of that right to privacy comes, we argue, the Wire Tap Act, Your Honors. But the defendants' argument is essentially that a URL cannot -- is not protected by the Wire Tap Act because it's addressing information, which we fervently disagree with. But if it's addressing information, then they violated the Pen Register Act, which also protects privacy.

JUDGE KRAUSE: Why isn't it address information? How is it really any different than subscriber-type information that also reveals the substance of where someone is going or a, you know, 1-800 number that has the name in it of the company?

MR. BARNES: Well, thank you, Your Honor. And the reason is that URLs which specify web search terms or the names of requested files or articles is different. The example we use in our brief, and we use it for explosive purposes, is: How do I reduce herpes breakouts? But it's not just that URL. If you look at our reply brief, there are a ton of footnotes that we purposely did to illustrate the point that URLs have information in them relating to the substance, purport or meaning of communications.

JUDGE FUENTES: The -- a cookie would disclose where I have been. The URL would disclose not only where I've been, but what I looked at?

MR. BARNES: It discloses the information contained within a communication --

JUDGE FUENTES: I mean, is that a fair --

MR. BARNES: -- being sent and received.

JUDGE FUENTES: Is that a fair characterization, or is that too simplistic?

MR. BARNES: No. I think a URL that includes search terms or the name of a requested file or article also includes information relating back to an electronic communication. So in the herpes example, the plaintiff receives a 1,500-word essay on precisely the topic they were seeking: How to reduce herpes breakouts. I think it offends common sense to suggest that that information has no substance, purport or meaning.

JUDGE KRAUSE: But what's being sent? What we're talking about is the URL, that is the particular address on the -- on the web of that document, right? So it's not the content of the document at issue. The transmission that -- what we're talking about is just the address of the document. Why isn't that akin to the physical address, knowing someone, for example, is calling this number and you have the subscriber information that shows that it's a herpes clinic?

MR. BARNES: It's --

JUDGE KRAUSE: How is it really different?

MR. BARNES: It's more than that, Your Honor, because look -- if you look at the definition of content, it is as broad as possible. It's any information relating to the substance, purport or meaning of electronic communication. And the defendants'

argument in this case is that if it's addressing information, it therefore can't be content; that they're mutually exclusive, but in a national security context, the FISA court rejected that interpretation.

And if you look at this broad definition of content, that phrase relates to the underlying substance, purport or meaning of both what the plaintiffs sent off that they are seeking and what they received back from the website, which is that 1,500-word essay on precisely the topic they were seeking information upon.

JUDGE FUENTES: I'm failing to follow. Why -- same point: Why isn't it simply disclosing the addresses that I have been at as opposed to the content of the articles, for example, or newspapers that I have visited?

JUDGE KRAUSE: Well, you haven't said, for example, that just because you can tie that telephone number to the herpes clinic that suddenly it becomes content. It's still record/subscriber type information.

MR. BARNES: Well, to use your telephone example, there's case law that we cite in our opening brief to suggest -- not to suggest -- that says post cut-through dialed digits contain content, so that's Brown vs. Waddell and the United States Telecom

Association vs. FCC. And the URL operates -- the phrase after the hubpages.com would be the equivalent of the address. The phrase after that is the equivalent of the post cut-through dialed digits: How to reduce herpes breakouts.

Or to give you another example, consider e-mails. The hubpages.com is the equivalent of a to or a from on the e-mail, and the "how to reduce herpes breakouts" is the equivalent of the subject line. And the subject line is protected under the Wire Tap Act, just like the sub -- very subject -- the information that relates to the underlying communication both being sent and received here is protected by the Wire Tap Act is the URL.

JUDGE FUENTES: Let me get you back and extend your time on rebuttal, but --

JUDGE KRAUSE: Okay.

JUDGE FUENTES: -- just to get over to the other side.

MR. BARNES: Okay. Thank you, Your Honor, Your Honor.

JUDGE FUENTES: So hold on to any further argument you have.

Mr. Rubin.

MR. RUBIN: Good morning, Your Honors.

May it please the Court, Michael Rubin for defendant Google. I'm also presenting argument for the other appellees.

You've heard a fair amount this morning --

JUDGE FUENTES: Right.

MR. RUBIN: -- but as the panel noted, we didn't hear anything -- in fact, we may have heard an admission that there was no allegation in the consolidated complaint that identified any injury in fact.

JUDGE KRAUSE: Why isn't it a fair inference from the complaint that given that there is a market -- even a burgeoning one -- for this kind of information and that the information was taken from them that its value is now diminished, it's diluted in the marketplace? Why can't we infer that?

MR. RUBIN: Well, let me start with three reasons. First, I don't think it's fair to infer the fact that would provide for standing for the Court. Second, the markets, such as they are, that the plaintiffs refer to, don't address the type of information that is actually subject to this case. And I would take issue with the use of the word "taken."

The information -- I think this was

subject a lot -- of a lot of the questions that were directed to plaintiffs' counsel. The information that's at issue in this case flows to the defendants in this case without regard to any cookies. The conduct that the plaintiffs are targeting is the placement of cookies on their browsers.

JUDGE FUENTES: Well, it's what the cookies do, not just the placement, and --

MR. RUBIN: That's not what they -- that's actually not what they allege. In Paragraph 41 of their complaint, plaintiffs allege that information flows automatically in connection with a publisher's request for an ad; that information flows automatically to the defendants, and includes the URLs.

JUDGE FUENTES: Can I ask you this --

MR. RUBIN: Sure.

JUDGE FUENTES: -- to understand this concept of cookies: How long do they last? How much information can they acquire? Do they have a permanent life?

MR. RUBIN: They can --

JUDGE FUENTES: Oh, no.

MR. RUBIN: -- or they can be -- or they can last an hour, or they can last --

JUDGE FUENTES: Well, who determines

that?

MR. RUBIN: The company who sets the cookies determines that -- the entity --

JUDGE FUENTES: Okay. So you can --

MR. RUBIN: -- who sets the cookie.

JUDGE FUENTES: -- send a cookie to my computer and have it sit there for years --

MR. RUBIN: That can happen.

JUDGE FUENTES: -- acquiring browsing information?

MR. RUBIN: The cookie doesn't acquire anything. And, in fact, if you look at Paragraph 46 of their complaint, they don't allege that the cookie here acquires anything, either. What they allege is that the cookie is a static, unique identifier and that the information that gets transmitted routinely day in and day out by everyone in this --

JUDGE FUENTES: It is the --

MR. RUBIN: -- (unintelligible) browsers --

JUDGE FUENTES: -- it is the sender that determines what a cookie should do and look for?

MR. RUBIN: The cookie doesn't look for anything. The cookie just sits on the browser and gets sent along with information that would otherwise be sent.

JUDGE FISHER: It soaks up data?

JUDGE FUENTES: No.

MR. RUBIN: I'm not sure I would -- I'm not sure it soaks up data at all. So let me see if I can give an example really clearly.

JUDGE FISHER: It soaks up identifiers?

MR. RUBIN: It only gets sent along with itself.

JUDGE FISHER: Okay.

MR. RUBIN: Maybe it's sort of like a bookmark. Information gets sent anyway every day, all the time.

JUDGE FISHER: Yeah.

MR. RUBIN: And then a cookie is placed. And thereafter the same information is sent, except that the cookie is there, too. It's unique. It's not personally identifying. It has nothing to do with the actual information that's being sent at that time. In fact, if it did, it wouldn't be useful.

JUDGE KRAUSE: It identifies that the material being sent is associated with the same browser?

MR. RUBIN: That is coming from one instance of that browser. Exactly right.

JUDGE KRAUSE: So you're asking us to sort of parse out those different components of what's

being sent, but under the Wire Tap Act, isn't the paradigm that we're supposed to work with, and what the statute provides is do we have an electronic communication defined extremely broadly?

And if we do, and if that is intercepted, it is acquired, then we can look at the carve-outs which carve out 99 percent of all communications, usually by virtue of consent. But the default of the statute is that the -- it's -- any communication that contains content is going to be covered.

Why aren't we looking here at a communication that includes a URL with the identifying information? Is that a fair way to look at one of these communications as we sort of walk through an example of how this might work?

MR. RUBIN: I think that's exactly what the Court needs to do here, and I think that's exactly what the District Court was called upon to do. It is --

JUDGE KRAUSE: If that's the case.

MR. RUBIN: It is -- if I may, I think it's challenging to do that here because the plaintiffs haven't alleged any actual URLs that were visited, so the Court can't actually look at any individual URL.

But let me suggest that I don't think the Court ever gets there, here, because the plaintiffs

alleged in Paragraph 41 that the URL flows -- and they concede in Paragraph 32 of their -- sorry, Page 32 of their opposition brief that this information flows to defendants -- the URL goes without the presence of a cookie -- and that means that a couple of other elements of the Wire Tap Act automatically aren't met.

It's not that every communication is covered by the Wire Tap Act. It's only those that involve the acquisition of contents through the use of a device. Here, the contents that they identified in their brief was the URL. So they admit in their brief that goes anyway. And the device that they identified in their complaint was on a fair -- on an inference reading of it is the cookie itself.

JUDGE KRAUSE: Well, let's -- we'll come back to the devices, but --

MR. RUBIN: Sure.

JUDGE KRAUSE: -- I just want to follow through on the communication that we're looking at, because if the paradigm is we've got a single communication here that includes the URL and now includes the browser identifier information of the cookie, then aren't we really looking at the question of consent?

Your argument is essentially the URL is sent anyway, so, you know, there's consent to that. But

if what we're talking about is the default of a single communication that has this combined information, to that, that has the identifier, there has not been consent.

And doesn't the Pharmatrak's case say that we can -- we can look at the scope of consent? It's the fact that they consented to 75 percent of the information coming through, but didn't consent to part of it means there wasn't consent for that communication to be intercepted. What's wrong with thinking about it in those terms?

MR. RUBIN: The error in that approach is that the only additional aspect of what's being sent is a cookie value, and a cookie value doesn't equal content under the Wire Tap Act.

JUDGE KRAUSE: But the -- the single --

MR. RUBIN: It has nothing to do --

JUDGE KRAUSE: -- communication does. It --

MR. RUBIN: I think you do have to look at every part of it. As the Court recognized in talking with Mr. Barnes, everything that's sent in that get request is transactional information except what you can identify as content information, right? That would be the URL, at best, under their allegation. They're not alleging that everything else

is in there.

The plaintiffs didn't plead that the cookie is contents. They haven't alleged it. They didn't argue it below, and they haven't argued it here. And there's no way a cookie could constitute contents. Contents has to, by the statutory meaning, relate to the substance, purport or meaning of the contents at issue. The contents --

JUDGE KRAUSE: But if we're talking about a single combined communication that, let's assume for the moment, has content -- we can talk about URLs in a second -- but assume it has content, then how is there consent just because there's a -- part of that is sent anyway? It's a single communication containing content.

MR. RUBIN: If one goes under that paradigm -- which, as I've explained, we don't think is the right approach to analyzing it -- but if you go under that approach, the consent comes from the interaction of the browser and the interaction with the publishers, right? This is a one-party consent statute.

And the publishers are directing the browsers -- the publishers understand there are cookies involved. That's the nature of this relationship. And they are directing the browsers to connect and send this information on. So there is consent all the way through

this process in the way the Wire Tap Act has always been understood. The DoubleClick case makes this absolutely clear.

JUDGE KRAUSE: Are you suggesting we should look at the consent of the initial web page, not the consent of the user's browser?

MR. RUBIN: I think that you should look at both, frankly. I think the user's browser is dispositive of this question, but if you look at the publisher's consent -- which is the way the DoubleClick case analyzed this -- it resolves the question, as well.

JUDGE KRAUSE: But the user's browser is the one that has the default setting under Safari and Internet as alleged not to allow for this type of transmission to take place.

MR. RUBIN: Well, but that's actually not how they allege it. They allege that Apple advertised that -- that the default setting didn't allow the placement of cookies, but they further allege in Paragraph 46 of their complaint -- sorry, at 76 of their complaint that there are exceptions to that.

JUDGE FISHER: What about the California Invasion of Privacy Act? It requires two-party consent. So you could prevail on the fact that there's one-party consent that exists under the Wire Tap

Act, but under the California Act, clearly you don't have consent from the person whose URL was being communicated.

MR. RUBIN: Under the proper analysis of parsing out the individual parts of the communication to see what element of the communication is potentially content, we do. And the California Invasion of Privacy Act only looks at all parties if the outside -- if it's an outside third party analyzing it and accessing the communication. That's not what happened here. That's not what's alleged to have happened here.

JUDGE FISHER: Well, who were the two parties?

MR. RUBIN: The two parties here for the purposes of the California Act --

JUDGE FISHER: Yes.

MR. RUBIN: -- would be the user's browser and the -- and in this case, because that claim is only brought against Google, would be Google.

JUDGE FISHER: But how can the user's browser consent when the user didn't consent?

MR. RUBIN: If we're talking about how the Internet operates --

JUDGE FISHER: Yes.

MR. RUBIN: -- and how software is developed --

JUDGE FISHER: Yes.

MR. RUBIN: -- the software was designed by -- we're talking about two pieces of software, Apple's Safari browser and Microsoft's Internet Explorer browser. These pieces of software were designed to function as the -- as Google, in this case, interacted with that software.

JUDGE FISHER: Right.

MR. RUBIN: There was nothing that Google interacted with the software in this way that --

JUDGE FISHER: But --

MR. RUBIN: -- deviated from how it was designed --

JUDGE FISHER: Then, in fact --

MR. RUBIN: -- and placed into the market.

JUDGE FISHER: -- the Safari software even advertises itself -- Apple advertises it as having a cookie -- that it blocks third-party cookies.

MR. RUBIN: I don't disagree that --

JUDGE FISHER: Correct?

MR. RUBIN: -- Apple has said that.

JUDGE FISHER: I mean, that's accurate?

MR. RUBIN: I don't disagree that Apple has said that.

JUDGE FISHER: So when I use my Safari browser on my iPad, it's been purported that third-party cookies will be blocked. But what is being alleged here is notwithstanding the blocking on a Safari browser, third-party cookies are still being sent and being placed on my browser that's picking up information; accurate? I mean, fairly accurate to what they allege, right?

MR. RUBIN: Yes. And in Paragraph 76 of their complaint they say that Safari's default settings provide an exception to the third-party cookie-blocking protection.

JUDGE FISHER: Okay. So if that's accurate, how can you then say that there is consent from the second party that is required under the California Invasion of Privacy Act?

MR. RUBIN: Because the only thing that can constitute contents is the URL, and the URL would be sent anyway. So the only thing that changes is the cookie, and the cookie is not implicated by the -- by the California version of the Wire Tap Act --

JUDGE FUENTES: What was --

MR. RUBIN: -- the same way it's not implicated by the federal version of the Wire Tap Act.

JUDGE FUENTES: What is the -- I mean, you purposefully trick the blocker so that you can get

around the blocker so that you can get information.

MR. RUBIN: I would take issue --

JUDGE FUENTES: So isn't that --

MR. RUBIN: I would take issue with that charge. I think --

JUDGE FUENTES: That speaks to the idea that you needed consent and you purposefully tricked that blocker to think that the consent was given.

MR. RUBIN: Again, I would -- that is a rhetorical claim in the complaint and a -- there's a lot of rhetoric in the complaint.

JUDGE FUENTES: That's not what actually happened?

MR. RUBIN: Code is used to place cookies all the time, at all times. It is not that one is invisible, one is visible. There's all sorts of various methodologies to place code depending on the various software settings of the browsers. Companies need to be able to rely on how software is designed in order to be able to interact with them and how that is placed into the market.

JUDGE KRAUSE: Can you talk about how there is even one-party consent with the Wire Tap Act if what we're looking at is the user's browser and Google, or the defendants'? Because what we have a separate --

it's an independent communication that's going on from the user's browser to Google, right?

MR. RUBIN: Uh-huh.

JUDGE KRAUSE: And along the lines that Judge Fuentes was just asking, the consumer -- the user hasn't agreed to send combined URL and identifier information.

MR. RUBIN: Well, under the argument that the plaintiffs have made, they may not have understood there to have been information passing to the defendants even prior to the placement of the cookie.

JUDGE KRAUSE: They may not have.

MR. RUBIN: So under an analysis that would require consent to look into the mind of the -- to the mind of the person using the browser at that stage, a Wire Tap claim could be brought against any party interacting with a user on the Internet at any point if there were a claim that that person didn't understand how their system was working at a technical level.

JUDGE FUENTES: Is a user --

MR. RUBIN: That's not what the -- that's not what the Wire Tap looks at.

JUDGE FUENTES: Is a user able to tell Google, "I do not consent to your sending me cookies"?

MR. RUBIN: Absolutely. Absolutely.

The user is able to do it in Safari and in Internet Explorer. The allegations here are that the users -- the four named plaintiffs used these pieces of software in their default state --

JUDGE FUENTES: So what you do --

MR. RUBIN: -- not --

JUDGE FUENTES: -- what you do is you assume consent unless I tell you otherwise?

MR. RUBIN: That the system's attempt to set cookies unless the -- unless the software rejects it. If the users here had gone in and said -- in Apple said "never," which is an easy thing to set, or they had gone to Google systems and downloaded what's called the opt-out cookie, which opts you out of all of this, there would -- this wouldn't happen. But if you rely on how browsers characterize their software only, the systems on the other end are going to interact with it.

And we have four -- or three particular defendants at issue in this case, but this is how systems across the entire Internet work. And whatever ruling this Court issues is going to affect broad swaths of companies and how they interact.

JUDGE FUENTES: But --

MR. RUBIN: And if consent is going to have to be peering behind the screen to -- and claims are

going to be able to be brought based on -- based on --

JUDGE KRAUSE: Why isn't it fair to attribute the default setting that a user has selected, you know, their consent, either yay or nay? Why isn't the default setting the proxy for that?

MR. RUBIN: Well, here it may be, but the default setting here had an exception. It had an exception that was in both these browsers that was -- that was designed. So it's not some freak aspect of the browser. It was designed in.

JUDGE KRAUSE: But the allegation is that you evaded the exception.

MR. RUBIN: That's the --

JUDGE KRAUSE: I mean, that's --

MR. RUBIN: That's rhetoric that colors the allegation.

JUDGE KRAUSE: There may be factual findings that need to be made on that, but that's the nature of the allegation.

MR. RUBIN: I take issue with that. I think the allegation is that the defendants in this case used code to set browsers that used that exception. Now, the plaintiffs are trying to make that look worse by using words like "trick," no doubt, but if that exception didn't exist in the browser, it hadn't been designed in there,

these cookies would never have been set.

JUDGE KRAUSE: Can you talk to us about whether -- again, thinking about this as sort of combined communication, are URLs content?

MR. RUBIN: We don't think the Court gets to that question here.

JUDGE FUENTES: But if we did?

MR. RUBIN: If you did, we don't think that that question is susceptible to a ruling as a matter of law. It's a fact-intensive question.

JUDGE KRAUSE: So if we get to that question, then you think that we would need to reverse and remand for fact finding and --

MR. RUBIN: Absolutely not. Absolutely not. There was no allegation of URLs here --

JUDGE KRAUSE: There's no allegation --

MR. RUBIN: -- of -- particularly there's --

JUDGE KRAUSE: -- in the complaint of URLs?

MR. RUBIN: If you look through the complaint, there is not a single allegation of any particular URL having been intercepted that would enable the Court to make a determination of whether or not that URL that constituted contents.

JUDGE KRAUSE: But there's multiple allegations that URLs are being transmitted.

MR. RUBIN: Sure. And there's a recognition by the plaintiffs in this case that lots of URLs don't constitute contents. And the District Court recognized, absolutely correct, that all URLs are location identifiers.

The question of whether a URL could in some contents -- contexts concern the subject, purport or meaning of the underlying content requires not only having the URL in front of you, but as the Court recognized earlier, you would actually need to have the page below, because you can't just look at the words in the URL and know whether they concern the subject, purport or meaning of the underlying page. There has to be a match. You have to see that to see whether the -- whether a full Wire Tap claim has been stated, because contents are an essential element.

JUDGE FUENTES: In thinking about the privacy intrusion under the California law, I think about United States vs. Jones, and think about a GPS device that's placed on a car, and whether that operates much like Google places a cookie on my computer, because when you put the GPS on a car, you can tell where that car has been and where it's going, the same thing as a cookie.

But that's an intrusion under Supreme Court doctrine --

MR. RUBIN: It's also a Fourth --

JUDGE FUENTES: -- leading to a privacy invasion.

MR. RUBIN: So there's a couple of significant distinctions. Number one, that's a Fourth Amendment case, and in those cases the individuals were identifiable. Here, everything was anonymous. If you look at actual California law that controls on these questions, the Fulkastrom (ph) case, I think, from the California Appellate Court is very instructive.

JUDGE FUENTES: But you're still attaching a device which is -- it works like a trespass, attaching a device on my computer just as you would attach a GPS device on a car to get further information.

MR. RUBIN: Well, there's no trespass claim, and I would quibble with whether a cookie is a device. But I think that the way to look at this is that under California law, under these claims that the plaintiffs have asserted, there has to be more than an allegation that the access to the information or the access to the -- that the acquisition of the information was wrongful, that the use itself has to be a serious invasion.

And online advertising, the harm here,

which is of sending, at most, a more relevant ad -- that's the sum total of what this case is about -- someone getting an ad that -- different than the ad they otherwise would have received -- that doesn't violate public policy in California.

That doesn't violate -- it's not an egregious violation of social norms. That doesn't rise to the level of violating California public privacy. That's exactly what the Fulkastrom case holds. Compiling anonymous information, even if they're prescription records, has held -- has been held in California in the Albertson's case not to be a violation of California privacy law.

Compiling and disclosing browsing history has been held in the Low vs. LinkedIn case not to be a violation of California privacy law. This is simply not a case that rises to that level. It doesn't come close. The cases that rise to the level of California privacy violations are directly monitoring student athletes during drug tests --

JUDGE FUENTES: Doesn't --

MR. RUBIN: -- police disseminating the headless corpse of victims.

JUDGE FUENTES: Isn't there a point at which it really becomes an intrusion on privacy because

when I -- when I hear that cookies can last indefinitely and can gather information indefinitely, let's say -- let's say it's a one-shot thing where I click on a -- let's say a yellow pad, that's what I want to buy, and all of a sudden for the next month I get ads for -- from Staples and things like that. But what if I keep getting this information for like six months, a year? Isn't there a point where you say, "This is really an intrusion on my privacy, and this is not what I bargained for when I used my computer"?

MR. RUBIN: We have to -- in order for there to be an invasion of privacy in this case, we have to have facts in this case to evaluate that, and we don't. Merely saying invasion of privacy, which is effectively all the plaintiffs have done, doesn't pass the test. They have to allege facts as well, and they haven't alleged any facts.

First of all, this concept of invasion of privacy is adequate for standing has been waived. They did not argue this before the District Court. This was never raised before the District Court.

JUDGE FISHER: But you can't waive standing. You can't waive standing.

MR. RUBIN: This particular argument as a basis for injury in fact was never presented to the

District Court.

JUDGE FUENTES: You don't disagree that you don't need an economic loss for -- to sustain a privacy invasion claim?

MR. RUBIN: I don't disagree with that, but you do need to have been -- you do need to state facts showing that you were aggrieved.

JUDGE KRAUSE: Or a claim under the Wire Tap Act or CIPA.

MR. RUBIN: We don't disagree with that, either. But you do need to show that you come within the scope of the statutory protections, which the plaintiffs here have not and could not do.

JUDGE KRAUSE: Could we go back to content for a moment?

JUDGE FUENTES: Sure.

JUDGE KRAUSE: Do you acknowledge, then, that there are URLs -- perhaps many URLs -- that you would concede constitute content for purposes of the Wire Tap Act?

MR. RUBIN: We acknowledge that there may be URLs that could constitute content.

JUDGE KRAUSE: And what about --

MR. RUBIN: But I'll say, there's been none alleged in this case that the Court could even begin

to look at to reach that conclusion.

JUDGE KRAUSE: Mr. Barnes made reference to forms and search queries. Do forms also contain content?

MR. RUBIN: I would need to see the form and look at it. I have no idea. And the -- and as a matter of process, whether forms get submitted in connection with these cookies, is not an allegation that can be fairly made based on how the technology operates, in any event.

JUDGE KRAUSE: So if we get to the point of looking at content then under the Wire Tap Act or CIPA, wouldn't we need to remand for fact finding on those issues?

MR. RUBIN: No. No, because, first of all, there's no device at issue here. They have to allege a device was used to do the interception --

JUDGE KRAUSE: Don't --

MR. RUBIN: -- and cookies don't -- the only device they allege under the Wire Tap Act is the code that set the cookies, and they vaguely point to the cookies themselves. So, at best -- at best -- the cookie is the device they alleged.

JUDGE KRAUSE: Paragraph 208 of the complaint talks about the defendants' third-party

tracking intercepted the class members' communications while they were in transit from the class members' computing devices to the web browsers of the first-party websites the class member used their browsers to visit.

In particular, during the course of populating advertising space on the first-party website the class member intended to visit, the defendants' transmitted copies of the communications to their own web servers as part of the third-party tracking.

Doesn't that show that there are at least three devices that are under discussion -- the user's computers, the first-party web servers, and the defendants' servers?

MR. RUBIN: They didn't identify any of those as the alleged devices in the complaint. What they identified as the alleged devices were the cookies. And to be -- may I finish this point?

JUDGE FUENTES: Yes, please.

MR. RUBIN: All of those -- that infrastructure is used when the cookies aren't involved, as well, to deliver the ads, so that can't constitute the infrastructure for a wire tap interception, if the only thing that is changed is the cookie, right? Every day, routinely, there are address shown in -- day-in, day-out. If the only thing that changes after the cookie is placed

is the presence of the cookie, those other things can't constitute the device for the Wire Tap claim.

The only thing that has changed is the cookie. The only thing that's plausibly a device for the Wire Tap Act claim is the cookie. Otherwise all of that other infrastructure exists and would be subject to an interception claim absent the cookie, and that would, again, bring us back to a place where people can be bringing Wire Tap claims in all sorts of contexts.

JUDGE FUENTES: Okay. We really have to finish up. Thank you, Mr. Rubin.

MR. RUBIN: Thank you.

JUDGE FUENTES: Mr. Barnes.

MR. BARNES: Your Honors, so many notes, I don't know where to begin here.

The -- I heard -- I've heard a lot of questions and things about arguments which are not before the Court. We appealed the issue on contents. The defendants failed to cross-appeal. All of the talk about devices, they didn't cross-appeal that. They're represented by able counsel. The Supreme Court has held that's a jurisdictional bar to raising it.

In addition to that, I heard a bunch of misstatements of fact about what's in the complaint. Page 25 explains how this deceit worked for Apple Safari.

Paragraph 126 describes the consent of the websites. And I'll just give you one, because I only have limited time here: "We were not aware of this behavior. We would never condone it," said one of the companies whose websites was at issue in this case.

JUDGE KRAUSE: But, again, looking to the default setting as a proxy for consent, you were aware of the URLs, the things that you're saying constitute the content, being transmitted in the ordinary course. What's new and different here, if I understand your argument in the complaint, is that there's now identifying information associating that -- what you're alleging to be content with the browser.

MR. BARNES: It's a difference in kind rather than a difference in degree, Your Honor. It completely transforms the nature of what is taken from the plaintiffs without their consent, and it strains credibility for the defendants to argue this is how the Internet works. We're not talking about consensual cookies.

If you look at the actual DoubleClick cookie that was -- DoubleClick case that was referenced a few times, the DoubleClick court made some important points. The websites in DoubleClick consented to the tracking. In this case, they didn't. The web browsers

in DoubleClick were not configured and did not -- and did consent to the tracking in DoubleClick. In this case, they didn't.

JUDGE KRAUSE: How is this a difference in kind? What is different -- if all we're talking about is a difference is identifier information and we're in agreement that that is -- that alone is record information that's not covered by the Wire Tap Act, then why is it a difference in kind to send that separate and apart from something that would've been sent anyway?

MR. BARNES: Well, Judge Fuentes hit directly upon the point. And the question you asked about how long these cookies last, a very -- could be forever; in some cases, two years. The cookies we're talking about here were long-lasting cookies tracking everything that you do on the Internet. And because of Google's ubiquity, it's 70-percent of websites on the Internet, so that's why it's a difference in kind.

JUDGE FUENTES: Is it the case at some point that the addresses become content themselves?

MR. BARNES: Well, the URLs are content where they include search terms, filled-out forms or requested files and articles, because when they add those three things, they include information relating to the substance, purport or meaning of communications that

plaintiffs were sending and receiving from the websites at issue.

You asked in addition about the Supreme Court case on GPS device -- devices. There's an even more relevant case from this summer, in Riley vs. California. The Supreme Court unanimously ruled that data held on personal computing devices is protected by the Fourth Amendment. And the court went out of its way to discuss the importance and the substantive difference -- the difference in kind, if you will -- between an Internet search and browsing history and other kind of data.

And that, Your Honors -- what defendants do -- their argument is about being a party to this communication. That turns every computer hacking statute upside down, because in every single computer hacking case, you're going to have a defendant who figured out how to work their way around the default setting of the electronic communication service. And if the defendants in this case are able to do it, there is no situation where there's a hacking case in which a hacker was unable to get around the default settings.

What they argue is essentially, we're smart enough to do this; therefore we shouldn't be liable; we're a party to the communication. But that clearly

can't be the case regarding computer hacking statutes, Your Honors.

JUDGE KRAUSE: Well, what do we do with the fact that as Mr. Rubin pointed out your complaint doesn't seem to allege any specific URL that's visited, any form or content of that form that's transmitted, or particular searches that were conducted by the representative class members?

MR. BARNES: Well, if you look at Paragraph, I believe it's 206, Your Honors, we talk about the interception of URLs, that the plaintiffs and class members requested from the first-party websites they were visiting. Included within that allegation of URLs is URLs.

And some URLs -- you heard the defendant talk about some UR -- it seemed almost an admission that some URLs may contain content, but contained within that sentence is including everything within that umbrella of URLs, including search queries, filled-in forms, detailed URLs which include the content articles.

JUDGE KRAUSE: Do you agree that other URLs don't include content information?

MR. BARNES: I do not. In the Zynga case, which comes from the Ninth Circuit, the Zynga court followed the same rationale as the FISA case found and

said search queries or similar communications requesting underlying purport, but found there wasn't content in some URLs. I think that is a -- that's a more difficult question, and it's our position that they do include content. But that's not all we're talking about here.

Of course, we're talking about URLs that include the article names and files requested, and the herpes example are the -- plenty of examples we've cited in our footnotes, Your Honors.

JUDGE KRAUSE: Can you address on the privacy point -- Mr. Rubin pointed out correctly that the California cases have taken a pretty strict approach when it comes to what is a privacy violation, if it is -- if it is highly offensive, if it is a serious invasion.

So how do you address those cases, and why does this -- when we're talking about information that is widely disseminated, including the pairing of the identifier and URL information for all those folks who have a different default setting on their browser, you know, when that's as common as it is, how do you get over that threshold here?

MR. BARNES: Those are much different fact patterns. Fulkastrom involved zip codes. The -- one of the other cases that you referenced involved consented-to interceptions that then later the

plaintiffs alleged could've been through reverse engineering correlated with them.

As for whether it's highly offensive or a serious invasion of privacy, California law is that if you allege a Wire Tap claim, you've adequately stated a claim under the common law for these items. That's the law, as well, in every other state of which we're aware. And in addition to that, Your Honor, look at what happened. The Federal Trade Commission levied the largest fine in its history because of this behavior.

JUDGE KRAUSE: But if the --

MR. BARNES: Nearly 40 different state attorneys general took action. I think those actions show how it's highly offensive and a serious invasion of privacy.

JUDGE FUENTES: We -- discuss this one more question and then we have to finish up.

JUDGE KRAUSE: The California courts have held that lots of things like Social Security numbers and credit card numbers and the prescription information, names and addresses -- those don't cross the line into a serious privacy invasion. Why would the -- a URL visited with an anonymous identifier type information --

MR. BARNES: Well, we would dispute whether it's anonymous or not. I think that's outside

the realm of the complaint. But in addition to that, look at the underlying conduct and how this was carried out. The chart on Page 25 explains it. I believe it's the paragraph before that where Google said, "If you had done something else" -- if you had gone to their website and clicked on a certain button, you could've blocked this. When this happened, Google had a web page up that told the public, "Oh, you don't need to take that step because we respect your privacy preferences on Safari. We won't violate those privacy preferences." I believe that's on Page 24. That's fraudulent --

JUDGE FUENTES: Gentlemen, I am afraid that we're going to have to finish up on that --

MR. BARNES: Thank you, Your Honors.

JUDGE FUENTES: -- on that last point. Thank you very much. May I ask counsel to arrange to get a transcript of the hearing today? Just speak to the clerk. You can share expenses, however you wish to do it. Thank you very much.

JUDGE KRAUSE: Thanks everyone.

(WHEREIN, the hearing was concluded.)

CERTIFICATE OF NOTARY PUBLIC

STATE OF MISSOURI

I, Sherri L. Jolley, within and for the State of Missouri, do hereby certify that the tape transcription in the witness whose testimony appears in the foregoing transcript in the caption hereof and thereafter transcribed by me; that said transcript is a record of the testimony given by said witness; that I am neither counsel for, related to, nor employed by any parties to the action; and further that I am not a relative or employee of any counsel or attorney employee of any counsel or attorney employed by the parties hereto, nor financially or otherwise interested in the outcome of the action.

_____

Sherri L. Jolley