ORAL ARGUMENT NOT YET SCHEDULED

Nos. 17-5217, -5232

United States Court of Appeals for the District of Columbia Circuit

---

IN RE: U.S. OFFICE OF PERSONNEL MANAGEMENT
DATA SECURITY BREACH LITIGATION

On Appeal from a Final Judgment of the United States District Court for the District of Columbia, No. 15-1394, The Hon. Amy Berman Jackson

BRIEF OF THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA AS AMICUS CURIAE IN SUPPORT OF APPELLEES

Steven P. Lehotsky
U.S. CHAMBER LITIGATION CENTER
1615 H Street, N.W.
Washington, D.C. 20062
(202) 463-5337

Alan Charles Raul
Kwaku A. Akowuah
Clayton G. Northouse
Daniel J. Hay
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
(202) 736-8000
araul@sidley.com

Counsel for The Chamber of Commerce of the United States of America

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES PURSUANT TO CIRCUIT RULE 28(a)(1)

A. Parties and *Amici*. All parties and intervenors appearing before the district court and in this Court appear in the Brief of the Federal Appellees and the Brief of KeyPoint Government Solutions, Inc.

B. Ruling under Review. An accurate reference to the ruling at issue appears in the Brief of the Federal Appellees and the Brief of KeyPoint Government Solutions, Inc.

C. Related Cases. An accurate statement regarding related cases appears in the Brief of the Federal Appellees and the Brief of KeyPoint Government Solutions, Inc.

CORPORATE DISCLOSURE STATEMENT

The Chamber of Commerce of the United States of America ("Chamber") is a non-profit, tax-exempt organization incorporated in the District of Columbia. The Chamber has no parent corporation, and no publicly held company owns 10 percent or more of its stock.

STATEMENT REGARDING CONSENT TO FILE AND SEPARATE BRIEFING

All parties have consented to the filing of this brief. No counsel for a party authored this brief in whole or in part, and no person other than the amicus curiae, its members, or its counsel contributed money that was intended to fund the preparation or submission of this brief. *See* Fed. R. App. P. 29(c)(5).

Pursuant to Circuit Rule 29(d), the Chamber certifies that a separate brief is warranted to ensure that the Court has before it the perspective of the Chamber, the businesses and associations that are our members, and the broader business community that it represents, in considering the Article III standing and derivative sovereign immunity issues presented by this case.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Cases

* Authorities chiefly relied upon are marked with asterisks

Statute and Regulations

Other Authorities

GLOSSARY

CAC	Consolidated Amended Complaint
NTEU	National Treasury Employees Union
OPM	U.S. Office of Personnel Management
PII	Personally Identifying Information

INTERESTS OF THE AMICUS CURIAE

The Chamber is the world's largest business federation. The Chamber represents 300,000 direct members and indirectly represents the interests of more than three million companies and professional organizations of every size, in every industry sector, and from every region of the country. An important function of the Chamber is to represent the interests of its members in matters before Congress, the Executive Branch, and the courts. To that end, the Chamber regularly files amicus curiae briefs in cases that raise issues of concern to the nation's business community. For example, the Chamber participated as an amicus before the Supreme Court at both the petition and merits stages in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016).

The Chamber has a significant interest in the Article III standing issue presented by this case because its members frequently are victimized by data breaches. These breaches are perpetrated by a variety of state and non-state actors for a range of motivations, including non-commercial ones. Further, many companies whose defenses are breached by hackers then face putative class action lawsuits. In these suits, plaintiffs frequently assert that the mere fact their personal information was exposed through a data breach qualifies, *per se*, as an "injury" sufficient to create Article III standing.

The district court properly rejected such an automatic approach to standing. It correctly recognized that, just as in other cases, "a case- and context-specific inquiry" into standing is necessary where data breaches are concerned. *Nat'l Ass'n of Home Builders v. EPA*, 786 F.3d 34, 43 (D.C. Cir. 2015). Moreover, the district court correctly recognized that the plaintiffs' failure to plead any allegations regarding the hacker's motives, combined with strong indications that the OPM breach was perpetrated for reasons other than financial gain, defeated any plausible inference that the OPM breach will likely cause plaintiffs future harm. The Chamber urges this Court to affirm both the district court's approach and its conclusion.

The Chamber also has a significant interest in the derivative immunity issue presented by this case because its members frequently serve as contractors for the federal government and rely on derivative sovereign immunity principles for purposes of predictability and pricing.

Plaintiffs do not allege that KeyPoint violated any express contractual duty to OPM or acted in any manner unauthorized by the contract. Under established immunity principles, that should be the end of the analysis: KeyPoint is immune from suit because it acted within the scope of its contract with the government. Plaintiffs claim, however, that KeyPoint should be held liable because the company (according to Plaintiffs) was obligated to go beyond the contract's

express terms and adopt additional security measures. If accepted, that theory would essentially nullify government-contractor immunity. Under current law, a contractor loses derivative immunity only when it exceeds its authority under the relevant contract or violates the government's *express* instructions. Plaintiffs now argue that immunity *also* should vanish when a contractor *does not* go beyond the contract's express terms. In addition to conflicting with controlling precedent, Plaintiffs' proposed rule would be unfair to contractors, unwieldy for the government and, ultimately, bad for the public fisc. The Court should instead affirm the longstanding rule that government contractors are protected by derivative immunity so long as they do not violate the express terms of a valid government contract.

ARGUMENT

I. Companies Face An Ever-Present Threat Of Data Breaches From A Variety Of State And Non-State Actors.

Data breaches have become a grim fact of life in the digital age. Entities in every sector of American society, including government, technology, manufacturing, healthcare, and finance, have been targeted by an unrelenting wave of cybersecurity attacks. Then-FBI Director Robert Mueller summed up the situation well in 2012, saying: "I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are

converging into one category: companies that have been hacked and will be hacked again."[1]

Companies have responded to this threat by going to great lengths to implement stronger protections. More than fifty percent of companies plan to increase their cybersecurity budgets by five percent or more in 2018.[2] And much more is on the way. Morgan Stanley estimates that cybersecurity will become a $128 billion market by 2020—more than double the amount spent as recently as 2015.[3] Cybersecurity tools and strategies also are advancing. Companies commonly deploy advanced cybersecurity monitoring tools to detect intrusions and hire full-time staff to develop access controls, process threat intelligence, and deploy defensive measures in real-time. Boards of directors are becoming more engaged on cybersecurity issues, and senior executives increasingly designate cybersecurity as a top corporate priority.

---

[1] Robert S. Mueller III, Director, FBI, Remarks at RSA Cyber Security Conference (Mar. 1, 2012), https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

[2] Council of Economic Advisers, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY 34 (Feb. 2018) ("THE COST OF MALICIOUS CYBER ACTIVITY"), https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

[3] *Id.*

No company, however, is immune from attack. In fact, in 2017, the number of significant breaches at United States businesses, government agencies, and organizations surpassed 1,300—an increase of nearly 45 percent over what had been a record total in 2016.[4] According to one recent estimate, prepared by IBM and the Ponemon Institute, more than *one-quarter* of U.S. companies will experience at least one material data breach at some point in the next two years.[5] Breaches are also increasing in scale. Over the last five years, the number of breaches affecting more than one million records has nearly doubled, from nine in 2013 to 16 in 2017.[6]

While no data breach should be taken lightly, the consequences for individuals whose personal information may be exposed in a breach varies widely from incident to incident. That is true, in part, because different intruders have very different reasons for launching attacks. The White House Council of Economic Advisers, for example, has identified six types of threat actors, "each driven by

---

[4] Victor Reklaitis, *How the Number of Data Breaches Is Soaring—In One Chart*, MARKETWATCH (May 25, 2018), https://www.marketwatch.com/story/how-the-number-of-data-breaches-is-soaring-in-one-chart-2018-02-26.

[5] The report defines a "material" data breach as an event involving a minimum of 1,000 lost or stolen records. Ponemon Inst., 2018 COST OF A DATA BREACH STUDY: GLOBAL OVERVIEW 3 & n.3 (July 2018), https://www.ibm.com/security/data-breach.

[6] IBM, *IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses* (July 11, 2018), http://newsroom.ibm.com/2018-07-11-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses.

distinct objectives and motivations."[7] The Council's summation of those threat categories is quoted at length below:

- **Nation-states**: The main actors are Russia, China, Iran, and North Korea, according to [the Director of National Intelligence]. These groups are well funded and often engage in sophisticated, targeted attacks. Nation-states are typically motivated by political, economic, technical, or military agendas, and they have a range of goals that vary at different times. Nation-states frequently engage in industrial espionage. If they have funding needs, they may conduct ransom attacks and electronic thefts of funds. Nation-states frequently target [personally identifying information ("PII")] in order to spy on certain individuals. Furthermore, per our interviews of cybersecurity experts, nation-states may engage in business destruction involving one or more firms, potentially as a retaliation against sanctions or other actions taken by the international community.

- **Corporate competitors**: These are firms that seek illicit access to proprietary IP, including financial, strategic, and workforce-related information on their competitors; many such corporate actors are backed by nation-states.

- **Hactivists**: These are generally private individuals or groups around the globe who have a political agenda and seek to carry out high-profile attacks. These attacks help hacktivists distribute propaganda or to cause damage to opposition organizations for ideological reasons.

- **Organized criminal groups**: These are criminal collectives that engage in targeted attacks motivated by profit seeking. They collect profits by selling stolen PII on the dark web and by collecting ransom payments from both public and private entities by means of disruptive attacks.

- **Opportunists**: These are usually amateur hackers driven by a desire for notoriety. Opportunists typically attack organizations

[7] THE COST OF MALICIOUS CYBER ACTIVITY 3.

using widely available codes and techniques, and thus usually represent the least advanced form of adversaries.

- **Company insiders**: These are typically disgruntled employees or ex-employees looking for revenge or financial gain. Insiders can be especially dangerous when working in tandem with external actors, allowing these external actors to easily bypass even the most robust defenses.[8]

Significantly, in the current Worldwide Threat Assessment of the US Intelligence Community, the Director of National Intelligence reported the following regarding China's motivation for cyberattacks:

> ***China will continue to use cyber espionage and bolster cyber attack capabilities to support national security priorities.*** The [intelligence community] and private-sector security experts continue to identify ongoing cyber activity from China, although at volumes significantly lower than before the bilateral US-China cyber commitments of September 2015. Most detected Chinese cyber operations against US private industry are focused on cleared defense contractors or IT and communications firms whose products and services support government and private sector networks worldwide. China since 2015 has been advancing its cyber attack capabilities by integrating its military cyber attack and espionage resources in the Strategic Support Force, which it established in 2015.[9]

---

[8] *Id.* (footnote omitted).

[9] *See* Daniel R. Coats, Director of National Intelligence, WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY 6 (Feb. 13, 2018) https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf. Significantly, the same report for 2014 made a point of highlighting that OPM's contractors relevant here, including KeyPoint "were involved in processing sensitive *PII related to national security clearances* for Federal Government employees." James R. Clapper, Director of National Intelligence, WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY 1–2 (Feb. 26, 2015), https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf (emphasis added).

It follows that the risk of harm an individual faces from a data breach will vary depending on the context. When a nation-state conducts cyber espionage to inform its economic and geopolitical strategies or a "hacktivist" breaches an organization's defenses to pursue a political agenda, the risk that the average customer will suffer economic loss—or indeed any tangible impact at all—differs materially from the risk involved when a cyber-criminal aims to commit financial fraud.

Further, cyber-espionage events are on the rise. The White House Council of Economic Advisers notes that cyber espionage represents the "fastest growing category of malicious cybersecurity incidents" featuring "the most technically skilled" attacks that often go unnoticed.[10] Such attacks are often difficult to detect because they "don't have external fraud detection as a potential discovery method"—that is, because there is no detectable harm to individuals.[11]

This is the multi-threat data security environment that U.S. companies confront every day, and the backdrop against which this and other data breach litigation must be evaluated.

[10] THE COST OF MALICIOUS CYBER ACTIVITY 4.

[11] Verizon, 2018 DATA BREACH INVESTIGATIONS REPORT 7 (11th ed. 2018).

II. In Data Breach Cases, As In All Others, The Article III Standing Analysis Must Be Highly Sensitive To Context.

Plaintiffs' core contention is that, for pleading purposes, a simple allegation that an individual's personal information was compromised is sufficient to establish Article III standing. NTEU Plaintiffs, for example, argue that "there have been data breaches through which Plaintiffs … had inherently personal information stolen from OPM's databases," and that this alone is sufficient to establish standing, without any need "for NTEU Plaintiffs to establish that their personal information has been used in a particular way." NTEU Br. 16–17. Class Plaintiffs similarly claim that "because Plaintiffs' personal information was disclosed in the Data Breaches, they have suffered an invasion of privacy" sufficient to establish standing. Class Br. 35.

The Chamber urges the Court to reject a one-size-fits-all presumption on standing and to reaffirm that standing is "always a case- and context-specific inquiry." *Nat'l Ass'n of Home Builders*, 786 F.3d at 43. Accordingly, the district court properly conducted just the kind of case-specific inquiry mandated by this Court's precedents, and appropriately declined to adopt a "tautological approach" that would treat the fact of a data breach as giving rise to standing for all plaintiffs in every data breach case. JA412–13 (Op. 24–25).

Indeed, the district court here was notably careful to parse the Consolidated Amended Complaint's allegations regarding the specific information that OPM had

collected from applicants for government employment, JA429–31 & nn.18–19 (Op. 429–31), as well as the natural (and indeed, almost universally accepted) inference about what kind of actor would want to collect background information about U.S. government employees and the plaintiffs' (virtually non-existent) allegations about the "purpose of the cyberattacks." JA430, 433–35 (Op. 42, 45–47). Consistent with Circuit precedent, all of this was done in service of an inquiry into "whether the complaint plausibly *alleges* that the plaintiffs now face a substantial risk of identity theft" or other injury. JA426 (Op. 38) (quoting *Attias v. CareFirst, Inc.*, 865 F.3d 620, 627 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018)).

This approach was entirely consistent with the mode of analysis followed in *Attias*. There, the Court observed, the data breach at issue involved a theft of social security numbers and credit card numbers at a health insurance company. On the facts there alleged, the risk that affected plaintiffs could suffer identity theft was so sufficiently clear that the defendant did "not seriously dispute" it. 865 F.3d at 628.

But to treat *Attias* as establishing a blanket rule creating standing in all data breach cases would conflict with the accepted reality that many cybersecurity attacks are launched by actors who have no intention to use stolen data to commit fraud or identity theft, or otherwise injure individuals. As noted, nation-states may penetrate the computer systems of a company or agency to gather intelligence,

companies may launch cyberattacks to gain competitive advantages, and hacktivists may intrude to obstruct or embarrass ideological opponents. *Supra* at 5-8. Where it readily appears that a breach was motivated by geopolitical rather than financial purposes, it would be inappropriate and unrealistic to presume that any individual whose personal information was exposed is likely to suffer harm. The correct approach is instead to require plaintiffs to plead more detail about why the breach in question gives rise to a sufficiently particularized and concrete risk of injury to any individual plaintiff to create an Article III injury-in-fact. *Cf. Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 & n.5 (2013) (holding that plaintiffs lacked standing based on a failure to plead "certainly impending" injury and finding that plaintiffs had only pled a "speculative chain of possibilities" and "attenuated chain of inferences necessary to find harm"). That is just the approach that the district court carefully followed here, and its conclusion should be affirmed.[12]

[12] A number of courts have reached similar conclusions, consistent with the Supreme Court's holding in *Clapper* that "'[a]llegations of *possible* future injury' are not sufficient" to establish injury in fact. 568 U.S. at 409 (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)). In *Beck v. McDonald*, the Fourth Circuit denied standing where the plaintiffs alleged "mere theft" of their social security numbers, holding that such a bare-bones allegation was "too speculative" to establish an inference of "enhanced risk of future identity theft." 848 F.3d 262, 274–75 (4th Cir.), *cert. denied*, 137 S. Ct. 2307 (2017). The same was true in *Reilly v. Ceridian Corp.*, where the Third Circuit found allegations that a hacker had merely "accessed" personal information were "insufficient to establish standing." 664 F.3d 38, 40–44 (3d Cir. 2011). The Court's decision in *Attias* is to

III. Class Plaintiffs Cannot Circumvent KeyPoint's Immunity With Conclusory Allegations Of Negligence And Breach Of Contract.

This Court should also affirm the district court's conclusion that the Class Plaintiffs' claims against KeyPoint are barred by government-contractor immunity.

The Supreme Court has long recognized that, just as the federal government is immune (absent waiver) from liability claims, the "uniquely federal interests" involved in federal contracting justify shielding government contractors from lawsuits that seek to micromanage work done at the government's behest. *See, e.g.*, *Boyle v. United Techs. Corp.*, 487 U.S. 500, 504–05 (1988); *Yearsley v. W. A. Ross Constr. Co.*, 309 U.S. 18, 20–21 (1940). In any given case, the scope of this so-called derivative sovereign immunity is defined not by the nature of the claim asserted, but rather by the scope of authority delegated by the government to the contractor. *See, e.g.*, *Campbell-Ewald Co. v. Gomez*, 136 S. Ct. 663, 672–73 & n.7 (2016). Thus, where a third party's claims arise directly out of an admittedly valid contract between a government agency and a private contractor, the contractor is immune from suits arising out of that contract unless the contractor's conduct deviates in some specific and identifiable way from what the government authorized. *See, e.g.*, *Yearsley*, 309 U.S. at 20–21 ("[I]f this authority to carry out

---

similar effect. There, based on a close reading of the particular claims in suit, the Court found that the plaintiffs had made sufficient factual allegations to conclude that the attacker had the "intent" to misuse their data. 865 F.3d at 628.

the project was … within the constitutional power of Congress, there is no liability on the part of the contractor for executing its will.").

In their Consolidated Amended Complaint, Class Plaintiffs fail to allege that KeyPoint exceeded its authority under its OPM contracted or violated OPM's express requirements. Instead, Class Plaintiffs allege that KeyPoint did not adopt data security measures that Class Plaintiffs now say were necessary, conspicuously omitting any allegation that *the government* ever required KeyPoint to take those steps. Because Class Plaintiffs do not contend that KeyPoint ever strayed from its contractual obligations to the government, derivative immunity bars their claims against the company. *See Campbell-Ewald*, 136 S. Ct. at 672–73.

A. The Consolidated Amended Complaint Does Not Plausibly Allege that KeyPoint Violated OPM's "Explicit Instructions" or "Exceeded [Its] Authority."

Class Plaintiffs advance three reasons why their claims against KeyPoint are not barred by government-contractor immunity. None is persuasive, and each would subvert the "uniquely federal interests" that underpin the derivative immunity doctrine.

1. First, Class Plaintiffs contend that government-contractor immunity applies only where the government "directed a contractor to do the very thing that is the subject of the claim." Class Br. 43. This argument directly conflicts with the established standard. The Supreme Court has made clear that a government

contractor is immune unless the complaint "allege[s] that the contractor "*violate[d]* … the Government's *explicit instructions*" or "exceeded [its] authority." *Cambell-Ewald*, 136 S. Ct. at 672–73 (emphasis added). In other words, the question is not (as Class Plaintiffs argue) whether the government required the contractor to undertake the exact act or omission that gave rise to the claim, but instead whether the government *prohibited* the contractor from acting as it did.

Campbell-Ewald demonstrates that government-contractor immunity analysis properly centers on whether the contractor violated the government's express contracting instructions or overstepped its contractual authority. In that case, plaintiffs sued a Navy contractor for violating the Telephone Consumer Protection Act ("TCPA") by allowing a third-party vendor to send unsolicited text messages to their phones. *Id.* at 667–68. The Court held that the contractor was not immune from suit over the unauthorized text messages because it departed from the Navy's instructions. The Navy "authorized [the contractor] to send text messages only to individuals who had 'opted in' to receive solicitations," impressed upon the contractor "the importance of ensuring that … all recipients had consented to receiving messages," and "relied on [the contractor's] representation that the list was in compliance." *Id.* at 673–74. The Supreme Court's conclusion that the claims could proceed was thus bound up with the plaintiffs'

contention that the contractor had violated specific instructions that the government had expressly issued.

The Consolidated Amended Complaint does not allege that KeyPoint violated any "express instruction[]" from OPM or in any way exceeded its authority under its OPM contract. There is no dispute that KeyPoint was authorized to do exactly what it did, *see* CAC ¶¶ 75–76, and no indication that KeyPoint strayed from the OPM's instructions, *see id.* ¶ 5 (acknowledging that OPM did not terminate KeyPoint's contract). Instead, Class Plaintiffs allege that KeyPoint should have implemented data security measures that OPM did not require KeyPoint to adopt. *See, e.g.*, *id.* ¶ 223.

Courts, though, have rejected Class Plaintiffs' theory that government contractors can be held liable for filing to take additional precautions not expressly required by the government. For example, in a recent failure-to-warn case, the Fourth Circuit held that a contractor cannot be held liable for not providing *additional* warnings "so long as the government dictated or approved the warnings that the contractor actually provided." *Sawyer v. Foster Wheeler LLC*, 860 F.3d 249, 256–59 (4th Cir. 2017). So too here, the government dictated certain safety measures KeyPoint was required to implement, and KeyPoint is immune from suit so long as it followed those directives.

Class Plaintiffs' expansive theory of liability would create mischief without end. One of the key benefits that the government gains through contracting is the private sector know-how, *i.e.*, the "specialized knowledge or expertise" of outside firms. *See Filarsky v. Delia*, 566 U.S. 377, 390 (2012). The practical effect of Class Plaintiffs' rule, however, would be for contractors to agree only to discrete, narrowly defined tasks subject to comprehensive instructions from the contracting agency. This would erode the benefit of delegating responsibility to expert contractors, who would risk sacrificing immunity each time they brought their expertise to bear (unless, perhaps, they paused to request and obtain express governmental blessing for each and every step in executing the contract).

Nor do Class Plaintiffs suggest that any countervailing policy benefit would be garnered by opening up government contracts to Monday morning quarterbacking by plaintiffs' lawyers. To the contrary, the rational policy, consistent with precedent, is to hold that a claim against a government contractor cannot proceed past the pleading stage unless the complaint alleges that the contractor "violate[d] … the Government's explicit instructions" or "exceeded [its] authority." *Campbell-Ewald*, 136 S. Ct. at 672–73.

2. Nor can Class Plaintiffs defeat government-contractor immunity through their allegation that KeyPoint's contract with OPM—like literally every other government contract that pertains to the maintenance "of a system of

records," 5 U.S.C. § 552a—"incorporates the requirements of the Privacy Act." Class Br. 46 (quoting CAC ¶ 123); *see* 48 C.F.R. § 24.102(c).

Class Plaintiffs' argument has several flaws. For one, the Privacy Act requires *OPM* (not its contractors) to set data security standards. *See* 5 U.S.C. § 552a(e); *see also Abdelfattah v. U.S. Dep't of Homeland Sec.*, 787 F.3d 524, 533 n.4 (D.C. Cir. 2015) ("[T]he Privacy Act creates a cause of action against only federal government agencies and not private corporations or individuals officials."). For another, the Privacy Act regulations on which Class Plaintiffs attempt to rely state expressly that any relevant civil claims properly run against the *agency*, not the contractor. 48 C.F.R. § 52.224-2(b) ("In the event of violations of the Act, a civil action may be brought against the agency involved …."). Indeed, as stated in the Department of Justice's guide on the Privacy Act, in a lawsuit under the Act "the agency—not the contractor—remains the only proper party defendants." Dep't of Justice, Overview of the Privacy Act of 1974, https://www.justice.gov/opcl/government-contractor (updated July 16, 2015) (citing numerous authorities).

Perhaps the most glaring problem with Class Plaintiffs' theory is that neither the Privacy Act nor any implementing regulations set out the "specific, industry-standard data security practices" that Class Plaintiffs now say KeyPoint should have adopted, nor do Class Plaintiffs allege that such practices were required by

the OPM-KeyPoint contracts. Class Br. 46. Class Plaintiffs' argument based on the Privacy Act thus amounts to little more than another version of their theory that they should be permitted to second-guess OPM's decision-making and impose crushing liability on government contractors who did not "violate[] … the Government's *explicit instructions*," *Campbell-Ewald*, 136 S. Ct. at 672 (emphasis added).

The law neither requires nor permits such an inequitable result. In fact, in the first (and thus far only) court of appeals decision to consider the contractor immunity holding in *Campbell-Ewald*, the Fourth Circuit held that a government contractor was immune from a TCPA claim even though its contract "required [the contractor] to follow applicable laws." *Cunningham v. Gen. Dynamics Info. Tech., Inc.*, 888 F.3d 640, 647 (4th Cir. 2018). *Cunningham* makes clear that a general incorporation of broad legal standards does not set forth "explicit instructions." There, immunity attached because the government did not affirmatively require the contractor to take the steps that plaintiffs contended were required by federal law. The same result should follow: because Class Plaintiffs do not allege that KeyPoint violated the express terms of its OPM contract or any OPM directive, KeyPoint is entitled to government-contractor immunity.

3. Finally, Class Plaintiffs cannot invoke bare allegations of negligence to end-run KeyPoint's immunity. As discussed above, a government contractor's

immunity is defined by the scope of its delegated authority and not by the label affixed to plaintiffs' claims. *See Campbell-Ewald*, 136 S. Ct. at 673 n.7 (government-contractor immunity is concerned with whether the contractor "perform[ed] in compliance with all federal directions."). Class Plaintiffs' claim that a plaintiff need only allege negligence—and nothing else—to defeat government-contractor immunity finds no support in precedent.

To the contrary, in a case Class Plaintiffs prominently cite, the Supreme Court held that a military contractor was immune from a claim that it *negligently* designed a helicopter. *See Boyle*, 487 U.S. at 503 (case cited at Class Br. 44–45, 46–47). In that case, the Court held that the immunity depends on what the government required and whether the contractor met those requirements. *Id.* at 512. Courts of appeals, similarly, are in accord that a government contractor may invoke immunity against negligence claims. *See, e.g.*, *Ackerson v. Bean Dredging LLC*, 589 F.3d 196, 206–07 (5th Cir. 2009); *In re Air Disaster at Ramstein Air Base*, 81 F.3d 570, 574 (5th Cir.), *modified on denial of reh'g on other grounds*, *Perez v. Lockheed Corp.*, 99 F.3d 340 (5th Cir. 1996). And in *Sawyer*, the court held a plaintiff cannot defeat government-contractor immunity based on allegations that the contractor negligently failed to adopt additional precautions over and above the precautions "the government dictated or approved." 860 F.3d at 256–59 (contractor had a "colorable" basis to invoke government-contractor immunity

against negligence claim and thus case was properly removed under officer removal statute).[13]

The effect of Class Plaintiffs' proposed rule would be effectively to eliminate government-contractor immunity as a pleading-stage defense in most cases. *But see, e.g.*, *Adkisson v. Jacobs Eng'g Grp., Inc.*, 790 F.3d 641, 649 (6th Cir. 2015) (directing district court to consider government-contractor immunity defense on a motion to dismiss); *Ackerson*, 589 F.3d at 204 ("[B]ased on the pleadings, the Contractor Defendants are entitled to government-contractor immunity …."). Virtually any cause of action could be recast as a negligence claim—indeed, here, there is hardly any daylight between the contract-based claims that Class Plaintiffs assert against KeyPoint and their negligence claim. *See* CAC ¶¶ 223, 232, 241, 250, 255, 274.

[13] The cases Class Plaintiffs rely upon do not hold or suggest otherwise. Class Plaintiffs place great reliance on *dicta* from *Brady v. Roosevelt Steamship Co.*, 317 U.S. 575 (1943), but that case did not deal at all with government-contractor immunity; it instead interpreted a specific immunity provision of the Suits in Admiralty Act. *See id.* at 577. In *Ackerson*, 589 F.3d at 207–08, which did address government-contractor immunity, the Fifth Circuit dismissed the plaintiffs' negligence claims (among others) with prejudice. Equally unpersuasive is plaintiffs' reliance on the district court's decision in *In re Fort Totten Metrorail Cases*, where "the very premise" of the lawsuit was that the contractor "acted *against* the 'will of the sovereign' by breaching its contractual duties … and by performing negligently." 895 F. Supp. 2d 48, 75 (D.D.C. 2012). Thus, Judge Walton's decision in *Fort Totten* was not based on the presence of a negligence claim, but rested on the case-specific allegation that the contractor's performance was contrary to the government's express will.

B. Class Plaintiffs' Position Would Undermine the Public's Interest in Efficient Government Contracting.

If Class Plaintiffs were correct that government-contractor immunity could be defeated by conclusory allegations of breach of contract or negligence, government contracting would become more expensive and much less efficient.

Unlike in private contracts, where the principal will ordinarily be at least jointly liable for any damages, the government and its employees are ordinarily immune from money-damages suits. As a result, without immunity comparable to that enjoyed by government employees performing the same tasks, contractors "could be left holding the bag—facing full liability for actions taken in conjunction with government employees who enjoy immunity for the same activity." *Filarsky*, 566 U.S. at 391. As the Supreme Court has recognized, such a rule would cause government contractors to "think twice before accepting a government assignment," and thus undermine the "public interest in ensuring performance of government duties free from the distractions that can accompany even routine lawsuits." *Id.*; *accord Campbell-Ewald*, 136 S. Ct. at 673 (recognizing "the risk that contractors will shy away from government work").

Moreover, contractors who chose to enter government contracts despite these risks would "predictably raise their prices to cover, or to insure against, contingent liability." *Boyle*, 487 U.S. at 512. In that event, "[t]he financial burden of judgments against the contractors would ultimately be passed through,

substantially if not totally, to the United States itself." *Id.* at 511–12. That result would be bad for the government (which would pay higher costs for contracted services), bad for taxpayers (who ultimately bear the government's costs), and bad for contractors (who would be forced to make highly complex, predictive judgments about potential liabilities if they chose to continue doing business with the government at all).

All this can be avoided if the Court endorses the time-tested, equitable, and predictable standard followed by the district court. The proper question at the pleading stage is "whether the complaint plausibly alleges that [the contractor] violated federal law and [the agency's] explicit instructions or exceeded its authority under the contract." JA426 (Op. 68). Because Class Plaintiffs concede that KeyPoint did not violate the Privacy Act directly, Class Br. 46, and do not allege that KeyPoint disregarded any explicit instruction from OPM or otherwise exceeded its authority under the contract, the district court correctly held that KeyPoint is shielded by derivative immunity.

CONCLUSION

The district court correctly applied recognized limits on Article III standing and the liability of government contractors. For the reasons described above, the district court's decision should be affirmed.

Dated: July 26, 2018

Respectfully submitted,

/s/ Alan Charles Raul

Steven P. Lehotsky
U.S. CHAMBER LITIGATION CENTER
1615 H Street, N.W.
Washington, D.C. 20062
(202) 463-5337

Alan Charles Raul
Kwaku A. Akowuah
Clayton G. Northouse
Daniel J. Hay
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
Telephone: (202) 736-8000
Facsimile: (202) 736-8711

Counsel for The Chamber of Commerce of the United States of America

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(g), I hereby certify that this brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(5) and 32(a)(7)(B) because it contains 5,104 words, excluding the parts exempted by Fed. R. App. P. 32(f) and Cir. R. 32(e)(1).

I further certify that 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 the brief was prepared in 14-point Times New Roman font using Microsoft Word.

Dated: July 26, 2018

/s/ Kwaku A. Akowuah
Kwaku A. Akowuah

CERTIFICATE OF SERVICE

I hereby certify, pursuant to Fed. R. App. P. 25(d) and Cir. R. 25, that on July 26, 2018, the foregoing was electronically filed with the Clerk of the Court using the CM/ECF system, which will send a notification to the attorneys of record in this matter who are registered with the Court's CM/ECF system.

Dated: July 26, 2018

/s/ Kwaku A. Akowuah
Kwaku A. Akowuah