9-Nextgov-Why the Lawsuit Against OPM

About

Why the Lawsuit Against OPM over the Massive Data Breach Faces an Uphill Battle

OPM Director Katherine Archuleta, left, and others, are sworn in on Capitol Hill in Washington, Wednesday, June 24, 2015, prior to testifying before the House Oversight and Government Reform Committee hearing on recent cyber attacks. From left are, Archul (AP Photo/Susan Walsh)

Get the latest federal technology news delivered to your inbox.

email

July 1, 2015

Demonstrating damages have been suffered will be the challenge, legal experts say.

A class action lawsuit against the Office of Personnel Management over a massive breach of federal employees' *[Legal Action]* data faces an uphill battle, privacy law experts say.

The American Federation of Government Employees says OPM and a contractor violated the 1974 Privacy Act by neglecting to secure employees' personal data, which resulted in financial and emotional harm. *[Disappointment]*

The failure to protect workers' data could hold up in court, but demonstrating damages have actually been suffered will be the challenge, legal experts say. The suspected thieves in this situation are foreign

government spies aiming for access to U.S. secrets, not financial fraudsters seeking access to people's bank accounts.

The real harm done for a federal employee or job applicant is now "living for the rest of your life knowing that all of your personal information is in the hands of another country and possibly terrorists, or possibly people that want to do harm to you, your family or the country," said Cheri Cannon, a partner at federal employment law group Tully Rinckey. "The United States can't fix that." *[Disappointment]*

But neither can any lawsuit, said Cannon, a former military attorney who says she's affected by the breach. AFGE, the country's largest government employee union, filed suit in U.S. District Court on Monday against the agency, OPM Director Katherine Archuleta, OPM Chief Information Officer Donna Seymour and the contractor, KeyPoint Government Solutions, which conducts background investigations for the government.

Past data breach cases resting on the Privacy Act largely have been unsuccessful.

According to AFGE's complaint , OPM disregarded federal information security statutes and inspector general recommendations dating back to 2007.

Last month, OPM acknowledged a breach of 4.2 million personnel records, containing Social Security numbers, and the compromise of an undefined number of invasive background investigations on individuals with access to classified intelligence.

Claiming that OPM knew its networks were vulnerable to attack and did nothing "opens the door a little bit wider" for making a case, said Cannon, a former Air Force deputy general counsel for fiscal, ethics and administrative law, who at one point held a security clearance *[Legal Action]*. She said she has been notified her personnel records were compromised by one of the hacks. The government has not notified victims of the background check breach. *[Deny]*

Demonstrating the Agency Did Not Lock the Door *[Disappointment]*

“AFGE has compelling case, particularly because OPM was on notice as to the security vulnerabilities,” said Marc Rotenberg, president of the Electronic Privacy Information Center. “It doesn’t matter who committed the breach. The central question is whether the federal agencies took necessary measures to protect the information collected.” *[Disappointment]*

By law, the agency was obligated to protect the volumes of information it collects.

That likely is why defendant OPM head Archuleta has consistently said she is “angry” about the hacks but has not expressed remorse *[Deny]*. Archuleta and other OPM officials “cannot apologize or take responsibility for” the breach publicly on Capitol Hill or in the press because that would hurt their legal defense, Cannon said.

OPM officials Tuesday would not comment on the lawsuit *[Deny]*.

In the past, Archuleta has insisted no one in the government is personally responsible for the network intrusion, rather the hackers are to blame *[Deny]*. Background check provider KeyPoint Government Solutions, from whom hackers stole a credential to open OPM systems, says the company has seen no evidence it is responsible for the breach.

AFGE’s complaint states the damages employees have or will suffer include “pecuniary losses, anxiety and emotional distress,” caused by among other things the compromise of personal information belonging to themselves, relatives, neighbors and acquaintances contained in investigative records. *[Disappointment]*

Also listed among the harms inflicted is “lost opportunity costs” associated with the effort and time spent preventing ID and medical theft.

Proving Your Data Has Been Misused

But past Privacy Act verdicts have narrowly defined who is eligible for compensation when personal data is compromised.

In 2004, the Supreme Court ruled an individual can file suit against the government to recover financial damages when such information is exposed — but only if an “actual damage” is proven. The definition of “actual damage” was left open in the case, which involved miners suing the Labor Department for disclosing their Social Security numbers. In 2012, the high court decided an individual — in that case, a Federal Aviation Administration employee whose HIV-positive status was divulged — cannot claim financial damages based on mental or emotional distress caused by a federal agency’s intentional or willful violation of the Privacy Act. In 2011, SAIC and the Pentagon were sued under the Privacy Act when Tricare military health insurance data on 4.9 million service members and their families was stolen. A D.C. federal judge dismissed most of the charges in May 2014, ruling that data loss alone, without evidence the information was misused, did not merit damages.

There have been recent legal proceedings that suggest some sort of settlement agreement might be brokered.

The National Labor Relations Board ruled earlier this year the U.S. Postal Service violated labor laws by not at least negotiating with postal unions on the agency’s response to its employees’ data being hacked in 2014.

In addition, the Supreme Court will hear a case in the next term, starting in October, that could set a new standard for whether data breach lawsuits can be based on future harm.

“The impossibility of forecasting what will happen to stolen data has intensified legal wrangling over the rights of data breach victims,” the Intercept reported in a June 12 article on the upcoming case that cited the OPM incident.

Up until now, the precedent on fear of prospective losses has been a 2013 decision, Clapper v. Amnesty International USA , where journalists and human rights advocates unsuccessfully sued for suffering the cost and inconvenience of protecting themselves against the likelihood of warrantless digital surveillance.

The forthcoming high court case addresses whether an unemployed Virginia man has legal standing to sue the search site Spokeo because it allegedly published incorrect details about his education, wealth and age, which he says hurt his employment chances.

Justice Department Staff v. Justice Department Staff?

According to AFGE, the union will contend federal workers suffered damages from the moment personal data was stolen *[Disappointment]*. The union has not provided the amount of money being sought, explaining the total sum will be figured out during the discovery period.

Costs already incurred involve replacing credit cards, closing accounts and other steps individuals may have taken in response to the breach, officials said during a Tuesday call with reporters. One attorney representing the union stressed employees do not have to be victims of identity theft to demonstrate damages.

It will also be interesting to see how breach victims at the Justice Department, which must defend claims against the United States, will handle legal proceedings.

“Justice lawyers are working against their own financial interests – they have a stake in OPM winning for their own personal financial reason,” Cannon said.

The complaint excludes “any judicial officer assigned to this case,” OPM, Archuleta, Seymour and KeyPoint as members of the proposed class action lawsuit.

“The Justice Department is reviewing the complaint,” DOJ spokeswoman Nicole Navas said, declining to comment further.

Rotenberg said he doubts the question of conflict of interest will lead to recusal.

The irony is that, although the Supreme Court has narrowed the legal protections established in the Privacy Act, “personal records of the justices,

their clerks and staff were likely among those disclosed in the OPM breach," he said.

Share This:

Nextgov Ebook: What's Next for Government Cloud

X

default settings according to your preference. You cannot opt-out of our First Party Strictly Necessary

Cookies as they are deployed in order to ensure the proper functioning of our website (such as prompting the

cookie banner and remembering your settings, to log into your account, to redirect you when you log out,

etc.). For more information about the First and Third Party Cookies used please follow this link.

Allow All Cookies

Manage Consent Preferences

Strictly Necessary Cookies - Always Active

We do not allow you to opt-out of our certain cookies, as they are necessary to

ensure the proper functioning of our website (such as prompting our cookie banner and remembering your privacy

choices) and/or to monitor site performance. These cookies are not used in a way that constitutes a “sale” of

your data under the CCPA. You can set your browser to block or alert you about these cookies, but some parts

of the site will not work as intended if you do so. You can usually find these settings in the Options or

Preferences menu of your browser. Visit www.allaboutcookies.org to learn more.

Sale of Personal Data, Targeting & Social Media Cookies

Under the California Consumer Privacy Act, you have the right to opt-out of the

sale of your personal information to third parties. These cookies collect information for analytics and to

personalize your experience with targeted ads. You may exercise your right to opt out of the sale of personal

information by using this toggle switch. If you opt out we will not be able to offer you personalised ads and

will not hand over your personal information to any third parties. Additionally, you may contact our legal

department for further clarification about your rights as a California consumer by using this Exercise My

Rights link

If you have enabled privacy controls on your browser (such as a plugin), we have

to take that as a valid request to opt-out. Therefore we would not be able to track your activity through the

web. This may affect our ability to personalize ads according to your preferences.

Targeting cookies may be set through our site by our advertising partners. They

may be used by those companies to build a profile of your interests and show you relevant adverts on other

sites. They do not store directly personal information, but are based on uniquely identifying your browser and

internet device. If you do not allow these cookies, you will experience less targeted advertising.

Social media cookies are set by a range of social media services that we have

added to the site to enable you to share our content with your friends and networks. They are capable of

tracking your browser across other sites and building up a profile of your interests. This may impact the

content and messages you see on other websites you visit. If you do not allow these cookies you may not be

able to use or see these sharing tools.

If you want to opt out of all of our lead reports and lists, please submit a

privacy request at our Do Not Sell page.

Save Settings

Cookie Preferences Cookie List

Cookie List

A cookie is a small piece of data (text file) that a website – when visited by a

user – asks your browser to store on your device in order to remember information about you, such as your

language preference or login information. Those cookies are set by us and called first-party cookies. We also

use third-party cookies – which are cookies from a domain different than the domain of the website you are

visiting – for our advertising and marketing efforts. More specifically, we use cookies and other tracking

technologies for the following purposes:

Strictly Necessary Cookies

We do not allow you to opt-out of our certain cookies, as they are necessary to

ensure the proper functioning of our website (such as prompting our cookie banner and remembering your privacy

choices) and/or to monitor site performance. These cookies are not used in a way that constitutes a “sale” of

your data under the CCPA. You can set your browser to block or alert you about these cookies, but some parts

of the site will not work as intended if you do so. You can usually find these settings in the Options or

Preferences menu of your browser. Visit www.allaboutcookies.org to learn more.

Functional Cookies

We do not allow you to opt-out of our certain cookies, as they are necessary to

ensure the proper functioning of our

website (such as prompting our cookie banner and remembering your privacy choices) and/or to monitor site

performance. These cookies are not used in a way that constitutes a “sale” of your data under the CCPA. You

can set your browser to block or alert you about these cookies, but some parts of the site will not work as

intended if you do so. You can usually find these settings in the Options or Preferences menu of your

browser. Visit www.allaboutcookies.org to learn more.

Performance Cookies

We do not allow you to opt-out of our certain cookies, as they are necessary to

ensure the proper functioning of our

website (such as prompting our cookie banner and remembering your privacy choices) and/or to monitor site

performance. These cookies are not used in a way that constitutes a “sale” of your data under the CCPA. You

can set your browser to block or alert you about these cookies, but some parts of the site will not work as

intended if you do so. You can usually find these settings in the Options or Preferences menu of your

browser. Visit www.allaboutcookies.org to learn more.

Sale of Personal Data

We also use cookies to personalize your experience on our websites, including by

determining the most relevant content and advertisements to show you, and to monitor site traffic and

performance, so that we may improve our websites and your experience. You may opt out of our use of such

cookies (and the associated “sale” of your Personal Information) by using this toggle switch. You will still

see some advertising, regardless of your selection. Because we do not track you across different devices,

browsers and GEMG properties, your selection will take effect only on this browser, this device and this

website.

Social Media Cookies

We also use cookies to personalize your experience on our websites, including by

determining the most relevant content and advertisements to show you, and to monitor site traffic and

performance, so that we may improve our websites and your experience. You may opt out of our use of such

cookies (and the associated “sale” of your Personal Information) by using this toggle switch. You will still

see some advertising, regardless of your selection. Because we do not track you across different devices,

browsers and GEMG properties, your selection will take effect only on this browser, this device and this

website.

Targeting Cookies

We also use cookies to personalize your experience on our websites, including by

determining the most relevant content and advertisements to show you, and to monitor site traffic and

performance, so that we may improve our websites and your experience. You may opt out of our use of such

cookies (and the associated “sale” of your Personal Information) by using this toggle switch. You will still

see some advertising, regardless of your selection. Because we do not track you across different devices,

browsers and GEMG properties, your selection will take effect only on this browser, this device and this

website.