Legal Sidebar

Is There a Judicial Remedy for Victims of Federal Data Breaches?

7/15/2015

The scope of information believed to have been compromised by a series of cyber-intrusions at the Office of Personnel Management (OPM) continues to grow. OPM recently announced that further investigation of the initial breach affecting 4.2 million current and former federal employees has led officials to conclude that sensitive information on 21.5 million individuals had been stolen from separate OPM databases used in connection with background investigations. In addition to the potential effects on domestic and foreign policy that may result from these breaches, which are discussed here, two recently filed lawsuits raise questions regarding what redress, if any, is due to affected individuals beyond the free credit monitoring that has been offered by OPM.

The two suits, filed separately by the American Federation of Government Employees (AFGE) and the National Treasury Employees Union (NTEU) allege a number of legal theories under which the plaintiffs believe recovery may be available, including claims citing the Privacy Act, the Federal Information Security Management Act (FISMA), common law negligence, and the Due Process clause of the Constitution. While, procedural obstacles to such suits, such as whether the plaintiffs have suffered a sufficiently concrete injury to have a right to sue, are important and may end up being dispositive, this post focuses instead on the extent to which selected sources of statutory, common, and constitutional law may provide a judicially enforceable remedy for current and former federal employees whose personal information may have been exposed during the breach of a federal information technology system.

Privacy Act

The Privacy Act, section 552a of title 5 of the U.S. Code, governs the means by which federal agencies and, in some instances, their contractors collect, maintain, use, and disseminate individually identifiable information in a system of records. The Privacy Act prohibits, with certain exceptions, the disclosure by a federal agency of "any record which is contained in a system of records" to any person or to another agency, except pursuant to a written request by or with the prior written consent of the record subject.

The Privacy Act, in relevant part, requires each agency that maintains a system of records to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained . . . ." In the AFGE lawsuit, the plaintiffs allege that OPM failed to comply with this provision of the Privacy Act.

The Privacy Act explicitly authorizes an individual to bring a civil action in federal district court whenever an agency fails to comply with the Privacy Act or a related rule in such a way as to have an "adverse effect on an individual." In such a suit, if it is determined that the agency acted in a manner that was intentional or willful, the United States can be liable for "actual damages" sustained by the individual as a result of the government's failure to comply with the law. Two major hurdles, however, may prevent recovery under the Privacy Act in the context of the OPM litigation. First, a plaintiff will need to prove that the agency acted in an "intentional or willful" manner and not merely in a "grossly negligent" fashion, a standard that has precluded recovery in several "information leak" cases under the Privacy Act. Second, a plaintiff will need to demonstrate that he has suffered "actual damages," a term of art recently interpreted by the Supreme Court to exclude damages for mental or emotional distress. In the past, plaintiffs in data breach litigation have had difficulty in proving concrete injuries, like financial losses, and have generally relied on psychic injuries (like emotional distress) as their source of recovery.

FISMA

Recently amended by the Federal Information Security Modernization Act of 2014, FISMA defines roles and responsibilities for the management and oversight of information security in the federal government. Specifically, FISMA requires federal agencies to protect federal information systems using security measures that are "commensurate with the risk and magnitude of the harm" that could result from a breach. Agencies are also statutorily directed to comply with standards, policies, and procedures issued by the Office of Management and Budget (OMB), as well as binding operational directives issued by the Secretary of Homeland Security. Compliance with FISMA is assessed in periodic reports by OMB, the Government Accountability Office (GAO), and agency Inspectors General, such as this report regarding OPM from November of 2014.

Suits brought by private parties to enforce the requirements of FISMA against federal agencies have generally been unsuccessful. Unlike the Privacy Act, FISMA does not contain an explicit private right of action. Nevertheless, FISMA has formed the basis of claims under the Administrative Procedure Act in both the AFGE's suit against OPM, and in a prior suit against the Veterans Administration (VA) following the loss of a hard drive containing personally identifiable information by that agency in 2007. The plaintiffs in the VA suit subsequently dropped the APA/FISMA claim upon appeal after it was dismissed by the district court. Earlier, in 2006, the D.C. Circuit had observed in dicta that the judicial branch is "notably absent" from the "multi-layered statutory scheme" of FISMA. While the amendments to FISMA at the end of 2014 modified this "multi-layered" scheme by clarifying the respective roles of OMB and Homeland Security, no private right of action was added.

Common Law Negligence

Those affected by the OPM breaches may also seek remedies for their injuries within tort law, which encompasses a number of civil wrongs including negligence. To successfully establish a negligence claim, a plaintiff must generally prove that (1) the defendant owed the plaintiff a legal duty; (2) the defendant breached that duty, often by failing to exercise reasonable care; (3) the defendant's action or failure to act caused the plaintiff's injuries; and (4) the plaintiff suffered harm as a result of the defendant's action or inaction. The elements of a specific tort claim are rooted in state common law. The plaintiffs in the AFGE suit have alleged that KeyPoint, an OPM contractor in charge of conducting background investigations, had a duty to take reasonable actions to protect the plaintiffs' personal information from cyberattack and breached that duty in a manner that caused the plaintiffs harm. Because tort law generally does not impose a duty on an individual to protect others from the unpredictable actions of third parties, the scope of OPM's duty may turn on how foreseeable the underlying data breach was to the government and whether the government's conduct created a risk that the breach would occur.

Whenever a tort suit is filed against the federal government, or its contractors, the Federal Tort Claims Act (FTCA) may enter the discussion. In general, because of its sovereign immunity, the United States cannot be sued without its consent. In the FTCA, Congress waived its immunity with regard to tort suits, allowing the U.S. to be held liable for its employees' tortious acts to the same extent a private person would be held liable under state law for similar behavior. However, the FTCA contains exceptions under which the U.S. could not be held liable for a tort claim. For example, the government is immunized from claims "based upon an act or omission of an employee of the Government, exercising due care, in the execution of a statute or regulation." Additionally, the discretionary function exception immunizes the government from claims based upon the exercise, or failure to exercise, a discretionary function. The viability of a hypothetical tort claim against OPM may turn on whether one of these exceptions applies to OPM's allegedly injurious action or inaction. Notably, the AFGE suit tort claim is alleged against a government contractor, not the government itself. The potential extension of FTCA principles to federal contractors, especially in the context of service contracts rather than manufacturing contracts, remains a matter of controversy and is discussed in detail in this CRS Report.

Due Process

In addition to the various statutory and common law standards for cybersecurity, the Constitution may impose requirements on federal agencies with respect to protecting private information within the government's possession. Specifically, in three cases over the past 40 years, the Supreme Court has suggested, but has not conclusively

recognized, that the Due Process Clause of the Fifth Amendment protects an interest in "avoiding disclosure of personal matters." In this vein, the NTEU suit has argued that OPM, by failing to adequately protect against a data breach, violated federal employees' rights to informational privacy. A constitutional challenge to OPM's practices may, however, find difficulty in court. In a 2011 case called *NASA v. Nelson*, the Supreme Court unanimously ruled against 28 NASA workers who argued that the extensive background checks required to work at NASA facilities violated their constitutional privacy rights. In so doing, the Court rejected the argument that a potential large scale data breach *could* result in the disclosure of personal information, thereby implicating constitutional rights, as the Court held that the "possibility that security measures will fail provides no 'proper ground' for a broad-based attack on government information-collection practices." Instead, the *Nelson* Court pointed to the existence of statutory protections provided under federal law as being sufficient to defeat a claim that the government is inadequately protecting informational privacy rights. While the plaintiffs mounting the constitutional challenge against OPM's security practices may be able to distinguish *Nelson* on the grounds that the 2015 data breach makes it more than a mere "possibility" that the government may be inadequately protecting government employees' personal information, the *Nelson* case may more broadly indicate the Court's reluctance to impose judge-made security standards on the federal government, especially in light of statutory standards imposed by the Privacy Act and FISMA.