Privileged & Confidential—Attorney Work Product

MEMORANDUM

TO: Helen Dixon, Data Protection Commissioner

FROM: Morrison & Foerster LLP (Andrew B. Serwin)

DATE: May 24, 2016

RE: Review of Certain Causes of Action

I. INTRODUCTION

This memorandum provides a non-exclusive overview of private remedies available to EU citizens, under federal law in the United States, against certain entities and individuals for alleged violations of data privacy arising from the gathering of personal information in the context of national security.[1, 2] It provides an overview of the most likely potential claims in the above-referenced situation, as well as a discussion of standing, which is an overarching issue. It further provides the contours of relief, including examples of significant open issues or splits in U.S. case law as well as potential limitations on recovery. Potential remedies arise under a number of different U.S. laws, resulting in the potential for a non-uniform approach to relief.

This memorandum does not opine on the effectiveness of these remedies for purposes of Article 47 of the Charter of Fundamental Rights of the European Union, or on whether such causes of action would be appropriate in any particular circumstance. Where relevant, however, it identifies those factors that may be barriers to suit or otherwise limit recovery.

One point of reference for the discussion below relates to the structure of the Courts in the United States. Article III of the United States Constitution created the Supreme Court, and permitted Congress to create such inferior courts as were appropriate. Those Courts are divided into 94 district level courts, and 13 Courts of Appeal, 12 of which are regional "Circuit Courts," and one of which is the Court of Appeals for the Federal Circuit, which has

---

[1] This memorandum provides only an analysis of remedies under federal law, and does not include a discussion of state law or regulatory provisions. Although application of state law is possible, it is unlikely to apply in a case brought by a foreign national for the alleged violations of data privacy analyzed by this memorandum. The doctrine of federal preemption originates from the Supremacy Clause of the United States Constitution. This doctrine provides that when state law conflicts with federal law, the state law is preempted and federal law applies. Additionally, the "dormant commerce clause" imposes an implicit limitation on the authority of states to enact laws affecting interstate commerce. 8 Witkin, Summary 10th (2005) Const. Law, § 1300, p. 1000.

[2] In the preparation of this memorandum, regard has been had to the assumed facts adopted by the Court of Justice of the European Union for the purpose of its analysis in its judgment in *Schrems v. Data Protection Commission*, Case No. C-362/14, 6 October 2015. This memorandum does not, however, review the facts of the *Schrems* case or make any factual finding or legal conclusion with respect to the *Schrems* case.

nationwide jurisdiction over certain areas of the law, and also hears cases decided by certain specialized United States Courts. The 12 regional Circuit Courts are not bound to follow the decisions of the other Circuit Courts, and district courts from one Circuit are similarly not bound to follow the decisions of courts not in their Circuit. Where the memorandum refers to splits among courts, it is a situation where 2 or more of the Circuit Courts, or district courts in different Circuits, have reached different conclusions and the Supreme Court has not yet resolved the conflict.[3]

II. REMEDIES AVAILABLE TO EU CITIZENS UNDER U.S. LAW

A. Foreign Intelligence Surveillance Act ("FISA")[4]

The Foreign Intelligence Surveillance Act authorizes warrantless electronic surveillance where a "significant purpose" of the surveillance is the gathering of foreign intelligence.[5] Remedies under FISA are generally available to both U.S. citizens and foreign nationals under multiple statutory sections.[6]

1. 18 U.S.C. § 2712

Section 2712(a) permits a person who is aggrieved by a "willful"[7] violation of certain portions of FISA, including the following, to bring a claim for money damages:

- Section 106(a) [50 U.S.C. § 1806(a)], which prohibits the use or disclosure by federal officers or employees except for lawful purposes of information acquired from an electronic surveillance within the United States for foreign intelligence purposes;
- 305(a) [50 U.S.C. §1825], which prohibits the use or disclosure by federal officers or employees except for lawful purposes of information acquired from physical searches within the United States for foreign intelligence purposes; and
- 405(a) [50 U.S.C. §1845], which prohibits the use or disclosure by federal officers or employees except for lawful purposes of information acquired from pen registers and trap and trace devices installed and used for foreign intelligence purposes.

---

[3] For a general overview of these issues, please see http://www.uscourts.gov/about-federal-courts/court-role-and-structure, last visited April 20, 2016.

[4] For a more detailed discussion of FISA, see Andrew B. Serwin, Information Security and Privacy, A Guide to Federal and State Law and Compliance §§ 10:1-10:178 (2015 ed.).

[5] *United States v. Wen*, 477 F.3d 896, 897 (7th Cir. 2007).

[6] *See* 50 U.S.C. § 1801 (defining, for purposes of FISA, that "Person" means "any individual, including any officer or employee of the Federal government, or any group, entity, association, corporation, or foreign power." *See also Suzlon Energy Ltd. v. Microsoft Corp.*, 671 F.3d 726 (9th Cir. 2011) (finding that the ECPA extends its protections to non-citizen).

[7] Because there is no statutory definition of "willful" for this provision, one court has applied the common-law definition that "willfulness" covers both knowing and reckless violations of a standard. *Fikre v. FBI*, 2015 WL 6756121, at *14 (D. Or. Nov. 4, 2015) (citing *Safeco Ins. Co. of America v. Burr*, 551 U.S. 47, 57 (2007)). Notably, the *Fikre* court rejected the argument that the "willfulness" element of Section 2712(a) requires showing that the government agents engaged in conduct with the conscious objective of committing a violation.

The Court may award as damages: (1) actual damages, but not less than $10,000, whichever amount is greater; and (2) litigation costs, reasonably incurred. In addition to damages, administrative discipline is available under Section 2712(e).

The requirement for a "willful" violation serves as a limitation to anyone, including an EU citizen, in bringing a suit under this provision.

Sections 106(a) and 305(a) also provide that information acquired under FISA concerning any United States person may be used and disclosed only in accordance with certain minimization procedures.[8] Section 405(a) also provides further provisions that must be complied with for use and disclosure of information acquired from pen registers or trap and trace devices concerning United States persons.[9] Because the minimization procedures or further provisions apply only to United States persons—defined as U.S. citizens and lawful residents or U.S. corporations—EU citizens who are not U.S. citizens or residents would not be able to bring a claim under Section 2712 for non-compliance with these minimization procedures or further provisions.

2. 50 U.S.C. § 1810

Under Section 1810, an affected person (other than a foreign power or an agent of a foreign power) who has been subjected to an electronic surveillance, or about whom information obtained by electronic surveillance of such person has been disclosed or used, in violation of the provisions of this law, can recover (1) actual damages, but not less than liquidated damages of $1,000 or $100 per day for each day of the violation, whichever is greater; (2) reasonable attorneys' fees and other costs; and (3) punitive damages. The Ninth Circuit, however, has held that Section 1810 does not operate as a waiver of sovereign immunity, which means that the United States cannot be held liable under this section.[10]

---

[8] For example, minimization procedures for electronic surveillance are defined in Section 101(h) [50 U.S.C. § 1801(h)], as: (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 subsection (e)(1) of this section, 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; (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; and (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person. Similar minimization procedures apply to physical searches. *See* 50 U.S.C. § 1821(4).

[9] *See* 50 U.S.C. § 1845.

[10] *Al-Haramain Islamic Found., Inc. v. Obama*, 705 F.3d 845, 855 (9th Cir. 2012) (contrasting liability under Section 1810 with liability under Section 1806, for which sovereign immunity is explicitly waived).

3. 50 U.S.C. § 1806

In addition to claims brought for willful violations of this provision under Section 2712, Section 1806 also provides an exclusionary remedy for a person against whom evidence gained by electronic surveillance is being introduced. The person against whom the evidence is being introduced has the right to bring a motion to suppress the evidence gained by electronic surveillance if it is shown that the information was unlawfully obtained, or that the surveillance was not made in conformity with an order of authorization or approval.

B. Privacy Act

The Privacy Act allows U.S. citizens to access their records or information pertaining to those individuals held by governmental agencies, and to review those records and have a copy made.[11] Heads of agencies may promulgate rules to exempt certain systems of records. The Privacy Act provides that the head of any agency may promulgate rules to exempt any system of records within the agency if the system of records is subject to the exemption found in section 552(b)(1) of the Freedom of Information Act.[12] This provision of FOIA exempts matters that are properly classified pursuant to an Executive Order to be kept secret in the interest of national defense or foreign policy.[13] The head of any agency may also promulgate rules to exempt a system of records if it is maintained by the Central Intelligence Agency or an agency engaged in investigatory efforts pertaining to the enforcement of criminal laws.[14] These are not blanket exemptions, and the agency must take the affirmative action of promulgating rules before an exemption applies to a system of records. There is one further exemption for information compiled in reasonable anticipation of a civil action or proceeding, which does not require an implementing regulation.[15]

As noted, there is no blanket exemption for records collected by a particular agency such as the NSA. Certain regulations do, however, set forth the exemptions that the National Security Agency ("NSA") may claim under the Privacy Act, and list specific systems of records that have been exempted.[16] In particular, these regulations confirm that disclosure of records pertaining to the functions and activities of the NSA is prohibited.[17] Furthermore, all systems of records maintained by the NSA are exempt from disclosure to the extent that the system contains information properly classified under an Executive Order and that is

---

[11] 5 U.S.C. § 552a. For a more detailed discussion of the Privacy Act, see Serwin, supra note 4, §§ 27:10 et seq.
[12] 5 U.S.C. § 552a(k)(1).
[13] 5 U.S.C. § 552(b)(1).
[14] 5 U.S.C. § 552a(j).
[15] 5 U.S.C. § 552a(d)(5). Courts have extended this exemption to documents prepared in anticipation of quasi-judicial administrative hearings and to investigatory documents, even if no proceedings are in fact initiated. *See Mobley v. C.I.A.*, 924 F. Supp. 2d 24, 60 (D.D.C. 2013), *aff'd*, 806 F.3d 568 (D.C. Cir. 2015). For more information regarding exemptions of the Privacy Act, see https://www.justice.gov/opcl/ten-exemptions, last visited April 25, 2016.
[16] 32 C.F.R. §§ 322.6, 322.7.
[17] 32 C.F.R. § 322.6(g).

"required by Executive Order to be kept secret in the interest of national defense or foreign policy."[18]

The Privacy Act also limits the extent to which federal agencies can share and disclose information about individuals.[19] Certain exceptions apply. For example, federal agencies may disclose information about individuals when the disclosure is for a "routine use," is for law enforcement investigations, or is required under FOIA.[20]

An individual may bring a civil lawsuit against a governmental agency pursuant to the Privacy Act in certain situations. For instance, an individual may bring suit if a governmental agency refuses to comply with an individual request for records or fails to comply with any other provision of the Privacy Act, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual.[21] A court may enjoin the governmental agency from withholding records and order the production to the complainant of any agency records improperly withheld from him or her.[22]

The U.S. Supreme Court recently held that financial harm, as opposed to non-economic harm, is required to state a claim for compensatory damages under the Privacy Act.[23] There is an open issue as to whether an agency can exempt its system of records from the civil remedies provision of the Privacy Act.[24]

C. Judicial Redress Act

The Judicial Redress Act was signed by President Obama on February 24, 2016 and goes into effect 90 days after the date of enactment.[25] The Act has its origins in negotiations between the United States and the EU on a Data Protection and Privacy Agreement (often referred to as the "umbrella agreement"). Those negotiations (which commenced in 2011) seek the continuation of robust information sharing between the United States and EU for law enforcement purposes.[26]

The Act provides EU citizens with the ability to bring suit in federal district court for certain Privacy Act violations by the U.S. federal government relating to the sharing of law

---

[18] 32 C.F.R. § 322.7(a). This regulation specifies information classified under Executive Order 12958, which has now been revoked and replaced by Executive Order 13526.
[19] 5 U.S.C. § 552a.
[20] *Id.*
[21] 5 U.S.C. § 552a(g).
[22] *Id.*
[23] *Fed. Aviation Admin. v. Cooper*, 132 S. Ct. 1441 (2012).
[24] Some courts have found that an agency cannot exempt itself from the civil liability provisions of the Privacy Act if the underlying substantive duty is non-exemptible (e.g., improper disclosure), while others have allowed an agency to escape liability by exempting its records. *See, e.g., Shearson v. U.S. Dept. of Homeland Sec.*, 639 F.3d 498 (6th Cir. 2011); *Doe v. F.B.I.*, 936 F.2d 1346 (D.C. Cir. 1991); *Tijerina v. Walters*, 821 F.2d 789, 795 (D.C. Cir. 1987); *Ryan v. DOJ*, 595 F.2d 954 (5th Cir. 1979); *Kimberlin v. DOJ*, 788 F.2d 434 (7th Cir. 1986); *Saleh v. United States*, No. 09-cv-02563, 2011 WL 2682803, at *6 (D. Colo. Mar. 8, 2011) (magistrate's recommendation), *adopted in pertinent part*, 2011 WL 2682728, at *1 (D. Colo. July 8, 2011) .
[25] Pub. L. No. 114-126.
[26] H.R. Rep. No. 114-294, at 2-3 (2015).

enforcement information.[27] In practical terms, it extends certain remedies afforded to U.S. citizens and lawful residents under the Privacy Act to citizens of countries designated as "covered" countries.[28] It provides that, with respect to covered records,[29] a citizen of a covered country may bring a civil action against a federal agency and obtain civil remedies, in the same manner, to the same extent, and subject to the same limitations, as a U.S. citizen or permanent legal resident may under the following provisions of the Privacy Act:

- 5 U.S.C. § 552a(g)(1)(D), "but only with respect to disclosures intentionally or willfully made in violation of" 5 U.S.C. § 552a(b).[30] Thus, a plaintiff may bring a civil action under the Judicial Redress Act when an agency intentionally or willfully discloses a record in violation of any provision of the Privacy Act that is *not* listed in subsections (g)(1)(A)-(C), and the disclosure has "an adverse effect" on the individual.[31] A plaintiff in a suit brought under this provision may recover actual damages (though "in no case shall a person entitled to recovery receive less than the sum of $1,000"), as well as costs and attorneys' fees.[32]

- 5 U.S.C. § 552a(g)(1)(A) and (B). Subsection (A) authorizes a civil action when an agency "makes a determination under [5 U.S.C. § 552a(d)(3)] not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection."[33] Subsection (B) authorizes a civil action when an agency "refuses to comply with an individual request under [5 U.S.C. § 552a(d)(1)]," which enables an individual to gain access to his own records or any information pertaining to him contained in the agency's system.[34] An action under either of these subsections may only be brought against a designated Federal agency or

---

[27] *See id.*

[28] Pub. L. No. 114-126. A "covered country" is any foreign country, regional economic integration organization, or member country of such organization, that is so designated by the Attorney General with the concurrence of the Secretaries of State, the Treasury, and Homeland Security. The country/organization/member country must also meet the following criteria: (a) it has entered into an agreement with the United States that provides for privacy protections for information shared to prevent, investigate, detect, or prosecute criminal offenses, or the Attorney General has determined that it has shared such information and has appropriate privacy protections in place; (b) it allows personal data to be transferred between itself and the United States; and (c) the Attorney General has certified that its policies for such transfers and related actions do not materially impede U.S. national security interests. *Id.* The "covered country" designation may be removed by the Attorney General with the concurrence of the Secretaries of State, the Treasury, and Homeland Security if the Attorney General determines that the country or organization: (a) is not complying with the agreement it entered with the United States in order to be designated a covered country; (b) no longer meets the criteria to be designated a "covered country"; or (c) impedes the transfer of information (for purposes of reporting or preventing unlawful activity) to the United States by a private entity or person. *Id.*

[29] A "covered record" is the same as a "record" under the Privacy Act, once the covered record is transferred "by a public authority of, or private entity within," a covered country, "to a designated Federal agency or component for purposes of preventing, investigating, detecting, or prosecuting criminal offenses". *Id.*

[30] *Id.*

[31] 5 U.S.C. § 552a(g).

[32] *Id.*

[33] *Id.*

[34] *Id.*

component.[35] Plaintiffs in suits brought under these provisions may receive injunctive relief (i.e., an order to amend or produce his records), as well as costs and attorneys' fees where the plaintiff has "substantially prevailed," but not damages.[36]

Notably, the Judicial Redress Act does *not* authorize a civil action for violation of 5 U.S.C. section 552a(d)(1)(C), which provides for a civil action under the Privacy Act where an agency "fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual."

Because the Judicial Redress Act operates by extending the range of persons who may access remedies under the Privacy Act, the starting point is that existing limitations that apply to such remedies as are available under the Privacy Act will also apply to the Judicial Redress Act. So far as the exemption of systems of records relating to national security are concerned, existing limitations under the Privacy Act are an important touchpoint to consider in any assessment of the manner in which the Judicial Redress Act will operate in practice. However, it cannot be assumed that the way in which such limitations are applied under the Privacy Act will provide an accurate guide as to how they will be applied under the Judicial Redress Act. Because the Judicial Redress Act was very recently enacted, questions as to the precise manner in which the exemptions provided for in the Privacy Act will apply under the Judicial Redress Act have not yet been resolved.[37]

There are potential ambiguities relating to certain of the definitions deployed in the Judicial Redress Act that could also be read to limit the remedies afforded non-U.S. citizens by its terms. The definition of the terms "designated Federal agency or component," "covered record" and "covered country" require consideration in this context.

The term "designated Federal agency or component" means a Federal agency or component of an agency designated in accordance with subsection (e) of this Act. An agency/component may be designated under subsection (e) if the Attorney General determines that: (a) information exchanged by the agency with a covered country is within the scope of an agreement with the United States that provides for privacy protections for information shared to prevent, investigate, detect, or prosecute criminal offenses; or (b) with respect to a covered country, designating the agency/component is in the law enforcement interests of the United States.[38] Section (e) also provides that, with a limited exception, no

---

[35] The term "designated Federal agency or component" means a Federal agency or component of an agency designated in accordance with subsection (e) of this Act. An agency/component may be designated under subsection (e) if the Attorney General determines that: (a) information exchanged by the agency with a covered country is within the scope of an agreement with the United States that provides for privacy protections for information shared to prevent, investigate, detect, or prosecute criminal offenses; or (b) with respect to a covered country, designating the agency/component is in the law enforcement interests of the United States.

[36] 5 U.S.C. § 552a(g).

[37] *See supra* Part II.B.

[38] Pub. L. No. 114-126.

agency or component thereof shall be designated "without the concurrence of the head of the relevant agency, or of the agency to which the component belongs." In principle, therefore, it would be open to an agency to opt-out of the Act. This could greatly narrow the Act's intended scope depending on the agency. Because the Act was very recently enacted, it is not yet clear whether particular agencies, such as the NSA, will be designated in the manner and for the purposes described.

A country or regional economic integration organization must meet certain requirements to be designated a "covered country," including entering into an agreement with the United States regarding privacy protections for shared information. A reading of this definition on its face implies that the United States itself would not be considered a "covered country."

The Act provides that the term "covered record" has the same meaning as the term "record" in the Privacy Act, once the record is transferred "by a public authority of, or private entity within," a covered country, "to a designated Federal agency or component for purposes of preventing, investigating, detecting, or prosecuting criminal offenses."[39] This definition is potentially ambiguous in two respects.

First, it is not clear if a record originating in a foreign covered country (or a private entity therein) that was provided to the designated agency or component indirectly (for example, by or through a related private entity established in the U.S.) could still be considered a "covered record."

Second, interpretation of the term "covered country" affects the designation of a record as a "covered record". As noted above, a strict reading of the definition of the term "covered country" would indicate that the United States itself would not be considered a "covered country."

Because the Judicial Redress Act implicates sovereign immunity, a court may strictly construe the statutory language to find that a record that was transferred to a designated U.S. Federal agency or component, not directly by an authority or private entity within a foreign covered country, but *indirectly* by or through a related private entity established within the United States, would thus not qualify as a "covered record."[40]

Clearly, a narrow reading of the terms "covered country" and "covered record" would greatly limit the accessibility of remedies under the Judicial Redress Act. Until such time as such matters have been addressed by a court of competent jurisdiction, however, it remains unclear whether such an approach would in fact be adopted or whether, in the alternative, a court would interpret the statutory language in light of the purpose of the Act and find, for example, that a record that originated in a foreign covered country but was provided to the designated agency or component *indirectly* could still be considered a "covered record." No court has addressed these issues to date. While the approach of courts when examining other statutes that implicate sovereign immunity may not accurately predict how the Judicial

[39] Pub. L. No. 114-126.

[40] *See Dep't of Army v. Blue Fox, Inc.*, 525 U.S. 255, 261 (1999) ("We have frequently held, however, that a waiver of sovereign immunity is to be strictly construed, in terms of its scope, in favor of the sovereign.").

Redress Act will be interpreted, the decision of the U.S. Supreme Court in *Department of Army v. Blue Fox, Inc.*, is nonetheless considered to be of some significance in this context.

The Judicial Redress Act provides that the District Court for the District of Columbia shall have exclusive jurisdiction over any claim arising under this section.[41]

There is a particular issue to be considered regarding standing and the Judicial Redress Act that is discussed below.

D. Electronic Communications Privacy Act (ECPA)[42]

The Electronic Communications Privacy Act is a law that governs when electronic communications and wire communications can be intercepted or monitored. It consists of the Wiretap Act[43] and the Stored Communications Act (SCA)[44]. The Wiretap Act applies only to conduct that occurs during transmission. This is in contrast to conduct that violates the SCA, which relates to the improper acquisition of the contents of stored communications—i.e., after their transmission. Thus, the difference between the two titles is a temporal one. The Wiretap Act applies only to the interception or accessing of information while in transmission, while the SCA applies to the unauthorized access of stored communications.[45]

Under the Wiretap Act, it is a crime for persons to intentionally intercept or procure electronic communications, including email, unless certain exceptions apply.[46] It is also a violation of the Wiretap Act to disclose communications if the person making the disclosure knew or had reason to know that the communication was intercepted in violation of the ECPA.[47]

Under the SCA, it is illegal to "obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage in such system" if a person "intentionally accesses without authorization a facility through which an electronic

---

[41] Pub. L. No. 114-126.
[42] For a more detailed discussion of the ECPA, see Serwin, supra note 4, §§ 7:1-7:122.
[43] 18 U.S.C. § 2510 et seq.
[44] SCA, 18 U.S.C. § 2701 et seq.
[45] Remedies under the ECPA are generally available to both U.S. citizens and foreign nationals. *See* 18 U.S.C. § 2510 (defining, for purposes of the Wiretap Act, that "person" means "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation."); *see also Suzlon Energy Ltd. v. Microsoft Corp.*, 671 F.3d 726 (9th Cir. 2011) (finding that the ECPA extends its protections to non-citizens).
[46] 18 U.S.C. § 2511(1)(a). The term intentional under the ECPA is narrower than the dictionary definition of "intentional." In certain cases employees continuing to access emails on a network, unless some barrier is put up or other notice is given, is not actionable under the SCA because of a lack of intent. *Lasco Foods, Inc. v. Hall and Shaw Sales, Mktg. & Consulting, LLC*, 600 F. Supp. 2d 1045 (E.D. Mo. 2009) (holding that because employee still was permitted access to the network misuse of trade secret information was not actionable under the SCA), citing *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F. Supp. 2d 817 (E.D. Mich. 2000).
[47] 18 U.S.C. § 2511(1)(c).

communication service is provided" or "intentionally exceeds an authorization to access that facility."[48]

Under 18 U.S.C. Section 2712, any person who is aggrieved by any willful violation of the Wiretap Act or the SCA may commence an action in U.S. District Court against the United States to recover money damages. The Court may assess as damages (1) actual damages, but not less than $10,000, whichever amount is greater; and (2) litigation costs, reasonably incurred. Before an action against the United States is commenced, the plaintiff must present the claim to the appropriate department or agency under the Federal Tort Claims Act.[49] Actions against the United States are barred unless the plaintiff presents it in writing to the appropriate Federal agency within two years after the claim accrues, or the action is begun within six months of the final denial of the claim by the agency.[50] In addition to damages, administrative discipline is available under Section 2712(e).[51] For Section 2712 claims under the ECPA, wrongful collection (and not just use and disclosure) is actionable.[52]

There is an uncertainty in the statutory language as to whether government entities can be held liable for violations of the Wiretap Act because the definition of a "person" under the Act does not include governmental entities.[53] There is also a split among the courts as to whether damages are permitted against governmental entities that violate the Act. While certain courts have held that government entities are liable for violations of the SCA,[54] others have held that government entities are not liable under the ECPA, though government officials can be.[55] Relying upon the provisions of Section 2707(a) as an interpretive guide, one court recently concluded that government entities are liable for wiretap violations.[56]

E. Freedom of Information Act ("FOIA")

The Freedom of Information Act gives individuals the right to access information from the federal government.[57] These disclosure obligations on the federal government are broad, but they are subject to several exemptions.[58] For example, classified national defense information shared via a classified channel is typically exempt from disclosure under FOIA.[59] FOIA also exempts records that are specifically exempted from disclosure by statute, if such statute either "requires that the matters be withheld from the public in such a

---

[48] 18 U.S.C. § 2701(a).
[49] 18 U.S.C. § 2712(b)(1).
[50] 18 U.S.C. § 2712(b)(2).
[51] Administrative discipline, but not damages, is also available under 18 U.S.C. § 2520 and 18 U.S.C. § 2707.
[52] *See Jewel v. Nat'l Sec. Agency*, 965 F. Supp. 2d 1090, 1107 (N.D. Cal. 2013) ("the plain language of Section 2712(a) does not limit the waiver of sovereign immunity for damage claims under the SCA and the Wiretap Act to claims for the use and disclosure of information").
[53] *Amati v. City of Woodstock, Ill.*, 829 F. Supp. 998, 1002-03 (N.D. Ill. 1993); *Abbott v. Village of Winthrop Harbor*, 205 F.3d 976, 980, (7th Cir. 2000); *cf. Conner v. Tate*, 130 F. Supp. 2d 1370 (N.D. Ga. 2001).
[54] *Adams v. City of Battle Creek*, 250 F.3d 980, 985 (6th Cir. 2001).
[55] *PBA Local No. 38 v. Woodbridge Police Dept.*, 832 F. Supp. 808 (D.N.J. 1993); *Amati*, 829 F. Supp. 998.
[56] *Walden v. City of Providence*, 495 F. Supp. 2d 245 (D.R.I. 2007).
[57] 5 U.S.C. § 552(a). Generally any person–United States citizen or not–can make a FOIA request. http://www.foia.gov/faq.html, last visited April 28, 2016.
[58] 5 U.S.C. § 552(b).
[59] 5 U.S.C. § 552(b)(1).

manner as to leave no discretion on the issue" or "establishes particular criteria for withholding or refers to particular types of matters to be withheld."[60] Additionally, FOIA exempts records compiled for law enforcement purposes, including for purposes of an active law enforcement investigation.[61]

F. Computer Fraud and Abuse Act ("CFAA")[62]

The Computer Fraud and Abuse Act is a law that started as an anti-hacking law, but its application has expanded, and it protects more than U.S. departments and financial institutions. The CFAA makes it a crime for anyone to intentionally access a computer without authority or exceeding authority that has been granted, regardless of whether the computer is owned by the government, if the conduct involved an interstate or foreign communication.[63] The CFAA also makes it a crime to knowingly, and with the intent to defraud, access a protected computer without authorization or beyond the scope of authorization, if the person furthers a fraud and an item of any value is obtained (as long as the value is over $5,000 in any one year period).[64] Courts have held that confidential data can constitute a thing of value under the CFAA.[65] Furthermore, it is unlawful under the CFAA for a person to (1) knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause damage to a protected computer; (2) intentionally access a protected computer without authorization, and as a result of such conduct, recklessly cause damage; or (3) intentionally access a protected computer without authorization, and as a result of such conduct, cause damage and loss.[66]

The CFAA provides for criminal penalties as well as private causes of action, although some courts have held that federal government agencies and officials are immune from suits involving this statute.[67] Under the CFAA, any person who suffers "damage or loss" due to a violation of the statute may bring a civil action to obtain compensatory damages and

---

[60] 5 U.S.C. § 552(b)(3).

[61] 5 U.S.C. § 552(b)(7).

[62] For a more detailed discussion of the Computer Fraud and Abuse Act, see Serwin, *supra* note 4, §§ 5:1-5:5:50.

[63] 18 U.S.C. § 1030(a)(2).

[64] 18 U.S.C. § 1030(a)(4). The term "protected computer" means a computer "(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States . . . ." 18 U.S.C. § 1030(e)(2).

[65] *United States v. Ivanov*, 175 F. Supp. 2d 367 (D. Conn. 2001); *see also Carpenter v. United States*, 484 U.S. 19 (1987).

[66] 18 U.S.C. § 1030(a)(5).

[67] *Garland-Sash v. Lewis*, 2007 WL 935013 (S.D.N.Y. Mar. 26, 2007), *aff'd in part, vacated in part*, 348 F. App'x 639 (2d Cir. 2009). Remedies under CFAA are likely equally available to U.S. citizens and foreign nationals. *See* 18 U.S.C. § 1030(e)(12) (defining "person" as "any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity"); 18 U.S.C. § 1030(e)(9) (defining "government entity" as including "the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country").

injunctive relief.[68] Injunctions, including temporary restraining orders, are often the most immediate and effective relief. Courts are split as to whether plaintiffs must allege both damage and loss to state a claim under the CFAA.[69] However, some courts have concluded that a plaintiff can satisfy the CFAA's definition of "loss" by alleging costs reasonably incurred in responding to an alleged CFAA offense, even if the alleged offense ultimately is found to have caused no damage as defined by the CFAA.[70]

G. Right to Financial Privacy Act ("RFPA")

The Right to Financial Privacy Act protects the confidentiality of personal financial records.[71] Except as otherwise provided by federal law, "no Government authority may have access to or obtain copies of, or the information contained in the financial records of any customer from a financial institution unless the financial records are reasonably described" and (1) the customer has authorized such disclosure; (2) such financial records are disclosed in response to an administrative subpoena or summons; (3) such financial records are disclosed in response to a search warrant; (4) such financial records are disclosed in response to a judicial subpoena; or (5) such financial records are disclosed in response to a formal written request that meets certain requirements.[72]

A financial institution cannot release any of this financial information until the governmental authority seeking the records certifies in writing to the financial institution that it has complied with the RFPA.[73] A customer may object to his or her financial information being provided to the governmental authority seeking access.[74] If, after the government files its

---

[68] 18 U.S.C. § 1030(g). The term "loss" is defined as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). The term "damage" is defined as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8).

[69] *Compare Garelli Wong & Assoc., Inc. v. Nichols*, 551 F. Supp. 2d 704, 708-710 (N.D. Ill. 2008), *with Motorola, Inc. v. Lemko Corp.*, 609 F. Supp. 2d 760, 766-67 (N.D. Ill. 2009).

[70] *See, e.g., Navistar, Inc. v. New Baltimore Garage, Inc.*, No. 11–cv–6269, 2012 WL 4338816, at *8 (N.D. Ill. Sept. 20, 2012) ("[A]t a minimum, Plaintiffs have stated a CFAA claim by alleging that they incurred costs in investigating an alleged CFAA offense."); *1st Rate Mortg. Corp. v. Vision Mortg. Servs. Corp.*, No. 09–C–471, 2011 WL 666088, at *2 (E.D. Wis. Feb. 15, 2011) ("[T]he CFAA allows recovery for losses sustained even if data or computers were not damaged"); *Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands Int'l Inc.*, 616 F. Supp. 2d 805, 811 (N.D. Ill. 2009) ("The CFAA states that a company that pays for damage assessment may satisfy the loss requirement."); *Motorola*, 609 F. Supp. 2d at 768 (stating that allegations of loss "related to damage and security assessments… are sufficient to allege loss for purposes of the CFAA").

[71] 12 U.S.C. §§ 3401 et seq. For a more detailed discussion of the Right to Financial Privacy Act, see Serwin, supra note 4, §§ 16:65-16:70.

[72] 12 U.S.C. § 3402.

[73] 12 U.S.C. § 3403(b). However, there are several exceptions pursuant to which financial institutions may disclose financial information or records to governmental authorities. *See, e.g.*, 12 U.S.C. §§ 3403, 3413. For example, the RFPA does not preclude a financial institution from disclosing to the government that it has information that may be relevant to a possible violation of any statute or regulation. 12 U.S.C. § 3403(c).

[74] *See* 12 U.S.C. § 3410. Remedies under RFPA are likely equally available to U.S. citizens and foreign nationals. *See* 12 U.S.C. § 3401 (defining "customer" as "any person or authorized representative of that

response, the court is unable to make a decision based on the parties' initial allegations and response, "the court may conduct such additional proceedings as it deems appropriate."[75] A governmental authority that has obtained financial records pursuant to the RFPA may not transfer those records to another department or agency unless the transferring authority certifies in writing that there is reason to believe that the records are relevant to a legitimate law enforcement inquiry, or intelligence or counterintelligence activity, investigation, or analysis related to international terrorism.[76]

III. STANDING[77]

Under Article III of the U.S. Constitution, a plaintiff must have standing to bring suit before a federal court as a precondition to bringing a claim. The party invoking federal jurisdiction bears the burden of establishing the following three elements:

- (1) That it has suffered an injury in fact—an invasion of a legally protected interest which is (a) concrete and particularized; and (b) actual or imminent, not conjectural or hypothetical;
- (2) That there is a causal connection between the injury and the conduct complained of—the injury has to be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court; and
- (3) That it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.[78]

A. *Clapper v. Amnesty International, USA*

In *Clapper v. Amnesty Intern. USA*, the U.S. Supreme Court examined the issue of Article III standing in a matter arising from allegations that certain amendments to FISA were unconstitutional.[79] The plaintiffs argued that they had standing because they believed that there was an objectively reasonable likelihood that their communications with foreign contacts would be intercepted in the future, or, alternatively, because they were presently suffering injury from taking costly and burdensome measures to protect the confidentiality of their international communications.[80] The Court held that the plaintiffs lacked standing

---

person who utilized or is utilizing any service of a financial institution, or for whom a financial institution is acting or has acted as a fiduciary, in relation to an account maintained in the person's name").

[75] 12 U.S.C. § 3410(b).

[76] 12 U.S.C. § 3412(a). The transferring authority must comply with certain notice requirements. *See* 12 U.S.C. § 3412. However, these notice requirements do not apply when a governmental authority seeks only the name, address, account number, and type of account of any customer associated with a financial transaction; or with a foreign country or subdivision thereof in the case of a government authority exercising financial controls over foreign accounts with the United States under Section 5(b) of the Trading With the Enemy Act. 12 U.S.C. § 3413(g).

[77] For a more detailed discussion, see Serwin, supra note 4, § 34:27.

[78] *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992).

[79] 133 S. Ct. 1138 (2013).

[80] *Id.* at 1143.

because "they could not demonstrate that the future injury they purportedly fear is certainly impending and because they cannot manufacture standing by incurring costs in anticipation of non-imminent harm.[81]

The Court held that the plaintiffs could not prove injury in fact.[82] The plaintiffs' argument rested on their "highly speculative fear" that: the Government would target their communications, the Government would choose the specifically challenged method of surveillance, the FISA court would authorize the surveillance, and the Government would succeed in intercepting their communications.[83] This "highly attenuated chain of possibilities" did not satisfy the requirement that "threatened injury must be certainly pending."[84] Furthermore, plaintiffs could not establish that the injury in fact would be "fairly traceable" to the challenged action, because they could only speculate regarding the authority for the asserted interception.[85]

Clapper also implicates a related but separate requirement for bringing a lawsuit in the United States. Federal Rule of Civil Procedure 11 requires the attorney presenting a pleading to the court to certify that "the factual contentions have evidentiary support or, if specifically so identified, will likely have evidentiary support after a reasonable opportunity for further investigation or discovery . . ."[86] The Court in *Clapper* held that the plaintiffs did not have standing due to the speculative nature of their claim. This analysis would seemingly apply to a Rule 11 analysis, as speculative claims that are unlikely to have available evidentiary support would not satisfy the Rule 11 requirement.[87] The Rule 11 and standing requirements are barriers that both U.S. and EU citizens would face in bringing a lawsuit.

B. *Spokeo, Inc. v. Robins*

In the recent U.S. Supreme Court case *Spokeo, Inc. v. Robins*, the Court analyzed whether allegations of a statutory violation are sufficient to satisfy the standing requirement under Article III.[88] The Court ruled that a plaintiff cannot establish standing based on the violation of a statutory right without adequately alleging that the violation caused some concrete harm.[89] However, the Court also stated that "[t]he violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury-in-fact."[90] Although a "bare procedural violation" does not satisfy Article III standing, a "risk of real harm" may

---

[81] *Id.*
[82] *Id.* at 1148.
[83] *Id.*
[84] *Id.*
[85] *Id.* at 1149.
[86] Fed. R. Civ. P. 11(b)(3).
[87] *See also Cooter & Gell v. Hartmarx Corp.*, 496 U.S. 384, 393 (1990) ("[T]he central purpose of Rule 11 is to deter baseless filings in district court . . . .").
[88] *Spokeo, Inc. v. Robins*, No. 13-1339, slip op. (U.S. May 16, 2016). This case involved an alleged violation of the Fair Credit Reporting Act.
[89] *See id.* at 9.
[90] *Id.* at 10.

sometimes satisfy the concrete injury requirement.[91] Thus, a fact-specific inquiry into the harm caused by a statutory violation is still required after this opinion.

C. Standing in the Lower Courts

Lower courts vary in their interpretation of standing in the data privacy context. The Ninth Circuit has found that individuals who had their personal information stolen, but not misused, suffered a sufficient injury to confer standing under Article III.[92] The Ninth Circuit's interpretation of Article III standing is broader than many other courts that have found that cases arising out of alleged data breaches fail for a lack of standing, unless there is a showing of misuse of data.[93] The Seventh Circuit has held that at least at the motion to dismiss stage, a plaintiff could establish standing, based upon allegations that the court felt created an "objectively reasonable likelihood" that injury would occur as a result of the breach.[94] On the other hand, the First Circuit has found that a plaintiff's failure to allege that his or her information was actually acquired by a third-party is fatal to the plaintiff's claims.[95]

The Ninth Circuit has also taken a broad view with respect to whether standing can be established through statutory rights, where the statutory cause of action does not require proof of actual damages. In *Jewel v. National Security Agency*, the plaintiffs' allegations of specific violations of ECPA and FISA, as well as the First and Fourteenth Amendments, coupled with the allegation that their communications were part of the alleged warrantless wiretapping, were sufficient for the Ninth Circuit to find standing under Article III, since Article III standing can exist in certain cases based upon the violation of a statutorily created right.[96] The Supreme Court's recent decision in *Spokeo* may alter the lower courts' analysis on this issue. [97] Based on this ruling, a plaintiff must allege that statutory violations caused a

---

[91] *Id.*

[92] *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), for additional opinion, *see* 406 Fed. Appx. 129 (9th Cir. 2010).

[93] *See, e.g.*, *Hammond v. The Bank of New York Mellon Corp.*, No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307 (S.D.N.Y. 2010) ("The Court concludes that Plaintiffs lack standing because their claims are future-oriented, hypothetical, and conjectural. There is no 'case or controversy'.") (citation omitted); *see also Bell v. Acxiom Corp.*, No. 4:06CV00485-WRW, 2006 WL 2850042 (E.D. Ark. 2006); *Smith v. Chase Manhattan Bank, USA, N.A.*, 293 A.D.2d 598, 741 N.Y.S.2d 100 (2002); *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046 (E.D. Mo. 2009); *Hinton v. Heartland Payment Sys., Inc.*, No. 09–594 (MLC), 2009 WL 704139 (D.N.J. 2009); *Giordano v. Wachovia Secs., LLC*, No. 06-476 (JBS), 2006 WL 2177036 (D.N.J. 2006) (holding that plaintiff lacked Article III standing because she could not show injury-in-fact that was actual or imminent as a result of the loss of PII).

[94] *Remijas v. Neiman Marcus Group, LLC*, 794 F. 3d 688 (7th Cir. 2015) (finding standing for class action arising from breach of payment card data at Neiman Marcus).

[95] *Katz v. Pershing, LLC*, 672 F.3d 64 (1st Cir. 2012).

[96] 673 F.3d 902 (9th Cir. 2011); *see also In re Google, Inc. Privacy Policy Litig.*, No. C-12-01382-PSG, 2013 WL 6248499 (N.D. Cal. Dec. 3, 2013) (noting that if plaintiffs had adequately alleged certain statutory violations—unauthorized access and wrongful disclosure of communications under the ECPA—that would be sufficient to establish standing).

[97] *See Spokeo*, No. 13-1339, slip op. (U.S. May 16, 2016). The District Court for the District of Columbia will be the likely forum of choice for EU citizens bringing claims, as this is the exclusive forum for any claims under the Judicial Redress Act. The D.C. Circuit has held that an individual has standing where Congress enacts statutes creating legal rights, the invasion of which creates standing. *Zivotofsky ex rel. Ari Z. v. Sec'y of*

concrete and particularized harm in order to satisfy the Article III standing requirement. However, a "risk of real harm" may be sufficient to establish standing in some circumstances, and it is yet to be seen whether lower courts will alter their analysis in light of this decision.[98]

D. The Judicial Redress Act

There is also an unlitigated issue regarding standing and the need to prove actual damages for claims brought under the Judicial Redress Act. Two Supreme Court cases on the Privacy Act shed light on this issue. In *Doe v. Chao*, the Court held that a party seeking to recover the minimum statutory award of $1,000 under the Privacy Act must still prove "actual damages" as a prerequisite.[99] In *Federal Aviation Administration v. Cooper*, the Court narrowed recovery even further by holding that, under the Privacy Act, pecuniary damages are a prerequisite to any attempt to recover civil damages, including statutory damages.[100] Because the Judicial Redress Act incorporates the remedial provisions that were addressed in *Cooper*, it is likely that any plaintiff proceeding under the Judicial Redress Act will also have to prove pecuniary damages before he or she can recover.

IV. CONCLUSION

If an EU citizen were to sue for a violation of data privacy in the context of national security, the most likely and effective causes of action are those analyzed in this memorandum, starting with FISA and the Judicial Redress Act. As noted, however, there are open questions regarding potential limitations in bringing suit under the Judicial Redress Act. For example, if a court strictly interpreted relevant statutory terms, or if it applied, without adjustment, existing Privacy Act exemptions designed to protect national security interests, then the remedies available under the Judicial Redress Act could become foreclosed in certain factual circumstances, contrary to an intent to extend those remedies to non-U.S. citizens.

Regardless of the cause of action asserted, the first hurdle that either a U.S. or EU citizen would face in bringing suit is Federal Rule of Civil Procedure 11, which essentially requires a good faith basis for the claims alleged in a pleading. Federal agencies have the ability to classify information. If an agency had gathered a plaintiff's personal information in the context of national security, that fact would likely be classified and difficult to prove to satisfy Rule 11. The challenges to satisfying the Rule 11 requirements thus appear to be greater for claims related to national security. However, we note that the purpose of the

---

State, 444 F.3d 614, 617-18 (D.C. Cir. 2006) (analogizing to statutory standing under FOIA). It is yet to be seen whether the D.C. Circuit will change its analysis in light of *Spokeo*.

[98] *Spokeo*, No. 13-1339, slip op. at 10. This ruling applies to all statutes, including ECPA. Prior to *Spokeo* there was a split in the case law as to whether a plaintiff must prove actual damages for claims of ECPA violations. *See In re Hawaiian Airlines, Inc.*, 355 B.R. 225 (D. Haw. 2006) (distinguishing *Doe v. Chao*, 540 U.S. 614 (2004)); *Van Alstyne v. Elec. Scriptorium, Ltd.*, 560 F.3d 199 (4th Cir. 2009) (concluding that proof of actual damages is required for statutory damages, but not for punitive damages or attorneys' fees).

[99] 540 U.S. 614 (2004).

[100] 132 S. Ct. 1441 (2012). The Court also found that "actual damages," in the context of this act, does not include mental or emotional distress alone. *Id.*

Judicial Redress Act is to afford remedies to non-U.S. citizens that were not available to them before. It remains to be seen how the Rule 11 requirements in conjunction with the Judicial Redress Act will be implemented in light of this purpose.

The next significant hurdle that a U.S. or EU litigant in U.S. federal court would face is establishing Article III standing, as summarized below:

- The plaintiff must show an actual or imminent injury that is caused by the challenged action. For allegations of future harm, a plaintiff must show that injury is "certainly pending." Speculative allegations that amount only to "possible future injury" do not suffice.[101]

- To bring a claim under the Judicial Redress Act, a plaintiff must prove pecuniary damages, assuming the Supreme Court cases on the Privacy Act apply to the JRA.

- For statutory causes of action that do not require proof of actual damages, plaintiffs still need to allege that the statutory violation caused plaintiffs a concrete harm.[102]

These challenges to bringing a lawsuit for a violation of data privacy in the context of national security are the same for both U.S. and EU citizens.

The remedies available under the causes of action discussed herein are also largely identical for U.S. and EU citizens, with two exceptions. First, because the minimization procedures of FISA apply only to U.S. citizens, EU citizens may not bring a claim for non-compliance with these minimization procedures. However, EU citizens may utilize the remaining remedies available under FISA. Second, an EU citizen may not bring a civil action under the Judicial Redress Act where an agency fails to adequately maintain any record concerning an individual "as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual."[103] These two differences in the remedies available to EU citizens are likely not material.

This memorandum provided an overview of the causes of actions and remedies that may be available to EU citizens for violations of data privacy, particularly for information gathered in the national security context. The causes of action most likely to be effective in a given case will necessarily depend on the factual circumstances. The Judicial Redress Act continues to evolve, and the conclusions of this memorandum regarding the Act and the Rule 11 requirements to bring claims under the Act may be impacted by future developments and implementations of the statute.

---

[101] *See Clapper v. Amnesty Intern. USA*, 133 S. Ct. 1138 (2013).
[102] *Spokeo, Inc. v. Robins*, No. 13-1339, slip op. (U.S. May 16, 2016)..
[103] 5 U.S.C. § 552a(d)(1)(C).