FINDING RELIEF FOR PRIVACY INFRINGEMENTS IN THE NEW WORLD

Mary Ellen Callahan[1]

AMERICAN FOUNDATIONS IN PRIVACY

The American commitment to privacy is built upon our Constitution, two centuries of common law, the seminal writing of Brandeis and Warren, government policy leaders who first articulated the Fair Information Practice Principles in 1973 and an extensive network of laws, regulations and policies. Consistent with this tradition, the U.S. is home to the largest international organization of privacy professionals[2] as well as the world's most active and well-organized privacy advocacy community.

Against this backdrop, it is no surprise that when the Department of Homeland Security (DHS or Department) was created in 2002, its establishing legislation included a specific statute to establish a Chief Privacy Officer (CPO) with a wide range of privacy powers.[3] This was the first statutorily mandated CPO with extensive authority to oversee privacy in a U.S. government agency. Soon after its creation, the Department made a policy commitment to protect all personal information regardless of the individual's citizenship status.[4] This commitment was implemented, in part, through the creation of various administrative redress programs within the Department. In 2007, Congress enhanced the authority of the DHS Privacy Office and created a new body to oversee privacy throughout those portions of the federal government that engage in counter-terrorism.[5] Today, American government privacy protections have evolved and grown to provide transparency and fairness for citizens and visitors alike.

Internationally, the U.S. and Europe have long honored one another's protections of shared values and freedoms. Despite different legal frameworks and government structures, the U.S. and Europe have practiced comity and mutual recognition to effectively work together on cross-border law enforcement and the enforcement of civil judgments from one side of the Atlantic to the other. Now, however, despite evidence to the contrary, some in the EU are calling into question whether the U.S. provides effective privacy protection for their citizens. This criticism is particularly acute in the context of security and law enforcement programs, where border protection systems impact European travelers. What is the source for this skepticism? Listening to our European critics, many of whom are independent data protection authorities, their doubts appear to be based largely on the lack of precise counterpart entities in the U.S.

UNDERSTANDING EU SOURCES OF DOUBT

Since the country's founding, Americans expect that the three independent branches of government created by the Constitution uphold the rights enumerated therein. It is difficult for

---

[1] Mary Ellen Callahan is the Chief Privacy Officer at the U.S. Department of Homeland Security. She wishes to thank Lauren Saadat and Shannon Ballard, Directors of International Privacy Policy at DHS, for contributions to this article.

[2] The International Association of Privacy Professionals (IAPP) headquartered in York, Maine, has over 6,000 members in the U.S. and around the world.

[3] Section 222 of the Homeland Security Act., 6 U.S.C. 552 (as amended)

[4] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf

[5] 9/11 Committee Recommendations Act of 2007 created additional authority for DHS's Privacy Office as well as a new body, the Privacy and Civil Liberties Oversight Board.

Americans to understand why independent oversight in the area of privacy is seen by the Europeans as a necessity; after all, other fundamental human rights enumerated in the European Convention on Human Rights[6] are not overseen by independent authorities, even within EU member states. Nor has the presence of an independent data protection authority been recognized as necessary by the three global conventions on privacy. Among the Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the Asia Pacific Economic Cooperation (APEC) Privacy Framework, and the United Nations (UN) Convention on Electronic Data Processing, none have prescribed a specific government structure for privacy oversight. The reason for the EU data protection community's insistence on an independent data protection authority is most likely tied to a legal concept central to democracies around the world: redress from wrongful action by the government.

The presumed reasoning of the EU's data protection community is that, without independence, "true application of the [data protection] principles would not arise."[7] In other words, the assumption is that anything less is the proverbial fox guarding the hen house, especially in the area of security and law enforcement programs. The linkage presumes that true restitution cannot occur outside of the independent data protection authority model, and, by virtue of having this government structure, redress is guaranteed under the EU framework. Those who subscribe to this logic should expect that European data protection authorities routinely grant individuals satisfaction for the errors and breaches that are bound to occur in large government systems that collect personal information and that miscreant public employees are punished, while under the U.S. system such redress would be impossible. However, a look at the U.S. system suggests quite a different conclusion.

To the exclusion of all other law, EU interlocutors have focused solely on the fact that the Privacy Act of 1974 only applies to U.S. persons (defined as U.S. citizens and legal permanent residents), and mistakenly assume that this prevents Europeans from obtaining redress from the U.S. government for mishandling or misusing personal information. This singular focus on the Privacy Act excludes other notable relief available. Part of the European skepticism may be rooted in a failure to understand the difference between their civil law and our common law systems. In fact, aggrieved non-U.S. persons have several options, some involving the courts and others involving administrative remedies, depending on the complaint. These options are not just theoretical, but are extensively used and publicized. Moreover, every year brings examples of U.S. federal employees who find out the hard way that misusing personal information brings severe consequences. The following hypotheticals – all with a nexus to DHS – can help illustrate the effectiveness of U.S. redress in the border security and law enforcement context.[8]

---

[6] The European Court of Human Rights sets forth the fundamental human rights identified by the Council of Europe and recognized by its members. Article 8 provides a right to respect for one's "private and family life, his home and his correspondence."

[7] Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data EXPLANATORY MEMORANDUM, Section 22, version 2.3, Feb. 26, 2009.

[8] While the hypotheticals discussed here use European travelers as examples, the redress issues discussed here apply universally to any individual regardless of country or region. Additionally, these examples only relate to DHS; other United States Government agencies will have similar examples.

REAL WORLD EXAMPLES TO THE CONTRARY

Hypothetical #1: A European traveler is repeatedly subject to additional questioning from U.S. officials upon entry to the U.S., but believes he has done nothing to incite suspicion. The traveler is aggrieved by this questioning, and decides to find out whether it is based on incorrect information.

The U.S. Freedom of Information Act (FOIA) allows persons, regardless of citizenship, to gain access to records held by government agencies. The European traveler may decide to file a FOIA request with DHS, the agency that oversees U.S. Customs and Border Protection, to find out what information may be leading to the additional questioning. Under FOIA, the Department must respond within 20 days; if the Department does not respond in a timely manner, the aggrieved traveler may compel a response with a court action. As with other access to information laws, FOIA has exemptions. If the aggrieved traveler believes the Department improperly conducted a search, wrongly withheld records or has otherwise not followed the FOIA law, he or she is entitled to challenge that determination in an administrative appeals process and later may bring a civil action against the Department to compel release of non-exempt material. Ultimately, the European (or any other) traveler may be entitled to appeal his or her case for access all the way to the U.S. Supreme Court. Indeed the personal information of any individual, regardless of citizenship, has been protected by the highest court of the U.S.[9] In addition, the traveler may also be entitled to attorney's fees incurred as part of pursuing his/her FOIA claim in court.[10]

Every year, tens of thousands of travelers (and tens of thousands of others) avail themselves of FOIA. DHS alone responded to 109,000 FOIA requests in fiscal year 2008.[11] It is likely that these numbers will go even higher in light of President Obama's announcement in his Freedom of Information Act memorandum of January 21, 2009, that "[a]ll agencies should adopt a

---

[9] In the FOIA context, the U.S. Supreme Court has recognized the privacy interests of foreign citizens when it upheld an agency's denial of personal data related to passport files. *United States Dep't of State v. Wash. Post Co.*, 456 U.S. 595, 602 (1982) *cf. Judicial Watch, Inc. v. Reno*, No. 00-0723, 2001 WL 1902811, at *8 (D.D.C. Mar. 30, 2001) (asylum application); *Judicial Watch, Inc. v. U.S. Dep't of Commerce*, 83 F. Supp. 2d 105, 112 (visa and passport data). It is worth noting that an individual's citizenship—seemingly the most basic, benign information—was protected from disclosure to individuals other than the affected party by the Supreme Court – the highest court in the U.S. (*United States Department of State v. Washington Post, 456 U.S. at 602-03*). In addition to citizenship information, courts have also upheld protections of information concerning identities of asylum applicants and related data. *See Shaw v. United States Dep't of State*, 559 F. Supp.1053, 1067 (D.D.C. 1983); *see also United States Dep't of State v. Ray*, 502 U.S. 164 (1991) (applying traditional analysis of privacy interests under FOIA to Haitian nationals); *Ctr. For Nat'l Sec. Studies v. United States Dep't of Justice*, 215 F. Supp. 2d 94, 105-06 (D.D.C. 2002) (recognizing, without discussion, the privacy rights of post-9/11 detainees who were unlawfully in the United States) (Exemption 7(C)), *aff'd on other grounds*, 331 F.3d 918 (D.C. Cir. 2003), *cert. denied*, 124 S. Ct. 1041 (2004); *Schiller v. INS*, 205 F. Supp. 2d 648, 662 (W.D. Tex. 2002) (finding that ''[a]liens [and] their families….have a strong privacy interest in nondisclosure of their names, addresses, and other information which could lead to revelation of their identities'') (Exemption 7(C)); *Judicial Watch, Inc. v. Reno*, No. 00-0723, 2001 WL 1902811, at *8 (D.D.C. Mar. 30, 2001) (protecting asylum application filed on behalf of Cuban émigré Elian Gonzalez).

[10] Regarding attorney fees (see 5 USC 552(a)(4)(E)), it is worth noting that in the OPEN Government Act Congress amended the attorney fees provision to provide that a plaintiff has substantially prevailed if he or she obtains relief through either a court order or enforceable written agreement or consent decree OR "a voluntary or unilateral change in position by the agency, if the complainant's claim is not insubstantial."

[11] http://www.dhs.gov/xlibrary/assets/foia/privacy_rpt_foia_2008.pdf

presumption in favor of disclosure, in order to renew their commitment to the principles embodied in FOIA, and to usher in a new era of open government."[12] Further, the Attorney General's new FOIA guidelines,[13] directing all executive branch departments and agencies to apply a presumption of openness when administering the FOIA, provide an additional incentive to file FOIA requests. Because nationality of the filer is not relevant to the government's response, such information is not collected and it is unknown how many of the 109,000 filers were U.S. citizens or citizens of other countries. Citizens and non-citizens alike will benefit from the President's openness philosophy and the Attorney General's new FOIA guidelines.

Whether or not the traveler in Hypothetical #1 decides to file a FOIA, he or she may seek to correct inaccurate information through the Department's Traveler Redress Inquiry Program (DHS TRIP). DHS TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experience during their travel screening at transportation hubs – like airports and train stations – or crossing U.S. borders, including:

- denied or delayed airline boarding;
- denied or delayed entry into and exit from the U.S. at a port of entry or border checkpoint; or
- continuously referred to additional (secondary) screening.

DHS TRIP provides travelers with a single process for addressing perceived watch list misidentification issues and other concerns arising from a traveler's screening experience. The number of cases filed and closed suggests that this program is an effective option. From the program's inception in February 2007 through February 2009, DHS TRIP has received over 51,000 redress requests. Over 30,000 cases have been adjudicated and closed, with final determination letters sent to those travelers. Approximately 5,000 cases are currently under review, with the balance of unresolved cases awaiting submission of supporting documentation from the traveler. There are now approximately 80,000 names on the Transportation Security Administration's "cleared" list, developed to avoid delays at U.S. airports for people whose names are similar to and thus easily confused with suspects on the terrorist watch list. DHS added about half of these names after travelers applied through DHS TRIP. While DHS does not currently track applicants by citizenship, DHS TRIP has served redress seekers in nearly 130 countries across the world, representing every geographic region.[14]

Independent of DHS TRIP, the traveler may also seek relief from the CPO of DHS. Section 222 of the Homeland Security Act, [6 U.S.C. 142] created the CPO at DHS with responsibilities to ensure privacy and transparency in government is implemented throughout the Department. The Advocate General to the European Court of Justice has recognized that the CPO is an authority with independence from the rest of the Department.[15] While the efforts of the CPO are primarily concentrated on ensuring that programs are privacy-compliant from inception, the CPO also is

[12] http://www.whitehouse.gov/the_press_office/Freedom of Information Act/
[13] http://www.usdoj.gov/ag/foia-memo-march2009.pdf
[14] Data aggregated by country provided in the address of record; it is not an indication of citizenship or permanent residency.
[15] OPINION OF ADVOCATE GENERAL LÉGER, delivered on 22 November 2005, Case C-317/04, European Parliament v Council of the European Union, para. 253.

responsible for complaints and investigations. The CPO and Director of Incidents and Inquiries are independent of the DHS component privacy offices, and provide non-judgmental redress for all complainants, whether they are U.S. or foreign citizens. The CPO reviews all privacy complaints received by the Privacy Office. For example, if an individual learns DHS holds incorrect information about them through FOIA and brings it to the attention of the Privacy Office, it would be Department policy to correct it.[16]

Hypothetical #2: A European who has traveled to the U.S. believes U.S. government personnel or others are accessing his/her Passenger Name Records (PNR) and improperly using the credit card or other personal information therein. (PNR is traveler reservation information collected by DHS from commercial airlines for the purpose of screening against terrorist and law enforcement databases.[17])

Like the traveler in Hypothetical #1, this individual may avail himself of FOIA, DHS TRIP or a complaint to the CPO to seek redress. In addition, he or she may file suit under the Computer Fraud and Abuse Act (CFAA). The CFAA criminalizes intentional unauthorized access (or exceeding authorized access) to obtain information from a financial institution, a U.S. government computer system or a computer accessed via the Internet. Any person who suffers injury, damage or loss by reason of a violation of this Act may maintain a civil action against the violator to obtain compensatory damages and injunctive or other equitable relief, regardless of whether a criminal prosecution has been pursued.

There are many examples of prosecutions under the CFAA. The most highly publicized recent cases include *U.S. v. Cross* and *U.S. v. Yontz*, where former State Department officials were the subject of criminal actions for unlawfully accessing hundreds of confidential passport files, including those of celebrities and presidential candidates. Criminal convictions under the CFAA apply to circumstances where the database contains personal information on U.S. and non-U.S. persons. For example, in *U.S. v. CBPO Carlos Garcia*,[18] Customs and Border Protection Officer Carlos Garcia was prosecuted in federal district court on a multi-count indictment, including improper use of a database.

Hypothetical #3: A European believes his Electronic System for Travel Authorization (ESTA)[19] information may be compromised because of a security breach at DHS, the U.S. agency that collects ESTA information.

DHS has a detailed framework for identifying, reporting and otherwise responding to security breaches in a timely, expeditious and meaningful manner.[20] If warranted by the circumstances, the individual in hypothetical #3 would be notified in a timely manner, with consideration given

---

[16] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf, specifically Data Quality and Integrity principle.

[17] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_atsupdate10plus2.pdf and http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats_updated_fr.pdf.

[18] http://www.ice.gov/pi/news/newsreleases/articles/070822miami.htm

[19] All nationals or citizens of Visa Waiver Program (VWP) countries who plan to travel to the U.S. for temporary business or pleasure under the VWP need to receive an electronic travel authorization prior to boarding a U.S.-bound airplane or cruise ship. See http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_esta.pdf.

[20] Privacy Incident Handling Guide at http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf

to the method of notification (email, telephone, etc.) and the appropriate language if the individual is not an English speaker. Notification would include advice about precautionary measures the subject may want to take, and, if appropriate, would offer credit monitoring paid for by the Department. The Department itself would bear a responsibility for mitigating damages and would take corrective or disciplinary action against DHS personnel who may have caused the breach through failure to implement safeguards. [21]

These are just three examples from hypothetical DHS incidents that cite laws other than the Privacy Act of 1974 from which individuals can seek rectification or remedy for privacy violations. Other laws from which non-U.S. Persons can seek redress include the Electronic Communications Privacy Act,[22] the Right to Financial Privacy Act,[23] the Internal Revenue Service Code,[24] and others.

CONCLUSION

Undoubtedly, judicial redress under the U.S. legal system is complex. But the many options available to persons regardless of nationality represent a robust and dynamic redress system consistent with U.S. – and EU – privacy principles. It could be argued that a unitary privacy commissioner attempting to address individual complaints such as those described above would be less effective than the current system, in which the agencies are directly accountable to the complainant. Ultimately, the fundamental priority for leaders in both the EU and U.S. must be to ensure that both systems provide avenues for *effective* redress for an individual claiming a violation of his or her privacy, rather than a debate about whether a particular government structure best serves all citizens.

[21] Disciplinary Action includes those disciplinary actions referred to in Office of Personnel Management (OPM) regulations and instructions implementing provisions of title 5 of the United States Code or provided for in comparable provisions applicable to employees not subject to title 5, including but not limited to reprimand, suspension, demotion, and removal. In the case of a military officer, comparable provisions may include those in the Uniform Code of Military Justice. Corrective Action includes any action necessary to remedy a past violation or prevent a continuing violation, including but not limited to restitution, change of assignment, disqualification, termination of an activity, waiver, or counseling.

[22] 18 U.S.C. § 2510

[23] 12 U.S.C. § 3401

[24] 12 U.S.C. § 3402