

# THE U.S. PRIVACY ACT IN COMPARATIVE PERSPECTIVE

Francesca Bignami  
Professor, Duke University School of Law  
Durham, North Carolina

## I. Introduction

This contribution analyzes the application of the U.S. Privacy Act of 1974 to national security, policing, and other related government activities. The purpose of the analysis is to facilitate comparison between the legal framework for data protection in Europe and the United States.

The Privacy Act is the closest analogue, in the United States, to European data protection laws. It regulates the government's collection, use, and disclosure of all types of personal information. In many respects, the provisions of the Privacy Act mirror those of European data protection laws. Most commentators agree, however, that the Privacy Act has been ineffective in curbing government data processing.<sup>1</sup> The reasons for this ineffectiveness are several: First, the Privacy Act contains a number of exceptions that have been interpreted broadly by government agencies and the courts. Second, the Privacy Act failed to create an independent government authority with responsibility for enforcing the Act. Although a number of special-purpose civil liberties officers have been established since September 11, 2001, none of them are functionally equivalent to data protection authorities in Europe. After briefly reviewing those U.S. laws that *do* curb government data processing in the fields of national security and policing, this contribution turns to the Privacy Act, its limitations, and possible reforms.

## II. Sector-Specific Data Protection Laws

In the United States, a number of specific laws applicable to certain types of personal data limit significantly government data processing. Generally speaking, telecommunications companies, financial institutions, and consumer reporting agencies are prohibited by law from disclosing their customer records to the government.<sup>2</sup> The police and other government officials may obtain such information only if they apply for a court warrant, court order, or grand jury or administrative subpoena.<sup>3</sup> Officers conducting a national security investigation may obtain such information if they receive a certification, from the Director of the Federal Bureau of Investigation or his designee that the information is relevant to an international terrorism investigation or one of the other

---

<sup>1</sup> Robert Gellman, *Does Privacy Law Work? in Technology and Privacy: The New Landscape* (Philip E. Agre & Marc Rotenberg eds., 1997).

<sup>2</sup> Stored Communications Act, 18 U.S.C. § 2702(a)(3) (telecommunications records); Right to Financial Privacy Act, 12 U.S.C. § 3402 (financial records); Fair Credit Reporting Act, 15 U.S.C. § 1681b (consumer reports).

<sup>3</sup> Stored Communications Act, 18 U.S.C. § 2703(c) (telecommunications records); Right to Financial Privacy Act, 12 U.S.C. § 3405, 3406, 3407, (financial records); Fair Credit Reporting Act, 15 U.S.C. § 1681b(a)(1) (consumer reports).

listed investigations.<sup>4</sup> The subpoena route is the one used by the Treasury Department to obtain the financial data held by SWIFT's operation centre in the United States: the Treasury Department issues administrative subpoenas under the International Emergency Economic Powers Act of 1977, which permits the government to compel the production of information pursuant to Presidential declarations of national emergency.<sup>5</sup> The difficulty with the Treasury Department's program is not so much the subpoena procedure as the expansive interpretation of the subpoena power: investigators have not been required to show a national security risk specific to certain individuals but rather have been allowed to use administrative subpoenas to obtain data relating to millions of individuals and transactions.<sup>6</sup>

These specific laws also limit the use, by the government, of personal information once it is obtained. For instance, financial records obtained by one government department may not be transferred to another government department

unless the transferring agency or department 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 within the jurisdiction of the receiving agency or department.<sup>7</sup>

In sum, in these sectors, the data protection guarantees of U.S. law are not significantly different from those of European national laws, especially as concerns the collection and use phases of government data processing operations.

### **III. The Privacy Act of 1974**

The Privacy Act covers the government's processing of all types of personal data, both the specially protected data discussed above and all other forms of personal data. In other words, the Privacy Act contains a least-common-denominator set of data protection principles applicable to all the government's activities. Airline passenger data is one example of personal information that does not benefit from a specific regulatory scheme and therefore is governed exclusively by the Privacy Act. Although the Privacy Act resembles data protection legislation in Europe, as we shall see, it is not as comprehensive or as vigorously enforced as in Europe.

---

<sup>4</sup> Stored Communications Act, 18 U.S.C. § 2709(b) (telecommunications records); Right to Financial Privacy Act, 12 U.S.C. § 3414(a)(5)(A) (financial records); Fair Credit Reporting Act, 15 U.S.C. § 1681u (consumer reports).

<sup>5</sup> Testimony of Stuart Levey, Under Secretary Terrorism and Financial Intelligence, U.S. Department of the Treasury Before the House Financial Services Subcommittee on Oversight and Investigations 3 (July 11, 2006).

<sup>6</sup> Art. 29 Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) 8 (Nov. 22, 2006).

<sup>7</sup> Right to Financial Privacy Act, 12 U.S.C. § 3412(a). See also Stored Communications Act, 18 U.S.C. § 2709(d) (telecommunications records); Fair Credit Reporting Act, 15 U.S.C. § 1681u(f) (consumer reports).

On its face, the Privacy Act is quite similar to European law, the principal point of reference for purposes of this discussion being the Council of Europe Convention on Personal Data Processing.<sup>8</sup> The Privacy Act requires transparency in personal data processing: The responsible government agency must alert the public to the existence of a personal records system by publishing a notice in the Federal Register (the U.S. equivalent to the Official Journal).<sup>9</sup> When information is collected from individuals, they must be told of the nature of the government database.<sup>10</sup> The Privacy Act restricts the *amount* of personal information that may be collected: government agencies may only gather such information as is relevant and necessary to the agency's legal purposes (purposes set down by Congressional statute or Presidential executive order).<sup>11</sup> It also restricts the *type* of personal information that may be collected by government agencies: personal data "describing how any individual exercises rights guaranteed by the First Amendment [right to freedom of expression and freedom of association]" may not be collected routinely.<sup>12</sup> Personal information stored by government agencies must be accurate, relevant, timely, and complete.<sup>13</sup> The Privacy Act prohibits information from being shared with another government agency without the consent of the person concerned.<sup>14</sup> It requires that technical measures be adopted to guarantee the security and confidentiality of the information.<sup>15</sup> And it gives individuals the right to check their personal information and, if necessary, demand that their information be corrected.<sup>16</sup>

To review briefly the parallel provisions of the Council of Europe Convention: Personal data processing must be "fair and lawful."<sup>17</sup> The Convention requires that personal data "be adequate, relevant and not excessive in relation to the purposes for which they are stored."<sup>18</sup> It also creates categories of specially protected personal data:

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.<sup>19</sup>

Personal data must be accurate and, where necessary, kept up to date.<sup>20</sup> Personal data must be stored for specific and legitimate purposes and must not be used in a way

---

<sup>8</sup> Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe Treaties No 108 (Jan 28, 1981).

<sup>9</sup> 5 U.S.C. § 552a(e)(4).

<sup>10</sup> 5 U.S.C. § 552a(e)(3).

<sup>11</sup> 5 U.S.C. § 552a(e)(1).

<sup>12</sup> 5 U.S.C. § 552a(e)(7).

<sup>13</sup> 5 U.S.C. § 552a(e)(5).

<sup>14</sup> 5 U.S.C. § 552a(b).

<sup>15</sup> 5 U.S.C. § 552a(e)(10).

<sup>16</sup> 5 U.S.C. § 552a(d).

<sup>17</sup> Convention, art. 5a.

<sup>18</sup> Convention, art. 5c.

<sup>19</sup> Convention, art. 6. As is evident from the text, the types of personal data that may not be collected routinely are more extensive in Europe than in the United States.

<sup>20</sup> Convention, art. 5d.

incompatible with those purposes.<sup>21</sup> The Convention requires that “security measures” be taken to protect personal data “against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.”<sup>22</sup> It also contains a “participation principle”<sup>23</sup> similar to the right of access and correction under the U.S. Privacy Act.

The one major substantive difference between the U.S. Privacy Act and the Council of Europe Convention concerns data retention. Under the Convention, personal data may be “preserved in a form which permits identification of the data subjects for no longer than is required for the purposes for which those data are stored.”<sup>24</sup> By contrast, the U.S. Privacy Act contains no provision that specifically addresses the length of time of data retention. Otherwise, however, the laws on the two sides of the Atlantic appear quite similar. The basic aim driving both laws is to ensure that as little personal information as possible is floating about the halls of government and that the personal information that is absolutely necessary to the work of government is reliable. If only limited amounts of reliable information are available, the theory goes, abuses of government power are less likely.

#### **IV. The Limitations of the Privacy Act**

##### *A. Exceptions under the Privacy Act*

Notwithstanding these common legal provisions and these shared commitments to liberal rights, the Privacy Act permits so many exceptions that it fails to constrain government to the same extent as data protection laws in Europe. These exceptions partially account for U.S. government programs like the Department of Homeland Security’s Automated Targeting System, the Treasury Department’s Terrorist Finance Tracking Program, and the National Security Agency’s call-records program. Under the Privacy Act, disclosure of information to other agencies is permitted even without consent if the public is notified upfront, when the record system is created, that such disclosure constitutes a “routine use” of the information. This is defined as a use that is compatible with the main purpose for which the information was collected. Even without advance notice of a “routine use,” personal information may be transferred to another agency if the transfer is for law enforcement purposes and is requested by the agency’s head. Records held by law enforcement agencies and the Central Intelligence Agency may be exempted from most of the requirements of the Act (“general exemptions”) if the agency head publishes a notice to that effect.<sup>25</sup> Records held by any agency may be exempted from some of the requirements of the Act (“specific exemptions”) if the agency head likewise publishes a notice to that effect and if they fall into one of a number of categories—investigatory material, statistical records, matters whose secrecy is in the

---

<sup>21</sup> Convention, art. 5b.

<sup>22</sup> Convention, art. 7.

<sup>23</sup> Convention, art. 8. Under the U.S. Privacy Act, however, individuals only have the right to demand that their information be corrected, not that it be deleted to come into compliance with privacy guarantees other than the duty of accuracy.

<sup>24</sup> Convention 108, art. 5e.

<sup>25</sup> 5 U.S.C. § 552a(j).

interest of national defense or foreign policy, and more.<sup>26</sup> Finally, the Privacy Act only applies to personal data held in a “system of records.” For a government database to be considered a “system of records” it must be used by the agency to retrieve information about specific individuals, using the names, social security numbers, or other identifying particulars of those individuals.<sup>27</sup>

The National Security Agency’s call-records program serves as an illustration of the limitations of the Privacy Act. In May 2006, the media reported that the National Security Agency (NSA) had created a database with the phone records of millions of citizens that was being used for purposes of anti-terrorism data-mining. This data was collected from private telecommunications carriers. Many aspects of the NSA program would appear to violate the provisions of the Privacy Act. Yet the Privacy Act’s numerous exceptions might indeed save the program.

Although the NSA does not qualify for the general exemption available to the FBI and the CIA, it generally takes advantage of the specific exemptions for national security records in its Federal Register notices.<sup>28</sup> Plus, even without specific mention in the Federal Register, the NSA may share personal information with other government agencies if requested to do so for law enforcement purposes.<sup>29</sup> Perhaps the most troubling aspect of this analysis is the question of whether the call database would even count as a “system of records” under the Privacy Act.<sup>30</sup> Is a phone number, without a name attached, an “identifying particular” assigned to an individual? If so, then it seems that searching the system by the phone number of an al Qaeda suspect, to obtain information on her activities or to identify other possible suspects would count as retrieving information about her. But what about using the country code for Afghanistan as a search term? Or, as is most likely the case, combining these and other criteria as part of complex algorithms to discover new relationships among the data and to generate better information on terrorist activity? The few courts deciding the question of what is a “system of records” have reached different, inconsistent conclusions. And most of them have defined the term quite narrowly.<sup>31</sup> Therefore, a database containing personal details on millions of citizens may not be covered at all by the Privacy Act.<sup>32</sup>

## B. *Enforcement of Privacy Rights*

---

<sup>26</sup> 5 U.S.C. § 552a(k).

<sup>27</sup> *See, e.g.*, *Williams v. Dept. Veterans Affairs*, 104 F.3d 670 (4<sup>th</sup> Cir. 1997).

<sup>28</sup> *See* National Security Agency/Central Security Service Privacy Act Program, 32 C.F.R. pt. 322 (2006).

<sup>29</sup> 5 U.S.C. § 552a(b)(7).

<sup>30</sup> For instance, a report issued by the Congressional Research Service assumes that the Privacy Act does *not* apply to data-mining and suggests that Congress consider “the possible application of the Privacy Act to these [data-mining] initiatives.” Jeffrey W. Seifert, *Data-mining and Homeland Security: An Overview*, Congressional Research Service Report for Congress 19 (Jan. 27, 2006).

<sup>31</sup> *See, e.g.*, *Williams v. Dept. Veterans Affairs*, 104 F.3d 670, 675 (4<sup>th</sup> Cir. 1997); *Henke v. Dept. Commerce*, 83 F.3d 1453, 1459-62 (D.C. Cir. 1996).

<sup>32</sup> In practice, given the far-reaching exemptions that apply even if the personal data is considered part of a system of personal records, this simply means that the NSA is not obliged to published a notice in the Federal Register.

Moving from the substantive provisions of the Privacy Act to their enforcement, the Act departs dramatically from the European model by failing to establish an independent authority tasked with enforcement. Although the original bill contained such an authority, it was removed in the end as part of the compromise necessary to pass the Privacy Act. Rather, the courts are the sole guarantors of privacy rights. The Privacy Act gives individuals the right to sue the government for damages and, in some instances, injunctive relief.<sup>33</sup> In addition, government officials may be criminally prosecuted for certain violations of the Privacy Act.<sup>34</sup>

Privacy litigation, however, has been spectacularly unsuccessful in the United States. Any sound remedial scheme should contain both a forward-looking and a backward-looking element. It should attempt to prevent privacy violations before they can occur, through good policy advice on new government programs and it should afford individuals a remedy should such privacy violations occur nonetheless. The courts have failed at both the backward and the forward-looking elements of privacy protection. The injuries suffered by individuals—not to speak of the polity—when the government secretly undertakes a program like that for call-records are generally not recognized by common law courts. When spying occurs through unobtrusive methods, without visible consequences like a criminal prosecution or civil action, it is almost impossible to prove the injury element of a tort claim. In addition, suing government is almost always more difficult than suing private parties. Even though the Privacy Act lifts sovereign immunity, the government still benefits from a form of qualified immunity: most violations of the Act must be proven “intentional or willful” before a plaintiff can recover.<sup>35</sup>

As for forward-looking policymaking, the courts suffer a special disadvantage when compared with administrative authorities. They generally can intervene only after a privacy violation has occurred, not beforehand when the government program is being designed. To be fair, common law courts often craft rules in deciding specific cases. These rules, like any other forward-looking government policy, serve as guidance for the state in the future. But when courts make data protection policy through adjudication, they are hampered by their lack of expertise and historical memory of the problem. They simply do not have the resources or the institutional agenda of administrative agencies. These shortcomings should come as no surprise to European privacy advocates: most data protection laws in Europe not only establish independent authorities but also give individuals the right to sue in court. Yet very rarely do individuals bring such lawsuits.

In recent years, a number of officers with responsibility for privacy oversight have been established within the federal government.<sup>36</sup> This is a welcome development. Yet, as will be discussed, these privacy officers are not functional equivalents of

---

<sup>33</sup> 5 U.S.C. § 552a(g).

<sup>34</sup> 5 U.S.C. § 552a(i).

<sup>35</sup> 5 U.S.C. § 552a(g)(4).

<sup>36</sup> This discussion is based largely on Marc Rotenberg’s excellent overview and analysis of these developments. *The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight After 9-11*, Social Science Research Network Working Paper Series (Sept. 2006).

European data protection authorities. There are two principal differences: these new privacy officers are not structurally independent of the government bodies that they are responsible for overseeing; and they do not have the power to investigate and sanction privacy violations.

The first privacy officer to be established after September 11, 2001 was the Chief Privacy Officer of the Department of Homeland Security.<sup>37</sup> The Chief Privacy Officer was created in 2002, at the same time as the Department itself. She serves in the office of the Secretary of Homeland Security. The Chief Privacy Officer is tasked with overseeing compliance with the Privacy Act, conducting privacy impact assessments, and screening proposed regulations and laws for adverse effects on privacy.<sup>38</sup> In an early assessment of the still-fledgling office, Marc Rotenberg finds that the Chief Privacy Officer has contributed to transparency in the work of the Department of Homeland Security—publicizing the privacy implications of new government programs—but has failed to pursue privacy complaints and enforce the law.<sup>39</sup>

Another post-September 11 development is the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. The legislation created the Office of the Director of National Intelligence, with responsibility for the seventeen government agencies considered to be part of the intelligence community.<sup>40</sup> The main thrust of the IRTPA was to mandate more effective information-sharing among the different agencies in the intelligence community: intelligence must be “provided in its most shareable form” and the heads of the relevant government agencies must “promote a culture of information sharing.”<sup>41</sup> These goals, of course, are antithetical to traditional good privacy practices: the sharing of personal information between government agencies is strictly limited under most data protection laws, including, in theory, the Privacy Act. In compensation, the IRTPA created two new government bodies with responsibility for privacy and civil liberties in anti-terrorism intelligence-gathering: the Privacy and Civil Liberties Board in the Executive Office of the President<sup>42</sup> and the Civil Liberties Protection Officer, who reports directly to the Director of National Intelligence.<sup>43</sup> Both have responsibility for guaranteeing rights in the new intelligence-sharing environment, but the Board’s duties run more to formulating policy recommendations and guidelines,<sup>44</sup>

---

<sup>37</sup> Homeland Security Act, 6 U.S.C § 142.

<sup>38</sup> 6 U.S.C. § 142. The E-Government Act of 2002 requires a privacy impact assessment whenever a government agency procures new information technology systems designed to collect, maintain, or disseminate personal information or begins a new initiative involving the collection of personal information to be processed using information technology. 44 U.S.C. § 3501 note. The information provided in a privacy impact assessment is substantially similar to the information provided in a notice of a system of personal records under the Privacy Act.

<sup>39</sup> Marc Rotenberg, *The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight After 9-11*, Social Science Research Network Working Paper Series 19 (Sept. 2006).

<sup>40</sup> 50 U.S.C. § 403. For a complete list of the agencies that constitute the national intelligence community see [http://www.dni.gov/who\\_what/members\\_IC.htm](http://www.dni.gov/who_what/members_IC.htm).

<sup>41</sup> 6 U.S.C. § 485(d).

<sup>42</sup> Marc Rotenberg, *The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight After 9-11*, Social Science Research Network Working Paper Series 48 (Sept. 2006).

<sup>43</sup> *Id.* 35.

<sup>44</sup> *Id.* 38.

those of the Civil Liberties Protection Officer to enforcement of privacy and other types of rights.<sup>45</sup> The Board, however, has yet to do much of anything. The Civil Liberties Protection Officer, by contrast, has undertaken a couple of policymaking initiatives, the chief example being the privacy guidelines for the new information-sharing environment.<sup>46</sup> However, no enforcement actions have been brought yet, at least insofar as has been disclosed to the public.

Finally, under a law enacted in December 2005, all government agencies are required to appoint a Chief Privacy Officer with responsibilities similar to those of the Department of Homeland Security's Chief Privacy Officer.<sup>47</sup> From a memorandum issued by the Office of Management and Budget, it appears that many agencies have complied with this requirement by designating their Chief Information Officer as their Chief Privacy Officer.<sup>48</sup> The same law requires that, every two years, each government agency hire an independent auditing firm to conduct an exhaustive review and assessment of that agency's privacy practices.

More privacy oversight can only be a positive development. None of these officers, however, serves as functional equivalents of European data protection authorities. European data protection authorities share two fundamental characteristics: independence and enforcement powers. Independence of data protection officers is generally guaranteed through fixed terms of office and appointment by the Parliament or other bodies removed from the government. As for enforcement, notwithstanding significant cross-country variation, all of these authorities exercise both the backward-looking and forward-looking powers discussed earlier. That is, they have the power to advise on new government initiatives as well as investigate allegations of misconduct and sanction privacy violations. Those sanctions might be as soft as reporting the matter to Parliament, as in the German case, or bringing criminal prosecutions, as in the French case, but they exist everywhere.

Compared to their European counterparts, the recent crop of U.S. privacy officers lacks structural independence. The Chief Privacy Officer of the Department of Homeland Security is appointed by the Secretary of the Department of Homeland Security and can be removed at will.<sup>49</sup> Likewise, the Civil Liberties Protection Officer is appointed by the Director of National Intelligence and can be removed at will.<sup>50</sup> The five members of the Civil Liberties and Oversight Board are appointed by the President

---

<sup>45</sup> *Id.* 48-49.

<sup>46</sup> Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment available at <http://www.ise.gov>.

<sup>47</sup> Consolidated Appropriations Act 2005, Pub. L. No. 108-447, § 522, 118 Stat. 3268, 3268-70 and 5 U.S.C. § 552a note (2000).

<sup>48</sup> Office of Management and Budget, Memorandum M-05-08, available at <http://www.whitehouse.gov/omb/memoranda/fy2005/m05-08.pdf>. For a list of senior agency privacy officials see <http://www.whitehouse.gov/omb/egov/documents/SAOPcontactlistfinal.pdf>.

<sup>49</sup> 6 U.S.C. § 142.

<sup>50</sup> 50 U.S.C. § 403-3d.

and serve at his pleasure.<sup>51</sup> In most agencies, the duties of the Chief Privacy Officer have been assigned to political appointees.

These newly established privacy officers also lack the backward-looking investigatory and enforcement powers of European data protection authorities. None of them has the power to compel the production of information from the government.<sup>52</sup> Moreover, they do not have the power to sanction rogue officials, not even by reporting on violations to Congress.

## V. Possible Reforms

A few modest changes to the Privacy Act would overcome most of these limitations. First, the many exceptions described earlier should be narrowed or eliminated. It should be made absolutely clear that the Privacy Act catches all government programs that involve large-scale personal data processing. A “system of records” covered by the Act should be interpreted to include all personal data processing. Furthermore, the Privacy Act’s exemptions for intelligence and law enforcement agencies should be narrowed considerably. Lastly, the exception in the Privacy Act for “routine uses” of personal data should be repealed. This exception has enabled federal agencies to share personal information with other federal agencies, as well as state and local bodies, virtually unchecked. When establishing a new government program, agencies should not be able to claim a vague “routine use” for the personal information involved in that program. Rather, they should be required to specify, upfront, exactly how personal data will be used and under what conditions it will be transferred to other government agencies.

These changes might be effected by legislative amendment, but not necessarily. The courts could narrow their interpretation of the Privacy Act’s exceptions. Furthermore, in establishing and running programs involving personal data processing, the government could interpret broadly a “system of records” and make limited or no use of the intelligence, law enforcement, and routine use exceptions. In the American system, this government duty to abide by the law, independent of the courts, flows from the President’s constitutional duty to take care that the laws be faithfully executed.

Second, the independence and enforcement powers of the new privacy officers should be improved. Better yet, an independent privacy agency charged with enforcing the Privacy Act and with oversight responsibility for the entire federal government could be established. Both of these changes would require legislative action. Both would result in a dramatic improvement in oversight. The courts are ill-equipped to enforce the Privacy Act and the privacy officers that exist today are woven too tightly into the fabric of their respective agencies to serve as civil liberties watchdogs. This institutional

---

<sup>51</sup> Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1061 (2004); <http://www.whitehouse.gov/privacyboard>. The appointment of the Chairman and the Vice-Chairman must be confirmed by the Senate.

<sup>52</sup> Marc Rotenberg, *The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight After 9-11*, Social Science Research Network Working Paper Series 34, 38-39, 54 (Sept. 2006).

change would also improve public confidence in the integrity of the Executive Branch, especially in the area of policing and national security. Much oversight of such activities must necessarily occur behind closed doors, to avoid the disclosure of sensitive information. This oversight is far more credible when it is entrusted to privacy officers independent of agency officials, with the power to report on misconduct to other institutional actors, such as Congressional committees.