TOWARDS A RIGHT TO PRIVACY IN TRANSNATIONAL INTELLIGENCE NETWORKS

Francesca Bignami[*]

I. INTRODUCTION

Antiterrorism intelligence sharing across national borders has been trumpeted as one of the most promising forms of networked global governance.[1] By exchanging information across the world, government agencies can catch terrorists and other dangerous criminals. Yet this new form of global governance is also one of the most dangerous. Even at the domestic level, secrecy and national security imperatives have placed intelligence agencies largely beyond legal and democratic oversight. But at the global level, accountability is missing entirely. Global cooperation among national intelligence agencies is extraordinarily opaque. The nature of the international system compounds the problem: these actors do not operate within a robust institutional framework of liberal democracy and human rights. Safeguarding rights in the transnational realm when governments conspire to spy, detain, interrogate, and arrest is no easy matter.

Privacy is one of the most critical liberal rights to come under pressure from transnational intelligence gathering. This Article explores the many ways in which transnational intelligence networks intrude upon privacy and considers some of the possible forms of legal redress. Part II lays bare the different types of transnational intelligence networks that exist today. Part III begins the analysis of the privacy problem by examining the national level, where, over the past forty years, a legal framework has been developed to promote the right to privacy in domes-

* Professor of Law, Duke University School of Law.

1. PHILIP B. HEYMANN, TERRORISM, FREEDOM, AND SECURITY: WINNING WITHOUT WAR 32, 119 (2003); ANNE-MARIE SLAUGHTER, A NEW WORLD ORDER 1–2 (2004).

tic intelligence gathering. Part IV turns to the privacy problem transnationally, when government agencies exchange intelligence across national borders. Part V invokes the *cause célèbre* of Maher Arar, a Canadian national, to illustrate the disastrous consequences of privacy breaches in this networked world of intelligence gathering. Acting upon inaccurate and misleading intelligence provided by the Canadian government, the United States wrongfully deported Arar to Syria, where he was tortured and held captive by the Syrian Military Intelligence Service for nearly one year.

Part VI begins the constructive project of redesigning transnational networks to defend the right to privacy, with the safeguards of European intelligence and police networks serving as inspiration for transnational networks more broadly. These European systems feature two types of privacy safeguards: multilateral standards, to which all network parties must adhere, and unilateral standards, applicable under the law of one network party and enforced against the others through the refusal to share intelligence with sub-standard parties. Moving to the global realm, this Article concludes that the multilateral avenue is more promising than the unilateral one. Multilateral standards require consensus on common privacy norms, and consensus will be difficult to achieve. Notwithstanding this hurdle, multilateral privacy standards are crucial, for they will both enable the cooperation necessary to fight serious transnational crime and provide for vigorous protection of basic liberal rights.

II. TYPES OF TRANSNATIONAL INTELLIGENCE NETWORKS

Transnational networks are quickly becoming one of the most common forms of international cooperation, alongside classic international organizations and treaty regimes. In such networks, national officials representing distinct regulatory communities, such as environmental protection and financial markets, come together to address common cross-border problems.[2] They do so through a variety of formal and informal techniques: information exchange on best practices, promulgation of standardized regulation, and mutual assistance in enforcing that regulation. As compared to more traditional forms of international cooperation, transnational networks are more flexible and informal and therefore can adapt more readily to changing circumstances.

Since the terrorist attacks of September 11, transnational networks have assumed an ever-growing importance in the national security arena. Intelligence-sharing networks draw on many different government enti-

2. SLAUGHTER, *supra* note 1, at 2–5.

ties: foreign and domestic intelligence agencies, police, customs officials, immigration agencies, and financial regulators. Intelligence-sharing networks also come in many different geographical constellations. Some, like the intelligence-sharing agreement between the United States and Canada discussed in Part V, are bilateral; others are regional, such as the European Police Office (Europol); and still others, like the International Criminal Police Organization (Interpol), are truly global.

Despite such variation, these systems share two critical attributes: their purpose and the institutional means chosen to accomplish it. Each network deploys a decentralized, transnational government process to fight terrorism and other forms of serious crime. A national agency—one node in the network—gathers the information. Another national agency—a different node in the network—acts upon the information. Such government action can take a number of different forms: further information gathering through surveillance and other investigative techniques, asset seizure, arrest, deportation, and prosecution. The network form of governance is quite obviously designed to match the fluid, borderless nature of the problem at hand; terrorism, drug trafficking, and other forms of serious crime generally involve individuals and funds in multiple countries that can move quickly from one jurisdiction to another.

For purposes of understanding the rights implications of networked global governance, the most significant difference separating intelligence networks is the degree to which the network is centrally coordinated. At one extreme, the only coordination mechanism is an agreement among the different participants on the terms of cooperation. One example discussed in greater detail in Part V is the information-sharing arrangement established between Canadian and U.S. intelligence agencies in the days following the September 11 attacks. Under this purely verbal agreement, intelligence was to be exchanged in "real time" through direct communication among the various agencies involved.[3] Another example is a recent European Union (EU) law on information sharing between law enforcement authorities in the member states.[4] The law facilitates information exchange by setting down a common procedure through which national police may request information from other national police, establishing a duty to cooperate with such requests, listing an exhaustive set of reasons for denying cooperation, and specifying response times for replying to information requests. Because only the national agencies in

3. COMM'N OF INQUIRY INTO THE ACTIONS OF CANADIAN OFFICIALS IN RELATION TO MAHER ARAR, I REPORT OF THE EVENTS RELATING TO MAHER ARAR: FACTUAL BACKGROUND, 31 (2006) [hereinafter ARAR COMMISSION: FACTUAL BACKGROUND I].

4. Council Framework Decision 2006/960/JHA, 2006 O.J. (L 386) 89 (EC).

the network exercise public power, rights serve to protect exclusively against intrusive action by those national agencies.

At the other extreme of the coordination spectrum, a central secretariat is entrusted with significant responsibility for collecting information from network participants, analyzing that information, and then retransmitting the (improved) information to network participants. Europol is one such intelligence network.[5] Located in The Hague, Europol is responsible for assisting the member states in combating a wide array of cross-border crime, including terrorism, counterfeiting, drug trafficking, smuggling of illegal immigrants, and motor vehicle crime.[6] It manages three related criminal intelligence systems: the Europol Information System, work analysis files, and an index system.

The Europol Information System (EIS) is largely designed to facilitate information exchange among national authorities, who supply information on individuals suspected of having committed, or planning to commit, one of the covered crimes. National authorities then extract information from the system in the course of national investigations involving a covered crime. The central office, however, also bears responsibilities for the EIS. It both manages EIS-related technology and solicits information from national police units to ensure that the system is complete.[7] The central office is also a consumer of the EIS. It consults the system to conduct long-term strategic analyses on different types of crime, which are then circulated to national police forces.[8] The central office can also use the system in connection with specific national investigations: one of its tasks is to assist with national criminal investigations by collecting and analyzing intelligence from the many different jurisdictions potentially involved in the crime, some of which is extracted directly from the EIS.[9] This criminal intelligence is stored in so-called work files and is also cross-referenced in an index system to permit easier access to the intelligence for purposes of related investigations.

Clearly, Europol is not a federal police force[10] but rather a network of national police forces. Nevertheless, it is a network in which the center—the office in The Hague—is charged with significant

5. Convention Based on Article K.3 of the Treaty on European Union, on the Establishment of a European Police Office, 1995 O.J. (C 316) 2 [hereinafter Europol Convention].

6. *See, e.g.*, Steven Peers, *Europol: The final step in the creation of an "Investigative and Operational" European Police Force*, Jan. 2007, at 2–3, http://www.statewatch.org/news/2007/jan/europol-analysis.pdf.

7. Europol Convention, *supra* note 5, arts. 3.1(2), 8.

8. *Id.* art. 3.2.

9. *See* Summaries of the Union's Legislation: Europol: European Police Office, http://europa.eu/scadplus/leg/en/lvb/l14005b.htm.

10. A number of proposed changes to Europol's legal framework, however, might bring it closer to the federal model. *See* Peers, *supra* note 6, at 4–6.

responsibilities, all with the aim of improving the information available through the network. Because of these powers, rights must be guaranteed both centrally and nationally.

Between these two extremes on the coordination spectrum lie networks with a central component performing only ministerial tasks for the participating states. In such networks, a free-standing government body can be charged with receiving information from and distributing information to national actors, but without responsibility for conducting an independent analysis of the information. In this type of arrangement, the central body does not actively seek intelligence from the participating states, scrutinize that intelligence to guarantee its accuracy, or assess its relevance for crime-fighting purposes. Because the powers of the center are relatively insignificant, the need for an additional layer of rights to complement national guarantees is less pressing.

The Schengen Information System exemplifies this intermediary form of network.[11] A small group of European states signed the Schengen Convention in 1985 to manage jointly the admission of foreign citizens to their territories. As part of the Convention, a common database was created to monitor foreigners admitted to the Schengen area with Schengen visas. Today, this database functions as an all-purpose, cross-border crime database, containing information on, among other things, individuals suspected of having committed serious crimes, extradition warrants, car thefts, and passport theft or loss. The Schengen Information System is located and maintained in Strasbourg, but national police enter and extract information from the system entirely independently of the Strasbourg office. Unlike Europol's office in The Hague, the Strasbourg office lacks control over the information contained in its database; neither does it have the power to assist national authorities with their investigations by soliciting and analyzing information held by other national authorities.

III. PRIVACY IN DOMESTIC INTELLIGENCE GATHERING

One of the most fundamental rights at issue in intelligence-gathering activities is information privacy. The right to privacy limits the government's use of personal information, thereby protecting individuals against a wide array of abuses of government power. Perhaps the most obvious of these abuses, especially in intelligence operations, are depri-

11. Convention Implementing the Schengen Agreement of 14 June 1985 Between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the Gradual Abolition of Checks at Their Common Borders, June 19, 1990, 30 I.L.M. 68 (1991).

vations of life, liberty, and property based on *inaccurate* information. Because of the ease with which data can be gathered, stored, and combined in the age of information technology, it is difficult to guarantee its accuracy. At the most basic level, data might be wrongly recorded through human error. When different data sets are combined, the information in one of the data sets may be wrongly interpreted because its coding and software systems differ from the other data set's systems. Moreover, the storage capacity of computer systems is so vast that information that has become obsolete, and therefore inaccurate, can be retained indefinitely.

The questionable quality of such data is particularly troubling in the domains of national security and law enforcement, in which reliance on inaccurate data can lead to wrongful surveillance, detention, deportation, prosecution, and even conviction. Many consider the right to procedural due process to be the primary guarantee against wrongful government determinations. Yet many of the harms caused by the government's use of bad information are kept secret. For instance, if such information gives rise to the belief that an individual is involved in a terrorist conspiracy, further surveillance will be conducted without alerting that individual. Other harms that result from inaccurate information are not legally recognized as constituting determinations against which individuals have recourse. Again, surveillance is a good example. Even if an individual is fully aware that she is being observed by the police, unless that observation rises to the level of harassment, she has no remedy. There is no procedure available to her for proving that the suspicions of the police are unfounded. By limiting the personal information that can be collected and by requiring accuracy when such information is collected, the right to privacy operates as a critical *ex ante* guarantee against such government harms.

Information about others can also be put to all sorts of illegitimate uses. An intelligence agency, of course, can legitimately use personal information to prevent terrorism. But if care is not taken, such information can also be used to suppress speech and political protest, as occurred in the United States during the 1960s and 1970s. Discrimination based on religion, race, or ethnic origin is another illegitimate use of knowledge of others. Given that much of today's terrorism originates in the Islamic world, both of these speech and discrimination concerns are implicated. Intelligence operations may target certain individuals based on their religion and country of origin rather than on actual facts connecting them to terrorist plots. Or critics of the U.S. presence in the Middle East might come under investigation, even though they neither explicitly encourage acts of violence nor serve as a cover for terrorist

groups. Distinguishing between legitimate suspicion and illegitimate discrimination and suppression of speech is often impossible, as terrorism can be associated with religious beliefs and critical speech. By limiting the information on ordinary individuals available to government investigators, privacy can defend against such abuses.

Even more fundamental to privacy are the principles of human dignity and individual autonomy.[12] At the core of liberalism is the free, equal, rational person capable of choosing her own life projects. Critical to this liberal being is the power to keep certain matters private and to make other matters public. The duty of others, in a liberal society, is to respect the individual's decision in favor of privacy. Yet when government agencies collect, combine, and manipulate information on individuals without their consent, they breach that essential liberal duty. The government is guilty of the high-technology equivalent of gazing at citizens without their consent.

Intelligence agencies, of course, routinely conduct intrusive, unrelenting surveillance. They are allowed this extraordinary privilege in liberal societies because such surveillance supports the critical mission of guaranteeing the survival of society in the face of threats to national security. When, however, surveillance is no longer used to protect national security and begins to serve more mundane public purposes, for instance preventing ordinary crimes like bank fraud, liberty is put at risk.

To safeguard privacy interests, most countries have enacted information privacy laws, known in Europe as data protection laws.[13] Such laws specify the conditions under which the government may collect personal information. Generally, individuals must either consent to the collection and the intended uses of their information, or a piece of legislation must specify the public reasons for mandating personal data processing.[14]

12. *See, e.g.*, Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, *in* NOMOS XII: PRIVACY 1 (J. Roland Pennock & John W. Chapman eds., 1971).

13. This discussion is based on U.S. and European legislation. In the United States, the relevant law is the Privacy Act of 1974, Pub. L. No. 93-579, § 3, 88 Stat. 1897 (codified as amended at 5 U.S.C. § 552a (2000). The Council of Europe Convention on Personal Data Processing serves as the point of reference for national European laws, since the Convention has been ratified and implemented by most European countries.

14. *See* 5 U.S.C. § 552(e)(3) (2000) (setting forth information that must be disclosed upon collection); *id.* § 552(e)(4) (describing publication of notice of records system in the Federal Register); Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data art. 5a, Jan. 28, 1981, Europ. T.S. No. 108 [hereinafter Convention 108] (addressing fair and lawful processing of personal data); Bundesdatenschutzgesetz [Federal Data Protection Act], Dec. 20, 1990, BGBl. I at 2954, § 4(1) (F.R.G.) ("The collection, processing and use of personal data shall be admissible only if permitted or prescribed by this Act or any other legal provision or if the data subject has consented."). To be entirely accurate, absent an authorizing law, European data protection laws require both disclosure of the purposes of data collection and consent to those purposes, whereas U.S. law requires only disclosure, not consent.

These laws restrict the amount and type of personal information that may be collected,[15] and they limit the time during which personal information may be retained.[16] The personal information stored by government agencies must be accurate, reliable, and up-to-date.[17] It may be put to uses different from those originally contemplated or shared with other government agencies only if doing so is necessary to fulfill the original purposes of the data collection or to satisfy imperative public needs.[18] Further, individuals have a right to apply to government agencies to ensure that information stored in their government files is accurate and that, in every other way, it is being used in accordance with the law.[19] Enforcement of these privacy guarantees is generally entrusted to an independent privacy agency with the power to hear individual complaints, initiate investigations, and conduct other forms of oversight.[20] The basic aim driving all of these laws is to ensure that as little personal information as possible is floating about the halls of government, and that the personal information that absolutely must be stored in government computers is reliable. If only limited amounts of reliable information are available, the theory goes, abuses of government power are less likely.

Complementing these blanket information privacy laws are laws regulating specific types of government surveillance considered to be especially intrusive. In the United States and Europe, these forms of intrusive surveillance include searches of physical premises, wiretaps of electronic communications, and access to commercial data such as bank

15. *See* 5 U.S.C. § 552a(e)(1) (requiring that personal data be "relevant and necessary" to the agency's purposes); *id.* § 552a(e)(7) (personal data "describing how any individual exercises rights guaranteed by the First Amendment" may not be collected routinely); Convention 108, *supra* note 14, art. 5c (personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are stored"); *id.* art. 6 (identifying types of data considered to be sensitive). The types of personal data that may not be collected routinely are more limited in the United States than in Europe, where information on race, ethnic origin, health status, and other personal characteristics is protected.

16. *See* Convention 108, *supra* note 14, art. 5e. This is the one privacy guarantee for which no U.S. equivalent exists.

17. *See* 5 U.S.C. § 552a(e)(5); Convention 108, *supra* note 14, art. 5d.

18. *See* 5 U.S.C. § 552a(b) (personal information may not be shared with other government agencies without the consent of the individual concerned); Convention 108, *supra* note 14, art. 5b (personal data is to be used only in accordance with the original purposes of the collection of such data).

19. *See* 5 U.S.C. § 552a(d); Convention 108, *supra* note 14, art. 8. Under the U.S. Privacy Act, however, individuals only have the right to demand that their information be corrected—not deleted.

20. *See* COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 106, 108–09 (2003). This is the only major point of difference, in the legislative text, between the United States and Europe. In Europe, enforcement is entrusted to such independent agencies, while in the United States, individuals have the right to sue the government in court for privacy violations.

and calling records.[21] Such surveillance is authorized for law enforcement and intelligence purposes. But the preconditions for collecting personal information are particularly stringent: the government must demonstrate that the information (1) relates to an individual believed to have committed a crime—or in national security cases, an individual who is plotting to do so—and (2) that such information will help prove these claims. This showing must generally be made to an independent magistrate or to an executive official not directly involved in the investigation. Once surveillance is authorized, the accuracy of personal information, and the individual's right to challenge such information, is guaranteed mostly through the law of criminal procedure.

The blanket information privacy laws described earlier generally apply to all government bodies, including police and intelligence agencies. Yet these agencies benefit from significant exemptions given the critical nature of their crime-fighting and national security missions and the importance of personal information—and keeping personal information secret—to accomplishing their missions. Turning to surveillance-specific laws, different standards are created for different types of government activities. Tougher standards are imposed on the police than on intelligence officers because of the different nature and impact of the two types of government action. Whereas the police investigate a concrete set of past events potentially leading to criminal convictions of the objects of surveillance, intelligence officers monitor an inchoate set of individuals and events that might, at some future date, pose a threat to national security. The primary purpose of such intelligence surveillance is disrupting terrorist plots rather than bringing prosecutions.

The extent to which law enforcement and intelligence agencies benefit from double standards, however, varies considerably from one country to another. The main differences between Europe and the United States concern the type of information that may be collected, the uses that may be made of such information, and the right of access to such information.

---

21. On the U.S. side, the principal law on police surveillance is the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522, 2701–2711, 3121–3127 (2000), and the principal law on intelligence-related surveillance is the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801–1862. In Europe, regulation of the police and intelligence agencies is mostly national. To take the German example, the standards applicable to the police are contained in the Code of Criminal Procedure while those applicable to Germany's domestic and foreign intelligence agencies are contained in the G10 Law of 1968. Gesetz zur Beschraenkung des Brief-, Post- und Fernmeldegeheimnisses—Gesetz zu Artikel 10 des Grundgesetzes [Law Restricting the Secrecy of Correspondence of Letters, Mail and Telecommunications—Law Applying to Article 10 of the Constitution], Aug. 13, 1968, BGBl. I at 949 (F.R.G.).

The law in the United States stringently regulates the collection of certain types of information by both police and intelligence officers—for instance what is said in a telephone conversation. The use of such information, however, is not comprehensively regulated, and indeed, since the September 11 attacks, police and intelligence agencies have come under heavy pressure to make wider use of information connected in any way to terrorism through information sharing.[22] Neither is there an individual right to check such information for accuracy unless it is used as part of a criminal or other legal proceeding. Furthermore, in the United States, unless personal information is covered by one of the surveillance-specific statutes, its collection and use goes almost entirely unregulated. That is because of the numerous exceptions for law enforcement and intelligence activities under the Privacy Act.[23] True, most federal agencies do have guidelines that impose general restrictions on intelligence gathering. These guidelines, however, are not enforceable in the courts and, as with privacy legislation, they focus on collection rather than subsequent use and transfer of intelligence.[24]

In Europe, by contrast, the government's access to and use of personal information is regulated as a personal data processing continuum in which no stage is considered more or less harmful than the next.[25] Privacy rights apply throughout. Moreover, privacy principles cover *all* personal information, as opposed to only certain types of especially private information gathered with particularly intrusive means. This broader coverage is a product of constitutional law and blanket data protection laws. Unlike the U.S. Constitution, the European Convention on Human Rights and national constitutions have been interpreted to confer a right to information privacy.[26] All government agencies and all types of per-

22. *Compare* 50 U.S.C. §§ 1802–1811 (requirements for intelligence-related wiretapping), *with* 50 U.S.C. § 1801(h) (restrictions on use of information acquired through intelligence-related surveillance). The main impetus for information-sharing between members of a broadly defined "intelligence community" came from the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 109-279, 118 Stat. 3638 (2004).

23. *See, e.g.*, 5 U.S.C. § 552a(j)–(k) (2007).

24. *See, e.g.*, U.S. DEP'T OF JUSTICE, OFFICE OF LEGAL POLICY, ATTORNEY GENERAL'S GUIDELINES FOR FBI NATIONAL SECURITY INVESTIGATIONS AND FOREIGN INTELLIGENCE COLLECTION (2003), *available at* http://www.usdoj.gov/olp/nsiguidelines.pdf [hereinafter 2003 FBI GUIDELINES].

25. *See, e.g.*, Bundesdatenschutzgesetz [Federal Data Protection Act], Dec. 20, 1990, BGBl. I at 2954, § 1 (F.R.G.).

26. Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221, Europ. T.S. No. 005. *See, e.g.*, Rotaru v. Romania, 2000-V Eur. Ct. H.R. 156 (holding that storage and use of personal information in a police file, together with the refusal of the right of correction, amounts to interference with private life under Article 8); Leander v. Sweden, 116 Eur. Ct. H.R. (ser. A) at 124 (1987) (holding that recording personal details in police files constitutes interference with private life under Article 8); Malone v. United Kingdom, 82 Eur. Ct. H.R. (ser. A) at 289 (1984) (holding

sonal information, therefore, are subject to constitutional privacy norms. And compared to the U.S. Privacy Act, the exceptions for law enforcement and intelligence activities in European data protection laws are more limited.[27]

IV. Privacy in Transnational Intelligence Networks

Intelligence sharing across national borders replicates and magnifies the privacy dangers of personal data processing performed by a single national government. In the transnational context, the danger of deprivations of life, liberty, or property based on inaccurate information is particularly acute. Personal information, in another government's database and organized using a different coding system, is susceptible to misinterpretation. This is a danger that has long been recognized in transferring data sets between agencies within a single government. The so-called practice of data matching—comparing information on an individual in one database with information on that same individual in another database—has led to many episodes of grave injustice in the domestic realm. One common example can be found in the area of welfare policing. In many instances, individuals have been struck off welfare rolls because their income data, collected for purposes different from those of distributing welfare entitlements, wrongly suggested that they were no longer eligible for public assistance.[28]

When such personal information moves not simply from one government agency to another, but from a government agency in one country to a government agency in another country, the danger of government decisions based on inaccurate information is magnified. These agencies are even less likely than agencies at the national level to share the same infrastructure and information technology protocols. And to repeat, in the intelligence domain, the possible wrongful government action is particularly grievous: surveillance, interrogation, detention, deportation, prosecution, or even conviction. Transnational intelligence exchange also triggers the privacy concerns identified earlier. The more

---

that open registers constitute an interference with private life under Article 8). For the German case, see Donald P. Kommers, The Constitutional Jurisprudence of the Federal Republic of Germany 323, 324–25 (2d ed. 1997) (Census Act Case), and for the French case, see CC decision no. 94-352, Jan. 18, 1995, Recs. 2–4 (Loi d'orientation et de programmation relative à la sécurité) and CC decision no. 2004-499DC, July 29, 2004, Rec. 2 (Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel).

27. *See, e.g.*, BGBl. I at 2954, § 19(3); 5 U.S.C. § 552a(j)–(k).

28. *See* Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. Pa. L. Rev. 707, 718 (1987).

widely available personal information is, the greater the danger that governments will harass individuals illegitimately based on their political views, religious beliefs, ethnicity, and so on. The opportunities for oppressive, liberty-destroying government surveillance are also multiplied.

If each national party to a transnational intelligence network adhered to the privacy guarantees discussed earlier, the dangers of transnational information exchange would be manageable. Each national node of the transnational network would guarantee the reliability of personal information and would restrict sharing with other national agencies, thereby reducing the prospect of wrongful uses of personal information.

In the chaotic international realm, however, not all countries adhere to privacy norms and other basic liberties. The right to privacy, therefore, is at the mercy of each and every intelligence agency in the network. Personal information can be collected by one national agency, used by a second for conducting surveillance, and transferred to yet a third for purposes of freezing financial assets or bringing a criminal prosecution. If only one of these many actors violates the right to privacy, individuals are at risk of all the harms identified earlier. All the other participating agencies, though entirely rights-abiding at home, become complicit in this privacy violation: they either supplied the personal information that produced the rights breach or they acted upon bad information, thus compounding the rights breach.

V. THE CASE OF MAHER ARAR

The recent case of Maher Arar offers a rare insight into what can go wrong in the secretive world of networked intelligence when the participating government agencies fail to respect privacy. Maher Arar is a Canadian citizen of Syrian origin who has resided in Canada since he was a teenager.[29] Although he was under surveillance in connection with a Canadian terrorist investigation, there was, and continues to be, no evidence suggesting he constituted a national security threat.[30] On September 26, 2002, he was traveling back to Montreal from Tunisia, a route that took him through John F. Kennedy International Airport in New York. At the airport, U.S. authorities detained him based on information provided by the Royal Canadian Mounted Police.[31] The Canadian

29. COMM'N OF INQUIRY INTO THE ACTIONS OF CANADIAN OFFICIALS IN RELATION TO MAHER ARAR, REPORT OF THE EVENTS RELATING TO MAHER ARAR: ANALYSIS AND RECOMMENDATIONS 27 (2006) [hereinafter ARAR COMMISSION: ANALYSIS AND RECOMMENDATIONS].

30. *Id.* at 9.

31. *Id.* at 30. Since the United States refused to participate in the Canadian inquiry, the Commission was unable to reach a definitive conclusion on this point. The report states, however, that "[i]t is very likely that, in making the decisions to detain and remove Mr. Arar to

government subsequently found this information to be inaccurate. A week later, on October 7, 2002, U.S. authorities deported Arar to Syria without any warning to the Canadian government. (Arar is also a Syrian citizen.) According to the deportation order of the Regional Director of the U.S. Immigration and Naturalization Service, the evidence "clearly and unequivocally reflects that Mr. Arar is a member of a foreign terrorist organization, to wit Al Qaeda."[32] Once in Syria, Arar was transferred to Syrian Military Intelligence, in whose custody he remained for almost one year. Only on October 5, 2003 was Arar released to the Canadian consul in Damascus.[33] During the first weeks of Arar's detention he was tortured.[34] Subsequently, according to the report of the Canadian Commission of Inquiry appointed to investigate the events,

> [w]hile the physical beatings had ended . . . the conditions of his imprisonment in the Palestine Branch [of Syrian Military Intelligence] . . . had been abysmal. He had been confined in a tiny cell with no natural light. He had slept on the floor and endured disgusting sanitary conditions. Mr. Arar had suffered enormously. He continues to experience the after-effects to this day.[35]

This set of events was the product of a transnational intelligence network. There is a long history of collaboration between the Royal Canadian Mounted Police (RCMP) and U.S. intelligence and law enforcement agencies. In the days following the September 11 attacks, however, Canadian and U.S. officials met and verbally agreed to improve such cooperation with what was known as a "free-flow-of-information agreement."[36] The agreement abandoned the numerous official protocols that had retarded or impeded information sharing in the past. Soon afterwards, Arar came to the attention of the RCMP when he was observed meeting with Abdullah Almalki, the target of a terrorist investigation. The meeting prompted an investigation of Arar during which Canadian officials shared information with U.S. authorities pursuant to the earlier free-flow-of-information agreement. As extensively documented by the Commission of Inquiry, much of the information on Arar turned out to be inaccurate and misleading. It was this very information that led the

---

Syria, the U.S. authorities relied on information about Mr. Arar provided by the RCMP. Although I cannot be certain without the evidence of the American authorities, the evidence strongly supports this conclusion." *Id.*

32. Jules Lobel, Op-Ed, *The Arar Report: The US Should Follow Canada's Lead*, JURIST, Sept. 26, 2006, http://jurist.law.pitt.edu/forumy/2006/09/arar-report-us-should-follow-canadas.php.

33. ARAR COMMISSION: ANALYSIS AND RECOMMENDATIONS, *supra* note 29, at 45.

34. *Id.* at 32.

35. *Id.* at 45.

36. ARAR COMMISSION: FACTUAL BACKGROUND I, *supra* note 3, at 38.

U.S. Immigration and Naturalization Service to conclude that Arar was a member of al Qaeda and to wrongfully deport him to Syria.

Although a complete chronicle of these missteps is beyond the scope of the current discussion, some specific examples will illustrate the risks inherent in intelligence sharing. In late October 2001, the RCMP requested both a Canadian and a U.S. border lookout for Arar. In both requests, the RCMP indicated that Arar was part of a "group of Islamic Extremist individuals suspected of being linked to the Al Qaeda terrorist movement,"[37] a claim supported only by the observation that Arar and Almalki had met at a café and had walked together in the rain for twenty minutes. Although the Commission of Inquiry agreed that the request for a border lookout was reasonable, it deemed the identification of Arar with al Qaeda "inaccurate and potentially inflammatory." Later, as chronicled by the Commission of Inquiry,

> Project A-O Canada [the RCMP division responsible for the Arar investigation] provided documents to the American agencies that variously described Mr. Arar as a suspect, a target, a principal subject of its investigation, a person with an "important" connection to Mr. Almalki, a person directly linked to Mr. Almalki in a diagram titled "Bin Laden's Associates: Al Qaeda Organization in Ottawa," and a business associate or a close associate of Mr. Almalki.
>
> These descriptions were either completely inaccurate or, at a minimum, tended to overstate Mr. Arar's importance in the Project A-O Canada investigation. I repeat that Project A-O Canada's view was that Mr. Arar was never a suspect—he was merely a person of interest. While it might be that, in meetings, the Project's officers communicated this actual view of Mr. Arar's status in the investigation, there was no justification for the improper and unfair labels attached to him in written documents.[38]

In the hands of the U.S. authorities, these inaccurate and unfair labels had consequences that were entirely unforeseen by the Canadian officers at the time the intelligence was originally gathered.

On the Canadian side, much of the blame for this disastrous chain of events rests with the post-September 11 free-flow-of-information agreement. In that agreement, the RCMP abandoned the privacy policies that ordinarily would have governed national security investigations. These

37. ARAR COMMISSION: ANALYSIS AND RECOMMENDATIONS, *supra* note 29, at 20–21.
38. *Id.* at 25.

official policies seek to assure the reliability of personal information and to restrict the sharing of such information—aims that should be familiar from the earlier discussion of privacy harms and legal remedies. In theory, whenever the RCMP gathers information in national security investigations, it must be assessed and rated for reliability on a scale of "reliable," "believed reliable," "unknown reliability," or "doubtful reliability."[39] When sharing such information with other agencies, the reliability rating must be attached. In addition, classified information—which includes practically all the information gathered in a national security investigation—may be shared with other agencies only on a "need-to-know basis." In other words, the officers involved must be satisfied that such information will assist with an ongoing investigation before releasing it. If a decision is made to share classified information with other agencies, domestic or foreign, the information must contain a written "caveat." That caveat prohibits the receiving agency from sharing the information without the consent of the RCMP and, in those instances in which the information is transferred to a foreign agency, limits the use of the information to the "intelligence community" of the foreign country.[40]

Because of the post-September 11 decision to dispense with standard privacy protocols, there were none of the red flags that ordinarily would have signaled the highly dubious connection between Arar and extremist terrorism. The Canadians failed to indicate the low reliability of the intelligence on Arar. They further failed to communicate that the information was to be used only by the U.S. intelligence community, not by a U.S. immigration agency with the power to detain and deport individuals.

The blame naturally does not rest entirely with the Canadian node of the transnational intelligence network. On the U.S. side too, privacy law failed. As explained earlier, when an intelligence agency uses personal information like Arar's, it is entirely free of the legal requirements imposed by the U.S. Privacy Act. Like the Canadian RCMP, U.S. intelligence agencies are governed by internal privacy policies. The officers from the Federal Bureau of Investigation (FBI) responsible for Arar's case would have been covered by the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigation (the Guidelines), replaced in 2003 by a modified set of guidelines.[41] Of course, the Guidelines might have been suspended or modified following the September 11 attacks. But even if the Guidelines had been fully opera-

39. *Id.* at 324.
40. ARAR COMMISSION: FACTUAL BACKGROUND I, *supra* note 3, at 31.
41. *See generally* 2003 FBI GUIDELINES, *supra* note 24.

tive, it does not appear that the information privacy lapses would have been caught. Both the pre- and post-2003 versions of the Guidelines focus largely on limiting the circumstances under which information may be collected. What happens to that information after collection receives little attention. Thus, the Guidelines impose no duty to ensure information reliability or to code such information based on different levels of reliability, as required by the Canadian system.[42]

The Guidelines do regulate the sharing of personal information with other federal and state agencies, albeit less so today than under the pre-2003 version. But even the more robust sharing restrictions contained in the pre-2003 Guidelines would not have applied to Arar: only U.S. citizens and permanent residents of the United States are covered and therefore, even under the pre-2003 Guidelines, information on Arar could have been used "for any lawful purpose."[43] The intelligence officers responsible for Arar's deportation, therefore, were under no duty to verify independently that the Canadian intelligence was reliable. Nor were they required to refrain from communicating sketchy intelligence to powerful law enforcement and immigration agencies.[44]

Of course, privacy was not the only right the U.S. node of the transnational intelligence network violated.[45] Rather than bring a

42. Recently, however, the reliability requirement has been adopted as part of another set of guidelines applicable to the entire intelligence community, including the FBI. *See* PROGRAM MANAGER, INFO. SHARING ENV'T, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, 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 5 (2006), *available at* http://www.ise.gov/docs/ise%20privacy%20guidelines%2012-4-06.pdf.

43. ATTORNEY GEN., GUIDELINES FOR FBI FOREIGN INTELLIGENCE COLLECTION AND FOREIGN COUNTERINTELLIGENCE INVESTIGATIONS 25 (1995), *available at* http://www.fas.org/irp/agency/doj/fbi/terrorismintel2.pdf.

44. Indeed, since September 11, intelligence officers are under the reverse duty: they must freely share terrorism-related intelligence with all members of the intelligence community. The intelligence community is comprised of intelligence, law enforcement, and immigration agencies at the federal, state, and local levels. *See* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004).

45. Interpol provides an illustration of these same privacy harms in the context of a multilateral, as opposed to bilateral, network. *See* About Interpol, http://www.interpol.int/public/icpo/default.asp. Interpol is an international police organization charged with, among other things, managing a system of international notices for its 186 member states. This system enables member countries to issue notices requesting the arrest of wanted individuals, information on criminal suspects, the identification of missing persons, and other types of action in the organization's other member countries. Interpol is responsible for communicating these notices to national police, and although national police are not legally bound to comply, they very often do take the requested action.

In a number of cases, member governments have abused the system by posting arrest notices for individuals wanted not for their criminal acts but for their political views, causing these individuals to be detained wrongfully by the police in other countries. *See generally* Charles R. Both, *International Police Force or Tool for Harassment of Human Rights Defend-*

criminal prosecution or deport Arar to Canada, U.S. authorities deported Arar to Syria; they delivered him into the custody of the Syrian Military Intelligence Service, where the likelihood of human rights abuses was high, to say the least. Although this example of the post-September 11 practice of extraordinary renditions falls outside the scope of this Article, it bears mentioning. It underscores the consequences of bad Canadian intelligence in the hands of another country's intelligence agency that failed to respect not simply privacy but human rights more generally.

The Canadian Commission of Inquiry aptly dubbed these liberty dangers the "ripple effect" of transnational information sharing. It is worthwhile repeating in full the lessons drawn by the Commission from Mr. Arar's case:

> sharing information from investigations in Canada with other countries can have a "ripple effect" beyond Canada's borders, with consequences that may not be controllable from within Canada. The legal power of Canadian courts and governments to require respect of constitutional rights and freedoms is exercised within Canada's territorial borders. Once a person or information moves outside of Canada, it becomes difficult to ensure treatment of that person or information in accordance with Canadian constitutional rights and values . . . .
>
> Canadian investigators may receive and act upon information from other countries. Use of this information may have significant personal consequences for individuals in Canada and their associates such as investigation, surveillance, arrest or prosecution. In some instances, such information may have been acquired in ways inconsistent with rights and freedoms protected here. For example, it may have been obtained through torture or other unacceptable investigation techniques, or in the absence of checks and balances to ensure reliability.[46]

The Commission therefore recommended establishing an independent review body with the power to conduct privacy and civil liberties investigations and to hear individual complaints. This review body would

---

ers and Political Adversaries: Interpol's Rift with the Human Rights Community, 8 ILSA J. INT'L & COMP. L. 357 (2002). In other words, law enforcement agencies that use information on their citizens to harass them at home have taken advantage of the Interpol network to harass them abroad. Similarly, member countries might legitimately request additional information on criminal suspects through the notice system, but the identification of suspects might lead receiving member countries not only to, say, search their criminal databases for entries under the suspect's name, but also to engage in illegitimate, illiberal harassment of those suspects.

46. ARAR COMMISSION: ANALYSIS AND RECOMMENDATIONS, *supra* note 29, at 431.

have jurisdiction only over the RCMP's national security activities. Oversight of other intelligence agencies would be left to other government watchdogs.[47] One important task of the review body would be to guarantee that the RCMP's privacy protocols were strictly followed in exchanging information with domestic and foreign agencies,[48] and that special policies were developed—and followed—when sending or receiving information from countries with poor human rights records.[49]

VI. REDESIGNING TRANSNATIONAL INTELLIGENCE NETWORKS TO PROTECT PRIVACY

Europe contains useful insights for protecting innocent individuals like Maher Arar caught in the web of transnational intelligence gathering. The European experience with government by network, including intelligence networks, is the longest and richest of any region in the world.[50] That is because European integration has proceeded not through the transfer of national sovereignty to a federal center, but through the sharing and pooling of sovereignty in the network form of governance. With this experience comes a host of institutional and legal mechanisms for promoting rights and democratic accountability in transnational networks.

Although these mechanisms have not always succeeded, European legislators have had ample opportunity to experiment with institutional design, particularly with regard to safeguarding the right to information privacy. In contrast with the United States, where information privacy is recognized only as a statutory, not a constitutional right, in Europe information privacy is considered a fundamental right no less vital than more traditional rights such as freedom of expression and the right to property.[51] Therefore, when establishing transnational networks, European legislators are under a constitutional duty to protect the right to information privacy.

47. *Id.* at 503.

48. *Id.* at 521.

49. *Id.* at 522.

50. *Cf.* Francesca Bignami, *Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network*, 26 MICH. J. INT'L. L. 807, 813–19 (2005).

51. Convention for the Protection of Human Rights and Fundamental Freedoms, *supra* note 26, art. 8. *See, e.g.*, Rotaru v. Romania, 2000-V Eur. Ct. H.R. 156 (2000) (holding that storage and use of personal information in a police file, together with refusal of right of correction, amounts to interference with private life under Article 8); Leander v. Sweden, 116 Eur. Ct. H.R. (ser. A) at 124 (1987) (holding that recordation in a secret register coupled with a refusal to allow review and refutation constitutes interference with private life under Article 8); Malone v. United Kingdom, 82 Eur. Ct. H.R. (ser. A) at 289 (1984) (holding that open registers constitute an interference with private life under Article 8).

There are a number of intelligence networks in Europe. Three prominent examples were mentioned earlier: Europol, Schengen, and an EU law on information exchange among national police forces. Of these, Europol offers the best illustration of the different possibilities for safeguarding privacy in transnational networks whose reach extends beyond Europe. Because Europol is a self-contained system, privacy rights are built directly into it rather than scattered throughout the different laws, regulations, and judicial decisions of the European Union. Furthermore, as a form of network that relies both on the nodes and the center to provide intelligence, privacy must be protected in the work of both actors—the participating national agencies and the central office. As a result, the privacy architecture of Europol is the most comprehensive of all three networks.

Under the Europol Convention, both national police authorities and the central office are held to data protection standards. The Convention requires each national participant to adopt the standards of the Council of Europe Convention on Personal Data Processing into its domestic law.[52] Without implementation, a state cannot enter information into or extract information from the Europol system. In other words, without a regulatory scheme for information privacy, that state is denied access to an extremely valuable resource in fighting cross-border crime. To guarantee privacy compliance by national police, each state is required to establish an independent national supervisory body with adequate oversight powers.[53] Similarly, the network center—the central office in The Hague—is bound by the privacy principles of the Council of Europe Convention on Personal Data Processing.[54] Compliance at the center is likewise guaranteed by a special-purpose independent supervisory body established under the Europol Convention and known as the Joint Supervisory Body.[55]

The network nodes and the network center are also held to a number of specific data protection guarantees articulated in the Europol Convention. As explained earlier, Europol is responsible for three different sets of information: the EIS, work files created to assist with specific national investigations, and an index system designed to make the information in the work files readily available. Under the Europol Convention, such information may only be used to combat specifically listed crimes.[56] The

52. Europol Convention, *supra* note 5, art. 14.
53. *Id.* art. 23.
54. *Id.* art. 14.3.
55. *Id.* art. 24.
56. *Id.* art. 8.

party that inputs personal data into one of the systems must also ensure that the data is accurate and up-to-date.[57]

Information in the different systems may be retained only as long as necessary to accomplish the crime-fighting purposes for which it was originally entered into the system. In fact, the Convention goes further: it establishes a specific three-year baseline for retention of personal data. Every three years, the national authorities responsible for entering information into the EIS must review that information to guarantee that it is still serving the original investigative purpose. If a national authority fails to make a decision in favor of retention, the information is automatically deleted from the EIS. By contrast, the information contained in work files and cross-referenced in the index system *must* be deleted after three years. That three-year period, however, may be renewed if the Director of Europol finds the information "strictly necessary" for the criminal investigation that originally led to the creation of the work file.[58] Indeed, when a work file is initially created, the Joint Supervisory Authority has the power to review the file to ensure that the planned collection and analysis of personal information accords with privacy principles.[59]

Individuals have a right to check on their information to learn whether they are covered by any of Europol's three systems. If such information exists, individuals have the right to have any inaccurate information corrected or, if it was collected and processed in contravention of data protection principles other than accuracy, to have it deleted. Individuals must file such requests with their national data protection body, which then forwards the requests to Europol. After checking the information, Europol replies directly to the individual, who can appeal to the Joint Supervisory Body if she is not satisfied with the reply.[60] The Europol Convention contains yet another privacy guarantee: to facilitate oversight by the Joint Supervisory Body, retrievals of personal information by the central office from the three systems must be recorded. In the case of the EIS, each retrieval must be documented; in the case of the other two systems, one out of every ten retrievals, at a minimum, must

57. *Id.* art. 15.

58. *Id.* art. 21, *amended by* Council Act of 27 November 2003 drawing up, on the Basis of Article 43(1) of the Convention on the Establishment of a European Police Office (Europol Convention), a Protocol Amending that Convention, 2004 O.J. (C 2) 1.

59. *Id.* art. 12.

60. *Id.* arts. 19–20. *See, e.g.*, EUROPOL JOINT SUPERVISORY BODY, THE SECOND ACTIVITY REPORT OF THE EUROPOL JOINT SUPERVISORY BODY 21–26 (2005), *available at* http://europoljsb.consilium.europa.eu/documents/45EA1FE4-5DAA-41ED-9356-FA169E5B0800.pdf; EUROPOL JOINT SUPERVISORY BODY, EUROPOL ACTIVITY REPORT 38–42 (2003), *available at* http://europoljsb.consilium.europa.eu/documents/12FE0898-A493-4E30-A2D7-D606D2D3C280.pdf.

be documented.[61] Lastly, national authorities and the central office are required to implement technical measures to protect Europol's information systems against unauthorized use and to enable recordkeeping.[62]

These specific provisions should be familiar from the earlier discussion of national information privacy law. The limitation on the purposes for which personal information may be used, the requirement of accuracy, the specification of a time period for data retention, and the need for security measures all have their equivalents in national law. Likewise, the different oversight mechanisms—the right to check on personal information held by Europol and independent supervisory bodies—have national counterparts.

A second type of data protection guarantee was created in the Europol Convention, applicable not to the immediate circle of network participants but to an outer circle of nonsignatory states. Under the Europol Convention, personal information may be transferred to third countries to assist with specific investigations involving terrorism, drug trafficking, counterfeiting, and any of the other crimes covered by the Convention. Third countries, however, must ensure an adequate level of data protection before personal information may be transferred.[63] Adequacy does not signify an identical set of privacy rights, but it does entail legislation that broadly tracks the guarantees of the Council of Europe Convention on Personal Data Processing and that is subject to enforcement by an independent government body. Only in "exceptional cases," in which the Director of Europol considers the transfer of personal information "absolutely necessary to safeguard the essential interests of the Member States," or "in the interests of preventing imminent danger associated with crime," can the requirement of adequacy be waived.[64] On the receiving end, when information is received from third countries, it must be checked independently by Europol's central office for reliability and lawfulness.[65]

Europol's laws and practices illustrate two fundamentally different sets of privacy guarantees available to intelligence networks. First, all participants can be required to adhere to the same multilateral privacy standards. Those standards might be written into the agreement on intelligence exchange or contained in an international instrument distinct

61. Europol Convention, *supra* note 5, art. 16.

62. *Id.* art. 25.

63. *Id.* art. 18.

64. *Id.*, *amended by* Council Act of 27 November 2003 Drawing Up, on the Basis of Article 43(1) of the Convention on the Establishment of a European Police Office (Europol Convention), a Protocol Amending that Convention, 2004 O.J. (C 2) 1.

65. *Id.* art. 15; Council Act of 3 November 1998 Laying Down Rules Concerning the Receipt of Information by Europol from Third Parties, 1999 O.J. (C 26) 17.

from the agreement. The Europol Convention makes use of both possibilities: the parties must implement the general guarantees of the Council of Europe Convention on Personal Data Processing as well as the specific provisions of the Europol Convention. Once all the parties adhere to these same privacy standards, information can be exchanged freely. In fact, under the Europol Convention and similar agreements, the parties are under a *duty* to share information that can assist the other parties in preventing crime and threats to national security. In addition, the network center—Europol's central office—is subject to nearly identical privacy duties.

Second, each network participant can unilaterally adopt privacy norms and unilaterally enforce those norms against sub-standard network participants. Before one network party transfers information to another network party, it may require that privacy assurances be given by the receiving party. Likewise, when one network party receives information from another network party, it may independently guarantee the reliability and lawfulness of that information. This is the mechanism created in the Europol Convention for relations with third countries, the outer-circle of the information-exchange network. Indeed, this form of unilateral enforcement of privacy standards by domestic intelligence agencies was recommended by the Canadian Commission of Inquiry to avert another case such as Arar's.[66]

The disadvantages of this second type of privacy guarantee are obvious: each privacy-abiding party to an intelligence network is required to review routinely the privacy arrangements of the other parties to the network with whom information is shared. Such privacy checks can stall the free exchange of information on serious crime and terrorism, the very *raison d'être* of such networks. A multilateral instrument, therefore, would appear to be a preferable mechanism for guaranteeing privacy in the work of intelligence networks.

VII. CONCLUSION

Liberal societies that permit their governments to conduct free–ranging surveillance risk sinking rapidly into illiberalism. That much is part of the philosophical and legal canon of liberal democracy. The danger of surveillance through the collection and combination of electronic data is also widely perceived—albeit somewhat more dimly—than that

66. *See* ARAR COMMISSION: ANALYSIS AND RECOMMENDATIONS, *supra* note 29, at 101–27, 343–44 (recommending that Canadian information privacy guarantees be imposed on information transferred to U.S. intelligence agencies); *id.* at 344 (recommending that caution be used in information transfers to or from countries with questionable human rights records).

of surveillance through conventional means. But the consequences of globalization for government surveillance and liberal rights are poorly understood. How does the right to privacy fare in today's borderless world of national security threats and networked spy agencies?

The answer to this question requires a careful assessment of both the values underpinning the right to privacy and the nature of transnational intelligence networks. Through privacy, liberal societies advance a number of goals: avoiding wrongful government determinations based on unreliable information, preventing the use of personal information for purposes of suppressing basic rights, and, most fundamentally, promoting individual autonomy. Whenever government agencies collect, combine, and utilize personal information, these privacy interest are put at risk. But the sharing of intelligence transnationally raises special concerns. Foremost among these is the danger that one or more of the state parties to the intelligence network will fail to respect privacy and other basic liberties. If only one of the many different national agencies that exchange personal information breaches privacy, the rights of citizens everywhere are compromised.

One place to look for a constructive response to the liberal flaw of transnational networks is Europe. For a number of years, police and intelligence agencies have exchanged information as members of Europe-wide networks. In these networks, two types of privacy safeguards have been adopted: multilateral standards, to which all the network parties must adhere, and unilateral standards, applicable under the law of only one of the parties and enforced against all the other parties by erecting barriers to information exchange with sub-standard parties. Because multilateral standards both promote government cooperation and advance liberal rights, they appear to hold the greatest promise for networks that extend beyond Europe.

Of course, it might not be possible to agree on common privacy standards or, even assuming agreement, guarantee effective implementation of such standards at the national level. It is well known that the United States and the European Union differ on a number of important points of privacy law, with the European Union favoring stricter limitations on government use of personal information. Furthermore, even though states might sign up to information privacy standards, they might not implement or enforce them, a problem common to many international human rights regimes.

Notwithstanding these obstacles, given the critical public mission of transnational intelligence networks, it seems well worth the effort to attempt to reach consensus on privacy norms. After all, it is hard to disagree with the fundamental purposes of information privacy. Who

objects to preventing wrongful determinations based on unreliable information, protecting liberal rights from officious government meddling, and defending individual autonomy from Orwellian government surveillance? It does not seem far-fetched to think that, in the future, agreement might be reached on the law necessary to promote such liberal aims in the networked world of government intelligence gathering.

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.[1] 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.[2] 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.[3] 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

[1] Robert Gellman, Does Privacy Law Work? in Technology and Privacy: The New Landscape (Philip E. Agre & Marc Rotenberg eds., 1997).
[2] 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).
[3] 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.[4] 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.[5] 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.[6]

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.[7]

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.

---

[4] 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).

[5] 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).

[6] 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).

[7] 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.[8] 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).[9] When information is collected from individuals, they must be told of the nature of the government database.[10] 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).[11] 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.[12] Personal information stored by government agencies must be accurate, relevant, timely, and complete.[13] The Privacy Act prohibits information from being shared with another government agency without the consent of the person concerned.[14] It requires that technical measures be adopted to guarantee the security and confidentiality of the information.[15] And it gives individuals the right to check their personal information and, if necessary, demand that their information be corrected.[16]

To review briefly the parallel provisions of the Council of Europe Convention: Personal data processing must be "fair and lawful."[17] The Convention requires that personal data "be adequate, relevant and not excessive in relation to the purposes for which they are stored." [18] 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.[19]

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

---

[8] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe Treaties No 108 (Jan 28, 1981).
[9] 5 U.S.C. § 552a(e)(4).
[10] 5 U.S.C. § 552a(e)(3).
[11] 5 U.S.C. § 552a(e)(1).
[12] 5 U.S.C. § 552a(e)(7).
[13] 5 U.S.C. § 552a(e)(5).
[14] 5 U.S.C. § 552a(b).
[15] 5 U.S.C. § 552a(e)(10).
[16] 5 U.S.C. § 552a(d).
[17] Convention, art. 5a.
[18] Convention, art. 5c.
[19] 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.
[20] Convention, art. 5d.

incompatible with those purposes.[21] 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."[22] It also contains a "participation principle"[23] 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." [24] 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.[25] 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

[21] Convention, art. 5b.
[22] Convention, art. 7.
[23] 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.
[24] Convention 108, art. 5e.
[25] 5 U.S.C. § 552a(j).

interest of national defense or foreign policy, and more.[26] 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.[27]

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.[28] 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.[29] 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.[30] 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.[31] Therefore, a database containing personal details on millions of citizens may not be covered at all by the Privacy Act.[32]

B. *Enforcement of Privacy Rights*

---

[26] 5 U.S.C. § 552a(k).
[27] *See, e.g.*, Williams v. Dept. Veterans Affairs, 104 F.3d 670 (4th Cir. 1997).
[28] *See* National Security Agency/Central Security Service Privacy Act Program, 32 C.F.R. pt. 322 (2006).
[29] 5 U.S.C. § 552a(b)(7).
[30] 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).
[31] *See, e.g.*, Williams v. Dept. Veterans Affairs, 104 F.3d 670, 675 (4th Cir. 1997); Henke v. Dept. Commerce, 83 F.3d 1453, 1459-62 (D.C. Cir. 1996).
[32] 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.[33] In addition, government officials may be criminally prosecuted for certain violations of the Privacy Act.[34]

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.[35]

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.[36] This is a welcome development. Yet, as will be discussed, these privacy officers are not functional equivalents of

[33] 5 U.S.C. § 552a(g).
[34] 5 U.S.C. § 552a(i).
[35] 5 U.S.C. § 552a(g)(4).
[36] 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.[37] 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.[38] 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.[39]

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.[40] 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."[41] 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[42] and the Civil Liberties Protection Officer, who reports directly to the Director of National Intelligence.[43] 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,[44]

---

[37] Homeland Security Act, 6 U.S.C § 142.
[38] 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.
[39] 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).
[40] 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.
[41] 6 U.S.C. § 485(d).
[42] 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).
[43] *Id.* 35.
[44] *Id.* 38.

those of the Civil Liberties Protection Officer to enforcement of privacy and other types of rights.[45] 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.[46] 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.[47] 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.[48] 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.[49] Likewise, the Civil Liberties Protection Officer is appointed by the Director of National Intelligence and can be removed at will .[50] The five members of the Civil Liberties and Oversight Board are appointed by the President

[45] *Id.* 48-49.
[46] 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.
[47] Consolidated Appropriations Act 2005, Pub. L. No. 108-447, § 522, 118 Stat. 3268, 3268-70 and 5 U.S.C. § 552a note (2000).
[48] 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.
[49] 6 U.S.C. § 142.
[50] 50 U.S.C. § 403-3d.

and serve at his pleasure.[51] 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.[52] 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

[51] 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.

[52] 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.