2014

# The Data Surveillance State in Europe and the United States

Joel Reidenberg
*Fordham University School of Law*, JREIDENBERG@law.fordham.edu

# THE DATA SURVEILLANCE STATE IN THE UNITED STATES AND EUROPE

*Joel R. Reidenberg*[*]

## INTRODUCTION

Europe and the United States recognize privacy as a fundamental pillar of democracy. The U.S. Constitution enshrines protection against state intrusions,[1] and the Charter of Fundamental Rights of the European Union ("Charter") as well as the European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR") each mandate that law and public authorities not interfere with "private life."[2] Over the last decade, however, law in Europe and the United States has progressively strengthened the ability of public authorities to obtain communications data at the expense of privacy. The justification for these incursions is often framed in terms of liberty and freedom, namely that public safety is a condition of liberty and freedom and that the protection of public safety necessitates the narrowing of privacy protections.

This Essay will focus on communications data—namely the transactional and geolocation information associated with network interactions. The thesis is that government data surveillance law in Europe and the United States has reached a turning point for the future of information privacy online. The democracies on both sides of the Atlantic are trying to balance the legitimate needs of public authorities to access online transactional data with the basic rights

---

* Microsoft Visiting Professor of Information Technology Policy, Princeton University; Stanley D. and Nikki Waxberg Chair and Professor of Law, Fordham University School of Law. This Essay began as the 6th Annual Berkeley Privacy Law Lecture. I am grateful to and would like to thank Axel Arnbak, Anu Bradford, Robert Gellman, Angus Johnston, Christopher Millard, Paul Schwartz, Stephen Wm. Smith, Alexander Tsesis, Kurt Wimmer and the participants at the Berkeley Lecture, the Princeton CITP Luncheon Series, and the *Wake Forest Law Review* Symposium for their comments.

1. U.S. CONST. amend. IV.

2. Charter of Fundamental Rights of the European Union, art. 6–8, 2000 O.J. (C 364) 1 [hereinafter Charter]; Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter ECHR].

of citizens to be free from state intrusions on their privacy. In Europe, for example, the European Commission notes that

> [l]aw enforcement authorities in most EU States have reported that retained data play a central role in their criminal investigations. These data have provided valuable leads and evidence that have resulted in convictions for criminal offences and in acquittals of innocent suspects in relation to crimes which, without an obligation to retain these data, might never have been solved.[3]

But, as illustrated by the U.S. government's massive collection of telecommunications data;[4] by the UK tapping of transatlantic telecommunications cables;[5] by the Swedish government's warrantless wiretap authority;[6] and by the wiretapping of journalists in France,[7] democratic societies have created a technological infrastructure of surveillance with a legal infrastructure of surveillance authorizations. In effect, the legal framework that each system has established will not be able to preserve, over the long term, citizen privacy and basic democratic values.

This Essay starts with a short overview of the basic rules for data retention and access on both sides of the Atlantic, including the special privileges accorded to national security claims. The rules lead to an assessment of the key intractable problems for citizen privacy of proportionality requirements, the privatization of state surveillance activity, and security oversight. The Essay next looks at how the reliance on proportionality and private actors fundamentally undermines the preservation of online privacy. The

---

3. *See What We Do: Data Retention*, EUR. COMMISSION HOME AFFAIRS, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/index_en.htm (last visited Jan. 31, 2014).

4. *See, e.g.*, Charlie Savage, *Broader Sifting of Message Data by N.S.A. Is Seen*, N.Y. TIMES, Aug. 8, 2013, at A1.

5. Tony Patterson, *Germany Prepares to Charge UK and US Intelligence over Fresh Bugging Allegations*, INDEP. (June 30, 2013), http://www.independent.co.uk/news/world/europe/germany-prepares-to-charge-uk-and-us-intelligence-over-fresh-bugging-allegations-8680249.html.

6. *Sweden Approves Wiretapping Law*, BBC NEWS (June 18, 2008), http://news.bbc.co.uk/2/hi/europe/7463333.stm.

7. Samuel Laurent, *Ecoutes de l'Elysée: du dementi a l'aveu* [*Elysée Wiretapping: From Denial to Confession*], LE MONDE (last updated Jan. 31, 2013), http://www.lemonde.fr/politique/article/2011/09/01/ecoutes-de-l-elysee-du-fantasme-a-l-aveu_1566117_823448.html; *see also* Jacques Follorou & Johannes Franck, *Révélations sur le Big Brother français* [*Disclosures of the French Big Brother*], LE MONDE (last updated July 7, 2013), http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html (reporting on the sharing of metadata within the French intelligence agencies).

Essay concludes with three proposals to revive privacy as necessary in democracy: (1) strengthening explicit limits on collection and storage of information with strict and specific limits on access, (2) establishing transparency of data access, and (3) establishing transparency of public security access combined with penalties for accountability.

## I. BASIC RULES

The United States and European approaches to data retention and access reflect important systemic differences between legal systems on the two continents. United States law is essentially silent on data retention but regulates access to data held in the private sector by public authorities.[8] This tracks the United States legal system's implementation of privacy rights that restrain state power and focus on individualistic freedoms.[9] By contrast, Europe extensively regulates the collection and retention of data by the private sector and focuses less on access restraints by public authorities. Europe's approach implements privacy rights through a governance model that looks to state power as the protector of citizens and emphasizes the regulation of all aspects of data processing.[10] Incongruously, at the same time, European data protection focuses less attention on the means of access by public authorities.[11]

### *A. Retention*

United States law does not impose a general data retention requirement. The only exception is in the context of telecommunications billing. Through a narrowly defined telecommunications regulation, U.S. law mandates that telephone toll records be retained for at least eighteen months in order for consumers to be able to dispute bills.[12] There is no requirement for deletion at the end of that time.

Communications service providers in the United States, however, have increasing incentives to retain traffic and location

8. Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1345 (2000).

9. *See id.* at 1344–49.

10. *Id.* at 1349–54.

11. Member-state constitutional regimes and the ECHR, as higher law, may however contain checks on state access to privately held data.

12. *See* 47 C.F.R. § 42.6 (2012) (stating that carriers that offer or bill toll telephone service "shall retain for a period of 18 months such records as are necessary to provide the following billing information about telephone toll calls: the name, address, and telephone number of the caller, telephone number called, date, time and length of the call").

data for data mining programs and for commercial revenue.[13] The most popular websites routinely collect and retain users' traffic data for commercial purposes.[14] Service providers typically retain communications data for long periods of time.[15] Yahoo, for example, stores Yahoo group activity log information for as long as a group is active—in other words, for a potentially unlimited time period.[16]

Europe, by contrast, has a complex set of rules applicable to data retention. The basic framework set out in Directive 95/46/EC that entered into force in 1995 (the "Data Protection Directive") prohibits the storage of data beyond the duration required to fulfill the purposes of data collection.[17] The obligations apply to all data processing and are not limited to any particular sector. As a framework approach, the Data Protection Directive does not provide any specific guidance for transaction and geolocation information. Seven years later, the European Union adopted Directive 2002/58/EC (the "E-Privacy Directive") to apply the general principles of the Data Protection Directive to the "electronic communications" sector.[18] The E-Privacy Directive provides that "traffic data relating to subscribers and users . . . must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication,"[19] but can be retained for certain

---

13. *See* 4syth.com, *For Big Data Analytics There's No Such Thing as Too Big*, FORSYTH COMMS. (Mar. 2012), http://www.cisco.com/en/US/solutions/ns340/ns517/ns224/big_data_wp.pdf.

14. *See* Ashkan Soltani et al., Flash Cookies and Privacy 3 (August 10, 2009) (unpublished manuscript), *available at* http://ssrn.com/abstract=1446862 (reporting that 50% of popular websites use clandestine flash cookies to track users).

15. *See, e.g.*, *Cell Phone Location Tracking Request Response—Cell Phone Company Data Retention Chart*, ACLU, https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart (last visited Jan. 31, 2014) (chart produced by the U.S. Department of Justice and released to the ACLU in response to a document request).

16. *See Compliance Guide for Law Enforcement*, YAHOO! 5, https://www.eff.org/sites/default/files/filenode/social_network/Yahoo_SN_LEG-DOJ.pdf.

17. Directive 95/46/EC, of the European Parliament and of the Council, art. 6, 1995 O.J. (L 281) 31 (EC) [hereinafter Data Protection Directive].

18. The European Community and Parliament adopted another directive in 1997 that applied the Data ProtectionDirective to the telecommunications sector. *See* Directive 97/66/EC, of the European Parliament and of the Council, art. 1, 1997 O.J. (L 024 30) 1 (EC) (concerning the processing of personal data and the protection of privacy in the telecommunications sector). This 1997 directive, however, did not address the data retention issue. *See generally* Christopher Millard, *Communications Privacy*, *in* IAN WALDEN, TELECOMMUNICATIONS LAW AND REGULATION 605 (4th ed. 2012).

19. Directive 2002/58/EC, of the European Parliament and of the Council, art. 6(1), 2002 O.J. (L 201) 37 (EC) [hereinafter E-Privacy Directive].

limited marketing purposes.[20] Traffic data can also be stored "for purposes of subscriber billing and interconnection payments" only so long as the bill may be challenged or payment pursued.[21] In all, the directives create a model that limits the duration and scope of data retention.

At the time of adoption, though, neither the Data Protection Directive nor the E-Privacy Directive applied to law enforcement.[22] This exclusion was necessary because the Maastricht Treaty,[23] then in force, did not provide for European Community competence in matters of criminal law and procedure.[24] Because of different rules among the member states relating to data retention for investigation, detection, and prosecution of crime, the European Union adopted Directive 2006/24/EC (the "Data Retention Directive") to apply to traffic and location data in order for it to be available to law enforcement.[25] The retention obligation applies to providers of publicly available electronic communications services and to providers of public communications networks,[26] and the period of retention may be no less than six months and no longer than twenty-four months.[27] This durational requirement derogates from the limits that would otherwise be imposed by the E-Privacy Directive and the Data Protection Directive.

More recently, the Proposed European Union Data Protection Regulation[28] creates uncertainty for the application of the Data Retention Directive. The proposed regulation seeks to create a "Right to be Forgotten" that seems to give individuals the power to override data retention and require the purging of personal information.[29] Article 17(3)(d), however, could create an exception

> for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of

---

20. *Id.* art. 6(3).

21. *Id.* art. 6(2).

22. Data Protection Directive, *supra* note 17, art. 3(2); E-Privacy Directive, *supra* note 19, art. 1(3).

23. Treaty on European Union, Feb. 7, 1992, 1992 O.J. (C 191)

24. *Id.*

25. Directive 2006/24/EC, of the European Parliament and of the Council, art. 1, 2006 O.J. (L 105) 54 (EC) [hereinafter Data Retention Directive]. By its terms, Directive 2006/24/EC does not apply to content information.

26. *Id.* art. 3(1).

27. *Id.* art. 6.

28. *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012) [hereinafter PDPR].

29. *Id.* art. 17.

> personal data and be proportionate to the legitimate aim pursued.[30]

This would seem to allow data retention as a "legitimate aim" for law enforcement purposes notwithstanding the Right to be Forgotten.

### *B. Access*

In contrast to the freedom for service providers to make decisions about retention, the U.S. legal tradition focuses its protection of citizens against the use of state power and regulates government access to data. At the constitutional level, the Supreme Court interprets the Fourth Amendment protection against warrantless searches and seizures to protect a "reasonable expectation of privacy," and has ruled that access to the contents of a telephone call required a warrant issued for probable cause.[31] The constitutional restriction on access does not, however, extend to information provided to a third party because the Supreme Court has also ruled that there is no "legitimate 'expectation of privacy'" in such information.[32] Since online traffic data are generated and maintained by third parties, the Supreme Court's third party doctrine means that public authorities will likely not face constitutional limits on data access.[33]

Technological advances, however, blur the distinction between the constitutional protection afforded to contents, but not to traffic data. The Supreme Court recognizes that there is a slippery slope between the information conveyed by discrete transactional data and by aggregations of transactional data. The aggregation of transactional data in the context of data processing can readily resemble contents. In *United States Department of Justice v. Reporters' Committee*,[34] the Supreme Court noted specifically that an aggregation of information otherwise publicly available—rap sheet data—was qualitatively different from the individual records themselves.[35] While the *Reporters' Committee* case addressed information disclosure under the Freedom of Information Act, the qualitative significance of data aggregation is relevant to the Fourth

---

30. *Id.* art. 17(3)(d).

31. Katz v. United States, 389 U.S. 347, 357–60 (1967).

32. United States v. Miller, 425 U.S. 435, 442–43 (1976).

33. *See* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1402–03 (2004); Susan Freiwald, *First Principles of Communications Privacy*, STAN. TECH. L. REV. ¶ 3–4 (2007); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009); Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1311 (2012).

34. 489 U.S. 749 (1989).

35. *Id.* at 764–65.

Amendment analysis. Recently, in *United States v. Jones*,[36] the Supreme Court began to question the applicability of the Fourth Amendment's third-party doctrine to aggregations of geolocation data.[37] While the Supreme Court held in the *Jones* case that the placement of a geolocation device on a suspect's car required a warrant based on the physical placement of a device on private property,[38] five justices in their concurrences indicated that the aggregation of data reflecting movements on the public street might constitute a cognizable privacy violation.[39]

Although the lack of constitutional standards for access to data appears in flux in the wake of *United States v. Jones*, Congress has sought to carefully limit access by public authorities to online data. The Electronic Communications Privacy Act[40] and the Stored Communications Act[41] each impose basic restraints on public authorities' access to information.[42] These statutes force public authorities to obtain warrants and subpoenas for access to online data.[43] The threshold, whether access requires a warrant based on probable cause, a court order based on "specific and articulable facts showing that there are reasonable grounds to believe . . . [the information is] relevant and material to an ongoing criminal investigation,"[44] or an administrative subpoena, depends on the type of information sought and the duration of storage.[45] In an extensive study of law enforcement data access rights, Professor Murphy has noted that a plethora of statutory provisions permit law enforcement

---

36. 132 S. Ct. 945 (2012).

37. *Id.* at 954, 957 (Sotomayor, J., concurring).

38. *Id.* at 949 (majority opinion) ("The Government physically occupied private property for the purpose of obtaining information.").

39. *Id.* at 956–57 (Sotomayor, J., concurring) (stating that "I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on," and writing that "[m]ore fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties"); *id.* at 961 (Alito, Breyer, Ginsberg & Kagan, JJ., concurring) ("[T]he Court's reasoning largely disregards what is really important (the *use* of a GPS for the purpose of long-term tracking) . . . ."). For an interesting discussion of the "mosaic theory" that articulates a rationale to protect aggregations, see generally Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).

40. 18 U.S.C. §§ 2510–2522 (2012).

41. *Id.* §§ 2701–2712.

42. *See generally* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004) (explaining the Stored Communications Act's applicability to online activity).

43. *Id.* at 1218–20, 1222–23.

44. 18 U.S.C. § 2703(d).

45. *Id.* § 2703(a).

access to privately held data, that the typical mechanism is a judicial subpoena rather than a warrant, and that the subpoenas, while easy to obtain, may be conditioned on prior notice or higher evidentiary standards.[46]

In Europe, the primary regulation of data access by public authorities does not come from the European directives. The Data Protection Directive prohibits disclosure of data for secondary purposes and limits access to legitimate purposes.[47] The provisions are, however, not applicable to law enforcement activity as such activity was within the exclusive legal authority of the member states.[48] Today, under the Lisbon Treaty, the European Union has shared competence with the member states for matters involving freedom, security, and justice.[49]

The E-Privacy Directive conditions access by public authorities on the adoption of a law that "constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection, and prosecution of criminal offences."[50] This leaves the articulation of access rules to Member State criminal procedure law. Member state criminal law varies on the mechanisms and means of access to data held by third parties.[51]

Similarly, the Data Retention Directive expressly allows public authorities access to retained data "in specific cases and in accordance with national law."[52] The European Court of Justice explicitly recognized that the Data Retention Directive in itself does

---

46. *See* Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 516–18 (2013).

47. Data Protection Directive, *supra* note 17, art. 6(1)(b).

48. *Id.* art. 3(2).

49. Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Dec. 13, 2007, 2007 O.J. (C 306) 1. The PDPR can, thus, also set access standards that would be applicable to public authorities pursuing data in the context of criminal investigations and public safety. *Id.*

50. E-Privacy Directive, *supra* note 19, art. 15(1).

51. *See, e.g.*, Winston Maxwell & Christopher Wolf, *A Hogan Lovells White Paper on a Global Reality: Governmental Access to Data in the Cloud*, at 1 (July 18, 2012), *available at* http://m.hoganlovells.com/files/News/c6edc1e2-d57b-402e-9cab-a7be4e004c59/Presentation/NewsAttachment/a17af284-7d04-4008-b557-5888433b292d/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20%2818%20July%2012%29.pdf; Lorenzo Picotti & Ivan Salvadori, Council of Europe Project on Cybercrime, *National Legislation Implementing the Convention on Cybercrime - Comparative Analysis and Good Practices*, 51–58 (Aug. 28, 2008), *available at* http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study2-d-version8%20_28%20august%2008.pdf.

52. Data Retention Directive, *supra* note 25, art. 4.

"not . . . involve intervention by the police or law-enforcement authorities."[53] Access rules must be established in member state criminal law like those under the E-Privacy Directive. The Data Retention Directive provides only limited guidance for those national laws. They must have "procedures to be followed and . . . conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements . . . [that are] subject to the relevant provisions of European Union law or public international law, and in particular the ECHR."[54]

The national rules on data access, though, are subject to important European treaty protections for citizens. The ECHR constrains access by public authorities.[55] Article 8 of the ECHR provides a "right to respect for his private and family life" and provides that there should be "no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or economic well-being of the country, for the prevention of disorder or crime."[56] Similarly, the Charter of Fundamental Rights of the European Union establishes a "right to the protection of personal data concerning him or her," but allows processing (which would include access) on the basis of a "legitimate basis laid down by law."[57] Unlike the United States' constitutional position, the ECHR and Charter apply protection to both content and transaction data.[58]

### C. *National Security Privilege*

The recent public revelations regarding the massive collection of telecommunications data by the U.S. government reflect the deviations and special legal rules for the national security context.[59]

---

53. Case C-301/06, Ireland v. European Parliament and Council of the European Union, 2009 E.C.R. I-593, ¶ 82, *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=72843&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=239948.

54. *Id.* ¶ 12 (quoting Data Retention Directive, *supra* note 25, art. 4).

55. ECHR, *supra* note 2.

56. *Id.*

57. Charter, *supra* note 2, art. 8.

58. Malone v. United Kingdom, 82 Eur. Ct. H.R. (ser. A) at § 84 (1984) (noting that ECHR article 8 applies to caller ID information and not just contents). The Charter applies to all personal data. *Id.*

59. *See* Preliminary Order, *In re* Application of the FBI, FISC Docket No. 13-80 (Apr. 25, 2013) (revealing metadata collection from Verizon by the FBI under 50 U.S.C. § 1861 (2006)); *see also* Memorandum Opinion, FISC Docket No. [classified] (Oct. 3, 2011), *available at* https://www.eff.org/sites/default/files/filenode/fisc_opinion_-_unconstitutional_surveillance_0.pdf (revealing collection of Internet communications data by the NSA under 50 U.S.C. § 1881).

The practices disclosed in these leaks are not new. During the Clinton administration, the United States and Europe had a privacy dispute over the ECHELON spying program.[60] ECHELON enabled the U.S. government to capture and data mine international communications.[61]

Similarly, in Europe, governments appear to engage in comparable collections of international communications. More than fifteen years ago, press reports revealed a French program parallel to ECHELON, executed in cooperation with Germany, that captured international communications traffic.[62] At a recent congressional hearing, the Obama administration testified that other European intelligence services gathered communications data and provided that information to the United States.[63] Shortly after the testimony, officials in the French Direction générale des services extérieurs ("DGSE") admitted that the DGSE massively tapped French communications and shared captured communications with the U.S. National Security Agency.[64] As it turns out, the British Government Communications Headquarters ("GCHQ") has also been capturing the international e-mail traffic of Google and Yahoo.[65] According to the Oxford Internet Institute's Senior Research Fellow, Ian Brown, it is likely that UK government access to private sector data without court authorization is systemic in the United Kingdom.[66] Revelations by the British press disclosed that the GCHQ, the UK intelligence service, is capturing all data entering or exiting the UK through fiber-optic cables.[67]

---

60. *See, e.g.*, Constant Brand, *Europeans Warned over Echelon Spying*, THEGUARDIAN (May 30, 2001), http://www.theguardian.com/world/2001/may/30/eu.politics.

61. *Id.*

62. Jean Guisnel, *Les Français aussi écoutent leurs allies* [*The French Also Wiretap Their Allies*], LE POINT (June 6, 1998), http://www.lepoint.fr/actualites-politique/2007-01-25/les-francais-aussi-ecoutent-leurs-allies/917/0/91357.

63. Michael S. Schmidt, *N.S.A. Head Says European Data Was Collected by Allies*, N.Y. TIMES (Oct. 29, 2013), http://www.nytimes.com/2013/10/30/us/politics/u-s-intelligence-officials-defend-surveillance-operations-on-capitol-hill.html.

64. Jacques Follorou, *Surveillance: la DGSE a transmi des donnees a la NSA americaine* [*Surveillance: The DGSE Transmitted Data to the American NSA*], LE MONDE, Oct. 30, 2013.

65. *See* Charlie Savage et al., *N.S.A. Said to Tap Google and Yahoo Abroad*, N.Y. TIMES, Oct. 31, 2013, at B1.

66. *See* Ian Brown, *Government Access to Private-Sector Data in the United Kingdom*, 2 INT'L DATA PRIVACY L. 230, 237–38 (2012), *available at* http://idpl.oxfordjournals.org/content/2/4/230.full.

67. *See* Kadhim Shubber, *A Simple Guide to GCHQ's Internet Surveillance Programme Tempora*, WIRED (June 24, 2013), http://www.wired.co.uk/news/archive/2013-06/24/gchq-tempora-101.

In the United States, statutory provisions provide privileged and exceptional access by public authorities to privately held communications data related to foreign intelligence gathering.[68] Section 702 of the Foreign Intelligence Surveillance Act of 1978 ("FISA")[69] permits the President through the Attorney General to authorize electronic surveillance without a warrant for foreign powers and their agents outside the United States.[70] These orders are issued on a secret basis.[71] FISA also authorizes the government to obtain from the FISA court an interception order for communications within the United States when the target of the surveillance is a foreign power, or agent of a foreign power, and the government can show that the electronic surveillance targets facilities used by the foreign power or agent.[72] The government must make a probable cause showing to the FISA court and demonstrate the application of data minimization procedures.[73]

Similarly, amendments to FISA contained in section 215 of the PATRIOT Act permit public authorities to obtain business records from the private sector if they are relevant to an authorized investigation.[74] Like the section 702 FISA order, a PATRIOT Act order, known as a "National Security Letter," is also secret and is accompanied by a gag order prohibiting the recipient from disclosing the existence of the National Security Letter.[75] The order can even be issued without any judicial oversight.[76] According to the Electronic Information Privacy Center, in the last five years the FISA court has only rejected two access requests out of 8,591 made by the government.[77]

In Europe, like in the United States, intelligence services are afforded privileged rights of access to data. For example, in the United Kingdom, a secretary of state (typically the foreign secretary or the home secretary) may order interception of communications

---

68. *See generally,* Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306 (2004) (describing FISA and its evolution).

69. Foreign Intelligence Surveillance Act of 1978 § 702, 50 U.S.C. § 1802 (2012).

70. 50 U.S.C. § 1802.

71. *Id.* § 1802(a)(3).

72. *See id.* § 1805(a)(2).

73. *Id.* §§ 1805(a)–(c).

74. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) § 215, 50 U.S.C. § 1861 (2012).

75. 18 U.S.C. § 2709(c) (2012).

76. *See id.* § 2709(b).

77. Claire Cain Miller, *Secret Ruling Put Tech Firms in Data Bind*, N.Y. TIMES, June 14, 2013, at A1.

without a court warrant;[78] the decision is entirely a ministerial choice. Under the Regulation of Investigatory Powers Act, interceptions may even be made "for the purpose of safeguarding the economic well-being of the United Kingdom."[79]

France similarly has mechanisms for the executive branch to gather communications data without a court order.[80] Although in 1991 France established the National Commission for the Control of Security Interceptions (Commission nationale de contrôle des interceptions de sécurité), the commission only has the power to make recommendations on the legality of interceptions and does not have the power to block them.[81] Thus, there is no truly independent supervision of government access for an important range of surveillance orders. And also like the United Kingdom, security interceptions on the order of the prime minister's office are permitted to safeguard France's economic interests thereby providing a very broad basis to engage in surveillance.[82]

Even liberal Sweden allows warrantless wiretapping for intelligence purposes,[83] as does the Netherlands.[84] And Germany,

---

78. *See* Intelligence Services Act, 1994, c. 13, §§ 5–6 (Eng.); Regulation of Investigatory Powers Act, 2000, c. 23, § 5(1); *see also* 10 June 2013, PARL. DEB., H.C. (6th Ser.) (2013) 32 (U.K.) (statement of William Hague, Sec'y of St. for Foreign & Commonw. Aff.), *available at* http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm130610/debtext/130610-0001.htm#13061011000001. *See generally* Ian Brown, *Government Access to Private Sector Data in the United Kingdom*, 2 INT'L DATA PRIVACY L. 230 (2012), *available at* http://idpl.oxfordjournals.org/content/2/4/230.full (discussing the statutory authorizations for government access to data).

79. Regulation of Investigatory Powers Act, 2000, c. 23, § 5(3).

80. *See* Loi 91-646 du 10 juillet, 1991 relative au secret des correspondances émises par la voie des communications électroniques [Law 91-646 of July 10, 1991 Concerning the Confidentiality of Electronic Communications], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], July 13, 1991, 9167, *available at* http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000173519 (allowing "security interceptions" to be ordered by the Ministry of Defense or by the Ministry of the Interior each with the permission of the Prime Minister's Office); *see also* Winston Maxwell, *Systematic Government Access to Private Sector Data in France*, 4 INT'L DATA PRIVACY L. 4 (2014), *available at* http://www.hoganlovells.com/files/Publication/7be5f777-22c1-4bd9-bac9-897dd220ba04/Presentation/PublicationAttachment/6e5def8a-c1bb-4816-b417-9162e67cb9c5/Article%20W%20Maxwell_20140217105006.pdf

81. Loi 91-646 art. 13–15.

82. *Id.* art. 3.

83. *Sweden Approves Wiretapping Law*, BBC NEWS, http://news.bbc.co.uk/2/hi/europe/7463333.stm (last updated June 18, 2009).

84. *See II. Surveillance Policies*, PRIVACY INT'L, https://www.privacyinternational.org/reports/the-netherlands/ii-surveillance-policies (last visited Feb. 8, 2014).

too, provides special privileges for "strategic surveillance."[85] According to recent reports, on the order of the German prime minister, the German intelligence agency has a direct tap into the equipment of Internet service providers.[86]

## II. INTRACTABLE CONFLICTS

United States and European democracies have had great difficulty grappling with the border between surveillance and privacy. At present, the technological infrastructure breeds systems of surveillance and the legal infrastructure embeds liberal permissions for access. In the United States, the former chairman of a congressional oversight committee was astonished to learn in the first public report that law enforcement made 1.3 million requests for user transaction data during 2011.[87] Globally, in the last three years, the Google Transparency Report shows that data access requests by public authorities have almost doubled.[88] United States authorities make the overwhelming majority of these requests, though six European countries are in the top ten.[89] The extraordinarily rapid growth in Europe and the United States in the number of access requests poses a structural challenge to privacy in democracy from three perspectives. First, data retention and access rules cannot be divorced from one another and the standards for linkage are elusive. Second, the apparatus for surveillance shifts the burden and role of public enforcement to private actors as agents. And, third, national security privilege creates a delicate balance for oversight that requires transparency.

### *A. Elusive Linkages*

Delimiting privacy requires combined policy rules on both retention and access because, if privacy is to be protected, more developed and extensive data retention necessitates more careful

---

85. Paul M. Schwartz, *Systematic Government Access to Private-Sector Data in Germany*, 2 INT'L DATA PRIVACY L. 289, 297 (2012), *available at* http://idpl.oxfordjournals.org/content/2/4/289.full.pdf+html.

86. Cyrus Farivar, *German NSA Has Deal to Tap ISPs at Major Internet Exchange*, ARS TECHNICA (Oct. 7, 2013), http://arstechnica.com/tech-policy/2013/10/german-nsa-has-deal-to-tap-isps-at-major-internet-exchange/.

87. Eric Lichtblau, *More Demands on Cell Carriers in Surveillance*, N.Y. TIMES, July 9, 2012, at A1.

88. *Transparency Report: Requests for User Information*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/ (last visited Feb. 8, 2014).

89. Between January 2013 and June 2013, the top ten requestors are, in descending order: the United States, India, Germany, France, the UK, Brazil, Italy, Spain, Australia, and Poland. *Transparency Report: Requests for User Information: Countries*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/countries/?t=table (last visited Feb. 8, 2014).

and restrictive access. In the United States, the parameters are essentially set by statute, while in Europe, the constitutional-level treatment found in the Charter and the ECHR provides a backdrop to the statutory framework.[90] Both systems, in effect, compel data retention—the United States by commerce and the European Union by law—and both continents, in effect, have accepted unclear access rules for public authorities.

Courts in the United States, for example, have had great trouble deciphering the application of the Electronic Communications Privacy Act ("ECPA").[91] One court notably stated that the statute was "famous (if not infamous) for its lack of clarity."[92] In practice, the largest secret docket in the United States, according to federal magistrate judge Stephen Smith, is the ECPA "warrant type applications" or secret electronic surveillance orders.[93] This indicates that the statutory protections constraining access to retained data by public authorities have an elusive boundary.

In Europe, data protection authorities have expressed strong, consistent objections to data retention.[94] The European Union data protection authorities have even declared that the Data Retention Directive "encroaches into the daily life of every citizen and may

---

90. *See, e.g.*, ECHR, *supra* note 2 (explaining the existence of a right to respect for private and family life).

91. 18 U.S.C. §§ 2510–2522 (2012).

92. Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994).

93. Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L & POL'Y REV. 313, 318–22 (2012) (citing TIM REAGAN & GEORGE CORT, FED. JUD. CTR., SEALED CASES IN FEDERAL COURTS 22 (2009), *available at* http://www.fjc.gov/public/pdf.nsf/lookup/sealcafc.pdf/$file/sealcafc.pdf).

94. *See, e.g.*, Art. 29 Data Protection Working Party, *Opinion 5/2002 on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on Mandatory Systematic Retention of Telecommunication Traffic Data*, at 3 (Oct. 11, 2002) [hereinafter *Opinion 5/2002*], http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp64_en.pdf; Art. 29 Data Protection Working Party, *Opinion 4/2005 on the Proposal for a Directive of the European Parliament and the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC*, at 5 (Oct. 21, 2005) [hereinafter *Opinion 4/2005*], http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp113_en.pdf; Art. 29 Data Protection Working Party, *Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC*, at 2 (Mar. 25, 2006) [hereinafter *Opinion 3/2006*], http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp119_en.pdf.

endanger the fundamental values and freedoms all European citizens enjoy and cherish"[95] and have called for restrictive implementation at the member state level. Francesca Bignami argues that the Data Retention Directive adequately protects privacy as the right is articulated in the ECHR.[96] But, others have argued that the directive itself fails the proportionality test.[97] There is even an inherent flaw with respect to the distinction the Data Retention Directive draws between content and transaction data. Article 5(2) bans the storage of content.[98] But, the application of data mining to traffic data can readily disclose the content of communications, thus transforming the retained traffic data into a vector of content data.

Throughout the adoption process of the Data Retention Directive, the European Union data protection authorities consistently objected to overreaching in the scope of the retention requirements.[99] Their objections nonetheless seem to have been minimized or ignored in the political process leading to the adoption of the directive. The opinions of the Article 29 Working Party, comprised of representatives from each of the national privacy commissions, were largely disregarded in the adoption of the directive itself and in the adoption of national implementing legislation. In July 2010, the Article 29 Working Party went so far as to declare that the implementation of the Data Retention Directive was unlawful.[100] The European Court of Justice is currently considering whether the retention obligation and duration of storage is compatible with the Charter.[101]

---

95. *Opinion 3/2006*, *supra* note 94.

96. *See generally* Francesca Bignami, *Privacy and Law Enforcement in the European Union: The Data Retention Directive*, 8 CHI. J. INT'L L. 233 (2007).

97. Lukas Feiler, *The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection*, 1 EUR. J.L. & TECH. 1, 19 (2010), *available at* http://ejlt.org//article/download/29/76.

98. Data Retention Directive, *supra* note 25, art. 5(2).

99. *Opinion 3/2006*, *supra* note 94; *Opinion 4/2005*, *supra* note 94; *Opinion 5/2002*, *supra* note 94.

100. *See Report 01/2010 on the Second Joint Enforcement Action: Compliance at National Level of Telecom Providers and ISPs with the Obligations Required from National Traffic Data Retention Legislation on the Legal Basis of Articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC Amending the e-Privacy Directive*,at 1, 10 (July 13, 2010) [hereinafter *Report 01/2010*], http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf. *Compare Opinion 3/2006*, *supra* note 94, at 3, *with* Data Retention Directive, *supra* note 25, at arts. 1, 4.

101. The high courts of Austria and Ireland have each referred questions on the legality of the Data Retention Directive to the European Court of Justice. *See* Joined Cases C-293/12 & C-594/12, Digital Rights Ir. v. Minister for Commc'n, Seitlinger & Others. In the referral, the ECJ will address whether

While not clearly articulated in the debate over data retention obligations, the data access mechanisms heighten the concern over the scope of the data retention requirements. Access controls remain elusive across Europe. The member states tilt in favor of broad public authority access and, in fact, the implementing laws for the Data Retention Directive of two member states are now before the European Court of Justice for potential violations of the Charter and the ECHR.[102] A few national courts have also struck down particular implementing statutes.[103]

The access rules are not defined in the treaty documents and are not defined in the directives. Rather, they must be established at the member state level based on balancing various amorphous interests. The ECHR permits intrusions on privacy if the intrusion is (1) authorized by law; (2) "in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime;" and (3) proportional.[104] The European Court of Human Rights has indicated that "in accordance with the law" requires that statutory measures spell out the access procedures and that secret processes do not qualify.[105] In addressing law enforcement access to stored biometric data, the European Court of Human Rights noted that

> it is as essential, in this context, as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.[106]

---

the directive's obligations for retention are compatible with article 8 in both the ECHR and the Charter. *Id.*

102. *Id.*

103. *See, e.g.*, *Czech Constitutional Court Rejects Data Retention Legislation*, EDRI (Apr. 6, 2011), http://edri.org/edrigramnumber9-7czech-data-retention-decision/.

104. ECHR, *supra* note 2, art. 8; *see also* Bignami, *supra* note 96, at 242–49.

105. *See* Liberty & Others v. United Kingdom, App. No. 58243/00, 48 Eur. Ct. H.R. 1, ¶¶ 62, 66, 69 (2008).

106. S. & Marper v. United Kingdom, App. Nos. 30562/04 & 30566/04, 48 Eur. Ct. H.R. 1169, ¶ 99 (2008), *available at* http://www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/S.%20AND%20MARPER%20v.%20THE%20UNITED%20KINGDOM%20EN.pdf.

However, the Strasbourg court gives deference to national authorities on the determination of a "pressing social need" as a legitimate aim of an access law.[107]

With respect to proportionality, the Charter elaborates on the requirement.[108] As explained by the European Court of Justice, proportionality means that

> measures adopted by [Union] institutions do not exceed the limits of what is appropriate and necessary in order to attain the objectives legitimately pursued by the legislation in question; when there is a choice between several appropriate measures recourse must be had to the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued.[109]

As reported by the Article 29 Working Party, however, the practices and determinations of proportionality in data retention requirements vary widely across the European Union, indicating a failure of the "proportionality" standard to be an effective protection for privacy.[110] Equally problematic is that the European Court of Human Rights tends to give a "wide margin of appreciation"[111] to member state laws in the realm of public safety, but looks strictly at infringements of fundamental rights.[112] This suggests that the European Court of Human Rights will face a constant struggle between liberal acceptance of public safety regulations and strict scrutiny for fundamental rights breaches.[113]

The German example shows the difficulty in assessing proportionality. Paul Schwartz writes that Germany distinguishes between data mining for the investigation of past crimes and data mining for the prevention of potential crimes.[114] The criminal procedure code applies to investigatory data mining and requires "sufficient factual indications to show that a criminal offense of significant importance has been committed."[115] But, data mining for crime prevention may impinge on citizens' rights to information

---

107. *Id.* ¶ 101.

108. Charter, *supra* note 2, art. 52(1).

109. Feiler, *supra* note 97, at 10 (quoting Case C-331/88, The Queen v. Min. of Agri., Fisheries and Food and Sec'y of State for Health, *ex parte* Fedesa and Others, 1990 E.C.R. I-4023, § 13; Joined Cases C-133/93, C-300/93, and C-362/93, Crispoltoni and Others v. Tabacchi and Srl, 1994 E.C.R. I-04863, § 40).

110. *Report 01/2010*, *supra* note 100, at 1.

111. *See, e.g.*, Leander v. Sweden, 9 Eur. Ct. H.R. 433, ¶ 67 (1987).

112. *See* Manoussakis v. Greece, 1996-IV Eur. Ct. H.R. ¶ 144 (1996).

113. Courts of individual member states may, however, apply more stringent standards to public safety regulators than those contained in the ECHR.

114. Schwartz, *supra* note 85, at 292.

115. *Id.* at 292–93 (translating the German criminal procedure code section 98a).

privacy when there is a "concrete danger to a legal interest."[116] Schwartz notes that law enforcement must show a risk of danger before preventive data mining will be permissible under the German constitution.[117] The problem with this approach is that danger is now a fact of life in a world of global terrorism, and more information will always be seen as a mechanism to reduce the risk of danger.

Interestingly, the German Constitutional Court struck down the Data Retention Directive's implementing statute because the law did not provide sufficient clarity on purpose limitations for data access and transparency about its use.[118] More recently, the European Commission referred Germany to the European Court of Justice for failure to implement the Data Retention Directive following the annulment of the German statute.[119]

France, as another example, enacted a statute in 2001 on public safety, *Loi sur la sécurité quotidienne*,[120] as an emergency measure to require the collection and retention of telecommunications traffic data. Yet, the decree to implement the law was not adopted for five years.[121] The delay suggests that the need for the data is neither as urgent nor as critical as publicly stated.

### *B. Burden of Enforcement*

The combination of data retention in the private sector and access to that data by public authorities shifts the burden of law enforcement to private actors. Private actors become responsible for the data sets that fuel law enforcement activity. This shift transforms private actors into the instrumentalities of privacy intrusions. This shift also imposes some of the costs of law enforcement onto private actors.[122]

---

116. *Id.* at 293.

117. *Id.*

118. *Id.* at 293–94.

119. Press Release, European Comm'n, Commission Takes Germany. to Court Requesting that Fines Be Imposed (May 31, 2012), http://europa.eu/rapid/press-release_IP-12-530_en.htm.

120. Loi 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne [Law 2001-1062 of Nov. 15, 2001 on Public Safety], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Nov. 15, 2001, 18215, *available at* http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000222052&dateTexte=20140209.

121. Decret 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques [Decree 2006-358 of Mar. 24, 2006 on the Retention of Electronic Communications Data], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Mar. 24, 2006, 4609, *available at* http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000637071&dateTexte=&categorieLien=id.

122. Not all costs are shifted to private actors, as Internet service providers do charge fees for access requests.

For Europe, the data retention requirement explicitly transforms the private sector into agents of law enforcement. By requiring service providers to store data in what would otherwise be a contravention of the Data Protection Directive, the Data Retention Directive obligates private parties to maintain a surveillance database for law enforcement. In effect, Europe has turned online intermediaries into sheriffs. This shift contradicts European legal traditions such as those of France and Belgium that place the state as the guarantor of citizen freedom. In other words, Europe has now enlisted private sector organizations as the "protectors" of societal rights to security and public safety.

This privatization of law enforcement has broad ramifications. Once private sector organizations are maintaining systems for the protection of societal rights, the scope of those rights are likely to be subject to function creep. Colin Bennett and Charles Raab wrote of "the tendency for new uses and applications to be found over time unrelated to the purposes for which the technology was originally designed."[123] Function creep pushes uses of the data into other spheres. For example, not surprisingly, data retention is used in some European countries by public authorities to assist in the enforcement of intellectual property rights—private economic rights. The French law on the digital economy, *Loi pour la confiance dans l'économie numérique*, requires that data be retained for use in the prosecution of intellectual property violations.[124] And the European Court of Justice authorized the use in Sweden of data retained by Internet service providers for intellectual property rights enforcement.[125] Thus, the retention of data to address antisocial crime becomes a means to enforce private economic rights,

123. COLIN BENNETT & CHARLES RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 139 (2003); *see also*, KIRSTIE BALL ET AL., A REPORT ON THE SURVEILLANCE SOCIETY FOR THE INFORMATION COMMISSIONER BY THE SURVEILLANCE STUDIES NETWORK 9 (David Murakami Wood ed., 2006), *available at* http://www.ico.org.uk/~/media/documents/library/Data_Protection/Practical_application/SURVEILLANCE_SOCIETY_FULL_REPORT_2006.PDF ("Personal data, collected and used for one purpose and to fulfill one function, often migrate to other ones that extend and intensify surveillance and invasions of privacy beyond what was originally understood and considered socially, ethically and legally acceptable.").

124. Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [Law 2004-575 of June 21, 2004 on Trust in the Digital Economy], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], June 21, 2004, art. 6, *available at* http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&dateTexte=&categorieLien=id.

125. Case C-461/10, Bonnier Audio AB and Others v. Perfect Commc'n Swed. AB, ¶ 61 (2012), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=121743&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=243715.

something unlikely to have been authorized if made as an initial purpose of the retention and access demands.

In the United States, there is an equivalent effect. The private sector retains extensive data sets because of the commercial pressures and the push for Big Data. As repositories of traffic and geolocation data, these private intermediaries become a central resource for public enforcement actions.[126] The statistics provided by the semiannual Google Transparency Report[127] demonstrate the growing extent of the use by public authorities of private sector data resources for state law enforcement activity. Like the contradiction of legal traditions in Europe, the shift in the United States also juxtaposes the American approach to state power. The Bill of Rights generally enshrines the philosophy that citizens should be protected from the State.[128] In contrast, easy access by public authorities to privately held data for law enforcement purposes transforms citizens into instruments of state power with respect to their fellow citizens. This transformation is in opposition to the underlying core values in the Bill of Rights approach.[129]

### *C. National Security Oversight*

The privileges for national security extend to oversight and have invariably conflicted with accountability. Public accountability necessitates an important degree of transparency in data processing operations. President Obama once argued that "[g]overnment should be transparent. Transparency promotes accountability and provides information for citizens about what their Government is doing."[130] The national security privileges, however, grant secrecy to data surveillance operations. There is consequently an inherent contradiction between the secrecy of intelligence operations and the requisite transparency for public accountability. The balance between these privileges for national security and effective oversight is unstable.

In the United States, oversight for the privileged access to data afforded to national security operations is intrinsically weak.

---

126. Jack Balkin warned of this "National Surveillance State." Jack Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 3–4 (2008).

127. *Transparency Report*, GOOGLE, http://www.google.com/transparencyreport/ (last visited Feb. 8, 2014).

128. *See* Steven J. Heyman, *The First Duty of Government: Protection, Liberty and the Fourteenth Amendment*, 41 DUKE L.J. 507, 525–27 (1991) (discussing the emphasis on negative rights, but also a positive right component).

129. This transformation may also mean that the state action doctrine is satisfied when private intermediaries are used as law enforcement agents.

130. Memorandum on Transparency and Open Government, 74 Fed. Reg. 4685, 4685 (Jan. 26, 2009).

Government access requests are secret.[131] When a FISA court order is required, the evidence is secret[132] and, as reported by the Chief Judge, often withheld from the court itself.[133] Most of the proceedings are ex parte and thus nonadversarial.[134] Finally, the decisions of the court are secret and can be released by the court only in a government-redacted form.[135] This structure of secrecy impedes effective oversight.

The lack of transparency goes even deeper and challenges the capacity for public accountability. In the United States, the Chief Judge of the FISA Court surprisingly admitted that "[t]he FISC is forced to rely upon the accuracy of the information that is provided to the Court."[136] In other words, unauthorized and illegal activity will only be brought to the court's attention by a guilty intelligence service. But, rather than present accurate information, the intelligence community appears to have a pattern of deceiving the secrecy-shrouded oversight bodies. The Director of National Intelligence even testified before Congress that the NSA was not collecting data on millions of Americans.[137] The testimony turned out be false.[138] More recently, General Keith Alexander, the Director of the National Security Agency, testified to Congress that the number of plots (fifty-four) reported by the government to

131. 50 U.S.C. § 1803(c) (2012); *id.* § 1861(d).

132. *Id.* § 1803(c).

133. Carol D. Leonnig, *Court: Ability to Police U.S. Spying Program Limited*, WASH. POST. (Aug. 15, 2013), http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_story.html.

134. *See* 50 U.S.C. §§ 1805(a), 1824(a), 1842(d)(1), 1861(c)(1).

135. *See* U.S. FOREIGN INTELLIGENCE SURVEILLANCE CT. R. P. 62. Summary statistics of the number of requests considered are, though, publicly reported to Congress. 50 U.S.C. §1807; *id* at § 1862(b) .

136. Leonnig, *supra* note 133.

137. *Hearing on Current and Projected National Security Threats to the United States Before the Senate Select Committee on Intelligence*, 113th Cong., 1st Sess., at 66 (Mar. 12, 2013), *available at* http://www.intelligence.senate.gov/131113pdfs/11389.pdf (testimony of NSA Director Clapper stating that the NSA does not collect data on millions of Americans).

138. Letter from James R. Clapper, Dir. of Nat'l Intelligence, to Senator Ron Woden (Mar. 28, 2014), *available at* http://s3.documentcloud.org/documents/1100339/letter-to-sen-ron-wyden-from-dni-james-clapper.pdf; *see* Barton Gellman and Ashkan Soltani, *NSA Maps Targets by Their Phones*, WASH. POST, Dec. 5, 2013, at A1, *available at* http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html (reporting that tens of millions of Americans are tracked abroad); James Risen and Laura Poitras, *NSA Examines Social Networks of US Citizens*, N.Y. TIMES, Sept. 29, 2013, at A1, *available at* www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html.

Congress as thwarted because of the intelligence data-mining programs, was not accurate and was significantly overstated.[139]

In Europe, the same conflict occurs. For example, the United Kingdom's Regulation of Investigatory Powers Act provides that data-gathering orders are secret.[140] Moreover, public authorities face little independent supervision when they engage in foreign data sharing arrangements that circumvent restrictions on domestic data gathering.[141] For example, the U.K. foreign secretary was asked explicitly in Parliament whether British intelligence services obtained information on U.K. residents from foreign intelligence services without the specific ministerial order that would be required for domestic surveillance.[142] The minister evasively responded:

> On the right hon. Gentleman's further questions about how authority is given, I cannot give him, for reasons that I cannot explain in public, as detailed an answer as he would like. I would love to give him what could actually be a very helpful answer, but because circumstances and procedures vary according to the situation, I do not want to give a categorical answer—in a small respect circumstances might differ occasionally. But I can say that ministerial oversight and independent scrutiny is there, and there is scrutiny of the ISC in all these situations, so, again, the idea that operations are carried out without ministerial oversight, somehow getting around UK law, is mistaken. I am afraid that I cannot be more specific than that.[143]

The obfuscation by the minister in his answer strongly indicates that information-sharing arrangements with foreign intelligence services circumvent at least some of the safeguards protecting privacy from domestic surveillance.

---

139. *Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act: Before the Senate Comm. on the Judiciary*, 113th Cong., 1st Sess. (Oct. 2, 2013), http://www.senate.gov/isvp/?comm=judiciary&type=live&filename=judiciary100213 (testimony of the Hon. Keith Alexander, Director of the NSA in response to a question from Senator Leahy beginning at 52:35).

140. Regulation of Investigatory Powers Act, 2000, §§ 49, 54 (U.K.).

141. The United States government has publicly acknowledged the existence of such sharing arrangements. *See* Schmidt, *supra* note 63.

142. 10 June 2013, PARL DEB., H.C. (6th Ser.) (2013) 36 (U.K.) (statement of William Hague, Sec'y of St. for Foreign & Commonw. Aff.), *available at* http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm130610/debtext/130610-0001.htm#13061011000001.

143. *Id.* at 37.

## III. THE PRIVACY TURNING POINT

The existence of retained traffic data, the reliance on uncertain access rules, the recourse to an elusive proportionality, the dependence on private actors, and the privileges accorded to national security collectively place privacy and values in democracy at a turning point. In the aggregate, these elements increase the transparency of citizens' online lives and reduce the sphere of privacy that citizens can enjoy. This transparency is destructive of many fundamental democratic values.

First, the transparency reverses the presumption of innocence. The presumption is central to the philosophy underlying the warrant requirement in the Fourth Amendment and the principle that citizens are innocent until proven guilty in the Fifth and Fourteenth Amendments.[144] In Europe, the presumption of innocence is also a fundamental tenent of the Charter of Fundamental Rights of the European Union: "Everyone who has been charged shall be presumed innocent until proved guilty according to law."[145] Yet, data that are collected and retained without any individualized cause or suspicion by private actors for subsequent access by public authorities contravenes the basic constitutional philosophies. If law generally requires collection and retention, the rationale is that all individuals in the data set are suspect. Similarly, if broad access is afforded to data sets that were created for commercial purposes, the core philosophy is that all individuals in the data set are suspect. These practices transform the presumption of innocence into a presumption of suspicion counter to the core constitutional philosophies.

Second, the forced transparency diffuses the monopoly of the state on law enforcement. Law enforcement, investigation, and intelligence activities are blurred when communications service providers must retain and make available client and user data. Function creep assures that this diffusion of resources for law enforcement to the private sector will lead to increasing demands and an expansion of the scope of enforcement activity to encompass private matters and not just public safety and security.

Third, the transparency from private data mining and publicly mandated surveillance (i.e., forced data retention) diminishes the zone of individual freedom. Where data retention is neither sharply limited nor combined with strong, clear access controls, the ability of citizens to make decisions about their personal information and

144. James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1466–67 (2004); Ira S. Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 263 (2008).

145. Charter, *supra* note 2, art. 48.

their ability to decide when and how to disclose their thoughts, beliefs, and activities, are impaired.[146]

Finally, the transparency of personal information through the national security exceptions assures troubling intelligence gathering from inevitable overreaching. Without a means for effective oversight, the privileges afforded to intelligence operations blur government information gathering into generic, ambient state surveillance.[147] Nondemocratic regimes strive for this level of knowledge of their citizenry's activities.

## IV. SECURING PRIVACY

At this turning point, societies need to better secure privacy than the existing framework allows. Substantive and procedural changes are necessary for the preservation of democratic values. And, accountability needs to be effective.

On the substantive side, stringent collection and storage limitations, as well as robust obstacles to state access, are all necessary conditions to online privacy. The existing demarcation lines are too unstable. Without clear, inviolable, red line boundaries, the resulting transparency of citizens' activities creates a powerful generic surveillance environment that undermines the policy objectives justifying access to extensive data trails in the first place: the investigation of crime and the protection of public safety and liberty. In short, the coupling of strict retention limitations and clear, firm access controls are essential for the future of citizens' online privacy. Red line boundaries should include (1) retention limits that, without a compelling justification specific to a target, do not go beyond a duration required for billing; (2) a ban on access without independent, public judicial oversight; and (3) no cross sharing between intelligence and law enforcement or between law enforcement and economic rights enforcement. These boundaries will need to be established in both national law and international agreements. International agreements are necessary because of the

---

146. Neil Richards refers to this freedom as "intellectual privacy." Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 387 (2008).

147. For example, in the United States, the personal information gathered through intelligence exceptions was used by the government for routine criminal investigations. *See* Charlie Savage, *Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence*, N.Y. TIMES (Oct. 27, 2013), http://www.nytimes.com/2013/10/27/us/federal-prosecutors-in-a-policy-shift-cite-warrantless-wiretaps-as-evidence.html?hpw&_r=0 (disclosing the use of data collected under intelligence authority for ordinary criminal cases as a result of earlier news reports); John Schiffman & Kristina Cooke, *U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, REUTERS (Aug. 5, 2013), http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805 (describing the information-sharing program between the NSA and the Drug Enforcement Agency).

global complexity of data flows along with the inherent and fundamental political choices associated with surveillance. National laws are necessary to constrain the domestic actors who are responsible for data surveillance activities.

In parallel to the substantive coupling of retention limits with strong access controls, new procedural obligations are needed to secure online privacy from state interference. First, the infrastructure of collection and access to personal information must be transparent. Furnishers of personal information to law enforcement should be obligated to keep a log of law enforcement access requests and to make that log available to clients whose information was accessed. For law enforcement, data transparency logs should be obligatory and available to those whose information is processed.[148] In the United States, there is a precedent for such logs. The Fair Credit Reporting Act requires that anyone furnishing a consumer report keep a log of recipients of the consumer report and provide the identity of those recipients to the consumer upon request.[149] This procedure creates a means of oversight for affected consumers that would apply equally, if not more significantly, to the law enforcement context. In the law enforcement context, the risk of surveillance overreaching is no less important than abusive disclosures of credit report information.

For the intelligence-gathering context, there must similarly be transparency of data access for public security unless transparency presents a clear and present danger to public safety. The determination of whether there is a clear and present public safety threat needs to be made by an authority that is independent of the executive branch. The executive branch should not be in control of the dissemination of access orders. The incentive for selective disclosure to distort the public's understanding of government behavior is too great if the executive branch controls disclosure of its activities.[150]

Lastly, democratic societies need true accountability for law enforcement and national security conduct. Individuals who overreach their authority must face penalties. Current laws often

148. This parallels a proposal made by Judge Smith for public docket sheets in the context of secret electronic surveillance orders under ECPA. *See* Smith, *supra* note 93, at 335.

149. 15 U.S.C. § 1681g(a)(3) (2012).

150. In the recent U.S. context, only a small number of FISA court orders have been released and they have been released only in a form heavily redacted by the U.S. government. *See, e.g.*, *In re:* Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, No. 08-01 (FISA Ct. 2008), *available at* http://www.fas.org/irp/agency/doj/fisa/fiscr082208.pdf. Because this is such a highly selective disclosure, the public does not know the true nature of the FISA court's activities and decisions.

do the opposite and give immunity, even retroactively, for data access violations.[151] When a senior government officer admits to deceiving a public oversight body, the failure to sanction the individual sends a powerful message of tolerance for wrongful intrusions into ordinary people's lives and abusive state action. Both legal immunity and expedient tolerance need to be reversed.

Unless democratic societies act quickly to rebalance data surveillance by states, those societies will lose a fundamental characteristic of democracy—the protection of a key individual liberty against the absolute control of the State.

151. *See, e.g.*, Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 50 U.S.C. §§ 1801–1871 (2012) (allowing the Attorney General to make a certification granting immunity); Regulation of Investigatory Powers Act, 2000, § 27(2) (U.K.) (providing immunity from civil liability); Loi 91-646 du 10 juillet, 1991 relative au secret des correspondances émises par la voie des communications électroniques [Law 91-646 of July 10, 1991, on the Confidentiality of Electronic Communications], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], July 13, 1991, art. 15, *available at* http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=81BB97D75A13C3D40B5E2596DBCD17DA.tpdjo16v_2?cidTexte=JORFTEXT000000173519&categorieLien=id (providing only for a recommendation to the Prime Minister without a cause of action).