IV. Divergent Formalities

There is wide divergence in the ways that liberal democracies view and protect individual privacy and identity. A recent multinational report sponsored by the European Commission compares legal and regulatory measures to enhance privacy and trust in the European Union, the United States, Japan, South Korea and Malaysia.[1] For each jurisdiction, the report examines self-regulatory and co-regulatory arrangements, enforcement mechanisms and the effectiveness of privacy and trust practices. Jurisdictions in which privacy is considered an inherent human right and is constitutionally protected tend to have a uniform regulatory framework that limits the way in which a data controller can collect and process information. These jurisdictions typically have statutory regulations that apply to all economic sectors and types of activities.[2] Jurisdictions in which personal information is not recognized in constitutional guarantees, even though privacy rights may be inferred from court decisions, tend to lack a uniform regulatory framework for privacy and identity protections. Typically, legal protections arise to address some demonstrated harm and protections tend to apply only to a given economic sector. Thus a complex tapestry of laws and regulation arises in these jurisdictions and, as the report notes, it often includes significant gaps in protection. Enforcement is scattered across a range of agencies, often with no strong original mandate to enforce privacy legislation. The report also found that even in jurisdictions in which constitutional privacy provisions exist, a prominent security threat such as that posed by South Korea's northern neighbor has a profound influence on the regulatory framework.

Nations such as Australia and India (see Appendix), which have no constitutional privacy provisions, have developed a diverse array of laws, regulations and other institutional mechanisms to accommodate privacy concerns. In part this is because they have close commercial ties to nations that do have these provisions. India in particular has developed a very large IT, software and associated international outsourcing industry that has led it to address privacy concerns above and beyond those emanating exclusively from domestic sources.

---

1 "Comparison of Privacy and Trust Policies in the Area of Electronic Communications", July 20, 2007. Available at: http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/final_report_20_07_07_pdf.pdf.

2 As will be seen in Section (B) below, however, limits on the European unification project mean that, despite the explicit recognition of a right to privacy in EU law, the EU statutory framework has thus far provided individuals with very little protection against intrusions on their privacy by governmental, as opposed to private, entities.

In India, the right to privacy derives from the Constitution as well as the common law of torts. The Constitution does not explicitly recognize the right to privacy but Article 21 provides for personal liberty,[3] and in various cases this has been taken by the Supreme Court to include the right to privacy against the state.

Although data protection is not explicitly provided for in India's Constitution, under its constitutional right to legislate in relation to matters not enumerated in the relevant lists, the central government has taken it to be an appropriate matter for its involvement. In 2009, the Information Technology (Amendment) Act 2008 was enacted in part to address domestic and regional security issues, including cybercrimes and cyberterrorism, but also, and importantly, the security concerns of foreign companies with respect to India's huge outsourcing industry. The Act provides penalties for various new cybercrimes (for example, cyberterrorism and identity theft), the recognition of new electronic documents (for example, electronic documents with e-signatures) and enhanced data security (for example, for intermediaries (any person who receives, stores, or transmits data for another person such as internet service providers)).

The establishment by the National Association of Software and Services Companies (NASSCOM) of the Data Security Council of India (DSCI) is part of the broader institutional response – in this instance, a self-regulatory part for the DSCI represents software companies and the business process outsourcing (BPO) and related IT industries. The function of DSCI is to establish, disseminate, monitor and enforce privacy and data protection standards for India's IT and outsourcing industry. Obviously, enforcement is the key challenge for DSCI – it is difficult to see how what is essentially a voluntary organization can effectively enforce the standards it establishes other than by the threat of expulsion.

The Information Technology Act 2000 and the Information Technology (Amendment) Act 2008 do not set out a comprehensive set of specific privacy and data protection principles in the manner of, say, the EU Directive or the OECD Guidelines. Rather, they require the use of "reasonable security practices and procedures", defined in terms of practices and procedures designed to protect sensitive personal information from unauthorized access, damage, use, modification, disclosure etc. The DSCI has recommended that companies implement one of the available industry-recognized standards such as the OECD Privacy Principles for Information Management Systems. Nevertheless, there is no requirement that companies undergo an audit to verify the existence and efficacy of the controls they have in place to meet any such industry standards.

3 This also enables India to partially fulfil its international obligations under the International Covenant on Civil and Political Rights, in which a basic right to privacy is recognized.

In India there is thus a heavy reliance on self-regulation and contractual provisions to protect individual privacy and identities, particularly for foreign citizens whose data are processed in that country.

Although Australia, like India, has no constitutional protection of privacy, it provides for a greater degree of privacy protection than does India. The key piece of Australian legislation pertaining to privacy is the Privacy Act 1988. The Office of the Privacy Commissioner is the federal agency responsible for overseeing the operation of the Privacy Act. Most law enforcement agencies in Australia are covered by the Privacy Act. The intelligence and defense intelligence agencies are, however, partially or completely exempt from it.

The Privacy Act gives effect to Article 17 of the International Covenant on Civil and Political Rights and the OECD's Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data. The Privacy Act regulates the collection, use, storage, disclosure and correction of personal information. The requirements of the Act include the National Privacy Principles (NPP) (applying to private sector organizations) and the Information Privacy Principles (IPP) (applying to Australian government agencies).

The Office of the Privacy Commissioner's (OPC) responsibilities include overseeing and monitoring compliance with the Privacy Act, investigating breaches of the Data-matching Program (Assistance and Tax) Act 1990 and monitoring compliance with record-keeping requirements of the Telecommunications Act 1997. As a consequence, the OPC conducts audits and examines records, receives and investigates privacy complaints and enforces the Act through determinations and court proceedings.[4]

Although the Privacy Act applies to private sector organizations as well as Australian government agencies, the OPC does not have the power to conduct audits of organizations in the private sector. Moreover, there are various public sector agencies that are exempt from the Privacy Act and, therefore, from oversight and monitoring by the OPC. Further, the Privacy Act does not cover businesses with less than AU$3 million annual turnover (that is, the majority of businesses in Australia).

The federal Privacy Act does not cover state public sector agencies and the OPC does not have jurisdiction with respect to state public sector agencies. These come under the jurisdiction of the various state privacy commissioners – for example, the Office of the Victorian Privacy Commissioner – and are covered by state legislation. Not all the states have privacy legislation or privacy commissioners.

---

4 See *The Operation of the Privacy Act: Annual Report 2008-2009* (Canberra: Office of the Privacy Commissioner, 2009).

In Australia, other than the Victorian Commissioner for Law Enforcement Data Security, there is no statutory body concerned exclusively with data security. At the federal level and in other states data security – specifically, law enforcement data security – is simply one of the functions of oversight agencies with a wider remit. Thus the Crime and Conduct Commission in Queensland oversees the Queensland Police (and other Queensland public sector agencies) and has a concern with data security.

Accordingly, although it does not have a constitutional protection of individual privacy and there are various gaps in its privacy legislation and enforcement mechanisms, Australia does have statutory protection of privacy from both government and non-government intrusion and it does have a range of enforcement mechanisms. Moreover, as will become evident, Australia affords a greater degree of privacy for individuals, notably from intrusion by corporations, other organizations and individuals in the private sector, than a country such as the US which has constitutional guarantees that do not apply to non-government intrusion.[5]

For our present purposes we will provide a detailed treatment of the particularities of liberal disagreement as they manifest themselves in differences between the US and the EU. In this chapter we endeavor to provide:

(A) An overview of US constitutional and statutory protections of the privacy of personal data and telephone and internet communications. We will also include some discussion of how US post-9/11 law "on the books" (primarily FISA and the Patriot Act) dealt with the tensions between national boundaries, cyberspace and globalization; how these statutes were contravened by the executive branch's post-9/11 surveillance of phone and cybercommunications; the lawsuits brought to remedy these violations and the barriers raised in response (e.g. telecommunications immunity and assertions of state secrets privilege); and, finally, brief general reflections on the (in)efficacy of the separation of powers in reining in surreptitious government abuses of power;

(B) An overview and comparison of EU data protection law with US law.

In Chapter V we provide an explanation of how the differences between EU and US law underlie the PNR and SWIFT disputes, and a discussion of the national identity card issue within the framework of EU law's weaker concern with data protection from government rather than from private parties (the reverse of the priorities of US law).

5 As will be explained in Section (A) below, however, some protections against intrusions on individual privacy are contained in the statutory law of the United States.

(A) United States of America

The basic structure of United States law

Three basic principles underlie the legal system of the United States: (i) the existence of constitutional, statutory and common law, (ii) federalism and (iii) the separation of powers. Under federalism, each of the fifty states has its own legal system which is separate and distinct from the federal legal system. The autonomy of state law is limited, however, by the Supremacy Clause of the US Constitution, which provides that the federal constitution is "the supreme law of the land".[6] The Due Process Clause of the Fourteenth Amendment places a further major limit on the autonomy of state law by providing that no state "shall deprive any person of life, liberty or property, without due process of law."

The basic American principle of judicial review, as first enunciated by the United States Supreme Court in *Marbury v. Madison*,[7] provides that as part of its power to "say what the law is" the judicial branch of the US government, as opposed to the executive or legislative branch, has the final say in interpreting the Constitution. This in turn means that the federal courts have the power to decide whether federal or state legislation or actions by federal or state officials conform to the Constitution's commands. Under the common law tradition of the United States, the meaning and application of various constitutional provisions is determined by precedent; that is, previous case law. As the highest federal court, the United States Supreme Court is the ultimate authority on the meaning and application of the Constitution; its interpretations are binding on the lower federal courts and the state courts. The Supreme Court and the lower federal courts also have the power to interpret and apply federal statutes and regulations. However, absent a determination of unconstitutionality, the legislature or executive has the power to rewrite statutes or regulations to counter judicial interpretations with which it disagrees.

In contrast with federal legislation and regulations, state law is not within the power of the federal courts to interpret or apply. The highest court of each state is the ultimate authority on the meaning and application of the state's constitution, legislation, regulations, and common law. Although a state's constitution and enacted laws cannot deprive its citizens of the rights guaranteed by the Due Process Clause of the Fourteenth Amendment, or other provisions of the Constitution, a state court can interpret its state constitution to provide its citizens with greater rights than the federal Constitution, as interpreted by the

6 United States Constitution, Article VI, 2.
7 5 U.S. (1 Cranch) 137 (1803).

Supreme Court, provides.[8] A state's legislature and executive can also issue laws and regulations that expand individual rights beyond the floor provided by the Supreme Court's interpretation of federal constitutional rights.

The protection of privacy under the United States Constitution

Although the word "privacy" is absent from the United States Constitution, rights to privacy are implicit in the Fourth Amendment's prohibition of unreasonable searches and seizures and the First Amendment's protection of freedom of speech and association.[9] These rights, like all those in the Bills of Rights, protect individuals only against the federal government. The United States Supreme Court has held, however, that the Due Process Clause of the Fourteenth Amendment incorporates both First and Fourth Amendment rights; in other words, it makes these rights effective against the governments of the states.[10] Individual rights under the United States Constitution are exclusively rights against government action; the federal Constitution does nothing to protect individuals against intrusions on their privacy by corporations, associations or private individuals.[11]

The protection of privacy under the Constitution has been importantly shaped by the Fourth Amendment exclusionary rule and the Sixth Amendment's right to counsel. The exclusionary rule, which the Supreme Court made effective against the federal government in *Weeks v. United States* (1914) and effective against the states in *Mapp v. Ohio* in 1961, makes evidence obtained through violations of the Fourth Amendment inadmissible in criminal prosecutions.[12]

---

8 Justice William Brennan was a vigorous advocate of interpreting state constitutions to expand individual rights. See, e.g., Justice William F. Brennan, Jr., "The Bill of Rights and the States", *New York University Law Review* 61 (1986): 535. For another view of the relations between judicial interpretations of the federal and state constitutions of the United States, see Paul W. Kahn, "Interpretation and Authority in State Constitutionalism", *Harvard Law Review,* 106 (1993): 1147.

9 The Ninth Amendment, which provides that the "enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage other rights retained by the people", has also been interpreted to protect individual privacy. See e.g. *Griswold v. Connecticut*, 381 U.S. 479, 486 (1965) (Goldberg, J., concurring); Charles Black, *Decision According to Law* (New York: Norton, 1981).

10 See e.g. *Gitlow v. New York*, 268 U.S. 652 (1925) (Fourteenth Amendment Due Process Clause incorporates First Amendment right to free speech); *National Association for the Advancement of Colored People v. Alabama*, 357 U.S. 449 (1958) (freedom of expressive association applied against the states); *Mapp v. Ohio,* 367 U.S. 643 (1961) (incorporating Fourth Amendment protections into the Due Process Clause of the Fourteenth Amendment).

11 See *Katz v. United States,* 389 U.S. 347, 351 (1967) (stating that "the protection of a person's general right to privacy – his right to be let alone by other people – is, like the protection of his property and of his very life, left largely to the law of the individual States" (footnotes omitted)).

12 *Weeks v. United States,* 232 U.S. 383 (1914); *Mapp v. Ohio,* 367 U.S. 643 (1961). Although the subject is beyond the scope of this study, it should be noted that the US Supreme Court has carved out increasingly severe exceptions to the exclusionary rule. *See e.g. United States v. Leon*, 468 U.S. 897 (1984); *Hudson v. Michigan*, 547 U.S. 586 (2006); *Herring v. United States*, 129 S.Ct. 695 (2009).

As a practical matter, criminal defendants are unlikely to obtain the suppression remedy unless they are represented by attorneys. In *Johnson v. Zerbst* (1938) the Supreme Court established that the Sixth Amendment entitles all indigent criminal defendants in federal court to government-provided attorneys.[13] In *Gideon v. Wainwright* (1963) the Supreme Court extended the Sixth Amendment right to government-provided counsel to indigent defendants in state courts.[14] Since the overwhelming majority of criminal defendants in the US are indigents,[15] the joint effect of these Fourth and Sixth Amendment cases was to increase the number of motions by criminal defendants to suppress evidence on Fourth Amendment grounds. This, together with the paucity of civil law suits brought to vindicate Fourth Amendment rights,[16] means that Fourth Amendment claims are typically brought by factually guilty people. Unless a criminal defendant was caught red handed there is no incriminating evidence to suppress. The case law interpreting the protection of privacy under the Constitution has been importantly shaped by the typical Fourth Amendment litigant's dual status as both (i) an apprehended criminal who seeks to suppress incriminating evidence and (ii) an assertor of the people's rights against government.[17]

The *Katz* expectation of privacy test and Fourth Amendment protections of telephone communications

Since the Fourth Amendment protects people from "unreasonable searches or seizures" a government intrusion must count as a search or seizure for Fourth Amendment requirements to apply. In *Katz v. United States* (1967) the United States Supreme Court was faced with the question of whether Charles Katz had been subject to a search or seizure when by means of a device attached to the outside of a public telephone booth law enforcement agents listened in to his side of telephone conversations transmitting illegal gambling information. In a departure from existing precedent, the Supreme Court reasoned that whether there had been a Fourth Amendment search or seizure did not depend on whether a public telephone booth was "a constitutionally protected area",

13 304 U.S. 458.

14 372 U.S. 335.

15 See e.g. Bureau of Justice Statistics, *State and Local Public Defender Offices,* at: http://bjs.ojp.usdoj.gov/index.cfm?ty=tp&tid=215 ("Publicly financed counsel represented about 66% of federal felony defendants in 1998 as well as 82% of felony defendants in the 75 most populous counties in 1996.").

16 Civil actions seeking damages for Fourth Amendment violations by federal and state agents are respectively available under *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics,* 403 U.S. 388 (1971) and 42 U.S.C. § 1983. See Anthony G. Amsterdam, "Perspectives on the Fourth Amendment", *Minnesota Law Review,* 58 (1974): 349, 428–34, and Yale Kamisar, "Remembering the Old World of Criminal Procedure: A Reply to Professor Grano", *University of Michigan Journal of Law Reform,* 23 (1990): 537, 562–65, for discussions of why such suits are difficult to win and seldom brought.

17 For an extended discussion of how these two views of the criminal defendant have shaped Fourth Amendment case law, see Adina Schwartz, "Homes as Folding Umbrellas: Two Recent Supreme Court Decisions on 'Knock and Announce'", *American Journal of Criminal Law,* 25 (1998): 545–94.

as "the Fourth Amendment protects people, not places."[18] Further departing from precedent, the Supreme Court reasoned that the fact that the wiretap was effected without physical penetration of the telephone booth did not mean that there was no Fourth Amendment search or seizure. "[T]he reach of [the Fourth] Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[19] The Supreme Court replaced those tests with the test that Fourth Amendment protections apply only when government action intrudes on (i) a person's "actual (subjective) expectation of privacy" and (ii) the subjective expectation is "one that society is prepared to recognize as 'reasonable.'"[20] Under this test, Katz was subject to a Fourth Amendment search or seizure when the agents listened in to his side of the conversations because he had sought to keep his conversations private by closing the door of the phone booth. Moreover, Katz's subjective expectation that his conversations would be kept private was objectively reasonable because of "the vital role that the public telephone has come to play in private communication."[21]

The consensual wiretap exception

Four years later in *United States v. White*, the United States Supreme Court carved out the so-called "consensual wiretapping" exception to Fourth Amendment protections of the privacy of telephone conversations. *White* dealt with the technique of third party bugging, wherein informants engage in conversations with suspects and simultaneously transmit those conversations to law enforcement agents who record them. The justices in *White* acknowledged that third-party bugging was possible only because suspects subjectively expected that their conversations would be kept private. "Our problem is not what the privacy expectations of particular defendants in particular situations may be or the extent to which they may in fact have relied on the discretion of their companions. Very probably, individual defendants neither know nor suspect that their colleagues have gone or will go to the police or are carrying recorders or transmitters. Otherwise, conversation would cease . . ."[22] The Supreme Court reasoned, however, that third-party bugging does not count as a Fourth Amendment search or seizure because it is not reasonable for criminals to expect that their conversations with their cohorts will remain private. "Inescapably, one contemplating illegal activities must realize and risk that his companions

18 *Katz v. U.S.,* 389 U.S. 347, 351 (1967).
19 *Ibid.,* 353.
20 This classic formulation of the *Katz* test is in Justice Harlan's concurrence. Interestingly, Harlan departed from the majority in reasoning that a person's location will usually determine whether he or she has a subjective expectation of privacy that counts as reasonable and is, accordingly, subject to Fourth Amendment protections. *Ibid.,*361 (Harlan, J., concurring).
21 *Ibid.,* 352.
22 *United States v. White,* 401 U.S. 745, 751–52 (1971).

may be reporting to the police. If he sufficiently doubts their trustworthiness, the association will very probably end or never materialize. But if he has no doubts, or allays them, or risks what doubt he has, the risk is his."[23]

In this assumption of risk analysis, the Supreme Court assumed that the only people who may be subject to third-party bugging are those who are, in fact, engaged in crime. The language about the risks that "one contemplating illegal activities" assumes contrasts interestingly with the language that the Supreme Court used in the *Katz* case in holding that Katz was entitled to Fourth Amendment protections. "No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[24] No mention is made of the fact that Katz (like White) was seeking to suppress conversations that revealed he was engaged in crime.

The pen register exception

In *Smith v. Maryland* in 1979, the United States Supreme Court carved out a further exception to the Fourth Amendment protections of telephone communications. There, at the behest of the police, a telephone company had used a pen register to record the numbers dialed from the defendant's home telephone. In reasoning that the use of the pen register did not constitute a search under the Fourth Amendment, the Supreme Court expanded on the idea, implicit in *White*, that one has no reasonable expectation that information one reveals to a third party will not, in turn, be revealed to the government. Since, under this analysis, one is entitled either to expect privacy against everyone or to expect it against no one, and telephone company employees have access to the numbers one dials from one's phone, the government's use of a pen register cannot infringe on any privacy one can reasonably expect.[25] However, the application of the *Katz* test to deny Fourth Amendment protections to information revealed to third parties would seem to be inconsistent with the holding that Katz was entitled to Fourth Amendment protections. Telephone company employees cannot only access numbers dialed; they can listen in on conversations as well. The *Smith* Court distinguished *Katz* away on the ground that "a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications."[26]

---

23 *Ibid.*, 752.

24 *Katz*, 389 U.S. at 352.

25 The *Smith* Court also reasoned that "people in general [do not] entertain any actual expectation of privacy in the numbers they dial." 442 U.S. 735, 742 (1979).

26 *Ibid.*, 741.

Fourth Amendment protections of email and internet communications

Thus far, the United States Supreme Court has avoided the question of whether individuals enjoy reasonable expectations of privacy and, hence, Fourth Amendment protections in regard to internet and other electronic communications. *City of Ontario v. Quon* (2010) is the Supreme Court's only Fourth Amendment decision on electronic communications.[27] The issue there was whether a police officer's Fourth Amendment rights were violated when police department officials requested from the service provider and read transcripts of text messages that the police officer had sent with a two-way pager provided by the department over the wireless service to which the department subscribed. In his opinion for the majority, Justice Kennedy avoided the question of whether the officer had reasonable expectations of privacy and hence Fourth Amendment rights in regard to his text messages, holding that even if this were the case, the department officials' acts of requesting and reading the transcripts of his text message were reasonable, and thus did not violate any Fourth Amendment protection that the officer might have enjoyed. Despite holding that the issue of the reasonableness of the officer's expectations of privacy need not be reached, Justice Kennedy dwelt at length on the difficulty that emerging changes in communications technology create for determining the reasonable expectations of privacy that individuals have today.

> The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. In *Katz*, the Court relied on its own knowledge and experience to conclude that there is a reasonable expectation of privacy in a telephone booth. It is not so clear that courts at present are on so sure a ground. . .
>
> Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. As one *amici* brief notes, many employers expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency. Another *amicus* points out that the law is beginning to respond to these developments, as some States have recently passed statutes requiring employers to notify employees when monitoring their electronic communications. At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve.

27 30 S.Ct. 2619.

> . . . [T]he Court would have difficulty predicting how employees' privacy expectations will be shaped by those changes or the degree to which society will be prepared to recognize those expectations as reasonable. Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own.
>
> A broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted. It is preferable to dispose of this case on narrower grounds.[28]

The Supreme Court's decision in *City of Ontario v. Quon* reversed the decision of the United States Court of Appeals for the Ninth Circuit's in *Quon v. Arch Wireless*.[29] There, the Ninth Circuit had faced the question that the Supreme Court subsequently avoided, holding both that the officer enjoyed reasonable expectations of privacy, and hence Fourth Amendment rights in regard to his text messages, and that the officer's Fourth Amendment rights were violated because department officials acted unreasonably in accessing and reading the transcripts of his text messages. In deciding in *Quon* in 2008 that reasonable expectations of privacy apply to text messages, the Ninth Circuit built on its decision in regard to email communications in *United States v. Forrester* (2007), reasoning that there is "no meaningful difference between the emails at issue in *Forrester* and the text messages at issue here."[30] The *Forrester* Court had applied the *Katz* test, as further developed in *Smith v. Maryland*, to hold that neither email addressing information nor the IP addresses of websites accessed from a particular email account were subject to Fourth Amendment protection.[31] Building on the principle articulated in *Katz*, *Smith v. Maryland*, and *Forrester* that Fourth Amendment protections apply to the contents of communications but not to addressing information on communications, *Quon* reasoned that users have reasonable expectations of privacy and hence Fourth Amendment protections in regard to the content of text or email messages. *Quon* further

---

28 130 S.Ct. at 2629-30 (citations omitted). Cf.City of Ontario v. Quan, 130 S.Ct. 2633, 2634–35 (Scalia, J., concurring in part and concurring in the judgment) (severely criticizing J. Kennedy's discussion of reasonable expectations of privacy).

29 529 F.3d 892 (9th Cir. 2008).

30 *United States v. Forrester,* 512 F.3d 500; *Quon v. Arch Wireless*, 529 F.3d 892, 905.

31 In a footnote (512 F.3d 500, 510 n.6), the *Forrester* Court indicated that since URLs provide more information than IP addresses about the information a person accesses on the web, Fourth Amendment protections might apply to surveillance techniques that enabled the government to determine the URLs of the web pages a person visited.

reasoned that the police department's formal policy of auditing officers' use of communications facilities provided by the department did not abrogate the officers' reasonable expectations of privacy because the department's informal policy was not to audit text messages so long as officers paid for any messages they sent beyond the quota allocated to their accounts.

The *Katz* test and the protection of personal records

In *United States v. Miller* (1976) the United States Supreme Court extended the notion that privacy is possessed by everyone or no one to imply that a person has no Fourth Amendment rights with regard to documents or records that he or she stores with a third party. The specific issue was whether Mitch Miller was subject to a search or seizure when, in response to a subpoena, his bank delivered his bank records to agents from the Alcohol, Tobacco and Firearms Bureau. In holding that Miller had no reasonable expectation of privacy and thus no Fourth Amendment rights in regard to his bank records, the Supreme Court cited *White* for the proposition that whenever one reveals information to a third party one assumes the risk that the information will in turn be conveyed to the government. "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. *United States v. White*, 401 U.S. 745, 751-752 (1971). This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[32] In other words, if Miller did not want the government to learn of his financial affairs he should have kept his money under his mattress.

Although the Supreme Court has not considered the issue, lower courts have applied the *Katz* test to hold that a subscriber's Fourth Amendment rights are not implicated when an ISP responds to a government request by providing the subscriber information corresponding to a particular email address, including the subscriber's name, address, telephone number, billing and account information and any other email addresses that he or she has with the ISP. In *Freedman v. America Online, Inc.* the United States District Court for the District of Connecticut applied *Smith v. Maryland's* distinction between contents of communications and non-content information to conclude that a person has no reasonable expectation of privacy with regard to his or her subscriber information. In so reasoning, the District Court did not so much as advert to the possibility of disagreement with its classification of an individual's credit card number and other financial information as "non-content information".[33]

---

32 *United States v. Miller,* 425 U.S. 435, 443 (1976) (footnotes and some citations omitted).

33 *Freedman v. America Online, Inc.,* 412 F.Supp.2d 174, 181 (D.Conn. 2005).

In addition, the *Freedman* Court relied on the notion that one has no reasonable expectation of privacy in regard to information revealed to a third party: "He [the subscriber] provided his name, address, credit card number, and telephone number to AOL when he registered to obtain internet access from AOL. That information was exposed to AOL employees in the normal course of business . . ."[34] In other words, anyone who subscribes to an ISP enjoys no Fourth Amendment protection in regard to the information he or she must provide in order to obtain an account.

The Fourth Amendment rights of record keepers

By contrast to the total absence of Fourth Amendment protection that an individual enjoys with regard to personal records in the possession of corporations or other entities, record-keeping entities have limited Fourth Amendment rights. Although the Fourth Amendment protects an entity that is subpoenaed for records, the United States Supreme Court has reasoned that because a subpoena is only a "figurative search" neither a warrant nor probable cause is required for its issuance. Rather, the Fourth Amendment requires that *after* a subpoena is issued, the party to whom it is addressed is able to obtain judicial review of the reasonableness of the subpoena's demands.[35] The reasonableness requirement for a subpoena is much less stringent than the probable cause requirement for a full-blown search. The requirement is met so long as an administrative subpoena is (1) "within the authority of the [issuing] agency"; (2) its demands are "not too indefinite"; and (3) the information sought is "reasonably relevant" to a proper inquiry.[36]

The Fourth Amendment and domestic and foreign threats to national security

In *Katz*, Justice White concurred separately for the purpose of insisting that, despite the decision's extension of the Fourth Amendment warrant requirement to wiretapping, the President or the Attorney General was still empowered to authorize warrantless wiretaps for national security purposes.[37] Justice Douglas, joined by Justice Brennan, wrote a separate concurrence in response to Justice White, asserting that a national security exception to the warrant requirement would violate the Fourth Amendment.[38] The *Katz* majority disposed of the issue

34 *Ibid.*, 183.

35 *See v. Seattle*, 387 U.S. 541, 541–45 (1967); *Oklahoma Press Pub. Co. v. Walling,* 327 U.S. 186, 217 (1946).

36 *United States v. Morton Salt Co.,* 338 U.S. 632, 652 (1950); *Oklahoma Press,* 327 U.S., 208.

37 *Katz v. United States,* 389 U.S. 347, 363 (White, J., concurring). In his concurrence, Justice White also insisted that the *Katz* test did not impinge on the government's right to use informants to obtain information, including through third-party bugging.

38 *Ibid.*, 359-60 (Douglas, J., concurring).

in a footnote that stated that the facts of the case did not present the question of whether the Fourth Amendment would allow warrantless wiretaps for national security purposes.

In *United States v. United States District Court* (1972), commonly known as the *Keith* case, the United States Supreme Court held that the Fourth Amendment does not allow the President to authorize warrantless wiretaps of domestic organizations for national security purposes. The Court emphasized, however, that the case did not require a "judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country."[39] While acknowledging that the distinction between domestic and foreign threats to national security might sometimes be difficult to draw, the Court stated that it was not faced with the issue. "No doubt there are cases where it will be difficult to distinguish between 'domestic' and 'foreign' unlawful activities directed against the Government of the United States where there is collaboration in varying degrees between domestic groups or organizations and agents or agencies of foreign powers. But this is not such a case."[40]

The Supreme Court has yet to decide whether there is a foreign intelligence exception to the warrant requirement. However, on January 12, 2009 the Foreign Intelligence Surveillance Court of Review (the FISA Court of Review) released a redacted version of a decision made on August 22, 2008, which held that under the Fourth Amendment there is an exception to the warrant requirement for surveillance directed at a foreign power or agent of a foreign power, where such person(s) are reasonably believed to be outside the United States and where foreign intelligence (as opposed to criminal investigation) is a significant purpose of the surveillance.[41]

Federal statutory protections of privacy

Federal statutes and state constitutions, statutes and case law expand on the protection of privacy that individuals are afforded under the Fourth Amendment. Neither state law nor such important federal statutes as the Right to Financial Privacy Act (RFPA), the Health Insurance Portability and Accountability Act of 1996 (HIPPA), the Cable Communications Policy Act of 1984 (Cable Act), the Video Privacy Protection Act of 1988 (VPPA), the Fair Credit Reporting Act (FCRA) or the Privacy Act of 1974 will be discussed here. The statutes to be discussed will be the Electronic Communications Privacy Act (ECPA),

39 407 U.S. 297, 308 (1972).

40 *Ibid*.

41 In re Directives [Redacted] Pursuant to 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004 (Foreign Int. Surv. Ct. Rev. 2008). This is one of only two published decisions by the FISA Court of Review.

which applies to surveillance of phone and internet communications by both government and private entities, and the Foreign Intelligence Surveillance Act (FISA), which regulates foreign intelligence surveillance. Also to be discussed are some of the post-9/11 amendments to ECPA and FISA and the US Federal Government's systemic evasion of the statutory limits on wiretapping.

The Electronic Communications Privacy Act (ECPA)

Enacted in 1986, ECPA is the successor to Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Whereas Title III dealt with private as well as government wiretapping of oral (face-to-face) and wire (telephone) communications, in response to changing technology Congress made the purview of ECPA extend to electronic (roughly, internet) as well as oral and wire communications. The protections of communications privacy in ECPA include not only those in its Wiretap Act but also those in its Stored Communications and Pen/Trap Acts. The Wiretap Act applies to the contemporaneous acquisition of the contents of communications and updates the protections provided in Title III of the Omnibus Crime Control and Safe Streets Act of 1968. The Stored Communications Act deals with subscriber records and subscriber communications stored by communication service providers (telephone companies and ISPs), while the Pen/Trap Act deals with "to" and "from" (addressing information) on telephone and electronic communications (roughly, phone numbers, email addressing information, URL's and IP addresses of websites and ISP subscriber accesses). As noted above, FISA, not ECPA, governs foreign intelligence wire taps and pen/traps.

The Wiretap Act of ECPA

The Wiretap Act prohibits wiretapping by the government or any individual or private entity, subject to three major exceptions. Firstly, a communications services provider may intercept communications where this is necessary for providing its services or for protecting its rights or property. A communications service provider may also record the fact that a communication was initiated or completed in order to protect itself, another provider providing services toward the completion of the communication, or someone using its services from fraudulent, unlawful or abusive use of the communication service.

Secondly, there is an exception for consensual wiretapping where the requisite consent is that of only one party to a communication. Thus, the ECPA, like the Fourth Amendment, does not protect individuals against the government's use of informants, including third-party bugging. Moreover, under the ECPA a person may be deemed to have implicitly consented to the interception of communications. For example, the consent exception may apply if an employer "banners" employees' computers so that when they log on a screen informs

them that their use of the computer is exclusively for business purposes and that internet communications will be periodically screened. Consent to interceptions may also be inferred if telephone callers are informed that their calls may be monitored and recorded.

Thirdly, state and Federal Government officials may intercept communications either by obtaining a warrant from a judge or magistrate or without a warrant in exigent circumstances. To obtain a warrant, the government must provide probable cause to believe that (i) a particular person(s) has committed or is about to commit one of certain enumerated crimes,[42] (ii) communications pertaining to the offense will be obtained through the interception and (iii) the facilities from which or the location at which the oral, wire or electronic communications are to be intercepted are being used or are about to be used to commit the particular offense, or are leased or commonly used by the suspect(s). A showing must also be made that other techniques besides wiretapping for investigating the crime have failed or would be too dangerous or unlikely to succeed. Judicial orders authorizing interceptions must specify that the interception is to last no longer than necessary to achieve the objectives of the interception and, in any event, no longer than thirty days, subject to an extension by the court for another such period. In addition, interceptions are to be conducted so as to minimize the acquisition of communications other than those specified in the warrant. A judicial order may direct a communications services provider or landlord to provide information, facilities or technical services to assist government officials in the authorized interception, subject to compensation for reasonable expenses.

The Stored Communications Act of ECPA

As a result of its definitions of ''electronic storage'', ''electronic communication service'' and ''remote computing service''[43] the Stored Communications Act (SCA) protects only voicemail or email stored on a public ISP once it is opened; it does not protect opened emails stored on a university or other non-public ISP. The SCA does, however, protect unopened voicemail or email regardless of whether it is stored on a public or private system.[44] In addition, the SCA accords some protection to records or other information that telecommunications services and communications storage facilities hold about subscribers.

The SCA criminalizes unauthorized access to a telecommunications service for purposes of obtaining, altering or preventing access to unopened email or voicemail, with exceptions for the provider of the service or a user of the service

42 The PATRIOT Act expanded the list of enumerated crimes.

43 The terms are defined, respectively, in 18 U.S.C. Sec. 2510 (17), 118 U.S.C. Sec. 2510 (15) and 18 U.S.C. Sec. 2711 (2).

44 The PATRIOT Act amended ECPA so that the acquisition of voicemail was no longer governed by the stricter requirements of the Wiretap Act.

with regard to his or her own communications. Telecommunication services and communications storage facilities are prohibited from disclosing the contents of their subscribers' wire or electronic communications, whether opened or unopened, to private individuals or entities, with exceptions for (i) addressees or intended recipients of the communications and their agents, (ii) employees or persons whose facilities are used to forward communications, (iii) disclosures that are necessary for rendition of the service or for protecting the rights and property of the service provider and (iv) disclosures with the consent of one of the parties to a communication. By contrast, telecommunication services and facilities are free to disclose records or information about their subscribers or customers to "anyone other than a governmental entity", so long as the records or information do not include the contents of communications.[45]

Under the SCA, the government must meet escalating requirements in order to be entitled to have telecommunications services and computer storage facilities disclose (i) subscriber records, (ii) opened email stored with a provider of computer services or facilities to the public or email or voicemail that the addressee or intended recipient has not opened for more than 180 days or (iii) email or voicemail that the addressee or intended recipient has not opened for 180 days or less.

To obtain records, including the subscriber's name, address, local and long distance telephone connection records or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service (including any credit card or bank account number), the government need present the telecommunications company or communications storage facility with only a federal or state administrative, grand jury or trial subpoena.[46] Notice need not be provided to the subscriber.

To obtain opened email or voicemail from a communications storage facility or unopened email or voicemail that has been stored with a telecommunications provider for more than 180 days, the government may use either a federal or state administrative, grand jury, or trial subpoena or obtain a court order for such disclosure by presenting "specific and articulable facts" that provide "reasonable grounds to believe that the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation."[47] In either case, prior notice to the subscriber is necessary. However, if it uses a subpoena, the government may delay giving notice for up to ninety days, subject to a further period of ninety days, if the prosecutor or other officials in charge of an

45 18 U.S.C. Sec. 2702 (c)(6).

46 The PATRIOT Act added "records of session times and durations" and "any temporarily assigned network address" to the information that the government can obtain with a subpoena under 18 U.S.C. Sec. 2703 (c) (2).

47 18 U.S.C. 2703(b), (d).

investigation certifies that the delay is necessary to avoid endangering a person's life or safety, jeopardizing the investigation or unduly delaying a trial. If the government obtains a court order for the emails, similar delays in notification may be obtained if the court finds them necessary to avoid endangering a person's life or safety, jeopardizing the investigation or unduly delaying a trial.[48] The requirement of notice does not apply, however, if the government obtains a warrant using the procedures described in the Federal Rules of Criminal Procedure.

By contrast to the more lax requirements that apply to records and voicemail and email that is either opened or unopened for more than 180 days, the government may require a telecommunications provider to disclose unopened email that has been stored with it for 180 days or less only if it obtains a warrant using the procedures described in the Federal Rules of Criminal Procedure.[49]

Does the SCA violate the Fourth Amendment by allowing the government to access opened emails or emails stored for more than 180 days without a warrant?

In *United States v. Warshak* (2011), the United States Court of Appeals for the Sixth Circuit confronted the question that the Supreme Court had declined to resolve in *City of Ontario v. Quon,* holding that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP.'"[50] On this basis, the *Warshak* Court further held that the Fourth Amendment requires the government to obtain a warrant backed by probable cause before it can compel a commercial ISP to turn over the contents of a subscriber's emails. As the *Warshak* decision recognized, this reasoning implies that it is unconstitutional for the SCA to provide that the government need only obtain a warrant in order to obtain emails that have been stored for 180 days or less: "[T]o the extent that the SCA purports to permit the government to obtain . . . emails warrantlessly, the SCA is unconstitutional."[51]

An unresolved controversy: Is email in transit covered by the wiretap or the stored communications provisions of ECPA?

Unless the *Warshak* decision results in a change in the Stored Communications Act, the Wiretap Act requires that the government meet more stringent conditions to obtain a warrant than the government is required to meet in order to obtain emails under the Stored Communications Act. The unresolved controversy over

48 18 U.S.C. Sec. 2705.
49 18 U.S.C. Sec. 2703(a).
50 631 F.3d 266, 288 (citation omitted).
51 *Ibid*.

whether the interception of an email before it reaches its intended recipient's mailbox counts as a wiretap or as access to a stored communication therefore has major implications regarding the protection of email from government intrusion.

This controversy arises because the Wiretap Act applies to "intercepts" or disclosures of intercepts of "electronic communications." An electronic communication is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system that affects interstate or foreign commerce."[52] Although this definition does not mention "electronic storage" of communications, in the course of traveling between their senders and recipients emails are broken into packets and then passed from one computer to another on the internet. "[E]ach computer along the route stores the packets in memory, retrieves the address of their destination, and then determines where to send it next based on the packet's destination."[53] This implies that, as they travel between sender and recipient, emails are in "electronic storage", which ECPA defines in part as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof."[54] The question is whether the absence of the term "electronic storage" in the definition of "electronic communication" means that an interception of an email as it travels between sender and receiver cannot count as an "interception of an electronic communication" and thus cannot be subject to the provisions of the Wiretap Act. In other words, does the fact that emails are temporarily stored in the course of their transition over the internet mean that they are stored communications subject to the lesser protections of ECPA's Stored Communications Act?

In *United States v. Councilman* (2005), the United States Court of Appeals for the First Circuit held in an *en banc* decision that the Wiretap Act applies to email messages that are temporarily stored in the course of transit.[55] In *United States v. Szymuszkiewicz* (2010) the United States Court of Appeals for the Seventh Circuit adopted *Councilman's* position.[56]

The Pen/Trap Act of ECPA

The Pen/Trap Act includes a general prohibition of the installation and use of "pen registers" and "trap and trace devices". These are defined respectively as devices that record or decode the "to" and "from" addressing information, but not the contents, of wire and electronic communications (e.g. telephone numbers,

52 18 U.S.C. 2510 (15).

53 *United States v. Councilman*, 373 F.3d 197, 205 (1st Cir. 2004) (Lipez, J., dissenting), *rev'd on rehearing en banc*, 418 F.3d 67 (1st Cir. 2005).

54 18 U.S.C. 2510 (17) (A).

55 418 F.3d 67, 79.

56 622 F.3d 701, 706.

email addresses, IP addresses of websites).[57] An exception to this prohibition exists for telecommunications providers with the consent of a subscriber, or in connection with providing, operating or testing their services, protecting their rights or property or protecting their users from unlawful or abusive use of their services. In addition, telecommunications providers may record the initiation and completion of communications in order to protect themselves, their users or other providers involved in the completion of a communication from fraudulent, illegal or abusive use of the service.

Federal and state courts may issue orders authorizing federal or state government officials to install and use pen/trap devices either on their own or with the assistance of telecommunication service providers. To obtain an order, an attorney for the Federal Government or a state law enforcement or investigative officer must certify ''to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.''[58] Although courts are to take such certifications at face value and not independently assess their veracity, the Pen/Trap Act does not allow the government to engage in dragnet surveillance. An order authorizing the installation and use of a pen/trap must specify (i) the offense to which the information likely to be obtained from the pen/trap relates, (ii) the identity, if known, of the person who is the subject of the investigation, (iii) the number or other identifier and, if known, the telephone line or other facility to which the pen/trap is to be attached and (iv) the identity, if known, of the person who leases or in whose name is listed the telephone line or other facility to which the telephone line is to be attached. A court is not to order the installation and use of a pen/trap for more than sixty days, though an order may be extended, upon application, but for no more than sixty days. In addition, the government is to use reasonably available technology to ensure that its recording or decoding of addressing information does not capture the contents of communications.

An exception to the requirement of a court order exists where the principal prosecuting attorney of a state, or various high level officials in the United States Attorney General's Office, ''reasonably determines'' that an emergency involving an immediate danger of death or serious bodily injury, conspiracy characteristic of organized crime, an immediate threat to national security or an ongoing attack on a ''protected computer'' (roughly, a computer connected to the internet) requires a pen/ trap to be installed and used before a court order

57 The PATRIOT Act expanded the definitions in ECPA so that pen registers and trap and trace devices include devices recording internet addressing information as well as telephone numbers. Pub. L. 107–56, Sec. 216 (c)(2) and (3) (2001).

58 18 U.S.C. Sec. 3123 (a) (1) and (2).

can be obtained. The use of the pen/trap must immediately terminate if a court order approving the installation or use is not obtained within forty-eight hours from the beginning of the installation.

Penalties for violations of ECPA

There are civil and criminal penalties for violations of the Wiretap, Stored Communications, and Pen/Trap acts of ECPA. Government wiretaps of oral and wire (telephone) communications are subject to a strong suppression remedy which prohibits the use of any illegally intercepted communication or part thereof "in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof."[59] The suppression remedy does not extend to illegal wiretaps of electronic communications or to violations of the Stored Communications or Pen/Trap acts.

FISA

The Foreign Intelligence Surveillance Act of 1978 (FISA) established a secret court to hear applications for warrants to conduct foreign intelligence surveillance. The FISA Court's hearings are closed to the public, and records of proceedings have been made available to the public only with classified information redacted.

The target of a FISA warrant must be a "foreign power" or an "agent of a foreign power", where a foreign power is defined as a foreign government or component, faction or entity directed by such or a group engaged in international terrorism or preparations for such. To obtain a warrant to wiretap telephone or internet communications, a national security or defense executive designated by the President must certify that the information sought is "foreign intelligence information". This is defined as information that is *relevant* to protection against foreign attacks, sabotage or international terrorism, or to the conduct of the national defense or foreign affairs. Information concerning a United States citizen or legal resident counts as "foreign intelligence information" only if it is *necessary* for the protection of the US against foreign attacks, sabotage or international terrorism, or for the conduct of national defense or foreign affairs. To issue a FISA warrant, a judge need find only probable cause to believe that the target of the surveillance is a foreign power or an agent of a foreign power and that the facilities or places at which the surveillance is directed are being used or about to be used by a foreign power or an agent of a foreign power. Activities protected by the First Amendment to the US Constitution cannot be the sole basis for a judicial finding of probable cause to believe that a citizen or permanent resident of the US is an agent of a foreign power.

---

59 18 U.S.C. Sec. 2515.

Instead of using FISA warrants for the purpose of obtaining foreign intelligence information, government officials might be tempted to use them to circumvent the stricter requirements that ECPA places on the use of wiretaps for criminal investigations. In 2001 the Patriot Act increased this danger by amending FISA so that the government no longer needs to certify in a warrant application that obtaining foreign intelligence information is "the primary purpose" of the surveillance. The designated government official need only certify that "a significant purpose" of the surveillance is obtaining foreign intelligence information. In 2002, in a decision considering the first appeal ever from a FISA court's decision on a warrant application, the FISA Court of Review held that the court had wrongly imposed the condition that the "primary purpose" of the surveillance could not be criminal prosecution of foreign agents for their foreign intelligence activities.[60] According to the court, the "primary purpose" test and its mandated wall between foreign intelligence and criminal investigations misinterprets FISA, especially as amended by the "significant purpose" language of the Patriot Act. The FISA Court of Review further held that the amendment did not violate the Fourth Amendment.

The Terrorist Screening Program

Debates about the legitimacy of the Patriot Act's extension of surveillance powers may be tantamount to debates about a distracting side show. On December 16, 2005, the *New York Times* reported for the first time that since 2001 the Bush Administration had engaged in massive, warrantless surveillance of telephone and email communications. In response to the article, Attorney General Gonzales confirmed the existence of a Terrorist Screening Program (TSP), conducted by the National Security Agency, and claimed that the FISA warrant requirements had been superseded by the Authorization for Use of Military Force Against Terrorists Act that Congress had passed on September 18, 2001. The Attorney General further claimed that the warrantless intercepts had been conducted only where the government had a reasonable basis to conclude that at least one party to the communication was outside the United States and that at least one party was affiliated with al-Qaeda or a related organization, or working in support of al-Qaeda. This claim was belied, however, when whistle blower Mark Klein informed the Electronic Frontier Foundation (EFF) that in its Folsom Street facility in San Francisco AT&T had given the NSA access to the contents of all of its subscribers' communications with subscribers of other ISPs.

60 *In re Sealed Case,* 310 F.3d 717 (FISC Rev. 2002).

Separation of powers and the difficulty of preventing surreptitious violations of the law by the executive power

This information about the massive evasion of the requirements of ECPA and FISA by the government and AT&T was brought to the attention of the Federal Court system in *Hepting v. AT&T*, a law suit in which the EFF sought damages against AT&T. This and other law suits were mooted, however, when Congress provided retroactive immunity to telecommunications providers who had participated in the Terrorist Screening Program. The FISA Amendments Act of 2008 required the dismissal of lawsuits against telecommunications providers if the government secretly certified to the court that the surveillance did not occur, was legal or was authorized by the President. In response to Congress' passage of the telecommunications immunity provision, EFF sued the government and named government officials directly in *Jewel v. NSA*, filed in September 2008. *Jewel* sought to stop the warrantless wiretapping and to hold the government officials behind the TSP accountable. On January 21, 2010, a federal district judge dismissed the *Jewel* case on the ground that the plaintiffs lacked standing to bring the lawsuit because they had not alleged an injury sufficiently peculiar to themselves or the class they represented: "[T]he harm alleged is a generalized grievance shared in substantially equal measure by all or a large class of citizens."[61] In other words, the judge held that legal redress was precluded by the enormous extent of the Executive's violation of the limits on surveillance that the Fourth Amendment, ECPA and FISA mandated. Although EFF plans to appeal the decision, the judge's interpretation of federal standing law may be correct.[62]

(B) European Union

The desire to remove barriers to commerce has been the primary impetus towards European unification since World War II. At the same time, state sovereignty has continued to be valued, particularly in the areas of national security and protection against crime. Reflecting these two aspects of the European unification project, EU law comprehensively and strictly regulates the collection, transmission and use of data about individuals by private entities, but its regulation of such activity by states is much less strict and much less comprehensive. In addition, private parties' obligations to protect data may be weakened for state purposes.

---

61 *Jewel v. NSA*, No. C 08-cv-4373, 2–3 (N.D.Cal. Jan.21, 2010).

62 *EFF Plans Appeals of Jewel v. NSA Warrantless Wiretapping Case,* January 21, 2010, at: http://www.eff.org/press/archives/2010/01/21.

Constitutional protections

The privacy of EU citizens is constitutionally protected by both the Convention for the Protection of Human Rights and Fundamental Freedoms (the European Convention on Human Rights (ECHR)) and the Charter of Fundamental Rights of the European Union. The constitutions of some of the individual states of the EU also give individuals rights to privacy, but the constitutional law of multiple member states cannot be given detailed treatment here. Instead we will provide only passing discussion of member states. However, at the end of this section on the EU we provide a somewhat more extensive discussion of the protection of individual privacy rights in one of the EU's member states, namely, the Netherlands. Accordingly, the Netherlands serves as an exemplification of the institutional embodiment of the EU's privacy rights.

The European Convention on Human Rights (ECHR)

The ECHR, which opened for signature in 1950 and went into effect in 1953, established rights that are incorporated in both EU law and the laws of each of the individual states of the EU. The ECHR also established the European Court of Human Rights, before which cases may be brought by any person who claims that a state party to the ECHR (including the EU states, other European states that belong to the Council of Europe and EU bodies such as the European Commission, the Council or the European Parliament) has violated his or her rights under the ECHR. State parties to the ECHR may also bring cases against other parties before the European Court of Human Rights, but this power is rarely used.

By contrast to the United States Constitution, the ECHR provides an explicit right to privacy. Article 8 states that:

> **Right to respect for private and family life**
>
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall 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 the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Unlike the right to privacy that courts have inferred from the First, Fourth, Ninth and Fourteenth Amendments to the United States Constitution, the right to privacy that Article 8 of the ECHR confers is not merely a negative right

against state interference but also a positive right to the enjoyment of privacy. The ECHR right to privacy does, however, resemble the right to privacy that courts have inferred from the US Constitution in not being an absolute right, but one that may be restricted for legitimate state purposes. National security, public safety and the prevention of disorder or crime are among the listed purposes for which Article 8, Section 2 of the ECHR allows states to interfere with privacy, subject to the requirements that such interference be in "accordance with law and . . . necessary in a democratic society" for furthering a listed purpose(s).

As discussed above, in *City of Ontario v. Quon* the United States Supreme Court explicitly declined to decide whether reasonable expectations of privacy and hence Fourth Amendment rights extend to electronic communications.[63] By contrast, the European Court of Human Rights has held that the protections of "private life" and "correspondence" in ECHR Article 8, Section 1 extend to emails and other internet communications as well as telephone calls, regardless of whether such communications take place in the workplace or at home.[64]

In a further contrast with US law, the European Court of Human Rights has reasoned that "information relating to the date and length of telephone conversations and in particular the numbers dialled . . . constitutes an 'integral element of the communications made by telephone'" that Article 8, Section 1 of the ECHR protects, and has extended that principle to email and other internet communications.[65] This contrasts with the US Supreme Court's position in *Smith v. Maryland* that reasonable expectations of privacy and Fourth Amendment protections extend to the contents of telephone communications but not to the numbers dialed, and with lower courts extensions of the distinction between protected contents and unprotected addressing information to email and other internet communications.[66]

The Charter of Fundamental Rights of the European Union

The Charter of Fundamental Rights of the European Union (the "EU Charter"), which was adopted in 2000 and went into effect with the Lisbon Treaty on December 1, 2009, applies to EU institutions. Individual countries of the EU are also subject to the Charter, but only insofar as they are implementing EU law, as opposed to matters on which the EU either has failed or lacks the competence to legislate.

---

63 130 S.Ct. 2619 (2010).

64 *Copland v. United Kingdom,* 45 Eur. Ct. H.R. 253, Section 41 (citing *Halford v. the United Kingdom*, *Reports of Judgments and Decisions* 1997–III, Section 44, and *Amann v. Switzerland*, 2000–II Eur. Ct. H.R. 247, Sec. 43).

65 *Ibid.*, Sec 43 (quoting *Malone v. the United Kingdom*, 82 Eur. Ct. H.R. (ser. A) Sec. 84).

66 See e.g. *Smith v. Maryland*, 442 U.S. 735 (1979); *United States v. Forrester,* 512 F.3d 500 (9th Cir. 2007); *Quon v. Arch Wireless,* 529 F.3d 892 (9th Cir. 2008).

The Charter's protections of privacy include Article 7 of the Charter, which is identical to the Article 8, Section 1 of the ECHR, and a special provision for protection of personal data in Article 8 of the Charter. The Charter provisions are:

> Article 7
>
> Respect for private and family life
>
> Everyone has the right to respect for his or her private and family life, home and communications.
>
> Article 8
>
> Protection of personal data
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

The interpretation of articles 7 and 8 of the Charter is guided by the European Court of Human Rights' interpretation of the right to privacy in the ECHR. The preamble to the Charter reaffirms the rights granted by the ECHR and by the case law of the European Court of Human Rights. Article 52(3) of the Charter indicates that the ECHR provides a floor, but not a ceiling, for interpreting the rights that the Charter provides.

The Lisbon Treaty entitles individuals to bring claims about an EU country's violation of their Charter rights in the courts of that country. The European Court of Justice can also rule on individual countries' obligations under the Charter, but only if a case is referred to it by the European Commission or a national court. Individuals may bring claims as to the violation of their Charter rights by an EU institution or body before the General Court (court of first instance) of the European Court of Justice, but only if a measure adopted by the EU institution or body has directly and individually affected them.

EU legislation

EU legislation on the collection, use and transmission of personal data is principally composed of three directives and one framework decision. These set forth goals that are binding on all EU states and that require each state to legislate forms and methods for achieving the goals. The directives and framework decision are:

- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data (the ''Data Protection Directive'');[67]
- Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (the ''e-Privacy Directive''),[68] as updated by Directive 2009/136/EC of the European Parliament and of the Council;[69]
- Directive 2006/24/EC 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 (the ''Data Retention Direction'');[70] and
- Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.[71]

Before turning to the specifics of the Directives and Framework Decision, it is crucial to note that although it is often claimed that EU law provides comprehensive standards for data protection, this is true only in regard to the collection, use and transmission of personal data by private parties for private purposes.[72] Until the Lisbon Treaty went into effect on December 1, 2009, policing and criminal justice in individual EU countries were outside the purview of EU law.[73] In a policy review of EU data protection law issued

67 Available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf and http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf.

68 Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML.

69 Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF.

In addition to updating the e-Privacy Directive, the 2009 Directive updated Directive 2002/22/E on universal service and users' rights relating to electronic communications networks and services and Regulation (EC) N. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

70 Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML.

71 Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:01:EN:HTML.

72 For the notion that EU data protection law is comprehensive see e.g. Monique Altheim, ''The Review of the EU Data Protection Framework v. The State of Online Consumer Privacy in the US'', EDiscoveryMap, March 17, 2011, available at: http://ediscoverymap.com/2011/03/the-review-of-the-eu-data-protection-framework-v-the-state-of-online-consumer-privacy-in-the-us; ''Data Protection in the European Union'', available at: http://ec.europa.eu/justice/policies/privacy/docs/guide/guide-ukingdom_en.pdf

73 This limitation of the scope of EU law resulted from the three-pillar structure which the Lisbon Treaty abolished. For a brief overview of the relations between the three pillars, the Lisbon Treaty and data

in November 2010 the European Commission stated that the Lisbon Treaty provided an opportunity "to lay down comprehensive and coherent rules on data protection for all sectors, including police and criminal justice. Under the review, data retained for law enforcement purposes should also be covered by the new legislative framework."[74] In particular, the Commission's policy review recognized, as will be discussed below, that in order to protect individuals' privacy, amendments are needed to Council Framework Decision 2008/977/JHA on Personal Data and Police and Judicial Cooperation.[75]

The Data Protection Directive

Scope

As discussed above, United States constitutional law limits only government activity, and the only further limits that federal law places on the collection, use and transfer of personal data consist of legislation and regulations that apply only to certain types of data collected by certain types of private or governmental entities (e.g. the Right to Financial Privacy Act (RFPA), the Health Insurance Portability and Accountability Act of 1996 (HIPPA), the Cable Communications Policy Act of 1984 (Cable Act), the Video Privacy Protection Act of 1988 (VPPA), the Fair Credit Reporting Act (FCRA) and the Privacy Act of 1974 (applying only to federal agencies)).[76] By contrast, the EU Data Protection Directive regulates

protection in the EU, see Daniel Cooper, Henriette Tielemans, and David Fink, "The Lisbon Treaty and Data Protection: What's Next for Europe's Privacy Rules?" *The Privacy Advisor*, at http://www.cov.com/files/Publication/44dd09f7-3015-4b37-b02e-7fe07d1403f4/Presentation/PublicationAttachment/8a89a612-f202-410b-b0c8-8c9b34980318/The%20Lisbon%20Treaty%20and%20Data%20Protection%20What%E2%80%99s%20Next%20for%20Europe%E2%80%99s%20Privacy%20Rules.pdf

74 EUROPA Press Releases Rapid, "European Commission Sets Out Strategy to Strengthen EU Data Protection Rules", IP/10/1462, Brussels, November 4, 2010, available at http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1462. The full text of the Commission's policy review, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, "A Comprehensive Approach on Personal Data Protection in the European Union", IP/10/1462, Brussels, November 4, 2010 ("Commission, 'A Comprehensive Approach on Personal Data Protection'") is available at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf. On the basis of the policy review and public consultation, the Commission intends to propose legislation in 2011 revising EU data protection law.

The European Commission, comprising Commissioners from each EU country, has the function of representing and upholding the interests of the EU as a whole by proposing new laws to Parliament and the Council, managing the EU's budget and allocating funding, enforcing EU law (together with the Court of Justice) and representing the EU internationally, for example, by negotiating agreements between the EU and other countries. See Europa, "European Commission", at http://europa.eu/about-eu/institutions-bodies/european-commission/index_en.htm.

75 Such amendment of the Council Framework Decision might assuage one scholar's concern that "[i]n the field of data-related police cooperation the importance of the EU is increasing. . . These developments on [sic] intelligence-led policing create enormous problems of legal protection, privacy and control as the legal framework of the EU does not focus on the rule of law questions in regard to police cooperation." Konrad Lachmayer, "European Police Cooperation and its Limits: From Intelligence-led to Coercive Measures", in *The Outer Limits of European Union Law*, ed. Catherine Barnard and Okeoghene Odudu (Oxford: Hart Publishing 2009), 106–07.

76 For an interesting discussion of how the development of the regulatory state under the New Deal may have led to diminished Fourth Amendment protections for records kept by third parties, see William J. Stuntz, "Privacy's Problem and the Law of Criminal Procedure", *Michigan Law Review* 93 (1995): 1016.

the collection, use and distribution of all records about individuals by private parties, except when this is done "by a natural person in the course of a purely personal or household activity."[77]

The broad scope of the Data Protection Directive comes from its application to all automatic processing of personal data and to all non-automatic processing of personal data that are contained or intended to be contained in filing systems that are structured so as to make personal data readily accessible. Processing is defined as any automatic or non-automatic operations on data, "such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[78] Under the Directive, personal data include any information pertaining to an identified person or to a person who can be directly or indirectly identified, "in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." [79]

Although the data controllers on whom the Directive imposes obligations include public authorities and agencies as well as natural persons and private legal entities, the Directive does not apply to data processing in connection with government activity that the EU was not empowered to regulate before the Lisbon Treaty. Accordingly, the Directive does not regulate "processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law."[80] Nor does the Directive apply to the "processing of sound and image data, such as . . . video surveillance" where this is done "for the purposes of public security, defence, national security, or in the course of State activities relating to the area of criminal law."[81] Even where the Directive applies, governments may enact legislation limiting the rights to access data and gain information that the Directive grants to individuals and restricting the obligations in regard to the quality of data that the Directive imposes on data controllers when such legislation is necessary to safeguard a broad variety of state functions. Article 12 of the Directive lists the state functions that may justify restrictions on the Directive's protections as national security, defense, public security, the prevention, investigation and prosecution of crime or professional breaches of ethics, important economic or financial interests of a State or the EU (including

77 Data Protection Directive, Article 3, Section 2. See also *ibid.*, Recital 12.
78 *Ibid.*, Art. 2(b).
79 *Ibid.*, Art. 2(a).
80 *Ibid.*, Art. 3, Sec. 2.
81 *Ibid.*, Recital 16. The video-surveillance that the Directive fails to regulate includes the use of CCTV in the United Kingdom which, with three million cameras in use, was the most extensive in the world as of 2009. See Alan Travis, "Lords: CCTV is Threat to Freedom", *The Guardian*, Feb. 9, 2009, available at: http://www.guardian.co.uk/uk/2009/feb/06/surveillance-freedom-peers.

monetary, budgetary and taxation matters) and monitoring, inspection, or regulatory functions that are connected, even occasionally, to the state's exercise of its powers in regard to public security and the preventing, investigating or prosecuting of crime or professional breaches of ethics or the state's or EU's important economic or financial interests. States may also limit data subjects' rights to information and access, and data controllers' obligations in regard to the quality of data in order to protect data subjects or the rights and freedoms of others.

Where it applies, the Directive requires EU countries to enact legislation that grants data subjects the following principal protections.

When can personal data be processed?

Sensitive data

The Directive imposes especially stringent conditions on the processing of sensitive data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, [or] concerning health or sex life."[82] States are to prohibit the processing of sensitive data without the explicit consent of the data subject except where such processing is necessary for the fulfillment of the data controller's rights and obligations under employment law, for the vital interests of the data subject or another where the data subject is physically or legally incapable of consenting to the data processing, or for health-related reasons where the processing is done by persons who are legally obligated to confidentiality. Trades unions, political and religious groups and other non-profit entities with religious, political or philosophical aims may also process sensitive data about their members without the members' consent if this is done in the course of their legitimate activities with appropriate guidelines and if the data are not disclosed to third parties without the data subject's consent.

States are empowered to enact additional exceptions to the requirement that sensitive data not be processed without the subject's consent for "reasons of substantial public interest", subject "to the provision of suitable safeguards",[83] and they are also free to determine when "a national identification number or any other identification of general application may be processed."[84] States may also enact exceptions, subject to specific legally established safeguards, to the rule that the processing of data relating to criminal offenses, convictions or security measures is to be controlled by official authorities.[85]

82 *Ibid.*, Art. 8.
83 *Ibid.*, Art.8, sec.4.
84 *Ibid.*, Art.8, sec.7.
85 *Ibid.*, Art.8, sec.5.

Other personal data

For other personal data, there are much broader exceptions to the requirement that data processing occur only with the subject's unambiguous consent.[86] Data may be processed in order to enable a data subject to enter into a contract, if necessary for the execution of a contract to which he or she is a party or if necessary to fulfill the data controller's legal obligations or to protect the data subject's vital interests. In addition, processing may occur where this is necessary for the public interest or for the exercise of official authority by the data controller or a third party to whom the data is disclosed. The legitimate interests of either the data controller or third party may also allow data to be processed without the subject's consent so long as these interests are not overridden by the data subject's rights to privacy or other fundamental rights.

However, the processing of non-sensitive personal data is limited by the data subject's right to object. Article 14 of the Directive provides that at least with regard to data whose processing is justified by the public interest or the legitimate interests or official functions of data controllers or third parties, a data subject has the right to object "on compelling legitimate grounds relating to his particular situation" at any time, and the processing must stop if the objection is justified.[87] Although the right to object does not apply where states have "otherwise provided by national legislation", the Directive prohibits states from limiting data subjects' right to object to the processing of personal data for direct marketing purposes on request and free of charge whenever data controllers anticipate such use of their data.[88] Data subjects must also be informed before their data are disclosed for the first time to third parties or used on these parties' behalf for direct marketing purposes, and explicitly offered the right to object free of charge to such disclosures or uses.[89]

The quality of data

The obligations of data controllers under Article 6 to ensure the quality of data include ensuring that processing is lawful and fair, that data are accurate and up-to-date and that reasonable steps are taken to rectify or erase inaccurate or incomplete data. In addition, data are to be collected only for specified, explicit and legitimate purposes and are not to be further processed for purposes that are incompatible with the original purpose of collection. The data controller's

86 *Ibid.*, Art. 7. Under the Directive, a data subject is deemed to consent only if there is a "freely given specific indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed." *Ibid.*, Art. 2 (h). This requirement of explicit consent contrasts with the notion of implicit consent that underlies much of United States law, including, among other instances, the lack of legal protection for information revealed to third parties, the notion of consensual wiretapping and the notion that people consent to certain uses of their data unless they opt out.

87 *Ibid.*, Art. 14 (a).

88 *Ibid.*, Art. 14 (a) and (b).

89 *Ibid.*, Art. 14(b).

obligations with regard to the quality of data also include ensuring that data be relevant and adequate to the stated purpose for collection and/or further processing, and that no more data than are needed for the stated purpose are collected or processed. Moreover, data are to be kept in a form that permits the identification of data subjects for no more time than is necessary to fulfill the stated purposes for collection and/or processing.

Data subjects' rights to information and access

Articles 10 and 11 of the Directive provide that, in regard to personal data obtained from either data subjects themselves or other sources, data subjects have the right to be informed of the purposes of the intended processing of the data and the identity of the data controller and any of his or her representatives. Where fairness to the data subject requires, he or she is also entitled to be informed of the recipients of the data and of his or her rights to access and to rectify data. Where the data subject is the source of personal data, he or she may also be entitled to learn whether replying to questions is mandatory, as well as the possible consequences of not replying. Where data is collected from sources other than the data subject, the subject may be entitled to learn the categories of data that the controller possesses or intends to disclose to a third party if this is required for the data processing to be fair.

Under Article 12, data subjects also have the right to obtain confirmation, at reasonable intervals and without undue expense or delay, of whether a data controller is processing data about them and, if so, to learn what data are being processed for what purposes and for what recipients. They are also entitled to any available information about the source of the data being processed and to be apprised of the logic underlying any automatic data processing operations that result in decisions that subject them to legal or other significant effects, such as determinations of creditworthiness or evaluations of their work. This right of access to one's personal data is linked to a right to correct the data held on one. Data subjects are entitled to have incomplete or inaccurate data, or data whose processing does not otherwise conform to the Directive's requirements, rectified, erased or blocked as appropriate and to have third parties notified of such changes.

Security and confidentiality of processing

Article 16 of the Directive provides that data processors and anyone acting under their authority or the authority of the data controller are not to process personal data except on the authority of the data controller.

Under Article 17, states are to mandate that data controllers "implement appropriate technical and organizational measures" to protect personal data from being accidentally or unlawfully destroyed, lost, altered, disclosed or accessed

without authorization or otherwise unlawfully processed.[90] Data controllers' obligations to ensure the security of data apply "in particular where processing involves the transmission of data over a network."[91] The security provided must be "appropriate to the risks represented by the processing and the nature of the data to be protected", taking account of "the state of the art and the cost of their implementation."[92] Even if they choose to have external providers perform the processing, data controllers remain obligated to ensure the security of data.

Transfer of data to non-EU countries

The Directive provides, in Article 25, that personal data may be transferred from an EU country to a third country only if the third country "ensures an adequate level of protection" for personal data. Adequacy is to be assessed by both the European Commission and individual EU countries, and beyond stating that adequacy should be assessed "in the light of all the circumstances surrounding a data transfer operation", the Directive provides no standards for assessing whether a third country's level of data protection is adequate.[93]

Article 26 provides a broad list of conditions under which states may allow data to be transferred to a third country even if the adequacy requirement is not met, including with the consent of the data subject, for contractual reasons, if "the transfer is necessary or legally required on important public interest grounds" and if the transfer is made from a register that is legally intended to provide information to the public and the legal conditions for consulting the register are met. In addition, individual states may authorize transfers of personal data on the basis of contractual obligations that data controllers impose on the entities to whom the data are transferred, and the Commission is empowered to decide that certain standard contractual clauses provide sufficient safeguards for transfers to countries whose overall level of data protection is inadequate.[94]

The Commission's criticisms of the Data Protection Directive's provisions for transfers to third countries

In its policy review of EU data protection law in November 2010, the European Commission opined that the ever-increasing globalization of data processing created a "general need to improve the current mechanisms allowing for international transfers of personal data, while at the same time ensuring that personal data are adequately protected when transferred and processed outside the EU and the EEA."[95] According to the Commission, "the Internet makes it

90 *Ibid.*, Art.17, sec. 1.
91 *Ibid.*
92 *Ibid.*
93 *Ibid.*, Art. 25, secs. 1 and 2.
94 *Ibid.*, Art. 26 (2) and (4).
95 Commission, "A Comprehensive Approach on Personal Data Protection," *supra*, at 2.4.1, available at: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.

much easier for data controllers established outside the European Economic Area (EEA) to provide services from a distance and to process personal data in the online environment; and it is often difficult to determine the location of personal data and of equipment used at any given time (e.g., in 'cloud computing' applications and services).''[96]

Among other things, the Commission criticized the lack of standards in the Directive for assessing the adequacy of a third country's level of data protection, stating that ''the exact requirements for recognition of adequacy by the Commission are currently not specified in satisfactory detail in the Data Protection Directive.''[97] In addition, the Commission criticized the lack of procedural guidelines for individual states' determinations of adequacy: ''This situation may lead to different approaches to assessing the level of adequacy of third countries, or international organisations, and involves the risk that the level of protection of data subjects provided for in a third country is judged differently from one Member State to another.''[98] In accord with its view that the Lisbon Treaty provides an opportunity for the extension of data protection principles to government operations, the Commission criticized ''the current Commission standard clauses for the transfer of personal data to controllers and to processors [in third countries whose level of data protection is inadequate on the ground] that they are not designed for non-contractual situations and, for example, cannot be used for transfers between public administrations.''[99]

Enforcement mechanisms in the Data Protection Directive

Under Article 28, each EU state is required to appoint an independent supervisory authority (or authorities) with the power to monitor compliance with the Directive within its territory, including investigative powers and effective powers of intervening to prevent the illegal processing of data or to order the blocking, erasure or destruction of illegally processed data. States' data supervisors are also to be empowered to bring legal proceedings when their state's laws implementing the Directive are violated and to hear claims concerning the protection of people's rights and freedoms with regard to

All European Economic Area (EEA) countries, including both the EU countries and the non-EU countries of Norway, Liechtenstein and Iceland, adhere to the Data Protection Directive. Strictly speaking, the Directive's provisions for data transfers to third countries are therefore provisions for transfers to non-EEA, as opposed to non-EU, countries. See School of African and Oriental Studies, University of London, ''Transfer Outside the EU'', available at: http://www.soas.ac.uk/infocomp/dpa/policy/outside.

96 Commission, 2.2.3. For an illustration of the tensions between the globalized nature of data processing and the EU's attempt to protect the privacy of its citizens, see Zach Whittaker, ''Microsoft Admits Patriot Act Can Access EU-Based Cloud Data'', ZDNet, June 28, 2011, available at: http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225.

97 *Ibid.*, 2.4.1.

98 *Ibid.*

99 *Ibid.*

the processing of personal data, including claims about the lawfulness of the abridgement of rights under the Directive for reasons of national security or other state purposes.

Although a state's supervisory authority may provide individuals with administrative remedies, each EU state is also required, under Articles 22–24, to provide individuals with judicial remedies for violations of their rights under the state's laws implementing the Directive, including the right to have data controllers compensate them for damages.

The Article 29 Working Party

Article 29 creates a Working Party comprising one representative each of the data supervisory authority (or authorities) of each EU state, the data supervisory authority (or authorities) established for EU institutions and bodies and the European Commission, for the purpose of contributing to the uniform implementation of the Data Protection Directive in the EU. Under Article 30, the Working Party is empowered to provide the Commission with opinions on the levels of protection of personal data in the EU and in third countries, to advise the Commission on amendments to the Data Protection Directive or other measures to safeguard individuals' rights and freedoms regarding personal data and to make recommendations on its own initiative on all matters relating to the protection of personal data. The Working Party is to present publicly available annual reports to the Commission, the European Parliament and the Council on the processing of personal data in the EU and third countries.

The e-Privacy Directive

Scope and relation to the Data Protection Directive

The principal United States legislation on telecommunications privacy, the Electronic Communications Privacy Act (ECPA) of 1986, is widely criticized for being based on outmoded assumptions about the technology it regulates.[100] By contrast, in enacting the e-Privacy Directive in 2002, the European Parliament and the Council recognized that the "development of the information society is characterised by the introduction of new electronic communications services."[101] It went on to say, "New advanced

100 See e.g. Mike Masnick, "Privacy: Senator Leahy Wants to Update Digital Privacy Law: Some Good, Some Bad", *TechDirt*, May 17, 2011, available at: http://www.techdirt.com/blog/?tag=ecpa; IAPP (International Assoc. of Privacy Professionals), "House Subcommittee Hears Call for ECPA Updates", June 25, 2010, available at: https://www.privacyassociation.org/.../2010_06_25_house_subcommittee_hears_call_for_ecpa_updates.

101 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (the "e-Privacy Directive"), Recital 5, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML.

digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user."[102]

The provisions of the e-Privacy Directive apply to personal data processed in connection with the provision of publicly available electronic communications services and networks. Thus its protections of privacy extend to telephone calls and any voice, text, sound or image messages sent over public communications networks and capable of being stored in the network or on recipients' terminals, and also apply to users' terminal equipment and information stored therein.[103] However, when communications are made over non-public electronic communications services and networks (e.g. university or corporate networks) the Data Protection Directive applies. In addition, the Data Protection Directive applies to any matters pertaining to the processing of personal data in connection with publicly available services or networks that the e-Privacy Directive does not specifically address.[104]

Like the Data Protection Directive, the e-Privacy Directive does not protect individuals' privacy against any government action that the EU was not empowered to regulate before the Lisbon Treaty. Therefore, the e-Privacy Directive does not limit individual states' power to intercept or otherwise limit the privacy of electronic communications when this is "necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law."[105] However, as indicated above, and as the Directive recognizes, the ECHR as interpreted by the European Court of Human Rights limits government power to restrict the privacy of electronic communications. The Directive states that any government restrictions "must be appropriate, strictly proportionate to the intended purpose, and necessary within a democratic society."[106]

The most important provisions of the e-Privacy Directive can be summarized as follows.

Confidentiality of communications

As discussed above, the Wiretap Provision of the ECPA accords individuals more protection against real-time interception of communications than the Stored

102 *Ibid*. In recognition of the continuing need for the law to keep abreast of technological changes, the e-Privacy Directive was amended by Directive 2009/136/EC of the European Parliament and of the Council, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF.
103 *Ibid.*, E-Privacy Directive, Articles 2(e) and (h) and 3(1), and Recital 14.
104 *Ibid.*, Recital 10.
105 *Ibid.*, Recital 11.
106 *Ibid*. See also *ibid.*, Art. 15(1).

Communications Provision provides against access to communications stored on terminals or other telecommunications equipment. By contrast, Article 5 requires EU states to enact laws prohibiting "listening, tapping, storage, or other kinds of interception or surveillance of communications and related traffic data" by anyone other than the parties to communications, unless they receive the consent of all the parties. This prohibition of all kinds of "interception or surveillance of communications" seems broad enough to cover both real-time interceptions and access to stored communications.

Article 5's prohibition of interception or surveillance of communications extends to "traffic data", defined in Article 2 as "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof". Thus, the term "traffic data" in the e-Privacy Directive includes, but is not limited to, what US law counts as addressing information: the telephone numbers between which calls are made, the IP addresses of accessed websites and the "to" and "from" information on email headers. This implies that, in contrast to the US Constitution and the ECPA and in accordance with the European Court of Human Rights' interpretation of the ECHR, the e-Privacy Directive accords equal protection to the contents of communications and associated addressing information.

Exceptions to the e-Privacy Directive's limits on interception or surveillance

As implied above, the e-Privacy Directive's broad prohibition of interception or surveillance does not limit a state's power to authorize interception or surveillance of communications and traffic data for national security, criminal defense and related state purposes.[107]

The only other exceptions to Article 5's prohibition of interception or surveillance are for technical storage or access to information stored in a user or subscriber's terminal by a telecommunication provider for the sole purpose of transmitting communications.[108] In addition, people may be legally authorized to record communications and related traffic data in the course of lawful business practices for the purposes of providing evidence of business transactions and communications.[109]

Retention of traffic data

Article 6 of the e-Privacy Directive limits telecommunication service or network providers' use of the information that Article 5 allows them to store and access by requiring providers to erase or make anonymous traffic data when they are

107 *Ibid.*, Art. 5(1) and 15(1).
108 *Ibid.*, Art. 5(1) and (3).
109 *Ibid.*, Art.5(2).

longer needed for the transmission of a communication, for billing purposes or for marketing purposes to which the user or subscriber has consented. Article 15(1) carves out a major exception, however, to the Article 6 limits on the retention of data, providing that member states may "adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph", namely, "to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system."

Although the e-Privacy Directive thus *permits* individual states to enact data retention legislation, the Data Retention Directive *requires* all EU states to mandate the retention of traffic data by telecommunications providers. The Data Retention Directive's provisions for the retention of traffic data are highly controversial.

Location data

The e-Privacy Directive defines location data as "any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available communications service.[110] While some location data are part of the traffic data needed for transmitting or billing electronic communications (e.g. the location of a mobile phone *vis-à-vis* cell phone towers), Article 9 applies to processing of location data that are not part of traffic data. Subject to a state's decision to legislate an exception for law enforcement or other purposes under Article 15(1), location data other than traffic data can be processed only if made anonymous, or if the subscriber or user of the electronic communications service or network consents to the processing after being informed of the purposes of the processing, the types of data that will be processed and any third party to whom data will be transmitted. The user or subscriber must also be able to withdraw consent at any time.

Security of processing and data breach notification

Like Article 17 of the Data Protection Directive, Article 4 of the e-Privacy Directive contains provisions for the security of personal data. However, unlike the Data Protection Directive provision, the e-Privacy Directive provides for notifying individuals in the case of breaches of personal data. The 2009 Amendment to the e-Privacy Directive considerably strengthened its data breach notification requirements by providing that not only affected individuals and subscribers but also a competent national authority must be notified without

110 *Ibid.*, Art. 2 (c).

delay. The national authority may adopt guidelines for notification and for security practices and will audit the adequacy of providers' measures to notify individuals and mitigate the effects of the breach.[111]

The need for more comprehensive data breach notification

In its policy review of EU data protection law in November 2010, the European Commission recognized the importance of data breach notification and suggested that the 2009 Amendment's provisions for notifications of data breaches in telecommunications services and networks need to be extended to other fields.

> It is . . . important for individuals to be informed when their data are accidentally or unlawfully destroyed, lost, altered, accessed by or disclosed to unauthorised persons. The recent revision of the e-Privacy Directive introduced a mandatory personal data breach notification covering, however, only the telecommunications sector. Given that risks of data breaches also exist in other sectors (e.g. the financial sector), the Commission will examine the modalities for extending the obligation to notify personal data breaches to other sectors.[112]

The need for comprehensive and uniform standards for data breach notification may be even greater in the US than in the EU. An article on the Citigroup data breach in June 2011 reported that, "Security is . . . hampered by a patchwork of data protection laws and regulatory agencies, each with limited mandates. 'We need a uniform national standard for data security and data breach notification,' said Representative Mary Bono Mack, a California Republican who is pushing for legislation on better consumer safeguards."[113]

The Data Retention Directive

The Data Retention Directive was issued in 2006 in response to the 2004 Madrid terrorist bombings and the 2005 London terrorist bombings.[114]

---

111 See Directive 2009/136/EC of the European Parliament and of the Council, Article 2(4).

112 Commission, "A Comprehensive Approach on Personal Data Protection", 2.1.2.

113 Eric Dash, "City Data Theft Points Up a Nagging Problem", NY Times, June 10, 2011, B1 and 7. See also Editorial, "The Cloud Darkens: As Online Security Threats Grow, Companies and Government Are Scarily Unprepared", NY Times, June 30, 2011, A26.

114 Data Retention Directive, Recitals 8, 10, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML. See also European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Evaluation Report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)", May 31, 2011, I.2, para. 4, available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf

Scope

The Directive requires EU states to enact laws requiring providers of publicly available telecommunications services and networks to retain traffic and location data that they generate or process in the course of providing their communications services, as well as related data needed to identify the subscriber or user of the service. Article 5 of the Directive lists the data to be retained as: data identifying the source and destinations of communications, including telephone numbers, user IDs and IP addresses and names and addresses of associated subscribers or registered users; data identifying the date, time, and duration of communications; data necessary to identify the type of communication (i.e. the ISP or telephone service used); data necessary to identify the users' equipment (e.g. the International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI) for both parties to a mobile phone conversation); and data necessary to identify the location of mobile communications equipment. By contrast, data revealing the contents of communications are not to be stored.

Article 6 of the Directive requires individual states to enact legislation requiring the listed data to be retained for a period, to be selected by each state, of between six months and two years from the time of a communication.

Access to the data

States have broad discretion as to the conditions for government officials' access to the retained data. Although the Directive specifies that the retained data be available only "for the purpose of the investigation, detection and prosecution of serious crime", each state may provide its own legal definition of a serious crime.[115] In addition, if a state's law so provides, data may be retained for any or all of the further purposes beyond the investigation, detection and prosecution of serious crimes for which Article 15(1) of the e-Privacy Directive allows states to order the retention of data.[116]

Article 4 further provides that only "competent national authorities in specific cases and in accordance with national law" are to access retained data and that the procedures and conditions for access are to accord with necessity and proportionality requirements. However, each state is left to define the requirements of necessity and proportionality in its own laws "subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights."

---

115 *Ibid.*, Recital 21 and Art. 1. See also EDPS, II, para. 24.

116 Data Protection Directive, Recital 12 ("Article 15(1) of Directive EC 2002/58/ED continues to apply to data . . . the retention of which is not specifically required under this Directive and which therefore falls outside the scope thereof, and to retention for purposes, including judicial purposes, other than those covered by this Directive"). See also EDPS, IV.3, paras. 71 and 72.

States' resistance to implementing the Directive

Although EU states were required to enact laws implementing the Directive by September 15, 2007, as of April 2011 Austria and Sweden had not enacted such laws. After the European Court of Justice ruled against Austria on July 29, 2010, for failing to implement the Directive, Austrian authorities transmitted drafts of implementing legislation to the Commission. By contrast, although the European Court of Justice issued a similar ruling against Sweden on February 4, 2010, the Swedish Parliament voted on March 16, 2011, to defer a vote on proposed implementing legislation for twelve months. The Commission then brought proceedings against Sweden in the European Court of Justice for a second time.[117]

In addition, the laws that Germany, Romania and the Czech Republic issued to implement the Directive were struck down by each of their constitutional courts as unconstitutional.[118] Although none of the courts found that the Data Retention Directive was unconstitutional *per se*, the German Constitutional Court found that the German law was unconstitutional because it did not contain sufficient protections for the security of the retained data or sufficient limitations on law enforcement access to the data. The German Court further reasoned that since data retention created a perception of surveillance that could interfere with people's exercise of fundamental rights, six months was the maximum period for which data could be retained.

Relying on decisions of the European Court of Human Rights, the Romanian Constitutional Court found that the Romanian law's imposition of an obligation to retain all traffic data for a continuous period of six months was too ambiguous in its scope and purpose and had too few safeguards to be compatible with Article 8 of the ECHR.

The Czech Constitutional Court found that the Czech law's definitions of the officials who were competent to access data and its procedures for access and use of data were not sufficiently clear to protect people's fundamental rights against abuse of power by government officials.

---

117 EUROPA – Press Releases – Frequently Asked Questions: Evaluation Report of the Data Retention Directive, April 18, 2011, available at: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/251&format=HTML&aged=0&language=EN&guiLanguage=en.

118 *Ibid*. See also European Commission, Evaluation Report on the Data Retention Directive (Directive 2006/24/EC), April 18, 2011 ("Commission Evaluation of Data Retention"), Sec. 4.9, available at: http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf.

The decisions of the Romanian, German and Czech Constitutional Courts are Decision No. 1258 from 8 October 2009 of the Romanian Constitutional Court, Romanian Official Monitor No 789, 23 November 2009; judgement of the Bundesverfassungsgericht 1 BvR 256/08, of 2 March 2010; Official Gazette of 1 April 2011, Judgment of the Constitutional Court of 22 March on the provisions of section 97 paragraph 3 and 4 of Act No. 127/2005 Coll. on electronic communications and amending certain related acts as amended, and Decree No 485/2005 Coll. on the data retention and transmission to competent authorities.

On May 5, 2010, the Irish High Court granted a civil rights group the right to refer the question of the legality of the Data Retention Directive's requirement of blanket and indiscriminate retention of individuals' traffic, location and subscriber data to the European Court of Justice.[119]

The European Commission's evaluation report

In accord with Article 14 of the Data Retention Directive, the Commission issued an evaluation report on the Directive to the Council and European Parliament on April 18, 2011. Despite acknowledging that the "evidence, in the form of statistics and examples, provided by Member States is limited in some respects", the Commission concluded that the EU should continue to require the retention of traffic, location and subscriber data. According to the Commission, the evidence established "the very important role of retained data for criminal investigation. These data provide valuable leads and evidence in the prevention and prosecution of crime and ensuring criminal justice."[120]

The Commission voiced its intent to propose revisions in the data retention framework on the basis of a thorough assessment of "the implications for the effectiveness and efficiency of the criminal justice system and of law enforcement, for privacy and for costs to public administration and operators, of more stringent regulation of storage, access to and use of traffic data."[121] The possible changes whose impact the Commission deemed particularly worthy of assessment were:

- consistency in limitation of the purpose of data retention and types of crime for which retained data may be accessed and used;
- more harmonisation of, and possibly shortening, the periods of mandatory data retention;
- ensuring independent supervision of requests for access and of the overall data retention access regime applied in all Member States;
- limiting the authorities authorised to access the data;
- reducing the data categories to be retained;
- guidance on technical and organisational security measures for access to data including handover procedures;
- guidance on use of data including the prevention of data mining; and
- developing feasible metrics and reporting procedures to facilitate comparisons of application and evaluation of a future instrument.[122]

---

119 Commission Evaluation of Data Retention, 7.2.
120 *Ibid.*, 8.1.
121 *Ibid.*, 8.5 and 8.6.
122 *Ibid.*, 8.5.

The Commission also proposed to consider how data retention might be complemented by data preservation or, in other words, court orders that obligate operators to retain data prospectively on specific individuals who are suspected of being engaged in crime.

The opinion of the European Data Protection Supervisor

The European Data Protection Supervisor (EDPS) issued an opinion on May 31, 2011, that was highly critical of both the Data Retention Directive and the Commission's Evaluation Report. Contrary to the Commission's exclusion of the possibility of repealing the Data Retention Directive, the EDPS claimed that the quantitative and qualitative data the Commission had obtained from EU states were not sufficient to show that data retention was necessary for law enforcement purposes. In particular, the EDPS criticized the Commission for only assessing data from states that had implemented the Directive and not comparing the criminal justice outcomes there with outcomes in states in which the Directive either had not been implemented or had been annulled.[123]

Furthermore, according to the EDPS, the Commission had not adequately considered whether data retention could be replaced by data preservation or some other less intrusive method of providing law enforcement with data.

> [I]t is unfortunate that in the conclusions of the report the Commission commits itself to examining whether – and if so how – an EU approach on data preservation might complement (i.e. not replace) data retention. . . the EDPS recommends the Commission during the impact assessment also to consider whether a system of data preservation, or other alternative means, could fully or partly substitute the current data retention scheme.[124]

The EDPS also faulted the Commission for failing to recognize that even if a data retention regime is necessary the Directive's restrictions on privacy were not proportionate to the purposes served. In particular, the EDPS claimed that the Directive left individual states too much discretion over the purposes for which retained data can be used and as to the authorities with access to the

123 EDPS, IV.1, para. 50. In accord with the EDPS's recognition of the need to compare crime control outcomes in EU countries that had and had not implemented the Directive, a recent study by the Scientific Services of the German Parliament of the effects of data retention on crime clearance rates in EU Member States concluded that, "In most States crime clearance rates have not changed significantly between 2005 and 2010. Only in Latvia did the crime clearance rate rise significantly in 2007. However, this is related to a new Criminal Procedure Law and is not reported to be connected to the transposition of the EU Data Retention Directive." See A.K. Vorrat, "Police Statistics Prove Data Retention Superfluous", *EDRI-gram*, Number 9.12, June 15, 2011, http://www.edri.org/edrigram/number9.12. Statistics published by Germany's Federal Crime Agency show that after the Constitutional Court's annulment of the German law implementing the Data Retention Directive on March 3, 2010, "registered crime continued to decline and the crime clearance rate was the highest ever recorded (56.0%)." Vorrat, *supra*.

124 EDPS, IV.1, para.57.

data.[125] Pointing to statistics in the Commission's evaluation report showing that 86% of requests were for access to data that had been retained for no more than six months, 12% were for access to data retained between six and twelve months and two per cent were for access to data retained for more than one year, the EDPS further concluded that the Directive allowed states to retain data for longer periods than necessary.[126] The requirement of proportionality was also violated, according to the EDPS, because the absence of adequate measures for the security of data in the Directive caused the privacy of personal data to be unnecessarily threatened.[127]

Further, the EDPS opined that the Directive failed to conform to the requirement, established by the European Court of Human Rights, that intrusions on privacy be foreseeable or, in other words, that they "have a legal basis in law and . . . be compatible with the rule of law."[128] The absence of predictability was created by the Directive's leaving states free to determine which officials are entitled to access retained data, and by the Directive's leaving individual states to define what counts as a serious crime and whether data can be accessed, under Article 15(1) of the e-Privacy Directive, for purposes other than combating serious crime.

Council Framework Decision 2008/977/JHA on Personal Data and Police and Judicial Cooperation[129]

Scope

Council Framework Decision 2008/977/JHA is the first EU legislation that establishes common standards for all EU states with regard to personal data processed as part of policing and criminal justice operations. The Decision governs the processing, "for the purpose of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties", of personal data exchanged between EU states.[130] The Decision also

125 *Ibid.*, IV.2, para. 59.

126 *Ibid.*, IV.2, para. 60 and n.51.

127 Cf. Lukas Feiler, "The Legality of the Data Retention Directive in Light of the Fundamental Right to Privacy and Data Protection", *European Journal of Law & Technology* 1, no. 3 (2010), available at: http://ejlt.org//article/view/29/75 (arguing that the Directive's restrictions on privacy conform to the requirement of necessity, but are not proportional to the stated purpose of combating serious crime, therefore violating the rights to privacy and data protection in articles 7 and 8 of the EU Charter); Lachmayer, "European Police Cooperation and its Limits", 108–09 ("The scope of the directive is very broad as the categories of data to be retained are manifold and the retention period is 'not less than six months and not more than two years from the date of the communication.' Its effects on the general human rights situation are dramatic."). But see Francesca Bignami, "Privacy and Law Enforcement in the European Union: The Data Retention Directive", *Chicago Journal of International Law* 8 (2007): 233 (finding that "privacy – as guaranteed under Article 8 of the European Convention on Human Rights and the Council of Europe's Convention on Data Protection – is adequately protected in the Directive").

128 EDPS, IV.3.

129 Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:01:EN:HTML.

130 Council Framework Decision 2008/977/JHA, Article 1(2)(a).

applies to individual EU states' transmission of personal data received from other EU states to private parties for criminal justice purposes and the prevention of serious threats to public safety or serious harm to human rights.[131]

The scope of the Framework Decision is limited by the fact that it does not replace "various sector-specific legislative instruments for police and judicial co-operation in criminal matters adopted at the EU level, in particular those governing the functioning of Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS)."[132]

In addition, the Framework Decision only partially governs EU states' transfers to non-EU states or international bodies of data received from other EU states. Article 13 requires EU states to provide that such transfers will occur only for criminal justice purposes and that data will be given only to non-EU authorities responsible for those purposes. In addition, personal data are to be transferred only to non-EU states or international bodies that ensure adequate levels of data protection and only with the consent of the EU state that originally provided the data. However, Article 13 of the Framework Decision leaves individual states to decide on the conditions under which they will consent to such transfers of data. In addition, the adequacy of the level of data protection in a non-EU country or international body is left up to the laws of the state that provided the data, and the conditions for waiving the requirement of an adequate level of data protection are left up to the laws of the state that transferred the data.

EU regulation of the use of personal data for policing and criminal justice is further limited as the Framework Decision does not apply to the collection, use or transmission of personal data within the confines of individual EU states, or to an EU state's transmission of data received from another EU state to private parties, such as defense lawyers and victims, in the context of criminal proceedings.[133] Nor does the Framework Decision apply to data received by an EU state from a non-EU country or to the processing of data for "essential national security interests and specific intelligence activities in the field of national security."[134]

Requirements for the processing of data

The Framework Decision's principal requirements for the processing of data exchanged between EU states for criminal justice purposes can be compared

131 *Ibid.*, Article 14.

132 Commission, 'A Comprehensive Approach on Personal Data Protection", 2.3; Council Framework Decision 2008/977/JHA, Art. 1(2)(b) and (c), Recitals 39-41.

133 *Ibid.*, Recitals 9 and 18.

134 *Ibid.*, Article 1 (4); Information Policy Division, UK Ministry of Justice, Circular 2011/01, "Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters 2008/977/JHA", Jan. 25, 2011, 2, available at: http://www.justice.gov.uk/publications/docs/data-protection-framework-decision-circular.pdf.

with those that the Data Protection Directive imposes for the processing of personal data for other purposes. While the Framework Decision agrees with the Directive in imposing especially stringent conditions for the processing of sensitive data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, [or] concerning health or sex life", it does not follow the Directive in making the data subject's consent the principal requirement for such processing.[135] Instead, Article 6 of the Framework Decision allows sensitive data to be processed "only when this is strictly necessary and when the national law provides adequate safeguards."

With regard to other personal data, Article 3 of the Framework Decision provides, similarly to Article 6 of the Data Protection Directive, that data are to be collected only for specified, explicit and legitimate purposes, are not to be further processed for purposes that are incompatible with the original purpose for collection and are to be relevant and adequate to the stated purpose for collection and/or further processing. In addition, no more data than are needed for the stated purposes are to be collected or processed. Under Article 11 of the Framework Decision, the permissible purposes for which data can be further processed beyond those for which they were originally transmitted are broad, extending to additional criminal justice purposes and related judicial and administrative proceedings, the prevention of serious and immediate threats to public security and any other purpose to which the EU state that transmitted the data consents in advance or to which the data subject consents in accord with national law.

Although the Framework Decision also resembles the Data Protection Directive in requiring that personal data be kept accurate and up-to-date and providing data subjects with rights to information and access, these protections are weaker than those in the Directive. Under Article 8 of the Framework Decision, competent authorities are to verify the accuracy of personal data "as far as practicable" and to take "all reasonable steps" to ensure that inaccurate, incomplete or outdated personal data are not transmitted. Article 4 requires rectifying inaccurate data or updating or completing them where "possible and necessary", and erasing, making anonymous or blocking data that are no longer needed for the original purposes or further purposes for which they were lawfully processed. Although Article 16 of the Framework Decision provides data subjects with the right to be informed of the collection or processing of their personal data, this right may be limited by the laws of both their own state and any other EU state with which their data are exchanged. Similarly, although Article 17 grants data subjects rights to receive confirmation that their personal data have or have not been transmitted, as well as information as to the recipients of the data and the data being processed, the right to access may be limited by individual EU states

135 Data Protection Directive, Art. 8; Council Framework Decision, Art. 6.

where this is necessary and proportional to avoid obstructing judicial or police procedures, to protect public or national security or to protect data subjects or the rights and freedoms of others.

Perhaps reflecting increasing awareness of the risk of data breaches, the Framework Decision's provisions in Article 22 for the security of data are more elaborate than those in the Data Protection Directive.

Enforcement

The Framework Decision requires each EU state to appoint an independent supervisory authority (or authorities) which may or may not be same as the Data Protection Supervisor appointed in accord with the Data Protection Directive.[136] Under Article 25 of the Framework Decision, each state's supervisory authority (or authorities) is to have the power to advise and monitor the application of the Framework Decision within its territory, including investigative powers and effective powers of intervening to deliver opinions before the processing of data or to order the blocking, erasure or destruction of processed data. States are also to empower data supervisors to bring legal proceedings when the state's laws implementing the Framework Decision are violated, and to hear individuals' claims concerning the protection of their rights and freedoms regarding the processing of personal data.

Although Article 20 of the Framework Decision grants data subjects rights to judicial remedies for breaches of the rights provided to them by their state's law implementing the Framework Decision, these rights may be limited by administrative remedies.

Criticisms of the Council Framework Decision by the EDPS and the European Commission

The European Data Protection Supervisor and the European Commission separately opined that the Council Framework Decision is an important – though only a first – step toward the goal of adequately protecting personal data in the context of policing and criminal justice.[137] In regard to cross-border exchanges of personal data within the EU, the EDPS and the Commission agreed that more limits are needed on the purposes for which the Framework Decision allows data to be further processed. In addition, both agreed on "the need to

136 Council Framework Decision, Recitals 33 and 34, Art. 25.

137 European Data Protection Supervisor Press Release, "EDPS Sees Adoption of Data Protection Framework for Police and Judicial Cooperation Only as a First Step", Nov. 28, 2008, available at http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/PressNews/Press/2008/EDPS-2008-11_DPFD_EN.pdf; Commission, 2.3.

distinguish between different categories of data subjects, such as suspects, criminals, witnesses and victims, to ensure that their data are processed with more appropriate safeguards."[138]

More fundamentally, the Commission and EDPS both criticized the limitations on the scope of the Framework Decision, stressing the need for common EU law to govern exchanges of data with non-EU countries and for EU legislation to extend to domestic policing and criminal justice operations. Notably, the Commission recognized that the distinction between cross-border data exchanges and domestic processing of data "is difficult to make in practice and can complicate the actual implementation and application of the Framework Decision."[139]

Institutional arrangements in an EU Member State: The Netherlands

It is now time to exemplify the institutional embodiment of the EU's privacy rights in a member state. We have selected the Netherlands for this purpose.

The Kingdom of the Netherlands is a constitutional monarchy and a representative parliamentary democracy. It has territory in the Caribbean (the former colonies of Aruba and Netherlands Antilles) as well as in Europe (the Netherlands). The Charter for the Kingdom of the Netherlands provides for the autonomy of the Caribbean territories. The Constitution of the Kingdom of the Netherlands provides for the regulation of the government of the Netherlands (but not of the government of the territories). It grants citizens an explicit right to privacy.

The monarch and the Council of Ministers of the Netherlands are the government of the Kingdom. The Dutch Prime Minister chairs the Council of Ministers of the Kingdom. Under Article 14 of the Charter, the Netherlands can conduct kingdom affairs if this does not affect Aruba or Netherlands Antilles; neither of the latter has this right. The Parliament is known as the States-General of the Netherlands and has two houses, the House of Representatives (which can propose legislation, as can the monarch) and the Senate (the upper house). The Netherlands is divided into twelve provinces. The Supreme Court of the Netherlands is the highest court. However, it cannot rule on the constitutionality of laws passed by the States-General or on treaties. In contrast to some countries in the EU, the Netherlands has no constitutional court. (There is a council of state that advises the government on serious judicial matters, including issues relating to international law.) However, the Dutch Constitution obliges the courts to review all domestic legislation, including acts of parliament, in

138 EDPS, see also Commission.
139 *Ibid*. (footnote omitted).

respect of their compatibility with relevant parts of the international treaties to which the Netherlands is a party (for example, the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950). Where there is incompatibility, the domestic legislation must give way. In particular, it must give way to conventions and directives that bind all member states of the EU, such as the 1995 directive 95/46/EC of the European Parliament and of the Council of Europe on the protection of personal data.

The Dutch Criminal Code defines many but not all criminal offenses. Various other statutes complement criminal law legislation – for example, the Economic Offenses Act 1950, the Narcotic Drug Offenses Act 1928 and the Military Criminal Code 1991. The Computer Crime Act 1993 allowed for the interception of all forms of telecommunications, including by means of long-distance target microphones.

Criminal procedure in the Netherlands has two phases: investigation by the police (under the direction of a public prosecutor – see below) and judicial investigation by an examining judge. The purpose of the police investigation is simply to gather evidence. Although the police have a right to ask questions of suspects, no one is required to answer questions put by the police. Under Dutch law there needs to be reasonable suspicion before a criminal investigation may be started. Police are able to use covert policing methods, such as surveillance, undercover operatives and the use of informants, under the Special Powers of Investigation Act 2000.

The Dutch police system is based on the Police Act of 1993. Law enforcement in the Netherlands is provided by twenty-five regional police forces and the Dutch National Police Agency (KLPD). The latter is responsible for the transport systems of the Netherlands (e.g. motorways and waterways). The National Criminal Investigation Department (responsible for serious and organized crime and cross-regional crimes) comes under the KLPD. The KLPD also has its own intelligence service, the National Criminal Intelligence Service (NRI). Each regional police force has a Criminal Intelligence Service (CIS). However, the establishment of communication systems and the processing and availability of information obtained from investigations is done at a national level. Currently, the records services are converting to a fully computerized system that will comprise criminal records, photographs of crime scenes and offenders, fingerprints etc.

The States-General generates the regulations governing the police while the Minister of the Interior is responsible for their central administration and the mayor of the largest municipality in the region for their regional administration (except in the case of the directly centrally administered KLPD). The regional police chiefs are responsible for day-to-day management. However, the relevant

public prosecutor (belonging to the Public Prosecution Service (OM) which is managed by the Board of Procurators General within the Ministry of Justice) is responsible for the police with respect to crime investigation. Although the police actually conduct most investigations, sometimes the public prosecutors take direct control of investigations into serious crimes. The OM is responsible for investigating and prosecuting criminal offenders and is the only body in the Netherlands that may prosecute criminal suspects. Accordingly, no single body in the Netherlands has sole authority over the police.

The prosecution office attached to the Supreme Court is not part of the OM. It is an independent statutory body concerned with the prosecution of the members of Parliament and the ministers in relation to criminal matters.

The duties and powers of the intelligence and security services in the Netherlands are set forth in the Intelligence and Security Services Act 2002. The General Intelligence and Security Service (AIVD) focuses on domestic intelligence and non-military threats including, in recent times, Islamic fundamentalism. It collects and assesses information and monitors suspected terrorists and the like. The Ministry of the Interior is responsible for the AIVD (see below). The Military Intelligence and Security Service (MIVD) focuses on foreign intelligence and international threats, specifically military- and government-sponsored threats such as espionage. It collects and assesses information. The MIVD works closely with NATO. The Minister of Defense is responsible for the MIVD. The MIVD is overseen by a committee appointed by the Committee for the Intelligence and Security Services and comprising the leaders of the four main political parties represented in the House of Representatives of the States-General.

The National Coordinator for Counter-terrorism (NCTb) exists to ensure coordination between these and other relevant agencies.

The Information and Communications Technology Agency is an agency of the Ministry of the Interior and is responsible for the provision of reliable and secure ICT services and for information management in the security and criminal justice sectors.

Under the Treaty of Lisbon (2009), the Treaty of Amsterdam (1999) and other treaties, the Netherlands is required to cooperate with other EU countries in criminal matters, including corruption, organized crime, terrorism, arms trafficking, trafficking in drugs and trafficking in human beings. Europol (based in The Hague) is the central police office for sharing and analyzing information on criminal matters among EU members. The Schengen Information System has been established to facilitate EU information sharing. Under the Europol Convention (1999), EU countries have agreed to share information and to

institute measures for data protection. As of 2010, Europol functions on the basis of a Council Decision that gives it Community status and subjects its budget to control by the European Parliament.

Post-9/11 cooperation on security among EU states and between the EU, including the Netherlands, and the US has increased. Within the EU, extradition processes have been simplified and expedited, agreement has been reached on the definition of the constituent elements of terrorism and the minimum sentences to be applied, and Europol's Terrorism Task Force has been established and thereby enables the exchange of information between the various counter-terrorism authorities. A cooperation agreement exists between Europol and the US.

These attempts at cooperation notwithstanding, the EU and the US standpoints on privacy and data protection are somewhat different. Thus in the US the approach to regulation in the private sector is essentially self-regulation whereas in the EU there is comprehensive privacy and data protection legislation as well as oversight bodies. In the case of the Netherlands, the Data Protection Authority has oversight and investigative powers, including with respect to the private sector (see below).

Privacy rights and data protection

As noted above, Dutch citizens have an explicit right to privacy under the Constitution of the Netherlands. Article 10 of the Constitution states:

1. Everyone shall have the right to respect for his privacy, without prejudice to restrictions laid down by, or pursuant to, Act of Parliament.
2. Rules to protect privacy shall be laid down by Act of Parliament in connection with the recording and dissemination of personal data.
3. Rules concerning the rights of persons to be informed of data recorded concerning them, of the use that is made thereof, and to have such data corrected shall be laid down by Act of Parliament.

Article 12 states:

1. Entry into a home against the will of the occupant shall be permitted only in the cases laid down by, or pursuant to, Act of Parliament, by those designated for this purpose by, or pursuant to, Act of Parliament.
2. Prior identification and notice of purpose shall be required in order to enter a home under the preceding paragraph, subject to the exceptions by Act of Parliament. A written report of the entry shall be issued to the occupant.

Article 13 states:

1. The privacy of correspondence shall not be violated, except in the cases laid down by Act of Parliament or by order of the courts.
2. The privacy of the telephone and telegraph shall not be violated, except in the cases laid down by Act of Parliament, by or with the authorization of those designated for this purpose by Act of Parliament.

The Dutch Data Registration Act 1988, which preceded the EU Data Protection Directive, protects personal data files and, speaking generally, requires consent, accuracy of data, use of data only for the purpose for which they were originally collected, security of data, disclosure only by consent or by statute and so on.

The Data Registration Act established the Dutch Data Protection Authority, which advises the government, deals with complaints and undertakes investigations.

The Decree on Sensitive Data under the Data Registration Act sets out the limited circumstances under which data on an individual's political and sexual persuasion, religious beliefs, race and medical and criminal history may be included on a personal data file. The Decree on Regulated Exemption under the Data Registration Act exempts certain organizations from the requirements of the Data Registration Act.

The Dutch Personal Data Protection Act of 2000 supersedes earlier legislation, including the Data Registration Bill 1998 and the Data Registration Act 1988. It brings Dutch law in line with the European Data Protection Directive; *inter alia* it regulates the disclosure of personal data to countries outside of Europe.

As noted above, interception of communications is regulated by the Criminal Code and requires a court order. The intelligence services (e.g. the AIVD and the MIVD) do not need a court order for interception of communications; their authorization comes from the Minister of the Interior.

The Telecommunications Act 1998 requires all internet service providers to have the capacity to intercept all traffic in the event of a court order.

The Intelligence and Security Services Act authorizes the interception, search and keyword scanning of satellite communications. Intelligence services can store intercepted communications for up to one year.

As noted above, the Netherlands has ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950, which recognizes a right to privacy. Article 8 states: "Everyone has the right to respect for his private and family life, his home and his correspondence." As a member of the Council of Europe in 1993 the Netherlands ratified the Convention for the

Protection of Individuals with Regard to Automatic Processing of Personal Data. Moreover, the Netherlands is a member of the Organization for Economic Cooperation and Development and has adopted the OECD Guidelines for the Protection of Privacy and Trans-border Flows of Personal Data.

The 2006 directive (Directive 2006/24/EC) on retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communication networks is highly controversial in the Netherlands. The directive allows the retention for lengthy periods – twelve months in the Netherlands, longer than the Directive's minimum requirement of six months – of so-called traffic data, including not simply who has been communicated with and when but also a person's movements (based on, for example, location of a mobile phone caller) and patterns of internet use. The claim of the authorities who have passed this legislation is that the data in question are not communicative of content and, therefore, that the legislation respects privacy. Moreover, the data are held to be useful in counter-terrorism initiatives and in combating organized crime. However, the counter-claim is that the traffic data are sufficiently rich and comprehensive to enable the creation of a map of the human associations and activities of any individual with respect to whom it has been retained – a profile of sorts – and their retention is, therefore, an infringement of the privacy of ordinary citizens.

The Netherlands has recently passed legislation that introduces biometric passports with an RFID-microchip containing digital information about the passport holder. The passport holder's fingerprints and a digital facial image are stored on the microchip for identification. Although this increases security by, for example, reducing the possibility of fraudulent use, the data on all biometric passports is stored in a central database accessible by law enforcement agencies in relation to criminal investigations and counter-terrorist activities. Because this central database contains information about all citizens who are passport holders it contains data about virtually every Dutch citizen irrespective of their criminality or suspected criminality. Accordingly, this new law would appear to breach the right to privacy and, arguably, Dutch privacy legislation.

Another controversy that has recently arisen is the decision by the Dutch government to direct Amsterdam's Schiphol airport to install full-body scanners and to use them to scan passengers traveling to the US. The decision comes in the wake of a Nigerian man carrying a non-metallic explosive device undetected through airport security at Amsterdam on Christmas Day 2009 before boarding a US plane and traveling to Detroit. His attempt to trigger the device was unsuccessful. There are privacy concerns – including from a legal perspective – about the intrusive nature of the images and the possibility of these images being stored, transferred or accessed without authorization.

Agencies

Dutch Data Protection Authority

The Data Protection Authority (DPA) is an independent statutory authority that supervises compliance with the legislation that regulates the use of personal data. The legislation in question includes the Personal Data Protection Act, the Police Data Act and the Municipal Database (Personal Records) Act.

The DPA makes recommendations regarding legislation, receives complaints, conducts audits and official investigations and initiates prosecutions. Appeals can be made against the DPA's decisions to the administrative law court and complaints can be made to the National Ombudsman.

In the past, the DPA has: conducted random investigations of the practices of Criminal Intelligence Service Units to determine the extent to which the regulations governing data processing were actually being observed; conducted an investigation in 2004 into the privacy aspects of data processing in police wiretapping rooms; conducted random checks on municipalities to see whether they had complied with their notification obligations in respect of the collection of personal data; approved in 2004 the Code of Conduct for processing personal data of the Netherlands Association of Business Information Agencies; and conducted in 2003 an investigation into a business information agency, finding that it had processed personal data illegitimately and informing the Public Prosecutor, with the result that a criminal investigation was conducted leading to prosecution of members of the agency.

General Intelligence and Security Service

The General Intelligence and Security Service (AIVD) is responsible for non-military intelligence gathering and assessment, conducting threat analyses, issuing warnings of risks to national security and monitoring individuals suspected of involvement in organized crime, cybercrime, terrorist activities (including radicalization) and the like. It passes information that is relevant to the investigation or prosecution of offenses in the form of official reports to the police and/or the relevant judicial authorities within the Public Prosecutions Service. The regional intelligence services conduct activities on behalf of the AIVD and for which the AIVD has ultimate responsibility. It also has an investigative capacity, for example, of terrorist incidents and it conducts background checks on individuals in sensitive positions, including public offices and important positions in industry.

The AIVD makes use of covert methods, including undercover operatives, use of informants and interception of electronic communications. As noted above, the AIVD intercepts telephone and internet communications and does so under the

authorization of the Minister of the Interior (rather than judicial warrant). It has unrestricted access to police intelligence and works closely with Dutch police intelligence agencies, other EU intelligence agencies and foreign intelligent agencies such as the CIA.

The Minister of the Interior is responsible for the AIVD. However, the Council for National Security, which is a Cabinet sub-committee comprising the Prime Minister, two Deputy Prime Ministers and the ministers of the Interior, Justice, Defense and Foreign Affairs, gives general direction to the AIVD and delegates much of the tasking of the AIVD to other bodies, such as the Joint Intelligence Services Committee (CVIN) (chaired by the Intelligence and Security Services Coordinator and various public servants) and the Joint Counter-terrorism Committee (GCT).

The AIVD is overseen by the Intelligence and Security Supervisory Committee (CTIVD), which is appointed by the Committee for the Intelligence and Security Services (CIVD). The CIVD comprises the leaders of all the political parties represented in the House of Representatives of the States-General (with the exception of the Socialist Party, which opted not to join). The Minister of the Interior is accountable to Parliament via the CIVD. When AIVD matters cannot be publicly disclosed, the CIVD meets in closed sessions.

The AIVD publishes an annual report including its budget. Sensitive information is omitted.

Under the freedom of information rules, the AIVD can be required by the courts to provide any records held on a private citizen to that citizen unless it is relevant to a current case. Moreover, even outdated material cannot be provided if it would compromise the AIVD's sources or methods.

Conclusions

Returning to the framework for data protection that is provided by EU law and is binding on all EU member states, and to a comparison of EU and US law, the criticisms of the Council Framework Decision by the EDPS and the European Commission highlight two crucial unresolved issues about the protection of privacy in the twenty-first century. First, how can state sovereignty be reconciled with the globalized nature of personal data and the concomitant globalized nature of threats to both individual privacy and national security? Second, what, if any, differences in restrictions on the collection, use and transfer of personal data are justified by differences between state and private entities and state and private purposes?

With regard to the second question, the preceding discussion has shown that the United States lags behind the EU in recognizing the need for comprehensive restrictions on the collection, use and transfer of personal data by private entities. There is a clear need for additional legislation in the US to protect the individual's privacy rights from intrusion by private entities. However, the EU has yet to face the major challenge of extending its legislative framework for data protection to policing and criminal justice within the individual EU states. The difficulty of doing this is evident in the Commission's statement that "the notion of a comprehensive data protection scheme does not exclude specific rules for data protection for the police and the judicial sector within the general framework, taking due account of the specific nature of these fields."[140] In the opinion of the authors, neither the US nor the EU has arrived at an adequate understanding of what it means for data protection safeguards to take "due account of the specific nature" of policing and criminal justice.

Nonetheless, our discussion suggests that the EU may be aided in answering this question by the expertise on technological and legal issues about data protection that its law has created through the institutions of the Article 29 Working Party, the European Data Protection Supervisor and the Data Protection Supervisors of the individual states. By contrast, although some governmental bodies in the US, such as the Federal Trade Commission, have become interested in questions of data protection, these bodies are interested in data protection only as it impacts on some other governmental function, for example, protecting consumers or advancing commerce.[141] Unlike the European Data Protection Supervisor, no American governmental body has the power or institutional competence to advocate and argue for a data protection framework that extends to both public and private entities and functions and that accounts for the globalized nature of personal data in the twenty-first century.

Given increasing inroads on personal privacy in the US, it seems unreasonable to advocate not only additional privacy legislation (both federal and state) in relation to intrusions by private sector entities but also, and related, the creation of a National Office of Data Protection that would seek to provide a set of national guidelines for the protection of personal data. This has occurred in a number of other countries and even if, as was the case with the American Law Institute's (ALI) projects,[142] such guidelines could not be enforced in the absence of relevant legislation, they would at least constitute a respected benchmark for

140 *Ibid*.

141 See e.g. The Department of Commerce Internet Policy Task Force, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework", 2010, available at: http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf; Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change", December 2010, available at: http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

142 See The American Law Institute web site at: http://www.ali.org/.

the review and revision of existing privacy protections as well as the initiation of others. Although we envisage a federally funded agency, the analogy with the ALI indicates that we also believe that it should be heavily populated by those who have an expertise in privacy issues: conceptual, moral, legal and political. Such a body would not only be charged with the development of privacy guidelines for consideration by both commercial and governmental bodies, and of recommendations for legislation, but it would also have a public responsibility to communicate its findings to a wide audience.[143] We further suggest that there is a need for a statutory body (whether the National Office of Data Protection and/or some other body or bodies) with the responsibility to oversee and monitor compliance with privacy legislation. Such a body should conduct audits and examine records as well as receive privacy complaints. It should also have the power to conduct investigations of breaches of the legislation.

We advocate that the process of developing a National Office of Data Protection for the US begin with a national public discussion concerning the legitimate extent and limits of privacy and of ways of protecting it. Such a debate would need to take into account not only the governmental collection, retention and use of personal data but also its collection, retention and use by commercial organizations. We believe that once it is widely recognized that the division between governmental and commercial collection, retention and use of personal data has been all but eroded under the current regulatory arrangements, such a national office will be seen as both reasonable and feasible.

It is our hope that in advocating a National Office of Data Protection we will see the development of a graduated series of guidelines and associated legislation for the oversight of personal data collection, use and retention by private and public agencies, including but not limited to soft law self-regulatory measures, privacy enhancement of software and administrative measures designed to protect privacy, along with recommendations concerning situations in which criminal penalties ought to be levied. The National Office of Data Protection should also have a communicative responsibility to ensure that the American public is aware of current concerns about the privacy of personal data as well as its recommendations concerning protection enhancements. Moreover, there is a need for an oversight body (perhaps the National Office of Data Protection) with statutory powers to monitor, receive complaints, conduct audits and investigate infringements of privacy rights.

---

143 We imagine some sort of parallel – inexact, to be sure – with the Law Reform Commission of Australia. The latter has produced impressive reviews of existing privacy regulations as well as conceptually rich accounts of privacy. See http://www.alrc.gov.au/media/2008/mr11108.html. A better understanding of how this adjustment to the US system may be achieved is provided in Chapter IX.

We further believe that it would be essential for a National Office of Data Protection to confer regularly with the EDPS of other similar institutions in other countries in order to develop a set of standards that can be generally implemented within such societies. As the EDPS and European Commission have recognized, the globalized nature of data in the twenty-first century means that no country can effectively protect its citizens' privacy on its own. A globalized problem demands globalized solutions.