Chapter 9
Privacy Law and Regulation: Technologies, Implications, and Solutions

Jasmine McNealy and Angelyn Flowers

9.1 Introduction

The early 21st century could easily be deemed the era of data collection and vulnerability. Governments collect rapidly increasing amounts of information, from voter registrations to driver license records to death certificates. Private corporations, too, compile databases of consumer information for marketing and advertising purposes. Of great assistance in the amassing of personal data, in both the public and private sectors, are new technologies able to track, retrieve, and decipher much of the information that individuals provide or leave behind while using networked services. Suffice it to say, on the Internet now, not only does everyone know that you are a dog, they may know your breed, where you were born, and the street where your dog house is located.

Of course some of the information collected could be considered benign, and many people subscribe to the "nothing-to-hide" perspective. This attitude asserts that the members of society should and would not care about the collection of their private information if they have nothing to hide. That is, if you are doing nothing wrong, privacy will not be a consideration. Professor Daniel Solove has identified the fallacies in this argument. The argument fails in that it reduces privacy to the hiding of things or information when privacy should be understood as "a plurality of related problems" [1]. Further, the argument deems the harms from possible privacy invasions as significant only if the outcome is tangible or sensationalistic. This ignores the harms that aggregated minor intrusions may cause [1].

J. McNealy (✉)
College of Journalism and Communications, University of Florida,
Gainesville, FL 32611, USA
e-mail: jemcnealy@jou.ufl.edu

A. Flowers
Department of Criminal Justice, Sociology, and Social Work,
University of the District of Columbia, Washington, DC 20008, USA

S. Zeadally and M. Badra (eds.), *Privacy in a Digital, Networked World*,
Computer Communications and Networks,
DOI 10.1007/978-3-319-08470-1_9

The failures of the nothing-to-hide argument may be best illustrated by detailing one of the major privacy outrages from the last few years. In 2013 Edward Snowden, an employee of defense contractor Booz Allen Hamilton, disclosed many top-secret documents to the public. The documents detailed a disturbing web of surveillance activities by government actors, particularly the National Security Agency (NSA), assisted by private communications providers [2, 3]. Of particular concern was the collection of metadata, or "data about data," as it is sometimes called. The NSA programs involved the collection of information about telephone calls, but not the contents of the calls, as well as collection of Internet data [2]. Far from benign, aggregated metadata enables the construction of inferences about private activities including medical issues, financial health, and intimate relations [2]. More importantly, the revelation of the surveillance programs demonstrated the global impact of one country's approach to privacy. Not only were US citizens targeted, but also the communications of citizens and political leaders in other countries, causing tension between the United States and other countries, as well as calls for inquiries and assurances about NSA activities [2].

Some of the strongest criticisms of US surveillance activities came from Brazil, which in 2014 passed the Marco Civil da Internet. The new law establishes rules with respect to many Internet-related issues. Of significance for the purposes of this chapter is its implementation of standards related to privacy and data retention. The law limits the amount of metadata that organizations can collect on Brazilian Internet users. As a whole, the law creates a framework for data protection similar to that of the European Union (discussed in Sect. 9.5) [4].

If nothing else, the Snowden anecdote demonstrates the immense range and complexities of government surveillance and information collection. Although US President Barack Obama has somewhat addressed the public and political concerns in connection to NSA activities, and privacy advocates and lawmakers are attempting to make changes by updating the various laws that allow law enforcement to access private information, what exists now in the United States is a hodgepodge of laws and regulations that affect personal information privacy either directly or indirectly. This chapter provides an overview of laws and regulations used to regulate privacy in the digital age, focusing on US law and how it interacts with other global privacy regulations.

First, this chapter considers the causes of increased data collection in this era. Following this, we examine the current state of law in the United States, including those laws directly and indirectly addressing privacy. Section 9.4 considers government surveillance and both the laws that allow it and those aimed at placing restraints on law enforcement activities. This is followed by an analysis of privacy regulation in the European Union. This chapter concludes with an examination of the opportunities for change with respect to privacy law and regulation.

9.2 Catalysts for Change

The late 20th century saw the rise in surveillance, sousveillance, and various privacy-limiting technologies. Yet even before the advent of these new technologies, both public and private organizations were collecting information about individuals in society. Governments have reason to collect some important private information. Censuses, for example, allow for a reasonable estimation of the population, as well as providing demographic information about the individuals within that population. These population counts also provide information integral to the administration of government.

Other forms of government information collection serve similar purposes. Driver license records provide the holder with a form of identification, while providing the state with a log of the holder's address, moving violations, and identifying characteristics. Birth, death, and marriage certificates similarly provide the state with records of human relationships and interactions that allow for the efficient administration of privileges, benefits, and mandates required under state law. Much of the information provided to, or collected by, the state has moved from paper copies to digital databases. On the federal level, the growth in government data collection mirrors the increase in government agencies and the growth in bureaucracy [5]. Government databases on both the state and federal levels provide ready fodder for private corporate databases used for advertising and marketing purposes.

By far the most significant cause of the increased collection of personal information is the war on terrorism. After the events of September 11, 2001, the US government and governments around the world expanded domestic and foreign surveillance and data collection activities. In the United States, prior to 9/11, there was a conscious effort to limit the amount of government use and collection of private information [6]. The barriers erected to prevent government sharing and possible abuse of private information were relaxed to allow collection of domestic and foreign intelligence thought to be useful in combating and preventing terrorism. Some of the anti-terrorism measures have come in the form of new laws that directly or indirectly affect personal privacy.

Anti-terrorism regulations have and continue to raise privacy concerns around the globe. As recent as July 2014 the United Kingdom passed the Data Retention and Investigatory Powers Act (Drip), which requires telecommunication providers to retain customer metadata for 12 months and to allow law enforcement and government agencies access to the information [7]. The law was met with criticism and concerns about the availability of personal data as well as claims that the government may have circumvented the democratic process by rapidly passing the law [8]. Of particular concern is that the law appears to conflict with privacy principles in both the European Convention on Human Rights and the European Charter of Fundamental Rights [8]. The passage of Drip and subsequent objections demonstrate continued tension between government regulations and legal principles with respect to privacy.

9.3 Current US Law

Privacy principles in the United States have their foundations in constitutional and common law, statutes, and the law of equity. In the United States the Constitution is the supreme law of the land. Under the system of federalism, each state or commonwealth has its own constitution as well. The federal Constitution provides, however, the foundation for the rights and privileges of individuals within the United States with respect to both state and federal governments. State constitutions may offer more rights or added protection, but may not encroach upon the rights of its citizens.

It is important to note that the word "privacy" is found nowhere within the Constitution. In fact, it was not until the 1965 case of *Griswold v. Connecticut* that the US Supreme Court ruled that individuals have a constitutional right to privacy that could be found in the "penumbras" of the guarantees enumerated within the Bill of Rights. *Griswold* was a case that involved the question of the legality of a Connecticut state law the criminalized contraceptive services for married couples. Writing for the majority, Justice William O. Douglas found that, although not specifically stated, the constitutional right to privacy could be formed from the "emanations" from the First, Third, Fourth, Fifth, and Ninth Amendments [9].

Within the First Amendment is found the right of association, that is, the right to freely meet and to have privacy in associations. The Third Amendment creates a zone of privacy in its prohibition against the government forcing the quartering of soldiers in any house during peacetime without the consent of the owner. The Fourth Amendment grants the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Self-Incrimination Clause of the Fifth Amendment prohibits the government from forcing an individual to surrender, either the person or information, to his or her detriment. Finally, the Ninth Amendment states, "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people" [10]. It should be noted that the US Supreme Court has ruled that most of the above named amendments, and some of those not mentioned, apply to the actions of state governments, as well, through the Incorporation Doctrine of the Fourteenth Amendment [11].

9.3.1 Laws Directly Affecting Privacy Rights

Of the aforementioned constitutional guarantees, perhaps, most connected to the right to privacy is the Fourth Amendment. It provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized [12].

The amendment has been used to "to protect personal privacy and dignity against unwarranted intrusion by the State" [13]. Early on the US Supreme Court interpreted the Fourth Amendment as invalidating laws and activities that invaded an individual's privacy with respect to the contents of domestic mail [14] and papers and other documents [15, 16]. These rulings have been restricted in the years since they were first announced.

The true nature of the Fourth Amendment controls the ability of government to conduct searches and seizures of objects. A seizure occurs when there is the physical taking of an object or an arrest [17]. Searches evoking the Fourth Amendment come in many different varieties including, dog sniffs outside of the home [18], examination of garbage within the curtilage of a home or building [19], as well as thermal imaging of a home [20]. Important for digital or electronic privacy are the cases that considered the constitutionality of electronic surveillance devices, discussed in Sect. 9.4.

Heretofore, the discussion has focused on constitutional privacy principles. It is important to note, however, that privacy protection has a basis in common law as well. In the United States, common law privacy has its foundations in an 1890 *Harvard Law Review* article by Samuel Warren and Louis Brandeis [21]. In it the two noted jurists argued that advances in new technology, at that time the handheld, instantaneous or "snap" camera, were allowing the press to invade the private lives of individuals [22]. The threat to privacy, therefore, required a legal solution.

Seventy years after Warren and Brandeis' article asserting the need for privacy, Professor William Prosser identified four separate actions that make up the tort of invasion of privacy:

1. Intrusion upon seclusion.
2. Public disclosure of private facts.
3. False light.
4. Appropriation [23].

The common law privacy tort most similar to the Fourth Amendment is intrusion. Intrusion, as defined by the Restatement (Second) of Torts, is the physical or other interference with the seclusion of another individual [24]. The intrusion must be highly offensive to a reasonable person to be actionable. As with the Fourth Amendment, this tort considers reasonableness with respect to what society is prepared to consider reasonable [25].

Intrusion is a claim about the behavior exhibited while gathering information, and whether an individual has a reasonable expectation in the sphere of privacy they claim was invaded. Similarly, the tort of public disclosure of private facts considers whether an individual has a reasonable expectation in the privacy of information that was disclosed. The courts have overwhelmingly ruled that once information is made public, a plaintiff no longer has a reasonable expectation of privacy in that information.

9.3.2 The Evolution of US Statutory Privacy Law

Most states have codified the torts of intrusion, public disclosure of private facts, and the other two privacy claims enumerated by Prosser. And, although there is no federal statute recognizing Prosser's privacy torts, a significant number of federal laws exist with direct and indirect implications for individual privacy. The underpinning for many of these laws was the 1973 Code of Fair Information Practices published by the US Department of Health, Education, and Welfare (HEW) [26]. The report established major principles enumerating the rights of individuals and the responsibility of government agencies with respect to private information:

- There must be no personal data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about them is in a record and how it is used.
- There must be a way for an individual to prevent information about him or her obtained for one purpose from being used or made available for other purposes without their consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him or her.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must ensure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data [27].

Congress incorporated many of these principles into the laws directly and indirectly affecting privacy both during this era and after.

One of the first federal laws passed with privacy implications was the Wiretap Act, also called Title III. Passed in 1968, the Wiretap Act codified Fourth Amendment protections with respect to electronic surveillance by law enforcement [28]. The law applies to the use of electronic listening and recording devices and technologies. Congress amended the Wiretap Act 1984 with the passage of the Electronic Communications Privacy Act (ECPA). The ECPA extended some of the Wiretap Act's protections to, at the time, new communications technology such as email. The law also addresses law enforcement surveillance and acquisition of stored communications, under the Stored Communications Act [28, 29]. The third section of the ECPA regulates law enforcement use of technologies that record the number and delivery information for electronic communications [28, 30].

Congress passed the Fair Credit Reporting Act (FCRA) in 1970. The FCRA regulates consumer-reporting agencies, and provides citizens with rights with respect to how information is shared and collected [31]. Congress amended FCRA in 2003 with the Fair and Accurate Credit Transactions Act, which adds protections against identity theft. Although FCRA regulates private agency collection and sharing of consumer information, thereby offering a measure of privacy protection, the Bank Secrecy Act passed the same year requires banks to maintain records of

consumers' financial transactions. These records are used to assist the government in criminal investigations [32].

Four years later, Congress passed the Privacy Act of 1974. The Privacy Act endows individuals with rights concerning the personal information about them stored by the federal government [33]. One of the most significant rights provided under the Privacy Act is that of the individual to inspect their personal records, and to have any inaccurate information corrected [33]. The same year brought the passage of the Family Educational Rights and Privacy Act (FERPA), also called the Buckley Amendment after its sponsor Rep. James L. Buckley. FERPA regulates the disclosure of personal information in the possession of a school [34].

Later laws reflected the major concerns of that specific era particularly with respect to new technology. Therefore, the expansion of media systems and computing in the 1980s brought the passage of laws with respect to those new systems with privacy implications. Along with the passage of the ECPA in 1986, Congress passed the Cable Communications Policy Act in 1984, mandating that cable companies protect the privacy of the consumer records [35]. The 1988 Computer Matching and Privacy Protection Act regulates government automated file comparison in investigations [36]. That same year, the Video Privacy Protection Act was passed to protect the privacy of videotape rental information [37].

The unifying theme of the laws passed in the 1990s was that of consumer protection. Therefore, Congress passed the Telephone Consumer Protection Act of 1991, allowing civil remedies against telemarketers [38], as well as the Driver's Privacy Protection Act of 1994, restricting the disclosure or sale of motor vehicle records [39], and the Identity Theft and Assumption Deterrence Act of 1998, criminalizing identity fraud [40]. This era also brought the passage of three important privacy-protecting laws. First is the 1996 passage of the Health Insurance Portability and Accountability Act (HIPAA). The law was supposed to make it easier for workers changing jobs to not be excluded from their new health plans because of pre-existing conditions [17]. This required the use of uniform transaction codes and the sharing of data by healthcare providers. The US Department of Health and Human Services promulgated rules to govern the privacy of medical records [17].

The second significant legislative enactment of the 1990s was the Children's Online Privacy Protection Act (COPPA) of 1998. COPPA restricts the collection and use of the personal information of children under the age of 13 by Internet service providers [41].

The Gramm-Leach-Bliley Act of 1999 is the third noteworthy piece of legislation enacted by Congress in the 1990s. The law requires financial institutions to provide consumers with privacy notices. Consumers must also be allowed to opt out of the disclosure of their personal information to other companies [42].

The 2000s saw the rise in anti-terrorism legislation following the attacks on the Pentagon and the World Trade Center on September 11, 2001. One of the most comprehensive laws enacted was the USA Patriot Act, which amended the ECPA, allowing for easier law enforcement acquisition of voicemail [28]. The Patriot Act also allows for the use of pen registers for the collection of metadata associated

with electronic communications [28]. The Patriot Act is used in conjunction with ECPA and laws like the Communications Assistance for Law Enforcement Act (CALEA) to allow government and law enforcement access to electronic communications to facilitate anti-terrorism measures. CALEA, passed in 1994, requires that telecommunication service providers allow law enforcement wiretap access to their systems [43].

9.4 Government Surveillance

It is axiomatic that when the framers of the US Constitution wrote the Bill of Rights, electronic surveillance did not exist. Therefore, the Constitution provides no exact guidance on the legality of government use of advances in technology to invade privacy. The first case to examine electronic surveillance was *Olmstead v. United States*, in which the US Supreme Court had to decide whether law enforcement violated the Fourth Amendment when evidence against a bootlegging conspiracy was obtained from listening devices placed in telephone lines. The Court found that the telephone wires, though connected to the home or business, were not a part of the home and, therefore, were not within the protection of the Fourth Amendment [44].

Though the majority opinion in *Olmstead* found no constitutional violations from the law enforcement activities, Justice Louis Brandeis' dissent is of particular importance. In it the Justice asserts that the general language of the Constitution, and in particular the Fourth Amendment, should not be interpreted in such a way that would limit the ability to consider the changes in the world. The government could develop more ways and new means of invading privacy and the Court's interpretation of that Fourth Amendment had to expand to deal with the new technology. This would necessitate that the Court's decisions with respect to Fourth Amendment search cases go beyond the consideration of whether there was actual physical intrusion or trespass into an individual's home or office. The Court's opinion in *Katz v. United States* took a step in this direction. But, as in *Olmstead*, it is not the majority's opinion that offers the most important guidance about law enforcement activities and privacy.

The *Katz* case considered the constitutionality of FBI agents' use of an electronic listening device to monitor the phone calls of an alleged gambler. The agents attached the device to the outside of the phone booth Charlie Katz used, and used the recordings to convict him of multiple counts of violating federal laws by transmitting wagering information by telephone. In an express rejection of the *Olmstead* requirement of physical trespass by law enforcement, the US Supreme Court found that the Fourth Amendment "protects people, not places" [45]. This meant that the information or activities that a person sought to keep private could be constitutionally protected. This did not mean, however, that the Fourth Amendment created a constitutional right to privacy.

It is Justice Harlan's concurring opinion in *Katz* that has become of paramount importance in understanding privacy in nearly all contexts. The Justice recognized two requirements that result from the past precedents that considered privacy with respect to people. First, the person claiming an invasion of privacy has to have "exhibited an actual (subjective) expectation of privacy." Second, to be perceived as legitimate, that expectation has to be such that society is prepared to recognize it as "reasonable" [46]. With respect to the actual facts of *Katz*, Justice Harlan agreed that society recognized the expectation of privacy in the conversation using the services of a phone booth.

Important to note, however, are the limitations placed on the reasonable expectation of privacy. That is, the courts in the United States, have carved out exceptions to the reasonable expectations test that have major implications for privacy with respect to new forms of technology. The "third-party doctrine," the principle that an individual may no longer claim privacy over information provided to a third party, is one of the most significant of these exceptions. The majority opinion in *Smith v. Maryland* is from whence this principle comes. The *Smith* case examined whether the use of a pen register—technology that monitors the numbers dialed by a specific telephone when installed at the telephone provider—without a warrant, violated the Fourth Amendment guarantee against unreasonable searches [47]. The US Supreme Court expressed doubt as to whether there is an expectation of privacy in the numbers that people dial. According to the Court, people who use telephones know that they are, in essence, giving the phone number that they are dialing to the telephone company. Further, telephone companies commonly use pen register-like technologies to record phone numbers, and to check for illegitimate uses. The Court also rejected the idea that society would recognize the expectation of privacy in the telephone numbers dialed as reasonable, because the individual voluntarily exposes information to another party. Once given to another party, the originator of the information has no control over it.

The *Katz* reasonable expectation recently came under scrutiny with respect to new surveillance technology in the form of Global Positioning System (GPS). In *US v. Jones*, the US Supreme Court held that the law enforcement's placing of a GPS tracking device on a drug-trafficking suspect's vehicle constituted a search within the scope of the Fourth Amendment [48]. But, instead of using the *Katz* reasonable expectation of privacy test, the Court ruled that the government violated the Fourth Amendment because it had physically occupied the suspect's private property by attaching the GPS to his SUV [48]. In her concurring opinion, Justice Sotomayor wrote that in the future the Court would have to address the government use of new technologies that facilitate surveillance and what this means for privacy [49]. In his separate concurrence, Justice Alito wrote that society had an expectation that the government would not record every move made by its citizens [50]. According to Professor Christopher Slobogin, both concurring opinions expressed endorsement of what is called the "mosaic theory" of the Fourth Amendment [51]. The mosaic theory expresses the view that the aggregated information from certain kinds of government surveillance is a violation of constitutional privacy [51]. Of course this is not law, but there has been a call for mosaic theory to be codified [51].

9.5 European Privacy

The European approach to privacy stands in stark contrast to that of the United States. This contrast is illustrated in Table 9.1, which provides a brief comparison of underlying tenets of US approaches to privacy protection compared with their European counterparts.

This difference is a dichotomy in how privacy rights are viewed in the United States and in Europe. The privacy framework for the US approach is based on a negative right requiring the government to refrain from identified privacy violating activities. The European approach, on the other hand, places an affirmative duty on government to safeguard individual privacy [52]. As previously described in this chapter, there is no expressly stated right of privacy in the US Constitution. Instead it is derived from the penumbras of other Constitutional rights that are expressly stated. In Europe, privacy was expressly declared to be a human right and fundamental freedom in 1950 in the Convention for the Protection of Human Rights and Fundamental Freedoms adopted by 47 European nation-states. Article 8 of the European Convention on Human Rights (ECHR), titled "Right to respect for private and family life," provides that:

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 as such as 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 of crime, for the protection of health or morals, or for the protection of the rights and freedoms of others [53].

Fifty years later in 2000, with the promulgation of the Charter of Fundamental Rights, the European Union consolidated then existing rights that had previously been guaranteed by separate charters, treaties, or case law; as well as incorporated new rights emerging in the modern era [54]. The Charter of Fundamental Rights became legally binding on EU institutions and its member nation-states in 2009.

Table 9.1 Comparison of selected US–EU privacy principles

United States	Europe
Privacy is not expressly mentioned in the Constitution	Privacy right is guaranteed in the European Declaration of Human Rights and the European Union (EU) Charter of Fundamental Freedoms
The individual relinquishes control of personal information voluntarily given to third parties	The individual retains ownership of personal information
Individual privacy is protected from the government	Individual privacy is protected by government from the private sector

Among the new fundamental rights codified was a right to data protection. Article 8, titled "Protection of personal data," mandates that:

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 [55].

Article 8 of the EU Charter for Fundamental Freedoms reinforced the long-standing push in the EU for protection of personal data. Digital privacy has been a concern of the European Union almost since its formal inception in 1993. The EU Data Protection Directive (Directive 95/46/EC) was adopted in 1995. It was intended to set limits on the permissible collection and use of personal data of EU residents while simultaneously facilitating the free movement of that personnel data within the European Union [56]. The personal data of EU residents is protected even when they are using services and products of non-EU companies [57]. The Data Protection Directive required that each member state establish its own independent national body to ensure that this data was protected. As a result of the release of information on *PRISM,* the NSA project that included spying on European Diplomats among others, Europeans are also concerned about protecting their data from the US Government. This has led to increased calls for the establishment of European-based cloud services, relieving the need for EU members to rely on US cloud companies [58].

The guidelines established pursuant to the Data Protection Directive relate to the: quality, legitimacy, excluded categories, disclosure of information regarding the collector or controller of the information, individual's right of access to the information, right to object, specified exceptions and restrictions, confidentiality, and notification requirements when personal data is collected. For example, among the key requirements of the Data Protection Directive is a prohibition on processing personal demographic-type data related to items such as racial or ethnic origin, religious or philosophical beliefs, health, and sex life except within certain delineated instances [56]. Individuals also have a right to object on legitimate grounds to having data processed about them [56].

To consolidate enforcement and implementing regulations, in 2012, the European Union began work on a consolidated comprehensive reform of the 1995 Data Privacy Directive designed to strengthen online privacy rights as well as boost Europe's digital economy [59]. The General Data Protection Regulation (GDPR) was adopted in March 2014 by the European Parliament and sent to the Council of Ministers, the next stage in the reform process [60]. A brief summary of new and enhanced protections to be provided by the GDPR is presented in Table 9.2.

The most striking distinction between the United States and the European Union is a difference in the perceived need for privacy protections. Europeans appear to be more concerned about privacy encroachments by the private sector or corporations,

Table 9.2 GDPR selected individual empowerment provisions [64]

A Right to be Forgotten	In the absence of legitimate reasons for retention individual data must be deleted at the individual's request
A Right to Data Portability	Individuals can transfer their data among service providers
Consent requires an express affirmation	When consent it required it must be expressly stated, not inferred by a failure to say no
Privacy by design and default for all products and services	Default settings must be privacy friendly

while Americans seem more concerned with the likelihood of government encroachments [61, 62].

Reminiscent of the adoption of the Patriot ACT in the United States following the September 11, 2001 events, the European Union a few short years later also confronted a situation where goals of personal privacy and national security appeared to collide. In the aftermath of the Madrid train bombings in 2004 and the London bombings in 2005, the European Union attempted to address the conflicting nature of a strong right to privacy with the need of law enforcement to conduct criminal investigations. The EU Data Retention Directive (DPD) of 2006 identified a category of data, referred to as "covered data," that it was permissible to retain for a period of 6–24 months [63].

Citing the demonstrated importance of traffic and location data in the investigation, detection, and prosecution of criminal offenses, the DRD required member states to retain data that was necessary to identify the following [69]:

1. Source of a communication.
2. Destination of a communication.
3. Duration of a communication.
4. Type of communication.
5. Users' communication equipment or purported equipment.
6. Location of the mobile communications equipment.

While data about a specific communication is to be retained, the DRD specifically directs that no data about the content of that communication is to be retained [69]. Covered data is to be retained by the operator and provided only to the designated national authority [69].

In April 2014, however, the European Court of Justice (ECJ) declared the Data Retention Directive inconsistent with the EU Charter of Fundamental Rights asserting that it violated two basic rights, the right for private life and protection of personal data [64]. In its decision, the ECJ did recognize the legitimate law enforcement and anti-terrorism purposes for data retention, but determined that the DRD violated considerations of proportionality. Following the adoption of the DRD by the European Union,member states promulgated their own laws, regulations, and administrative provisions necessary for compliance with the DRD [69].

The subsequent decision of the ECJ left those member state directives in place but subject to judicial review. States responded to this challenge in different ways. For instance, the United Kingdom, after initially continuing to utilize the regulations it had developed for the DRD, in July 2014 passed the Drip Bill. As noted in Sect. 9.2, the passage of Drip proved controversial, and failed to abate the continuing tension between government regulations and legal principles in regards to privacy [70].

9.6 Challenges and Opportunities

Each time a bonus or savings card is used by someone in a grocery store, the individual's purchases are recorded. Targeted advertising appears on a computer monitor based on the tracking of the websites visited by the user or by their online purchases. "Do Not Track" prohibitions are the primary efforts used to protect individual privacy by restricting advertisers from tracking online behavior. But their activation often requires that the user take several affirmative steps.

Consider those insidious mechanisms such as the GPS locator on cell phones and the app that directs those phones to locate "friends" in the same geographic space. But what if the individual doesn't want to be located? Data mining of customer information is a lucrative enterprise. It has been estimated that in 2012 the value of the online data market was $62 billion [65]. This has led to complaints by US companies about the limitations placed by EU states on their ability to gather customers' personal information when doing business in the European Union, and it has been a continuing source of tensions between US companies and the European Union [61].

Traditional adherence in US privacy law to notions of the separate nature of government and the private sector is inconsistent with the operations of today's digital environment. Most users of many popular apps, for example, are unaware of the extent to which those apps "leak" personal information, which is then available for capture by government agencies, criminal enterprises, or other data mining companies [66]. An overarching challenge is to determine the appropriate levels of privacy protection that should be applicable.

The challenges and opportunities presented by the need to effectively shape personal privacy laws and regulations that meet the needs of the 21st century are myriad. The issues highlighted when comparing the two opposing approaches of the United States and the European Union raise several questions for consideration. For instance:

- What do we actually want to regulate to protect individual privacy—the government, the private sector, or both?
- How do we ensure that users are actually fully informed of the personal information that will be collected in a manner that is comprehensible to the user and offers them a viable choice?

- What is the feasibility of providing services in a way that is minimally intrusive on individual privacy by minimizing the personal information collected and the length of time it is held?

More importantly, it may be that the greatest challenge is recognizing that the nature of the questions makes a statement about the values that a society deems important with regard to personal privacy. The opportunity is in determining what those values should be.

As such, it may be instructive to look again at the guidelines aimed at strengthening privacy or information in the past. The five principles form the 1973 Code of Fair Information Practices noted in Sect. 9.3.2, for example, could prove, and has been, useful for constructing policy related to individual rights with respect to control over information [26]. An examination of these five principles, as well as the laws, policies, and court opinions detailed above, reveals the key themes of information access and control with respect to individual privacy.

The theme of access encompasses both the right of citizens to know that government collection of information exists, as well as the right to know what personal information is being collected. Government agencies, then, would be required to inform citizens about ongoing surveillance activities. This, of course, would not necessarily mean that specific individuals would be informed that they were being investigated. The citizenship, as a whole, should be informed, however, of ongoing government data collection, and what this may mean for their activities, digital or otherwise. In this way, there may not be a need for a repeat of the Edward Snowden saga.

Control of collected information would allow citizens the ability to correct the information collected. It also may include the right to force the deletion of information stored in government, or private, databases. This may be the most important and yet controversial principle to implement. By definition, this kind of right, as conceptualized in the right to be forgotten mentioned above, provides individuals with control over information in another's possession. This control would allow a person to force the erasure of that information.

In considering the ways to implement the principles of access and control, it may also be instructive to consider the privacy laws and policy frameworks from other parts of the globe. Japan, for instance, regulates the use of personal information contained in certain business databases, requiring data subjects to be provided with notice about the purpose of the use of their data [67]. The law also requires that businesses obtain consent from the data subject for any uses outside of the stated purpose, and before allowing third-party access to personal data [67].

Of particular note is that of Privacy by Design (PbD), a framework developed by Ann Cavoukian, the former information and privacy commissioner of Ontario, Canada. PbD is based on seven principles that incorporate both consumer control and access to information. The principles are:

1. Proactive not reactive (measures).
2. Privacy as the default.
3. Privacy embedded into design.

4. Full functionality.
5. End-to-end security.
6. Visibility and transparency.
7. Respect for user privacy [68].

Although the PbD framework appears to focus on business or organizations, the foundational principles evoking, again, the values of control, access, and, additionally, transparency would be beneficial for integration into government activities evoking personal privacy.

9.7 Conclusion

Privacy law is made up of a hodgepodge of statutory, constitutional, and common law ideas and principles that are adapting to developments in new technology. The United States has a long history of evolving its Constitutional interpretation and its laws to meet changing conditions. But technological changes are increasing rapidly. To keep pace, regulators must find ways to accelerate the amendments to laws implicating both government and private access and use of personal information.

The US approach to privacy is noticeably different from the EU model. The former has its basis in prohibitions against government activity, which have been applied to privacy, while the later focuses on privacy and data protection as express rights that protect the individual from corporate data-gathering efforts. To be effective, privacy laws and regulations must grow in tandem with the technology that is being regulated. Approaches to privacy that exclude information voluntarily disclosed to third parties from protection may be outdated in a world where digital technology is so intertwined in our lives that ordinary activities of daily living are predicated on some type of voluntary disclosure to access an essential service. It may be inevitable that as technology expands so too does its insidious creep into the private spaces of our lives. But there has to be an approach to maintaining some semblance of personal privacy without opting out of the benefits of the digital world.

References

1. Solove DJ (2007) I've got nothing to hide and other misunderstandings of privacy. San Diego Law Rev 44:745
2. G. U. interactive team, MacAskill E (2013) NSA files decoded: Edward Snowden's surveillance revelations explained. The Guardian
3. Gellman B, Blake A, Miller G (2013) Edward Snowden comes forward as source of NSA leaks. The Washington Post, 10-Jun-2013
4. Marco Civil da Internet (2014) vol. Lei No. 12.965
5. Solove DJ (2004) The Digital Person New York University Press, New York
6. De Rosa M (2003) Privacy in the age of terror. Wash Q 26(3):27–41

7. Fiveash K (2014) UK gov rushes through emergency law on data retention The Register, 10-Jul-2014
8. Travis A Drip (2013) surveillance law faces legal challenge by MPs. The Guardian, 22-Jul-2014
9. Griswold v. Connecticut (1965) US Reports vol 381, p 479
10. U.S. Const. am. 9
11. Lieberman JK, A practical companion to the constitution: how the Supreme Court has ruled on issues from abortion to Zoning. University of California Press, Oakland
12. U.S. Const. am. 4
13. Schmerber v. California (1966) US Reports vol 384, p 757
14. ex parte Jackson (1877) US Reports, vol 96, p 727
15. Boyd v. United States (1886) US Reports, vol 116, p 616
16. Gouled v. United States (1921) US Reports, vol 255, p 298
17. Solove DJ, Rotenberg M, Schwartz P (2008) Information privacy law
18. Florida v. Jardines (2013) US Reports, vol 133, p 1409
19. California v. Greenwood (1988) US Reports, vol 486, p 35
20. Kyllo v. United States (2001) US Reports, vol 533, p 27
21. Kalven H Jr (1966) Privacy in Tort law-were Warren and Brandeis wrong. Law Contemp Prob 31:326
22. Warren SD, Brandeis LD (1890) The right to privacy. Harv Law Rev 4(5):193
23. Prosser WL (1960) Privacy. Calif Law Rev 48(3):383–444
24. Restatement of the Law, Second, Torts, §652 (2014). http://cyber.law.harvard.edu/privacy/Privacy_R2d_Torts_Sections.htm. Accessed 13 April 2014
25. Solove DJ (2002) Conceptualizing privacy. Calif Law Rev 1087–1155
26. Rotenberg M (2001) Fair information practices and the architecture of privacy: (what Larry doesn't GET). Stan Tech Rev 2001:1–4
27. U.S. Dep't. of Health (1973) Education and Welfare, Secretary's Advisory Committee on automated personal data systems, records, computers, and the Rights of Citizens viii
28. Freiwald S, Metille S (2013) Reforming surveillance law: the swiss model. Berkeley Tech J 28
29. Stored wire and electronic communications and transactional records access, US Code, Title 18, sections 2701–2711
30. Pen registers and trap and trace devices, US Code, Title 18, sections 3121–3127
31. Fair Credit Reporting Act (1970) Public Law No. 90-32, US Code, Title 15, section 1681 et seq. 1970
32. Bank Secrecy Act (1970) Public Law No. 91-508
33. Privacy Act of 1974, US Code, Title 5, section 552a
34. Family Educational Rights and Privacy Act of 1974, US Code, Title 20, sections 1221 note, 1232 g
35. Computer Matching and Privacy Protection Act of 1988, US Code, Title 5, section 552a
36. Video Privacy Protection Act of 1988, US Code, Title 18, sections 2710–2711
37. Telephone Consumer Protection Act of 1994, US Code, Title 47, section 227
38. Driver's Privacy Protection Act of 1994, US Code, Title 18, sections 2721–2725
39. Health Insurance Portability and Accountability Act of 1996, Public Law No. 104–191
40. Identity Theft and Assumption Deterrence Act of 1998, US Code, Title 18, section 1028
41. Children's Online Privacy Protection Act of 1998, US Code, Title 15, sections 6501–6506
42. Gramm-Leach-Bliley Act of 1999, US Code, Title 15, sections 6801–6809
43. Communications Assistance for Law Enforcement Act of 1994, Public Law No. 103–414
44. Olmstead v. United States (1928) US Reports, vol 277, p 438
45. Katz v. United States, (1967) US Reports, vol 389 p 347
46. Katz v. United States (1967) US Reports, vol 389, p 361 (Justice Harlan concurring)
47. Smith v. Maryland (1979) US Reports, vol 442, p 735
48. US v. Jones (2012) Supreme Court reporter, vol 132, p 947
49. US v. Jones (2012) Supreme Court reporter, vol 132, p 954 (Justice Sotomayor concurring)
50. US v. Jones (2012) Supreme Court reporter, vol 132, p 957 (Justice Alito concurring)

51. Slobogin C (2012) Making the most of United States v. Jones in a Surveillance Society: A statory implementation of mosaic theory. Duke J Const Law Public Policy 8:1–37
52. Kuner C (2013) The transatlantic divide over data privacy rights 20 May 2013. https://www.privacyassociation.org/privacy_perspectives/post/the_transatlantic_divide_over_data_privacy_rights. Accessed 30 March 2014
53. Council of Europe (2014) European convention on human rights, 4 November 1950. www.echr.coe.int/Documents/Convention_ENG.pdf. Accessed 2 April 2014
54. Justice European Commission (2014) EU charter of fundamental rights, 25 July 2013. www.ec.europa.eu/justice/fundamental-rights/charter/index_en.htm. Accessed 5 April 2014
55. European Convention (2014) Charter of fundamental rights of the European Union, 7 December 2000. www.europarl.europa.eu/charter/pdf/text_en.pdf. Accessed 5 April 2014
56. Protection of personal data, 2 Jan 2011. http://europa.eu/legislation_summaries/information_society/data_protection/114012_en.htm. Accessed 5 April 2014
57. Fromholz J (2014) The European Union data privacy directive. Berkeley Technol Law J 15 (1):461–484
58. PRISM Fuels Cries for EU Clouds (2013) Information Management, September/October, p 6
59. European Commission Justice (2014) Commission proposes a comprehensive reform of the data protection rules, 25 Jan 2012. http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm. Accessed 25 March 2014
60. European Commission (2014) Data protection: progress on EU reform now irreversible after European Parliament vote. European Commission, 12 March 2014. http://europa.eu/rapid/press-release_MEMO-14-186_en.htm. Accessed 25 March 2014
61. Sullivan B (2014) "La Difference" is Stark in EU, U.S. Privacy Laws, 19 Oct 2006 http://www.nbcnews.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws/#.U1CwB_mwJcQ. Accessed 10 April 2014
62. Fromholz J (2014) The European Union data privacy directive. Berkeley Technol Law J 15 (1):461–484 (note 2)
63. Taylor M (2006) The EU data retention directive. Comput Law Secur Rep 22:309–312
64. Digital Rights Ireland Ltd (C-293/12) v. Minterter for Com munications, Marine and Natural Resources, et al and KarnterLandesregierung (C-294/12) and others. European Court of Justice. Decided: 8 April 20
65. Dwoskin E (2014) Study: Digital Marketing Industry Worth $62 Billion. Blog: Wall Street Journal, 14 Oct 2013. http://blogs.wsj.com/digits/2013/10/14/study-digital-marketing-industry-worth-62-billion. Accessed 5 April 2014
66. Ball J (2014) NSA and GCHQ target 'Leaky' phone apps like Angry Birds to scoop user data. The Guardian, 27 Jan 2014. http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data. Accessed 6 April 2014
67. Act on the Protection of Personal Information 2003
68. 7 Foundational principles. Privacy By Design. http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/. Accessed 28 Jul 2014
69. European Parliment and Council of the European Union, "Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006. Off J Eur Union L105:54–63. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF. Accessed 26 Jul 2014
70. Ermert M (2014) EU data retention directive finally before European Court of justice. Internet Policy Rev: J Internet Regul (05 Jul 2013). http://policyreview.info/articles/news/eu-data-retention-directive-finally-european-court-justice/162. Accessed 26 Jul 2014