CHAPTER 12

# Privacy

*"If everybody minded their own business," the Dutchman said in a hoarse growl, "the world would go round a deal faster than it does."*

*—Lewis Carroll, Alice's Adventures in Wonderland*

**LEARNING OBJECTIVES**

**After you have read this chapter, you should be able to:**

- **Explain the American approach to the regulation of privacy**
- **Understand constitutional sources of the right to privacy**
- **Discuss common law torts for the invasion of privacy**
- **Explore the privacy concerns arising out of online marketing, including online behavioral advertising, unsolicited commercial email and the use of web beacons**
- **Explain the key federal laws that regulate privacy including the GLB Act, COPPA, HIPAA, and the Electronic Communications Privacy Act**
- **Analyze emerging data security requirements**
- **Identify key cases in privacy law**

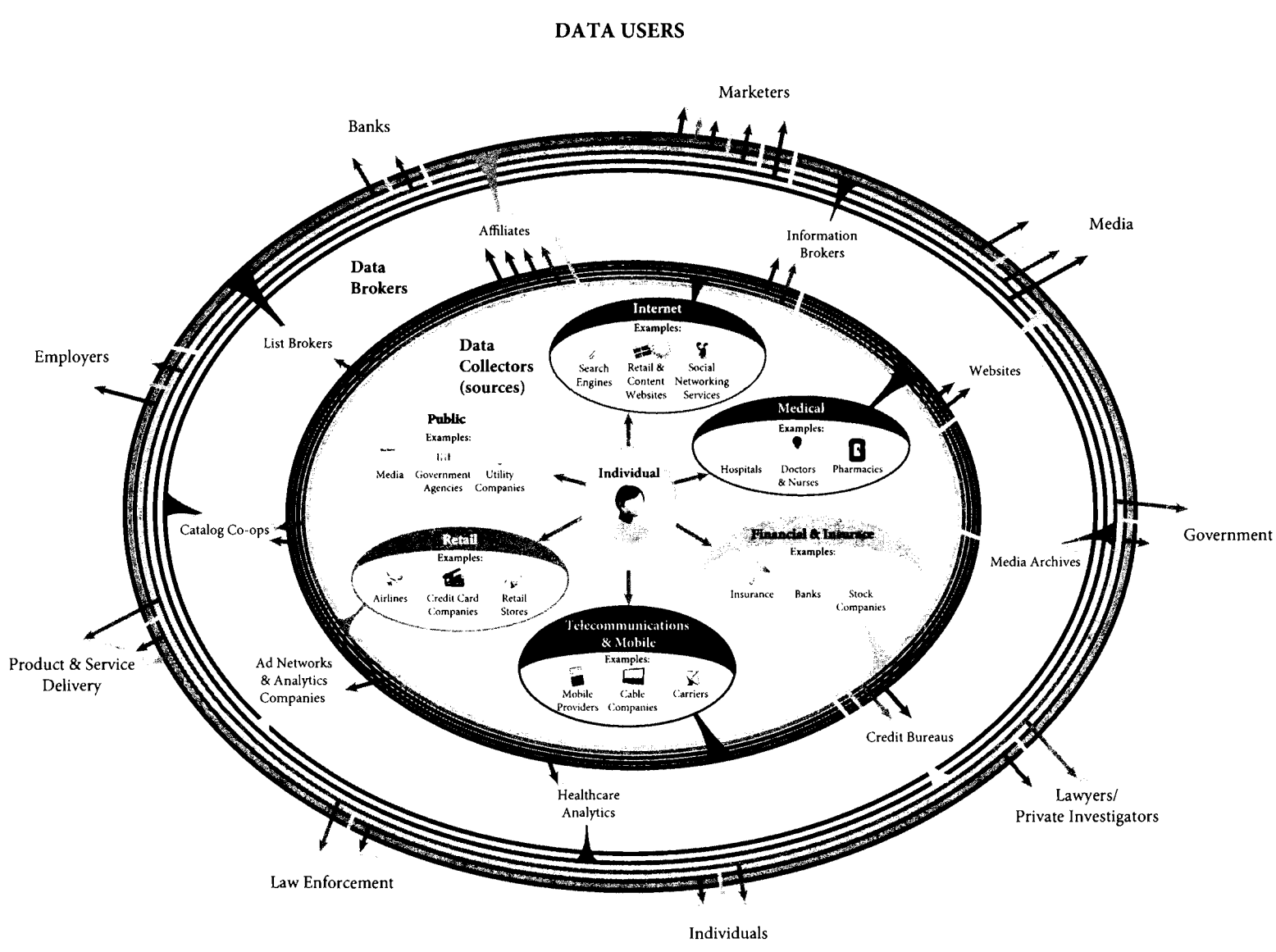
## Introduction

One well-regarded definition of privacy classifies it as the right "to be let alone."[1] In a *Harvard Law Review* article from 1890, Samuel D. Warren and Louis D. Brandeis contend: Recent Inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone."

Looking back, it seems that Warren and Brandeis were prophetic. Considering their references to "recent inventions and business methods," one can't help but wonder if they could have foreseen a time when the right "to be let alone" would be increasingly threatened by complex online social networks; global positioning systems (GPS) that allow rental car companies, employees and others to track one's location and speed; surveillance cameras in public places; massive data aggregation services; and other modern privacy threats. The scope of modern data collection practices is evident in startling clarity in Exhibit 12.1, which depicts a **personal data** ecosystem flowchart, which was distributed at series of recent workshops on privacy conducted by the **Federal Trade Commission** (**FTC**).

[1]Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," 193 Harv. L. Rev. 4 (1890).

**EXHIBIT 12.1** Personal Data Ecosystem



This chapter provides an overview of existing privacy law and examines privacy concerns arising out of a variety of online activities. In doing so, students are encouraged to consider whether the existing legal framework adequately protects the privacy of those active in on the Internet.

# Sources of the Right to Privacy

## U.S. Constitution

Although the U.S. Constitution does not specifically recognize a right to privacy, there are important privacy protections enshrined in the U.S. Constitution. Consider, first, the Ninth Amendment, which reads:

> *The enumeration in the constitution of certain rights shall not be construed to deny or disparage others retained by the people.*

This amendment was likely the genesis of the privacy right that has evolved in the courts and through the teachings of scholars such as Warren and Brandeis. In addition, the Fourth and Fifth Amendments are also sources the "right to privacy." The **Fourth Amendment** provides:

> *The right of the people to be secure in the persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no Warrants shall issue, but on probably cause, supported by the oath or affirmation, and particularly describing the place to be searched, and the person or thing to be seized.*

In *Griswold v. Connecticut,*[2] the U.S. Supreme Court declared unconstitutional a state law prohibiting the use of birth control devices and the provision of advice concerning their use. The Court also recognized that the Bill of Rights provided us with what it deemed to be "zones of privacy," or areas or locations where privacy is expected.

Later cases held that an important element of this right was to establish the existence of a "reasonable expectation of privacy" in the particular zone of privacy. The following are the minimum requirements for establishing a "reasonable expectation of privacy":

1. **The person exhibits an actual expectation of privacy.**
   To understand this concept of an expectation of privacy, consider what you expect when entering an area or location, such as your bedroom, which you desire to be off-limits to others. Alternatively, consider the level of privacy that an employee should anticipate with respect to his or her computer, email, or voicemail.
2. **Society recognizes the expectation as reasonable.**
   In addition to your own expectations regarding privacy, what do others believe to be your expectation of privacy when you close the door to your bedroom or office, or when you send an email or surf a website?

For the purpose of our discussion on privacy rights online, these requirements have to be satisfied concerning the mass of information (much of which is personal in nature) being disseminated over the Internet.

Next, consider the Fifth Amendment, which protects us from government action that could result in self-incrimination. That provision reads in part:

> *No person ... shall be compelled, in any criminal case, to be a witness against himself.*

This does not apply when a person voluntarily turns over documents, records, files, and papers to a law enforcement agency or official. Similarly, the public records of a corporation are not subject to this provision, even if they contain incriminating evidence.

---

[2]381 U.S. 479 (1965).

Although the Fifth Amendment may be commonly associated with the right to refrain from testifying against oneself in a criminal trial, the Fifth Amendment also has application to the online world. An interesting application of the Fifth Amendment to cyberlaw involves the act of encrypting a file that contains possibly incriminating information.

Encryption involves encoding methods to block access to certain documents. In *Doe v. United States*,[3] the Supreme Court held that an individual could "be forced to surrender a key to a strongbox containing incriminating documents, but not to reveal the combination to his wall safe ... by word or deed."

This case seems to imply that a law enforcement agency, pursuant to a valid search warrant, could obtain an encrypted file. However, the decision in *Doe* would likely prevent the agency from forcing a defendant to supply the private key, password, or code that could enable decryption or decoding. *Doe* raises questions regarding employees who store potentially criminal information on their employer's computers. If the information belongs to the employer and not the employee, it is possible that a court would allow the employer to access it and use it not only to fire the employee but also in connection with any law enforcement action. Of course, this presupposes that the company has the ability to require the employee to allow access, either through company policy or applicable law.

### State Constitutions

In addition to the U.S. Constitution, state constitutions are a source of important privacy rights. In general, rights established by state constitutions mirror the amendments mentioned earlier in content and, similarly, apply only to public employees. However, some states afford greater protection against government violations of privacy. Beyond constitutional protections, states are playing a significant role in privacy regulation, with many enacting laws to address a range of privacy and data security considerations. Several of these measures will be discussed further below under State Privacy laws.

## Common Law Torts for the Invasion of Privacy

There are four main privacy-related torts recognized by common law and by the Restatement (Second) of Torts. These torts provide monetary and injunctive relief for an unreasonable or unwarranted invasion of the right to privacy. They could also provide remedies for a cause of action in cases involving privacy rights online.[4] The four torts are: (1) intrusion upon seclusion; (2) public disclosure of private facts causing injury to reputation; (3) publicly placing another in a false light; and (4) appropriation of a person's name or likeness causing injury to reputation, each as discussed further below:

### Intrusion Upon Seclusion

The right of each of us to be able to go to a place of seclusion and to be left alone is not absolute. But when another individual, without permission or legal justification, violates a place of seclusion, that individual may be found to have committed this tort. The Restatement (Second) of Torts defines **intrusion upon Seclusion**[5] as:

> *Intentionally intruding, physically or otherwise, upon the solitude of another or his private affairs or concerns.*

---

[3]487 U.S. 201 (1988).

[4]For example, in the *Boring v. Google* case, discussed later in this chapter, the plaintiffs claimed that Google had committed certain privacy torts in connection with its Street View service.

[5]Restatement (Second) of Torts § 652B (1977).

In order to proceed, a plaintiff would need to prove the following elements:

- There was an intent to intrude, or knowledge that the intrusion would be wrong
- There was a reasonable expectation of privacy
- Intrusion was substantial and highly offensive to a reasonable person.

The tort of *intrusion upon seclusion* can apply in the online world. Consider the following case.

## STEINBACH v. VILLAGE OF FOREST PARK
## No. 06-4215, 2009 WL 2605283 (N.D. Ill. Aug. 25, 2009)

### FACTS

[Steinbach, a local elected official, had an email account issued by the municipality. A third-party company, Hostway, provided the technology for the account. Steinbach logged in to her Hostway webmail account and noticed eleven messages from constituents that had been forwarded by someone else to a political rival.]

[Steinbach sued the municipality, her political rival and an IT professional employed by the municipality. She brought numerous claims, including violation of the Federal Wiretap Act, the Stored Communications Act, and the Computer Fraud and Abuse Act. She also brought a claim under Illinois common law for intrusion upon seclusion.]

### JUDICIAL OPINION (JUDGE ZAGEL)

[The plaintiff in this case brought a number of claims. Of most relevance here is the Court's discussion of the intrusion upon seclusion tort:]

While it is true that the Illinois Supreme Court has not explicitly recognized the tort of intrusion upon seclusion, this Court has found that the tort does exist. *Ludemo v. Klein,* 771 F. Supp. 260 (N.D. Ill. 1991) (Zagel, J.). When state tort law is unclear, a federal district court can follow the decisions of the state appellate court governing the geographical area where the alleged tort took place, unless there is reason to believe the Supreme Court of Illinois would decide the question differently. Id. at 261-62. In diversity cases it is the determination of what the highest court of the state would do that is the key question. Forest Park is located in Cook County, which is in the First District, case law from First District Appellate Court governs. The First District formally recognized the existence of the tort in Illinois. *Busse v. Motorola, Inc.,* 813 N.E.2d 1013 (Ill. App. Ct. 2004). Therefore, this Court recognizes the existence of the tort under the First District ruling, since there is no hint of contrary reasoning from the highest court in Illinois. (Footnotes omitted).

Under *Busse,* all four elements of the tort must be satisfied. Id. at 1017. These elements are: (1) defendant committed an unauthorized prying into the plaintiff's seclusion; (2) the intrusion would be highly offensive to the reasonable person; (3) the matter intruded upon was private; and (4) the intrusion caused plaintiff to suffer. Id.

Calderone first argues that his access to Steinbach's email was authorized by Illinois statute. Section 3.1-35-20 states that "the mayor or president at all times may examine and inspect the books, records and papers of any agent, employee or officer of the municipality." 65 ILL. COMP. STAT. 5/3.1-35-20. It is true that "records" includes all "digitized electronic material," thus including email within the definition. 5 ILL. COMP. STAT. 160/2. While there is minimal case law interpreting the statute, it is clear that it does not give a mayor carte blanche access to use the records for his own use. In one case, the court found a city mayor was authorized under the statute to access private juvenile records which discussed questionable police officer behavior. *People v. Urbana,* 338 N.E.2d 220, 221, 222 (Ill. App. Ct. 1975). That access is different from what Calderone is accused of here. In *Urbana,* the mayor was not using the access for his own personal use, but for an official city investigation related to his position as mayor. Id. at 221. Here, Calderone did not access Steinbach's email for any official purpose, but rather for his own personal gain. Therefore, Defendant's argument that his actions were statutorily authorized fails. Calderone also argues that Steinbach did not sufficiently plead the privacy of the emails. In the Verified Third Amended Complaint, Steinbach alleges that the emails were meant and intended to be private. Complaint, ¶¶ 28, 40, 43.

(Continued)

Steinbach sufficiently pled the third element of the tort to survive a Motion to Dismiss. Whether the emails actually were private is a question of fact which cannot be determined at this stage. Therefore, Count 8 must stand.

**CASE QUESTIONS**

1. What are the elements of the tort of intrusion upon seclusion?
2. ***Ethical Consideration:*** Do you think that there is a role for the tort of intrusion upon seclusion in the online world or is it better limited to the "real" world?
3. While plaintiffs have had success in bringing claims for the tort of intrusion upon seclusion for online activities, other plaintiffs have not enjoyed similar success. What are the particular challenges of bringing claims for the tort of intrusion upon seclusion for privacy violations occurring online?

## Public Disclosure of Private Facts Causing Injury to Reputation

**Public disclosure of private facts causing injury to reputation** concerns the public disclosure or transmission of highly personal facts or information about an individual that results in injury to reputation. In some instances, the tort is associated with the tort of defamation, and both may be used as separate causes of action arising out of the same case.

In addition to the elements of "intent or knowledge" and "highly offensive to a reasonable person," the public disclosure of private factors causing injury to reputation requires: (1) the facts must be private; and (2) communication or publicity must be disclosed to a significant segment of the community. Further, this tort is committed when the facts publicized would be (1) highly offensive to a reasonable person and (2) are not of legitimate concern to the public.

## Publicly Placing Another in False Light

According to the Restatement (Second) of Torts:

> *One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if*
>
> *(a) the false light in which the other was placed would be highly offensive to a reasonable person, and*
> *(b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.*[6]

**Publicly placing another in false light** is also associated with the tort of defamation and involves falsely connecting a person to an immoral, illegal, or embarrassing situation resulting in injury to one's reputation. To date, this tort has not been the subject of much, litigation concerning online activities.

## Misappropriation of a Person's Name or Likeness Causing Injury to Reputation

The appropriation of a person's name or likeness causing injury to reputation[7] typically involves using a living person's name or likeness for a commercial and non-newsworthy purpose without the individual's permission. There are three elements that must be shown to prove that this tort has been committed: (1) the person's name, portrait or picture was used; (2) for purposes of trade or advertising; (3) without the person's written consent.

[6]Restatement (Second) of Torts § 652E (1977).

[7]Restatement (Second) of Torts § 652C (1977).

An example from the Restatement (Second) of Torts is as follows: "A is an actress, noted for her beautiful figure. B, seeking to advertise his bread, publishes in a newspaper a photograph of A, under the caption, 'Keep That Sylph-Like Figure by Eating More of B's Rye and Whole Wheat Bread.' B has invaded A's privacy."[8]

# Federal Privacy Laws

As compared with other countries including the member states of the European Union, the United States has adopted a rather piecemeal approach to data privacy. Instead of having a single comprehensive data privacy law that applies across all industries, American lawmakers provide special protections to certain types of data, such as consumer credit information, medical records, and even video rental data.

While U.S. legislators have not yet elected to enact privacy legislation that applies to all types of personal data, lawmakers have passed significant federal laws that apply to particular types of personal data. Although these laws have a limited scope, they generally establish broad requirements and stringent restrictions with respect to the collection and use of the particular types of personal data to which they apply.

## Privacy Protection Act

Congress enacted the **Privacy Protection Act (PPA)**[9] to reduce the chilling effect of law enforcement searches and seizures on publishers. The PPA prohibits government officials from searching or seizing any work product or documentary materials held by a "person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication,"[10] unless there is probable cause to believe the publisher has committed or is committing a criminal offense to which the materials relate. The PPA effectively forces law enforcement to use subpoenas or voluntary cooperation to obtain evidence from those engaging in First Amendment activities.

## Privacy Act of 1974

The Privacy Act of 1974[11] covers nearly all personal records maintained by federal agencies and some federal contractors. It applies to military health records, veterans' records, Indian Health Service records, Medicare records, and medical records of other federal agencies. The Privacy Act of 1974 does not apply to most hospitals, clinics, or physicians, even if they receive federal funds or are tax-exempt. Generally speaking, the Privacy Act of 1974 grants people four rights: (1) to find out what information the government has collected about them; (2) to see, and have, a copy of that information; (3) to correct or amend that information; and (4) to exercise limited control of the disclosure of that information to other parties.

## Cable Communications Policy Act

The **Cable Communications Policy Act**[12] ("Cable Act") was enacted to amend the Communications Act of 1934.[13] The Cable Act establishes a comprehensive framework

---

[8]Restatement (Second) of Torts § 652C (1977).

[9]Privacy Protection Act, 42 U.S.C.A. §§ 2000aa, 2000aa-12 (1980).

[10]*Id.*

[11]5 U.S.C. § 552a (1974).

[12]Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 1984 Stat. 66 (codified at 47 U.S.C. § 521 (1984)).

[13]47 U.S.C. § 151 (1934).

for cable regulation and establishes strong protections for subscriber privacy by restricting the collection, maintenance, and dissemination of subscriber data. It prohibits cable operators from using the cable system to collect "personally identifiable information" concerning any subscriber without prior consent, unless the information is necessary to render service or detect unauthorized reception. It also prohibits operators from disclosing personally identifiable data to third parties without consent, unless the disclosure is either necessary to render a service provided by the cable operator or if it is made to a government entity pursuant to a court order.

## Video Privacy Protection Act

The **Video Privacy Protection Act**[14] aims to protect the privacy of consumers' video rental histories. Subject to certain limited exceptions, the Act prohibits videotape service providers from disclosing personally identifiable information about individuals who rent or buy videos to third parties. The Act provides that customers may bring an action against any video store that discloses personally identifiable information. Actual damages are recoverable under the Act but must not be less than liquidated damages in the amount of $2,500. In addition, punitive damages, as well as reasonable attorney's fees and litigation costs, and "preliminary and equitable" relief may be recoverable as deemed appropriate. There is a two-year statute of limitations on proceedings brought pursuant to the Act.

## Telephone Consumer Protection Act

The **Telephone Consumer Protection Act of 1991 (TCPA)**[15] was enacted in response to consumer complaints about intrusive telemarketing practices and concerns about the impact of such practices on consumer privacy. The Act amends Title II of the Communications Act of 1934 and requires the **Federal Communications Commission (FCC)** to promulgate rules "to protect residential telephone subscribers' privacy rights." In response to the TCPA, the FCC issued a Report and Order requiring any person or entity engaged in telemarketing to maintain a list of consumers who request not to be called.

The TCPA further restricts the use of automated dialing systems, artificial or prerecorded voice messages, SMS text messages received by cell phones, and the use of fax machines to send unsolicited advertisements. It also restricts solicitors from calling before 8 a.m. and after 9 p.m. Individuals are entitled to collect damages directly from the solicitor for $500 to $1,500 for each violation, or recover actual monetary loss, whichever is higher.

## Electronic Communications Privacy Act

The **Electronic Communications Privacy Act (ECPA)**[16] legislation places restrictions on the interception of electronic communications and creates privacy protections for stored electronic communications. The ECPA was built on past law and was enacted to guard against potential abuses and constitutional violations in the area of electronic surveillance.

---

[14]Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (codified at 18 U.S.C. § 2710 (2002)).

[15]Telephone Consumer Protection Act of 1991, Pub. L. No.102-243 (codified at 47 U.S.C. 227 (2005)).

[16]Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2510–2521, 2701–2710, 3117, 3121–3126 (1986)).