6

Privacy Issues in Communication

Fritz Messere, Dean Emeritus

School of Communication, Media and the Arts

State University of New York–Oswego

Privacy is a relatively new and emerging right. At the turn of the twentieth century the issue of privacy was just starting to be recognized in the courts in the United States. Troubling issues began to develop when the mass media and the government became technically sophisticated enough to begin threatening individual privacy. Prior to some early legal cases, the issue of privacy often related to the concept of "*being left alone*" without having to worry about having one's likeness being used without permission or having to worry about one's personal information or identity being stolen. With the development of computer networks, the internet, digital media technology, mobile communication, and social media software, and, with advances in scientific research, the ability to disseminate personal information has become both easy and instantaneous.

Today many issues related to privacy have become increasingly difficult, raising questions that reflect the complexity of modern-day society, yielding questions of policy that mass communication research can impact. For example, "Should private information stored on our cell phones be completely confidential?" Or "Is there a governmental interest in accessing private information to ensure national security?" Or, "Should a company be able to market a list of names of five million people who have problems with diabetes?" These issues are very different than

conventional issues, such as when a media outlet publishes the name of a rape victim or when pictures assumed to be private suddenly appear on Facebook. Some scholars note that privacy can be used to denote a very broad set of issues, not necessarily at all related (BeVier, 1995). This chapter reviews the historical basis for developing legal definitions of privacy briefly and then examine the current issues related to the execution of this concept.

Early Issues Related to Privacy

The earliest notions of privacy are loosely attached to development of society and the hypothesizing that even within the earliest cultures there would be the desire and some basic need for solitude. To remove one's self from a larger group. One can point to both biological and anthropological needs within primitive and early cultures for the need to be alone on some occasions. In early Greek and Roman societies, private homes and apartments were atypical for the general population. Public baths and illustrations of sex drawn on walls from these eras suggest that communal living was common (Ferenstein, 2015). Scholars point to Greek philosophers such as Aristotle, who distinguishes between private and communal spheres (the *idion* and *koinon*) as indications of early recognition for some sort of need to be apart from society on occasion (Peterman, 1993).

Christian monks helped to refine the concept of and need for seclusion, where one can be contemplative and alone. Philosopher Hannah Arendt (1958) suggests our contemporary understanding for solitude and some form of private space can be traced to the relationship between the expansion of Christianity through the middle Ages and the increasing awareness of the private

sphere. Various texts found in the New Testament refer to activities that Christians pursue in private, such as prayer and reflection. While public oratory was common through most early and medieval times, the invention of the printing press made it possible for quiet study and personal reflect to exist.

Chaucer use of deception in *The Miller's Tale* reflects the genre's reliance on the "private and the secret" to make the farce work (Farrell, 1989). In Shakespeare we see the recurrent use of disguise, often causing characters to misinterpret information or fail to understand that information is kept from them. Plays such as Merchant of Venice, Romeo and Juliet, and Twelfth Night are a few illustrations where characters use disguise and deception to hide their true nature (Kreider, 1934). Literature reflects human nature in this regard. People through the ages felt the need to keep information private or to disguise their looks or true nature, often to obtain some desired end or simply to keep their images from being tarnished.

The Beginning Concerns for Privacy

The refinement of printing presses led to the development of printed newspapers and opinion pieces. These early weekly papers began in Germany in the early 17th century and by 1830 high-speed presses made daily papers possible. Published printed stories were often riddle with unsubstantiated facts and used unflattering language or misinformation. When brought to court, claims that people were injured as a result of false stories were usually treated under common laws of libel and slander laws or as sedition, not as issues of invasion of privacy.

During revolutionary times, colonists were upset when the British government began to quarter

troops in homes, and ordered "writs of assistance" that unilaterally provided troops with the ability to search houses and/or seize papers and property. The colonists thought this violated their rights as Englishmen, and while the courts back in England tended to support this view, violations persisted throughout the revolutionary times. Colonists used the printing press to disperse information supporting the revolution. Thomas Paine's influential monograph *Common Sense* was widely published and sold nearly 100,000 copies in 1976 (Foot and Kramnick, 1987, p. 10). As the colonists formed new laws for our governments these rights became clearly expressed. As the Continental Congress moved toward ratification of the U.S. Constitution, the Fourth Amendment which gave *"the right of people to be secure in their persons, houses, etc…. against unreasonable searches and seizures…."* was included in the Bill of Rights (Dripps, 2013). Even though the Constitution does not specify privacy as a right given to individuals, the 4th Amendment right, to be secure in one's home from government intrusion, along with the First Amendment become important later as the courts took up issues of privacy.

Just as it did when Gutenberg invented the printing press, technology has the ability to change the social landscape quickly. With the development of photography starting in the mid-1800s, it became possible to use the camera to permanently record and duplicate one's likeness. Also, the inventions of the working telegraph (1837) and then telephone (1876) made it possible to provide instantaneous communication between distant places. News (and rumors) could be instantaneously communicated over great distances. The development of these technologies revolutionized the newspaper, publishing, and advertising businesses. Now newspapers, magazines, and advertising could use pictures and these images could be quickly distributed far and wide. With these technical developments intrusion into the sphere of one's private self became important.

The Legal Recognition of Privacy

The issue of whether privacy should be considered a specific right legally was taken up in one of the most famous legal articles of all times. In 1890, Samuel D. Warren and Louis D. Brandeis published *The Right to Privacy* in the Harvard Law Review arguing the right of privacy should be included either under common law or under statutory law. They argued, "(G)ossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery" (p.196). Adopting a phrase penned by Judge Cooley (1879) the authors stated that recent inventions and business methods called for the next step of protection under the law, the right "to be left alone."

It took almost a dozen years before a relevant case came before the New York appellate court. In this early case the picture of Abigail Robertson was used without her permission in a flour advertisement. The court refused to recognize the "right of privacy" and she lost the case (*Robertson v. Rochester Folding Box Co.,* 1902). However, in 1903, the New York State legislature enacted laws under sections of the New York Civil Rights Law stating, "Any person whose name, portrait, picture or voice is used within this state for advertising purposes or for the purposes of trade without written consent..." (New York Consolidated Laws, Civil Rights Law – CVR sec. 51.) 1 While this law set a president for a tort called *misappropriation*, it did not really address many of the issues related to invasion of privacy.

As a result of court findings in a number of cases, over the next 40 years two legal concepts began to emerge. First was the idea that news media do not need someone's consent to publish stories that are about newsworthy subjects. However, when a person's likeness or name was to be used in a commercial situation, it must be with the person's permission. While various issues

related to privacy were being tested in state and federal courts, the U.S. Supreme Court began to recognize a constitutional right of privacy using the Fourth and Fifth Amendment protections against invasions of the "sanctity of a man's home and the privacies of life" (Belmas et al., 2016). The issues of how one makes decisions about a woman's right to choose, about sexual orientation, and about whether society should be able to enforce laws pertaining to social mores is closely related to how society perceives privacy rights. In a case involving a married couple's right to use contraceptives, the decision in *Griswold v. Connecticut* (~~381 U.S. 479,~~ (1965)) was pivotal in that it associated the concept of privacy with the right of the individual to make decisions about one's body. In this landmark decision, Justice William O. Douglas linked the various rights under the Bill of Rights, which taken together, provide individuals with to a right of privacy. Several years later, in *Roe v. Wade* (1973) the courts focused these newly expanded theories of personal privacy in determining that abortions were matters best decided between a woman and her physician. Over the years the *Roe* decision has been challenged in the court and by state legislatures enacting statutory laws restricting a woman's rights numerous times. In 2007, by a narrow majority the court revised the original opinion in *Roe* and said that the "the life of the unborn" as well as a woman's privacy rights needed to be consider. (Roe v. Wade, 410 U.S. 113 (1973)

Today the debate about abortion and the right of a woman to choose continues to be argued by state legislators, the courts, and people on both sides of the issue (*Steinberg v. Carhart*, 2007). Similarly, the right to make decisions about sexual behavior and sexual orientation has evolved over the past 60 years. In 1986, the courts ruled that homosexual sodomy was not a protected privacy right but overturned that decision in 2003. Recently restrictions on gays serving in the military and same sex marriage have been lifted. Today issues of the rights of transgender

individuals have created discussion and conflict among state legislatures as well as groups seeking to protect individual rights (Pearson, 2016).

The Four Basic Privacy Torts

William Prosser, one of the leading legal scholars of the 20th century published a seminal analysis on privacy law that broke down invasion of privacy into four different legal rights. (William L. Prosser, *Privacy*, 48 Calif. L. Rev. 383 (1960). These rights deal with intrusion, disclosure of private facts, false light, and as mentioned previously, misappropriation. This classification has been used widely and is the basis for many court decisions regarding privacy rights. Though these four areas are not necessarily interrelated, they generally reflect that invasion of privacy is an interference with the right of an individual to be left alone (Belmas et al., 2016).

Intrusion

Journalists and media professionals work in an environment where the courts have ruled that anytime people are in a *public place* there is no expectation of privacy. Thus, if you are in a public setting, you do not have a basis for an intrusion case. Reporters can ask questions or take video/stills without the risk of facing a lawsuit, but *intrusion occurs when that reporter/videographer unduly intrudes into an individual's seclusion or private affairs*. In today's

media landscape with miniaturized cameras and recording equipment and with the ability of smartphones to record events, often without detection, the ability to gather information has expanded. Courts usually give a fair amount of latitude to journalists covering newsworthy stories, but the threat to intrusion of one's private space has increased. The courts have ruled against television broadcasters who have used hidden cameras and microphones for intrusive newsgathering in private or semi-private locations, but they have also allowed broadcast of audio when a third party had surreptitiously recorded conversations and provided tapes to broadcasters. Usually intrusion is handled as a civil lawsuit, but journalists can also face criminal charges such as trespass and assault. Public figures such as movie and recording stars find it nearly impossible to maintain any sense of privacy as they can be followed nearly anywhere in public. The only alternative is to cloister themselves away from the public, but necessarily this is a two-edged sword. On many occasions, stars speak out on political or social issues and they receive attention precisely because of the celebrity status. Reporters can rightly ask "why should they get to choose when they are public figures and when they should be left alone."

Disclosure of Private Facts

This legal action is used to remedy situations when revelation of private facts have caused great embarrassment to individuals. Often the revelation of those facts cannot qualify in a libel suit when the publisher can use truth as a defense against a libel suit, thus the injured party sues under this tort. Many states require the plaintiff (the person claiming injury) must prove that there was a disclosure of private facts, that the facts are not really newsworthy, and the manner in which the facts were released would be *found to be objectionable to a reasonable person*. Sometimes cases

arise when a person's past activities are made public. For example, when the fact that a female student, who was the class president at a community college, had gone through a sex change operation appeared in the *Oakland Tribune*, the plaintiff sued for disclosure of private facts. While the newspaper ultimately won the suit, the disclosure raised ethical question about its newsworthiness. Often, it is difficult to assess whether a story is truly newsworthy. California courts have used a "social utility" test to ascertain whether the publication rises to a newsworthiness standard and will rule in favor of the plaintiff if the publication fails the test (Bellmas et al., 2016). Sometimes the publication of the name of a rape victim is seen as a disclosure of a private fact, but the Supreme Court has ruled that criminal trials are public events and the victim may not sue in this circumstance. However, publication of names of sex crime victims and juvenile offenders pose other ethical issues.

False Light

This infringement involves placing a person in a false light before the public. It is a recognized issue in many but not all states. Where the tort is recognized, a person may sue when that person is portrayed falsely, in a manner that would be *considered highly offensive to a reasonable person*. Perhaps one of the best-known examples of a false light suit was when a woman's face was shown clearly in a Washington, D.C., television report on the growing concern about the spread of herpes in the U.S. The plaintiff sued claiming that a reasonable person watching the newscast would conclude that she had herpes (*Duncan v. WJLA-TV,* 1984).

Misappropriation

This infringement of privacy protects individuals from the unauthorized commercial exploitation of their names, likenesses, and other similar aspects related to their public face or their public persona. This infringement on privacy is also referred to as an *infringement against one's right of publicity and it extends beyond just a person's likeness*. It may also include the voice or actions that may become associated with that celebrity. As an illustration, anyone can attend a NBA basketball game and a person might be able to get a really good action photo of an NBA star. While that person could post the picture on a Facebook page or have it printed and displayed in the home, that person would not be able to sell the photo for commercial purposes without permission of the star. The basketball star would retain his *right of publicity*, but it should be noted that news media do have the right to publish such a photo as it has a newsworthy quality. While the media does have the right to publish photographs that are newsworthy, the media outlet cannot use that photograph as an implied endorsement. A sports magazine cannot publish a photo of a sports figure and claim that the athlete reads their magazine, without the athlete's permission.

Privacy and the First Amendment

The right to be left alone is weighed against the First Amendment rights of the media. Television networks frequently do docudramas of personalities without obtaining the consent of everyone portrayed in the program. As long as the storyline is based on *reported facts*, the court generally assumes there is a First Amendment right to produce the program. As with most issues involving privacy, this right is not absolute. If a news story or broadcast prevents the personality from making

a profit by exercising the personality's right of publicity, then a suit may be initiated.

Finally, in some situations the right of publicity may become a property right after the personality's death. The court ruled that Elvis Presley's right of publicity was a property right that could be transferred to a business entity that could maintain exclusive rights to use his name after death (Elvis Presley Enter. V. Elvisly Yours, Inc., 936 F.2d. 889 (6th Cir. 1991).

Privacy Defense

There are a number of defense options that can be used to defend against a privacy suit. Briefly, *newsworthiness* is usually considered where the media are defendants in a privacy suit. While the courts tend to provide wide latitude to media companies as long as the coverage is accurate, there is no guarantee that they will be successful in fighting such suits. In 2016, Terry Gene Bollea, known professionally as Hulk Hogan, won a large settlement against Gawker Media after it posted portions of a sex tape of Bollea and the wife of a radio personality (*Bollea v. Gawker Media, LLC,* 913 F.Supp.2d 1325 (2012). Bollea sued in Florida civil court claiming invasion of privacy, infringement of personality rights and intentional infliction of emotional distress. The jury awarded Bollea $115 million, including $60 million for emotional distress. That amount was ultimately reduced to $31 million but forced Gawker Media into Chapter 11 bankruptcy. It is clear that the media may be sued for unscrupulous reporting, and while Gawker did not create the sex tape, it chose to publish it (Madigan and Somaiya, 2016).

Another potential defense against an invasion of privacy suit is whether the event or person was in *plain view*. Generally, media can record events and people in public view or plain sight,

however, use of electronic devices, hidden cameras, and other similar technologies can be problematic. Intrusion is considered an *intentional* physical, electronic, or mechanical invasion of a person's solitude that would be seen as highly offensive to a reasonable person. *Consent* can also be used to prevent an invasion of privacy suit. Did the media have consent to use the information? But as is frequently the case, suits against the media may touch upon several possible facts that can trigger a lawsuit. In 2017, ESPN and reporter Adam Schefter were sued by New York Giants defensive end Jason Pierre-Paul after Schefter tweeted a picture of the athlete's hospital records after a firework injury caused a finger amputation (28 U.S.C. § 1446). Pierre-Paul claimed that the reporter had shown disregard for the private and confidential medical records, a public disclosure of private facts. If the case was carried to a conclusion, the court would have to decide whether the release of the information was sufficiently newsworthy to merit publication. Though settled out of court for an undisclosed among of money, this case illustrates the point that it can be difficult for the media to prove newsworthiness but also difficult to win suits against the media outlets (Payne, 2017).

Not all highly publicized privacy suits are against media outlets. In 2016, a jury awarded Fox Sportscaster Erin Andrews $55 million after she sued both the hotel and Michael David Barrett who secretly taped her in the hotel room (Andrews v. Marriott International, Inc., 2016 IL App (1st) 122731). Barrett, who had served time in prison for taping Andrews on previous occasions, asked to be placed in a room next to Andrews. He then used a hacksaw to alter the peephole of Andrews' hotel room. He subsequently recorded video footage of Andrews naked and posted the material online where it was shared widely. Andrews claimed emotional distress as a result of the incident and the jury agreed with her claim (Victor, 2017).

Government Information: The Evolution of Privacy

With the development of sophisticated computer databases in the mid-1960s, it became possible for government agencies and later private corporations to collect and store large amounts of information about individuals. The Freedom of Information Act (FOIA), enacted by Congress in 1966, provided Americans with access to information held about them by the federal government. Most states have subsequently passed similar FOIA laws. While not strictly privacy laws, they provide individuals with the ability to file a FOIA request about information the government holds. Most frequently, FOIA is used by news media and often this information provides the basis for investigative reporting on government corruption. There are significant limitations as to what can be accessed, for example, information about ongoing criminal investigations is restricted; this marked a step forward in making government transparent to citizens. Since passage of FOIA, Congress has enacted a number of statutory laws geared toward protecting the private information of individuals.

With the passage of the Privacy Act of 1974 (The Privacy Act of 1974, 5 U.S.C. § 552a, pp. 44-56), Congress attempted to regulate the collection, maintenance, usage, and dissemination of information that could enable someone or some entity to identify an individual through data records. Since passage of the Act, federal efforts to protect privacy have focused on specific concerns (Adams et al., 2005). For example, the Health Insurance Portability and Accountability Act (HIPPA), passed in 1996, restricted the release of medical information without a patient's consent. Today, doctors and other medical professionals must get the patient's permission to share

medical records. The 1998 Children's Online Privacy Protection Act (COPPA) limited the ability of corporate and government entities from collecting information about children under age 13, without parental consent.

Keeping financial information private is also one of the major concerns Americans have. Several different pieces of legislation provide consumers with varying degrees of protection related to their financial information. Most notably the Financial Modernization Act of 1999, also known as the Gramm-Leach-Blily Act (15 USC 6801, 1999), removed federal limitations prohibiting mergers of financial institutions such as banks and insurance companies. Advocates for consumer protection expressed concern that newly merged financial institutions would be able to collect, share and disseminate private information among their affiliates and partners. Several states have passed more stringent privacy requirements believing that the 1999 Act did not go far enough to protect consumers (Adams et al., 2005, p. 6).

Both government and employers monitor email. Employees often use company email for non-work related messaging. The courts have ruled that when a computer is provided for the employee, she/he has no expectation of privacy. Critics say that this policy violates the Fourth Amendment safeguards against unreasonable search, but the Supreme Court has ruled the monitoring is allowed. Corporations and the media began to create guidelines about computer privacy and research suggests that there are a number of different outcomes, depending on those guidelines (Dodd and Stacks, 2013; Terilli et al., 2007). Misuse of private data on Facebook in 2018 has led many companies to review their policies. Government has had the ability to read emails of Americans for many years. The Electronic Frontier Foundation has been pushing to amend the Electronic Communication Privacy Act (ECPA) of 1986 (18 U.S.C. § 2510-22) . The Act allows the government to read any emails over 180 days old by providing a simply subpoena

for the information. In recent years, privacy experts have criticized the act, saying that technology had made its safeguards inadequate.

The terrorist act on the World Trade Center and the Pentagon in September 2001 dramatically changed the debate about what information should or should not be kept private. The U.S. was already collecting information on potential threats and a nationwide security program was already in place well before 2001. On that September morning, the CAPPS computer system flagged 10 of the 19 hijackers. Unfortunately, all were allowed the board the aircrafts because their checked baggage showed no detectable explosives. Many experts claim that inadequate surveillance provided opportunities for terrorists to plan and execute the attack. Passed overwhelmingly after the attack was the USA PATRIOT Act (P.L. 107-56, 2001, 18 U.S.C. § 2331).

The bill was very complex and impacted many different federal statutes and regulations regarding the collection of data and surveillance of Americans. Among the changes that occurred were new authorizations that allowed for roving surveillance of individuals instead of the usual wiretap in a specific location, the expanded use of the FISA (Foreign Intelligence Surveillance Act) court to issue search orders, encouraging financial institutions to share information, and allowing the Attorney General to collect DNA samples from prisoners convicted of federal crimes of violence or terrorism. These new surveillance tools were set to expire in 2011, but President Obama signed extensions of key provisions including roving wiretaps, searches of business records and surveillance of “lone wolves” (Doyle, 2011; Mascaro, 2011). One significant concern about the PATRIOT Act was that it allowed collection of large amounts of bulk personal telecommunication information on Americans. Government agencies were allowed to sweep and record most cell telephone conversations of Americans.

In June 2013, Edward Snowdon released thousands of classified NSA documents describing the bulk data collection programs by the NSA. In 2015, the USA Freedom Act renewed many provisions of the PATRIOT Act but imposed new limits on collection of telecommunications metadata on U.S. citizens by American intelligence agencies, including the National Security Agency. The Act also imposed new disclosure requirements related data collected approved by FISA courts including an estimate of the number of people targeted and affected by surveillance. The Act now extends government surveillance operations until the end of 2019 (Liu, 2015; Flegenheimer and Huetteman, 2017).

Interestingly, the Trump Administration has charged the previous Obama Administration with wiretapping and using FISA court gathered intelligence to spy on Trump Tower during the presidential election transition period. Earlier President Obama charged the Russian government with cyber warfare and election tampering. Soon after the election events related to members of the Trump Administration suggested that there were potentially improper meetings between Russian government officials and members of the Trump transition team. As of this writing, several investigations are underway into both of these allegations (Hays, 2016).

The Internet, Social Media and Informational Privacy

From a modern communication perspective, the internet and wireless mobile networks have become the media used by most individuals for daily communication. Cellular telephones interface with the internet through smartphone technology. Applications provide amazing capabilities to meld information and entertainment together. The underlying communications network powers

voice interaction, social media, email, online news, opinion blogs, streaming of entertainment, information programs and more. Because the different communication systems are now integrated, mobile devices such as smartphones and tablets are incredibly powerful, but also subject to widespread invasion by corporate entities, by governments (both U.S. and foreign) and criminal actors. So, features in modern devices that we take for granted provide many opportunities for individuals to sacrifice privacy.

Part of the issue related to electronic communication data security concerns the *Third-Party Doctrine* (Ormerod and Trautman, 2017). Courts have ruled that information given to a third party, such as a bank, does not need to treated as private data. This allows government agencies to obtain personal information—often without a search warrant—and, as noted in our discussion about Financial Modernization Act, banks can share that information with their partners and affiliates. Often this information can be sold to other private corporations who want to offer you special interest rates on credit cards or the best rates on a new car loan. The *Third-Party Doctrine* also applies to Google, Microsoft, and Facebook. Using cookies, small data programs embedded within apps, Google can determine that you are searching for men's shirts and what brand you prefer. It maintains that information in its database and sells it to potential clothing providers. The next time you use that search engine banner ads and recommended links will provide you with information on where to buy that particular clothing line. Will Hayes (2016), CEO of a San Francisco enterprise search company, says that ad networks have the ability to track user's every move across the internet, whether they are logged into one particular site or not. However, cookies have wide possible uses and it is not always clear what the purpose of this data collection is. Most recently, Facebook has been under scrutiny for lack of security in dealing with the research company Cambridge Analytics, a London-based computer firm that worked with the Trump presidential

team, gathering millions of personal information from Facebook users' friends without permission of the company or the individuals (Rosenberg et al., 2016).

Some of the activities common to computer and smartphone usage include tracking websites you visited, videos watched, ads you click on, your location, the kind of device you are using, and the IP address. Corporations, such as Google, Apple, Facebook, and Microsoft, collect data and track usage as well. If you use email then your name, email address, password, phone number, and other personal information can be tied to this data, allowing companies to build a detailed profile of your information usage. The ability to collect, assess and integrate information is becoming increasingly common and most users have waived many of their privacy rights when they accepted the terms to use email, iTunes, Facebook, and other applications (apps) on their mobile device. While the FCC proposed new 'opt-in' privacy requirements in 2016, those requirements were set aside when the newly led Republican FCC and Senate moved to dismantle proposed rules, which would have required telecommunications companies to ask consumers for permission before tracking their browsing histories and collecting sensitive data (Kang, 2017).

In addition to the well-known practices described above, Google and others have been fined for violating basic privacy rights. For example, Google's illegal "wi-spy" program swept information from home server using its Street View cars that drive through local neighborhoods. Information collected included medical histories, sexual preferences and other sensitive personal information. Google was fined when the Federal Communications Commission found the company guilty of deliberately trying to delay investigations into its practices. Other questionable activities included using personal information for targeting ads for subprime mortgages and loan modifications to consumers caught in the financial crisis of 2007, but Google is not the only company that has been found to misusing private information (Newman, 2013). In 2012, Facebook

was found to be doing market research on its users without telling them (Hill, 2014). Facebook manipulated *News Feeds* by removing either positive or negative posts of more than 680,000 users to test how these changes affected the users' mood. Although criticized for this activity the manipulation of user accounts for study purposes is allowed under Facebook's data use policy.

Apple tangled with the federal government in 2016 when it refused to disable encryption safeguards built into an iPhone after the tragic terrorist attack in San Bernardino, California. Law enforcement officials who supported the government's request thought that Apple's refusal to cooperate provided a significant court test to examine the issues balancing national security and individual privacy. While a federal court upheld the FBI's request, Apple refused to comply warning of the "chilling" breach of privacy posed by the government's demand. Many privacy experts expressed concern that by giving decryption capability to the FBI it would create an opportunity for government intrusion into Apple devices (Lichtblau and Benner, 2016; Vindu and Perlroth, 2016). Ultimately the FBI used hackers to break into the terrorist's phone, ending the standoff.

Throughout the presidential campaign in 2016, embarrassing emails from the Democratic National Committee and its leaders were leaked to numerous news operations. At the end of 2016, the Obama Administration stated that the leaks resulted from cyber-attacks by the Russian Government attempting to discredit the campaign of Hillary Clinton. In addition to these seemingly politically motivated attacks, the Identity Theft Resource Center estimated that U.S. companies and various government agencies suffered more than 1000 data breaches in 2016 (www.idtheftcenter.org). The intrusions exposed a wide range of personal information including social security numbers, bank user account info, log-in names, and passwords. These attacks, known as "phishing" were substantially higher in 2016, despite more aggressive cyber-security.

Criminals can use stolen information to file false tax returns, order credit cards, and steal money from bank accounts among other things. In December 2016, Yahoo informed users that more than 1 billion accounts had been hacked starting back in 2013 (Vindu and Perlroth, 2016). A widely publicized cyber-attack at SONY Pictures in 2014, allegedly done by hackers with ties to North Korea, stole and disseminated sensitive personal and corporate information about SONY. Security experts believe the attack was in retaliation of SONY releasing an unflattering comedy that ridiculed North Korea leader Kim Jung-un. These numerous cyber-attacks leave sensitive information exposed to unwanted use by hackers and drive the cost of services up as companies spend billions of dollars to protect their computer systems. Recently a report by Pentagon's Defense Science Board task force for security (Task Force on Cyber Deterrence, 2017) expressed concern about the safety of national infrastructure systems like power grids, nuclear facilities, and water systems. The report points to Russia and China having a significant ability to threaten critical U.S. infrastructure as well as interfering with potential U.S. military responses to such attacks.

The Continuing Evolution of Privacy in a Digital Era

The desire to retain privacy and protection of one's personal space has existed from the earliest times. People desire to have some control over their personal information and who knows what about them, but technology has eroded some of the controls individuals traditionally have had. The debate about whether privacy rights were included under the protections of the Bill of Rights began when the development of printing and photographic technology enabling widespread dissemination by the media.

U.S. law makes a distinction between rights afforded under the constitution, rights and the freedom to make one's own decisions without undue interference, and statutory protections and limitations, which include legislated attempts to provide some framework for informational privacy within society. While constitutional rights are seen as absolute, legislative attempts to regulate informational privacy are *ad hoc* and subject to change with evolution of technology, governmental and corporate needs, and social desires. As a result, as the situations surrounding the collection of information changes, so too do normative attempts to develop policies for privacy rights.

Recent development of new devices and our growing technical capabilities to monitor behavior could threaten traditional safeguards to individual privacy. The evolution of mobile communication devices from laptops to smartphones and tables has transformed the ways information could be made available and used by individuals. While we tend to think of technology as operating on the device or individual level, the opposite is actually true. Information technology is comprised of a complex set of interactive systems.

Technology's forward movement is creating new devices such as drones, wearable sensors, and RFID tagging that will continue to impact daily lives as well as our understanding of what constitutes informational privacy. Large scale use of surveillance networks, facial recognition, and cellphone GPS capability allows for individual tracking while the growth of online retail develops a database of our purchasing behaviors. This information is accumulated and integrated with email, address, financial, and other personal information that can provide a fairly detailed analysis of the individual. One can see that private physical space is becoming less of an issue as social media encourages sharing information about one's daily routine. Experts disagree about the relative positive or negative aspects of data collection possible with the new information technology.

Connectivity increases everyone's access to information and this can have a leveling effect among different social and demographic groups, but at the same time corporate and government entities could use this information for discriminatory purposes.

The growth of social media outlets like Facebook, Instagram, Linkedin, and Twitter expand both personal and commercial opportunities for communication. Studies indicate that teens are more likely to share information about them, but often regulate who has access to that information. At the same time there is a growing concern among users that their personal information is less secure today than it was 5 years ago. This was particularly high among Americans age 50 and older. A Pew Research Center study (Olmstead and Smith, 2017) found that a majority of Americans have experiences some form of data breach and many feel the federal government and social media sites are not doing enough to protect their personal information.

The lines between public and private domains of information are blurred and continue to evolve. Privacy laws are designed to protect the private space surrounding the person while information laws often provide opportunities for commercial enterprises to use information. Social movements can use the new technologies to hold rallies, raise money and practice rights granted under the First Amendment, irrespective of time or place. But, significantly, terrorists and criminals can use the same technology to plan and execute destructive attacks on society.

The late Anne Wells Banscomb (1994), noted communication and computer legal scholar said, "(W)e are in the process of designing a new paradigm for our information society, one that offers room for great economic, intellectual, social and political growth." But she warns, "(W)e must recognize legitimate rights to withhold personal information and prevent intrusions upon private information environments…We must clarify the responsibilities of the public custodians and redefine the circumstances under which third parties are to be permitted access" (p. 185).

Clearly the debate about what constitutes privacy and who should have access to personal information will continue to evolve as the level of informational connectivity increases.

Notes

[1] A tort is an act deemed wrongful or an infringement of a right that results in injury to another person, property, or reputation (Wikipedia, n.d.). Accessed March 21, 2018.

[2] See also: *Pavesich v. New England Life Insurance Co.* (1905). 50 S.E. 68; *Sidis v. F-R Publishing Co.*(1940). 113 F.2nd 8060); and *Boyd v. U.S.* (1986). 116 U.S. 616.

[3] See: *Bowers v. Hardwick* (1986). 478 U.S. 186; *Lawrence v. Texas* (2003). 539 U.S. 558; *Obergefell v. Hodges* (2015) 576 U.S.

[4] For a complete discussion of the Electronic Communications Privacy Act see: Electronic Privacy Information Center, epic.org. Accessed March 10, 2017. https://epic.org/privacy/ecpa/

[5] The USA PATRIOT Act passed in 2001 stands for "Uniting and Strengthening America by Providing Appropriate Tools.

References

Adams, H.,. Bocher, R., Gordon, C., and Barry-Kessler, E. (2005). *Privacy in the 21st Century: Issues for Public, School and Academic Libraries.* Westport, Conn: Libraries Unlimited.

Arendt, H. (1958). *Human Condition*. Chicago: University of Chicago Press.

Barrington, M. (1984). *Privacy: Studies in Social and Cultural History.* Armonk, NY: M.E. Sharpe).

Belmas, G., Shephard, J., Overbeck, W. (2016). *Major Principles of Media Law,* 2016 Ed. Boston: Cengage Learning.

BeVier, L. (1995). Information about Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection, *Wm. & Mary Bill Rights Journal*. pp. 455, 458.

Bowers v. Hardwick (1986). 478 U.S. 186.

Boyd v. U.S. (1986). 116 U.S. 616.

Branscomb, A. (1994). *Who Owns Information: From Privacy to Public Access*. Harper Collins: New York.

Dodd, M., and Stacks, D. (2013). Organizational Social Media Policies and Best Practice Recommendations. In H.S. Noor-Aldeen and J.A. Hendricks, Eds. *Social Media and Strategic Communications*. London, Palgrave McMillan. pp. 159-179.

Donald A. Dripps. (2013). "Dearest Property:" Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure, *Journal of Criminal Law & Criminology* 49, p. 103. http://scholarlycommons.law.northwestern.edu/jclc/vol103/iss1/2

Doyle, C. Terrorism: Section by Section Analysis of the USA PATRIOT Act. *CRS Report for Congress*, Updated December 10, 2001. https://epic.org/privacy/terrorism/usapatriot/RL31200.pdf

Duncan v. WJLA-TV, (1984). 106 F.R.D. 4..

Electronic Privacy Information Center. (n.d.) epic.org. Accessed March 10, 2017. https://epic.org/privacy/ecpa/

Farrell, T. (1989). Privacy and the Boundaries of Fabliau in The Miller's Tale. *ELH, 56*(4), 773-795. doi:10.2307/2873159

Ferenstein, G. (2015). The Birth and Death of Privacy: 3000 Years of History Told Through 46 Images. Accessed March 2017. https://medium.com/the-ferenstein-wire/the-birth-and-death-of-privacy-3-000-years-of-history-in-50-images-614c26059e

Flegenheimer, M., and Huetteman, E, (2017). Senate Intelligence Committee Leaders Vow Thorough Russian Investigation. *New York Times*. Accessed April 1, 2017. https://www.nytimes.com/2017/03/29/us/politics/senate-intelligence-committee-burr-warner-russia-investigation.html?_r=0

Foot, Mi., and *Kramnick, I.* Eds. (1987), *The Thomas Paine Reader*. New York: Penguin Classics. *ISBN 0-14-044496-3.*

Goel, V., and Perlroth, N. (2016). Yahoo Says 1 Billion User Accounts Were Hacked. *The New York Times*. Accessed April 1, 2017. https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html

Griswold v. Connecticut (1965). 381 U.S. 479

Hayes, W. (2016). 5 (Not So Obvious) Ways to Protect Your Privacy Online. *Forbes*. Accessed March 27, 2017. https://www.forbes.com/sites/willhayes/2016/01/28/five-ways-to-

protect-your-privacy-online/2/#342b5e7540f0

Hill, K. (2014). Facebook Manipulated 689,003 Users' Emotions for Science. *Forbes*. Accessed March 15, 2017. https://www.forbes.com/sites/kashmirhill/2014/06/28/facebook-manipulated-689003-users-emotions-for-science/#7c32d4f4197c

Kang, C. (2017). Congress Moves to Strike Internet Privacy Rules from Obama Era. *The New York Times.* Accessed March 23, 2017. https://www.nytimes.com/2017/03/23/technology/congress-moves-to-strike-internet-privacy-rules-from-obama-era.html

Kennerly, M. (2016) *Hulk Hogan v. Gawker* Legal FAQ – In Their Lawyer's Words. http://www.litigationandtrial.com/2016/05/articles/attorney/hogan-v-gawker-legal-faq/.

Kreider, P. (1934). The Mechanics of Disguise in Shakespeare's Plays. *The Shakespeare Association Bulletin, 9*(4), pp. 167-180. Retrieved from http://www.jstor.org.ezproxy.oswego.edu:2048/stable/23675558

Lawrence v. Texas (2003) 539 U.S. 558.

Lichtblau, E., and Benner, K. (2016). Apple Fights Order to Unlock San Bernardino Gunman's iPhone. *The New York Times*. Accessed March 15, 2017. https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html?_r=0

Liu, J. (2015). So What Does the USA Freedom Act Do Anyway. LAWFAREAccessed March 28, 2017. https://www.lawfareblog.com/so-what-does-usa-freedom-act-do-anyway

Madigan, N., and Somaiya S. (2106). Hulk Hogan Awarded $115 million in Privacy Suit Against Gawker. *The New York Times*. Accessed April1, 2017. https://www.nytimes.com/2016/03/19/business/media/gawker-hulk-hogan-

verdict.html?_r=0.

Mascaro, L. (2011). Patriot Act provisions extended just in time. *The Los Angeles Times.* Accessed March 28, 2017. http://articles.latimes.com/2011/may/27/nation/la-na-patriot-act-20110527.

National Commission on Terrorist Attacks Upon the United States: The 9/11 Commission Report, Executive Summary. http://govinfo.library.unt.edu/911/report/911Report_Exec.htm.

Newman, N. (2013). Why Google's Spying on User Data Is Worse than the NSA's. *The Blog, Huffington Post*. Accessed March 16, 2017. http://www.huffingtonpost.com/nathan-newman/why-googles-spying-on-use_b_3530296.html

Obergefell v. Hodges (2015) 576 U.S.).

Olmstead, K., and Smith, A. 2017). Americans and Cybersecurity. *Pew Research Center Report*. Accessed March 28, 2017. http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

Pavesich v. New England Life Insurance Co. (1905). 50 S.E. 68.

Payne, M. (2017). Jason Pierre-Paul and ESPN reach settlement in invasion-of-privacy lawsuit. *The Washington Post.* Accessed on April 1,2017. https://www.washingtonpost.com/news/early-lead/wp/2017/02/03/jason-pierre-paul-and-espn-reach-settlement-in-invasion-of-privacy-lawsuit/?utm_term=.d35caef36905.

Pearson, M. (2016). LGBT rights: the national battle of the bathroom. Accessed March 31, 2017. http://www.cnn.com/2016/08/23/us/transgender-bathroom-policies/

Peterman, L. (1993). Privacy's Background. *The Review of Politics*, Vol. 55, No. 2, 217-246.

Roberson v. *Rochester Folding Box Co.* (1902). 64 N.E. 442.

Roe v. Wade (1973) 410 U.S. 113.

Rosenberg, M., Confessore, N., and Cadwalladr, C. (2016). How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times*. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. Accessed March 21, 2018.

Sidis v. F-R Publishing Co. (1940). 113 F.2nd 806.

Steinberg v. Carhart (2000). 530 U.S. 914

Task Force on Cyber Deterrence. (2017). Homeland Security Digital Library. Center for Homeland Defense and Security, Naval Postgraduate School. Released February 2017. Accessed April 6, 2017. https://www.hsdl.org/?abstract&did=799190

Terilli, S.A., Driscoll, P.A., and Stacks, D.W. (2007). *Corporate Bloggers and the Commercial Speech Legal Blog*.

Cooley, T. (1879). *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract*. Chicago: Callaghan.

Victor, D. (2016). Erin Andrews Awarded $55 Million in Lawsuit Over Nude Video at Hotel. *The New York Times.* Accessed on March 28, 2017. https://www.nytimes.com/2016/03/08/business/media/erin-andrews-awarded-55-million-in-lawsuit-over-nude-video-at-hotel.html.

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), pp. 193-220. doi:10.2307/1321160

Suggested Readings