Privacy and Technology: A 125-Year Review

Lori B. Andrews
Chicago-Kent College of Law, landrews@kentlaw.iit.edu

Follow this and additional works at: http://scholarship.kentlaw.iit.edu/docs_125

Part of the Legal Commons, Legal Education Commons, and the Legal History Commons

Recommended Citation
http://scholarship.kentlaw.iit.edu/docs_125/9

This Article is brought to you for free and open access by the 125th Anniversary at Scholarly Commons @ IIT Chicago-Kent College of Law. It has been accepted for inclusion in 125th Anniversary Materials by an authorized administrator of Scholarly Commons @ IIT Chicago-Kent College of Law. For more information, please contact dginsberg@kentlaw.iit.edu.
The year the Chicago-Kent College of Law was founded, a new consumer product arrived on the scene: the portable camera. Before then, taking someone's photo was a big deal. A person would get dressed up and go to a studio. Photos were not taken without a person's permission. But the portable camera changed all that—and in the process led to the development of legal rights of privacy that endure today.

An 1890 newspaper article warned:

Have you seen the Kodak fiend?
Well, he has seen you. He caught your expression yesterday while you were innocently talking at the Post Office. He has taken you at a disadvantage and transfixed your uncouth position and passed it on to be laughed at by friend and foe alike. His click is heard on every hand. He is merciless and omnipresent and has as little conscience and respect for proprieties as the verist hoodlum. What with Kodak fiends and phonographs and electric search lights, modern inventive genius is certainly doing its level best to lay us all out bare to the gaze of our fellow-men.

Like Facebook, Twitter, Instagram,
Snapchat and YouTube today, the portable camera fundamentally changed the way other people and institutions could peer into people’s lives. But the issues raised by today’s cutting-edge technologies are similar to those raised by the Kodak fiend.

In the late 1800s a lawyer, Samuel Warren, married the daughter of a Senator. He was unprepared for the incessant media attention to their union, fueled by the newly-developed portable camera. After his children were born, paparazzi would snap photos of the babies when the family took walks down the street. Annoyed, he thought about what legal recourse he might have. Were there any legal precedents for a “right to be let alone”? He pondered the issue with a friend from law school, Louis Brandeis. They could have suggested that people no longer had a right to be left alone because technologies could now track and record what they did. Instead they noted that the intrusiveness of technologies like the portable camera made it even more important for people to have control over information about themselves. “The intensity and complexity of life attendant upon advancing civilization has rendered necessary some retreat from the world,” they wrote, “so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasion upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.”

Their article, “The Right to Privacy,” was published in 1890 in the Harvard Law Review. They demonstrated that a privacy right had a basis in fundamental Constitutional values, such as the right to refuse to testify against oneself, and common law principles, such as the “right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others.”

“The protection afforded to thoughts, sentiments, and emotions . . . is merely an instance of the enforcement of the most general right of the individual to be let alone,” they said. “It is like the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed.”

Their ideas were incorporated into law through the creation of four distinct legal actions for invasion of privacy: for intruding on someone’s seclusion, for publicly disclosing private information, for putting a person in a “false light” in the public eye, and for appropriating someone’s name or likeness for commercial use. They advocated that information about and photos of people could be disseminated if they had consented or if the matter was of legitimate public interest. Since then, the fundamental Constitutional right to privacy has additionally been in-
interpreted to include a right to make important personal decisions, such as whether to use contraception or whether to homeschool your child.

The mode of analysis of the two Boston lawyers from a century ago has been used to analyze each new technology that has reached the courts. How does it affect the individual and society? How do fundamental legal values help to protect the individual when the technology is used? As each new technology has been adopted—including forensic technologies, medical technologies, and computer technologies—the application of fundamental values has been used to protect, and often expand, people’s privacy rights. Sometimes courts, lacking the comprehensive analysis of technology like the one undertaken by Warren and Brandeis, took missteps when they first encountered a technology. But ultimately, privacy prevailed.

When Charles Katz entered a public phone booth in 1965, he never imagined that cops would tap the phone line. The cops charged him with placing illegal bets—and he protested that they had infringed the Fourth Amendment limits on governmental intrusion into a person’s private life. The trial judge said that wiretapping didn’t violate the Fourth Amendment because the Founding Fathers drafted the Constitutional provision to honor people’s privacy in their homes. In this case, the police hadn’t trespassed into his home. In fact, there had even been a Supreme Court decision on the matter, back in 1928, when cops had used earlier wiretap technology to learn that someone was violating Prohibition.

In that earlier case, Olmstead v. United States, 277 U.S. 438 (1928), the five-justice majority of the U.S. Supreme Court had held that a

(The Kodak Fiend) Hawaiian Gazette, December 9, 1890, Chronicling America Collection, Library of Congress.
Forty years after the *Olmstead* decision, when Charles Katz’s case was appealed to the U.S. Supreme Court, the majority of the justices applied Brandeis’s logic. Even though Charles Katz was using a public phone booth, the Court said that the Constitutional right of privacy “protects people, not places.” What a person seeks to preserve as private, even in a public place, may be Constitutionally protected.

The Supreme Court protected Katz’s privacy by enunciating a legal test that is still used today: Did the person have an “expectation of privacy” and was that an expectation that society was willing to protect? As a result, police need to get a warrant, based on probable cause, before they tap someone’s phone.

The march of law enforcement technology continued, and in 2001, a new forensic technology reached the court. A federal agent suspected Danny Kyllo of growing marijuana. Since growing pot indoors requires high-intensity lamps, the agent sat in a car across from the home and used an Agema Thermovision 210 thermal imager to scan Kyllo’s home. The scan showed that the roof over the garage and a side wall of the home were relatively hot compared to the rest of the home and substantially warmer than neighboring homes in the triplex. The agent concluded that Kyllo was growing pot and convinced a judge to allow him to search Kyllo’s home. The agent found pot,
and Kyllo was convicted on a drug charge. Because the thermal scanner did not physically intrude on the house and did not show any private human activities, the trial court said that it hadn’t infringed Kyllo’s Constitutional rights.

The appellate court, too, held that Kyllo had shown no subjective expectation of privacy because he had made no attempt to conceal the heat escaping from his home, and “even if he had, there was no objectively reasonable expectation of privacy because the imager ‘did not expose any intimate details of Kyllo’s life,’ only ‘amorphous “hot spots” on the roof and exterior wall.’”

When the U.S. Supreme Court took the case, it reversed Kyllo’s conviction. “It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology,” wrote Justice Antonin Scalia. “Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a ‘search’ and is presumptively unreasonable without a warrant.”

In 2012, the U.S. Supreme Court in United States v. Jones, 132 S. Ct. 945 (2012), assessed the use of a GPS tracking device installed on a car driven by Antoine Jones, a D.C. nightclub owner. Jones was the target of a narcotics investigation by police and the FBI. The Court held 9 to 0 that the twenty-eight-day warrantless use of the GPS violated the Fourth Amendment. In her concurrence, Justice Sotomayor pointed out how the fundamental right to privacy was salient even in today’s world. “GPS monitoring generates a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations,” wrote Sotomayor, adding, “People disclose the phone numbers they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries and medication they purchase to online retailers. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year.” Justice Sotomayor also was concerned that “[a]wareness that the government may be watching chills associational and expressive freedoms.”

Contemporary medical technologies, such as genetic testing, have also raised disputes about the reach of privacy principles. When genetic testing became possible, people were tested without their knowledge or consent. Doctors and researchers would use blood that people had
given to labs for routine cholesterol or pregnancy tests and perform additional testing, without the person's consent, for everything from breast cancer to Alzheimer's disease. The argument was, what's the harm? The person had already been pricked; the additional tests involved no additional intervention. And even if the blood was collected anew—as in a forensic DNA test—blood tests were safe and noninvasive.

But then employers and insurers started discriminating against healthy people based on their genetic predisposition to future disease. With certain genetic mutations, for example, some women had a higher risk of developing breast cancer than other women. Even with those mutations, half the women would not develop breast cancer. Some women didn't want to know whether they had the mutations or not. They said they would feel like they had a time bomb ticking away inside them. But employers and insurers wanted that information to make their decisions. There were no legal limits on what could be done with that information.

During routine physicals, an employer in California asked the company doctor to surreptitiously test the female employees to see if they were pregnant and the African-American employees to see if they carried the sickle cell anemia gene mutation. The results were not disclosed to the employees, but they were put in to their personnel files.

When the existence of the files leaked, the employees sued. The trial court dismissed the case, saying that the test was a modest intrusion, no more than what people usually undergo in a physical. But the appellate court held that genes contain personal information that is protected by the fundamental right to privacy. “One can think of few subject areas more personal and more likely to implicate privacy interests than that of one's . . . genetic make-up,” wrote the Court of Appeals for the Ninth Circuit in Norman-Bloodsaw v. Lawrence Berkeley Laboratory, 135 F.3d 1260, 1269 (9th Cir. 1998). Since then, Congress has passed a law, the Genetic Information Nondiscrimination Act, specifically prohibiting employers and insurers from discriminating against people based on the results of genetic tests. People's privacy rights include the right not to have genetic information generated about them or used against them.

Even computer technologies that collect data about people have been subject to a fundamental rights analysis. When Judge Robert Bork was nominated for the U.S. Supreme Court in 1987, Michael Dolan, a Washington, D.C. newspaper reporter, attempted to discredit him by publishing his video store rental records. In today's world, Judge Bork's choices seem tame: British movies, Bond movies, costume dramas. The reporter was disappointed not to see legal movies such as 12 Angry Men
or *To Kill a Mockingbird*. Instead, Judge Bork had rented “only one truly court-related tape”: *The Star Chamber*.

Bork did not get the Supreme Court nomination. But the publication of his video rentals did get the attention of Congress. “It is nobody’s business what Oliver North or Robert Bork or Griffin Bell or Pat Leahy watch on television or read or think about when they get home,” said Senator Pat Leahy. “In an era of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones, all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch, who are some of the people they telephone. . . . I think that is wrong. I think that really is Big Brother, and I think it is something that we have to guard against.”

Senator Paul Simon agreed. “There is no denying that the computer age has revolutionized our world. Over the past twenty years we have seen remarkable changes in the way each one of us goes about our lives. Our children learn through computers. We bank by machine. We watch movies in our living rooms. These technological innovations are exciting and as a nation we should be proud of the accomplishments we have made. Yet, as we continue to move ahead, we must protect time honored values that are so central to this society, particularly our right to privacy. The advent of the computer means not only that we can be more efficient than ever before, but that we have the ability to be more intrusive than ever before. Every day Americans are forced to provide businesses and others personal information without having any control over where that information goes. . . . These records are a window into our loves, likes, and dislikes.”

The legislators applied the fundamental Constitutional right to privacy and passed a law in 1988 forbidding disclosure of people’s video rental records (or, in this day and age, what they watch on Netflix). The bill prohibits video stores from disclosing “personally identifiable information”—information that links the customer or patron to particular materials or services. In the event of an unauthorized disclosure, an individual may bring a civil action for damages.

The concerns raised by the disclosure of Bork’s video records are mild when compared to today’s digital invasion of privacy. A billion people have joined Facebook, a population only slightly smaller than either of the two largest countries, India and China. Marketing companies, political candidates, law enforcement agencies, employers, and other social institutions peer through
the keyholes of people’s lives by assessing the information and photos that individuals post and that third parties post about them. Even more troubling, data aggregators use surreptitious tracking mechanisms to follow people across the web and use that information to make judgments about them. If a woman does a Google search for old guitars and then seeks a credit card, she will be offered a credit card with less advantageous terms—not because her credit is bad, but because garage rock bands in general are less likely to pay off their credit cards. If she has a photo of herself with a wineglass in her hand, she may be denied a job. Seventy-five percent of employers look at people’s social network presence; one-third reject people who have alcohol in a Facebook photo. And, as with past technologies, courts and legislatures have been slow to protect privacy, initially holding that privacy rights are lost “on affirmative keystroke.”

In just the past two years, however, courts and lawmakers have begun to protect freedom of expression and privacy on social networks. In *Layshock v. Hermitage School District*, 650 F.3d 205 (3d. Cir. 2011), and *J.S. v. Blue Mountain School District*, 650 F.3d 915 (3d. Cir. 2011), the Third Circuit Court of Appeals held that public high school students had a First Amendment right that covered their posts on social networks even if those posts were critical of school administrators. And a few state legislatures—including that of Illinois—passed laws prohibiting employers from asking for the social network passwords of an employee or a job applicant. That Illinois law went into effect 125 years after Chicago-Kent College of Law opened its doors. The Illinois governor came to the campus to sign the bill into law.
and was introduced by a Chicago-Kent student who was working on internet privacy issues.

The Warren and Brandeis article not only created a legal framework that still applies today to safeguard people’s privacy, it also established a method for judging new technologies. The authors analyzed how fundamental values inherent in the U.S. Constitution and common law provide a basis to make judgments about new technologies. They also assessed how new technologies affected individuals, institutions, and the larger society. Warren and Brandeis did not suggest that individuals adapt to each new technology, but instead advocated that society assure that each technology was employed in a way that was consistent with fundamental societal values.

When Brandeis was appointed to the U.S. Supreme Court 26 years after his privacy article appeared, he continued to champion the application of Constitutional values to modern technologies. He also wrote about the nature of a Constitution. “Time works changes, brings into existence new conditions and purposes. Therefore a principle, to be vital, must be capable of wider application than the mischief which gave it birth. This is peculiarly true of Constitutions. They are not ephemeral enactments, designed to meet passing occasions. They are, to use the words of Chief Justice Marshall, ‘designed to approach immortality as nearly as human institutions can approach it.’ The future is their care, and provision for events of good and bad tendencies of which no prophecy can be made. In the application of a Constitution, therefore, our contemplation cannot be only of what has been but of what may be.”

When the law school opened its doors 125 years ago, it would have been difficult to imagine the high-tech world of today. But by learning about cutting edge technologies as well as fundamental legal principles, the students at IIT Chicago-Kent College of Law have been well educated, in every era, to face their generation’s legal challenges.

Sources and Further Reading
- Jeffrey Rosen and Benjamin Wittes, eds., Constitution 3.0: Freedom and Technological Change (2011).

Lori Andrews is a graduate of Yale College, summa cum laude, and Yale Law School. She directs the Institute for Science, Law and Technology at IIT Chicago-Kent College of Law and teaches courses about the law’s response to new technologies. She’s written 14 books, including three mysteries. The American Bar Association Journal calls her “a lawyer with a literary bent and the scientific chops to rival any CSI investigator.”