Grasping the Intangible: Privacy and the Law

December 20

2009
Grasping the Intangible: Privacy and the Law

In this information age, our personal data and records are not more than a keystroke away. While some may find this convenient, the truth is, our government and various companies have found ways of gathering that valuable information without our knowledge, and this fact should make us all feel extremely uncomfortable. We are Americans, not subjects of a king, and the right to keep our personal life under lock and key is backed up by our history, protected by our laws, and should be respected as our right by all who deal with us.

Writing in *Social Theory and Practice*, Alfino and Mayes define privacy as “the right to restrict access to the person (whether it is him or herself)” and “the right to control what happens to personal information” (Alfino and Mayes 3). However, government officials did not always respect that right. In an article called “Privacy in Peril,” freelance writer Marcia Clemitt reports that in the fifteenth century, “the British government began challenging citizens’ views that their homes were effectively their castles - where privacy was sacrosanct - by authorizing government agents to search homes and businesses if they suspected the owners of criminal activity, heresy or political dissent” (Kurland and Lerner 970). Clemmitt describes how the government in England did not exhibit enough scrutiny in releasing search warrants. In fact, warrants were given out so frequently and indiscriminately, they became little more than tickets to a live showing of anyone’s home.
The home at this point in British history was not a sanctuary for families, but rather, a cardboard box easily moved and trampled on by the government. In their five-volume work, *The Founders’ Constitution*, Philip Kurland and Ralph Lerner observe that “by the mid-18th century, however, English citizens fed up with general warrants successfully sued government agents for trespassing… England’s Court of Common Pleas found that the defendants had no right to use the warrants asserting ‘there is no law in this country to justify the defendants in what they have done. If there was, it would destroy all the comforts of society’” (Kurland and Lerner. cited in n. pag.). It would seem that even then, privacy and the sanctity of the home were important to society. As this was happening, American colonists expressed their own grievances over “writs of assistance” (Clemmitt 970). These “writs of assistance” (general warrants) did not have expiration dates, and allowed anyone pegged as an English officer to “search anyplace they wanted without responsibility for damages and could be transferred from officer to officer” (Clemmittt 970). Eventually, these search warrants became part of the impetus for the Colonies’ Declaration of Independence. Writes Thomas Jefferson: “[King George of England] has erected a multitude of new offices, and sent hither swarms of officers to harass our people and eat out their substance.” Thus we see that the common citizen’s right to privacy was one of the foundational thoughts that led to the establishment of the United States.

However, this was not the only time in American history that the issue of privacy had to be confronted. In his thought-provoking essay “Privacy Under Attack,” writer Patrick Marshall reports that in post-Revolutionary War times, “it was not uncommon for the person delivering a letter to read it and even, on occasion, add to it.” He notes that “as literacy expanded … more Americans came to rely upon the mail system” and retaining that reliability became increasingly important. The necessity to be certain of who was the author of one’s mail eventually forced
Congress to make it illegal for anyone to tamper with U.S. mail, writes Marshall. He adds that it was not “until 1877 [that the Supreme Court ruled] that mail was protected by the Fourth amendment” (Marshall 517-518). However, the process by which the Supreme Court protected other forms of communication took a long time.

The prevalent use of the telegraph in the nineteenth century generated new problems, since information could travel faster than before. Although Western Union “had the practice of not disclosing the contents of telegrams to anyone but the recipient,” that form of communication was not protected by the laws that were protecting the U.S. mail (Marshall 518). In his book “Ben Franklin’s Web Site: Privacy and Curiosity from Plymouth Rock to the Internet” author Robert Smith points out that citizens could be victimized by the power of Congress to subpoena the contents of telegrams, as happened in January of 1877. Western Union President, William Orton, “resisted [the] congressional subpoena,” claiming his company was asked by Congress “to become spies and… informers against the customers who have reposed in [Western Union] the gravest confidence concerning bother their official and their private affairs” (Smith 69). Orton eventually gave in after facing arrest. Some 30,000 telegrams were delivered to Congress (Marshall 518). From that point on, Western Union kept its records of telegrams for shorter amounts of time (Clemmitt 973).

In that same year (1877), a new form of communication was developed that changed the landscape of America and brought the issue of privacy straight to the fore: the telephone. It is important to note that when the telephone was first developed, it was considered a party line. Multiple neighbors would share one line, and the operators that were connecting neighbor to neighbor had the power to listen in to their calls (Clemmitt 973). But eventually, “in the 1890’s [when call routing came into use] Americans began to expect privacy during telephone calls”
Little did citizens know, “police agencies were quick to see the telephone’s potential… [and] figured out how to ‘tap’ phones,” and this practice continued until 1916, when the act of tapping was defined as criminal (Clemmitt 973). Former National Director of Electronic Countermeasures Kevin Murray informs us that the American public became outraged when it was discovered that “the government had set up ‘a complete central-office switchboard… in the New York Customs House, with taps running into it from all parts of the city. Every time a suspected alien lifted his receiver a light showed… and a stenographer… took a record of the conversation’” (“Tapping the Wires”). Although public outrage was great, the police continued to practice wiretapping until it was declared to be restricted by the Fourth Amendment, which prohibits unreasonable searches and seizures (Clemmitt 973). A revealing case occurred during Prohibition, when “Seattle police officer Roy Omnstead was arrested for bootlegging” after Omnstead’s phone was tapped (Clemmitt 973). The officer’s argument was that his constitutional rights were compromised and that his protection from warrantless searches was violated (United States v. Olmstead). In a 5-4 decision, the Court ruled the practice that condemned Omnstead perfectly legal. Speaking for the majority, Justice Howard Taft wrote that “The evidence was secured by the use of the sense of hearing and that only” (United States v. Olmstead). In a dissenting opinion, Justice Louis D. Brandeis protested that “subtler and more far-reaching means of invading privacy have become available to the government… the progress of science… is not likely to stop with wiretapping. Can it be that the constitution affords no protection against such invasions of individual security? [Surely, the Constitution protects against] ‘every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed’” (Clemmitt 973). This judgment was not reversed until 1967, when the courts began to contour their interpretations of the law around the existence
of new technology. In *Katz v. United States*, the Court deemed that wiretapping was unconstitutional, and a violation of the Fourth Amendment. Finally, the interpretation of law caught up with the technological advances of the electronic age, recognizing that unreasonable searches and seizures were not limited to physical structures. “Once it is recognized that the Fourth Amendment protects people – and not simply ‘areas’ – against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure” (*Katz v. United States*).

Privacy has evolved over the years, but, as seen with history, has always been a hot issue for any society. Today, with the growing significance of computational data keeping, it is under vigorous attack. Granted, there are a few protections in place. In 1996, Congress passed the Health Insurance Portability and Accountability Act. This ensured that patients had access to their medical records and that they had the right to decide who would have access to those records. If any health care provider, insurance company, or pharmacy would want to release information about a particular patient, they would have to consult and get the approval of that very patient before revealing those records (Marshall 511). The catch is that companies have found ways to release that information anyway. Today it is possible for health-care providers to share medical information with marketers, such as pharmaceutical companies. This practice has led to an annoying deluge of direct mail from companies who are not necessarily involved with, or interested in, a patient’s health. Ronald Weich, a consultant for the American Civil Liberties Union (ACLU), maintains that “Patients should not be receiving mailings unless they specifically ask for them” (Marshall 514). The catch is that if the patient does not opt out of the mailings the first time he receives it, the mailings will continue to be sent until they do. Weich claims, “There shouldn’t be a first time.”
When it comes to private companies, there is a severe lack of regulation on what happens to the information. In his enlightening book, *The End of Privacy*, Charles Sykes’ claims, “Your salary and consumer credit report can be obtained from and information broker for $75; your stock, bond, and mutual-fund records for $200. For $450 brokers can obtain your credit- card number… Not all of this information can be obtained ethically or legally. But it can be obtained.” It is as if the companies are playing poker with people’s information. In an attempt to limit this, Congress in 1999 passed the Gramm – Leach – Bliley Act. This tore down the legal barriers that prevented the mergers of financial institutions, and “required the financial institutions to notify customers how their personal information would be used and offer them the chance to ‘opt-out’ of having that information shared with third parties” (Marshal 510). The problem is that each change in privacy policy sent by a financial institution to the consumer is too confusing to read and understand. In fact, most of the time, the consumer is not even aware of how their information is used and allow these companies to shuffle their information. However, “the current dollar savings due to information sharing total about $17 billion a year… [but] the cost of implementing [the Gramm-Leach-Bliley Act]… [is] estimated at over $400 million” (*Customer Benefits* 1-17).

Now, with the existence of the internet, and the growing significance of internet browsing for shopping, research, and any sort of data transfer, the question of where that information goes is an important one. Furthermore, who owns that information, do we have rights to that information, and is that information protected from prying eyes? Currently, as of January 8, 2008, “A cable operator shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information” (Protection of Subscriber Privacy). Mark Rasch, formerly
part of the United States Department of Justice computer crime unit, reports that the attorney general and the FBI have “asked that ISPs [Internet Service Providers] retain all their records just in case someday… the government may want to use them in some future case” (Rasch). If these internet service providers are made to hold this information, how would they offset the expenses from this data storage (Clemmitt 969)? Furthermore, would not the records of communications from law enforcement agencies also be compromised by this proposed data storage? Peter P. Swire believes they could. Data retention increases “the risk of the exposure of undercover police and confidential informants” (Swire n. pag.). In fact, the information stored by the internet service providers could contain records of communication from law enforcement, thereby, increasing interest of this data for crime groups (Swire n. pag.).

Let us take a look at this from different angle. Suppose that an individual researches about breast cancer for the past few months. In doing so, if a health insurance company who covers this individual or may cover this individual could potentially research that person’s internet history activity (Marshall 507). It is then possible for that insurance company to revoke that person’s eligibility for that health insurance because that insurance may find them to be a liability to their coverage. Is the insurance right to discriminate via these underhanded means? What if that individual was researching treatment for a family member? The argument of privacy should not be shunned because of a person asking, “What do you have to hide?” Rather, privacy should be looked at as a necessary human right that is protected by law.
Works Cited


Customer Benefits from Current Information Sharing by Financial Service Companies.


