International In-house Counsel Journal
Vol. 7, No. 27, Spring 2014, 1

Information Privacy and the Law within these United States

JOSEPH BAMBARA
Attorney at Law, UCNY, USA

To begin with, the right to privacy is not explicitly stated anywhere in the Bill of Rights. The idea of a right to privacy was first addressed within a legal context in the United States. Curiously not unlike today's world, in 1884 advances in technology called for changes in the law. The invention of the Eastman Kodak "Brownie" a handheld camera made it possible to take candid snapshots in public places. Attorney's Samuel D. Warren and future U.S. Supreme Court Justice Louis Brandeis feared this new technology would be used by the "sensationalistic press". They published an article called "The Right to Privacy" where they argued that the U.S. Constitution and common law allowed for a general "right to privacy". Although their article did not immediately lead to any new law, eventually in the 1950's tort expert Dean Prosser argued that "privacy" or the "right to be left alone" was composed of four separate torts. The four torts were:

- Appropriating the plaintiff's identity for the defendant's benefit
- Placing the plaintiff in a false light in the public eye
- Publicly disclosing private facts about the plaintiff
- Unreasonably intruding upon the seclusion or solitude of the plaintiff

In this article, we will primarily address the third bullet as it relates to "information privacy", i.e., an individual's right to control his or her personal information held by others. We will provide an overview of how U.S. and the individual States currently protect information privacy. The current privacy laws in the United States, are relatively new and designed to regulate specific types of information including: health, financial, information about children under 13, social media and communications.

In state legislatures around the country, concern about the collection, trade and hacking of personal data, has spawned privacy laws. Over two dozen State privacy laws were passed in 2013. State lawmakers have acted because of the lack of action in Washington on legislation to strengthen privacy laws. For business and organizations using the internet, email and mobile messaging the matrix of rules has necessitated the need for practitioners to watch evolving laws to avoid noncompliance and ensuing penalties. The privacy landscape is growing in complexity with multiple states addressing the same issue, especially with respect to online privacy, a national as well as an international issue. The White House in February 2012, proposed a Consumer Privacy Bill of Rights., but Congress has not yet taken action. And a proposed update to the 1986 Electronic Communications Privacy Act has also stalled.

According to a survey conducted in late 2013 by the Pew Internet Center, most Americans said they believed that existing laws were inadequate to protect their privacy online, and a clear majority reported making great efforts to mask their identities online. Today nearly every state has some form of information privacy law. Our New York State information privacy legislation from 2005 includes the Information Security Breach and Notification Act (discussed later) as well as the Personal Privacy Protection Law (Public

Officers Law, Article 6-A, sections 91-99) to recognize and address public concern about privacy and the relationship between government and the people. The law is intended to protect your privacy by regulating the manner in which the state collects, maintains and disseminates personal information about you. Generally, the law grants rights of access to you for records about you that are maintained by state agencies; permits you to correct or amend information if you believe that it is inaccurate or irrelevant; and prohibits an agency from collecting personal information, unless it is "relevant and necessary" to a purpose of the agency that must be accomplished by law.

Let's quickly review some of the existing Federal law pertaining to privacy. This will hopefully provide a good overview and set the table for future articles on this expanding and evolving area of the law.

Electronic Communications Privacy Act (ECPA)

The 1986 Electronic Communications Privacy Act (ECPA) 18 U.S.C. § 2510 sets out provisions for the access, use, disclosure, interception, and privacy protections of electronic communications. ECPA proscribes the unauthorized access of electronic communications service facilities, and any electronic communications in storage. ECPA prohibits "electronic communications service providers" from divulging the contents of such communication while it is in electronic storage.

The law prevents government entities from requiring disclosure of electronic communications, such as email messages, from a provider without proper procedure (for example, via a trial subpoena or warrant). Despite the strict mandates against disclosure, there have been many instances where service providers have been compelled to disclose information upon receipt of a court order. For example, within the ECPA framework, certain e-mails held in "electronic storage" by an "electronic communications service" could only be accessed by law enforcement with a warrant (which requires probable cause), whereas a subpoena alone (which does not require prior judicial approval) would be sufficient to access the same e-mail if "stored" by a "remote computing service." The ongoing debate is where to limit the government's power to see into civilian lives while balancing the need to curb national threats. The ECPA falls directly in the middle of this debate both sides wanting revisions and clarifications made by the courts and legislation. Since this law setting standards for how the government can access digital information of citizens passed in 1986, technology has changed dramatically, but the law has not. For a proposed amendment, see https://www.govtrack.us/congress/bills/113/hr1847. Proponents of ECPA reform say the most egregious portion of the law involves the rights the government has to obtain electronic files without needing a warrant. Sadly compared to an email, a paper letter sitting in your home or office drawer has a higher level of constitutional protection. The ECPA allows the government to obtain access to digital communications including email, social media, and information sitting in your public cloud provider's databases, and a variety of other files with only a subpoena and not a warrant once those items are 180 days old. To provide a scope of how much information companies hand over the government, Google reported that it has provided upward of 18,000 requests for information from the government in the second half of 2013. Another portion of ECPA dictates when the government has access to GPS tracking using cell phones. There has been some support in the House for the GPS Act, which would set policies for when the government can access location information of citizens, but the Senate bill passed last year was silent on this issue. There have been numerous efforts to change this, but they all have failed because everyone wants an exemption. For a deeper review see http://beta.congress.gov/bill/113th/senate-bill/607.

Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act of 1998 (COPPA) 15 U.S.C. § 1301, revised July 1, 2013, applies to the online collection of personal information by persons or entities under U.S. jurisdiction from children under 13 years of age. It details what a website operator must include in a privacy policy, when and how to seek verifiable consent from a parent or guardian, and what responsibilities an operator has to protect children's privacy and safety online including restrictions on the marketing to those under 13. Noncompliance may result in penalties of up to $16,000 per violation. While children under 13 can legally give out personal information with their parents' permission, many websites altogether disallow underage children from using their services due to the amount of paperwork involved. The FTC has been fairly vigilant and strict with COPPA enforcement.

To coincide with the amended COPPA, the FTC has also continued to designate five companies to administer "safe harbor" programs. Under COPPA, safe harbor status allows these companies to create comprehensive self-compliance programs for their members. Companies that participate in a COPPA safe harbor program are generally subject to the review and disciplinary procedures provided in the safe harbor's guidelines in lieu of formal FTC investigation and law enforcement.

Health Insurance Portability and Accountability Act

The federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) P.L.104-191, establishes a comprehensive regulatory framework controlling the use and disclosure of individually identifiable health information by "covered entities," principally health care providers and health plans.

In January 2013, HIPAA was updated via the Final Omnibus Rule. Included in changes were updates to the Security Rule and Breach Notification portions of the HITECH Act. See the next section. The changes relate to the expansion of requirements to include business associates, where previously only "covered entities" had to uphold the law.

Additionally, the definition of "significant harm" to an individual in the analysis of a breach was updated to provide more scrutiny to covered entities with the intent of disclosing more breaches which had been previously gone unreported. Protection of protected health information ("PHI") was changed from an indefinite time frame to 50 years after death. Severe penalties were also approved for violation of PHI privacy.

Health Information Technology for Economic and Clinical Health Act

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) part of American Recovery and Reinvestment Act of 2009 (ARRA) (Public Law 111-5, 123 Stat 115), enacted as part of the American Recovery and Reinvestment Act of 2009, establishes new breach notification requirements that apply to HIPAA covered entities and their business associates which access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured PHI. HITECH Act requires HIPAA covered entities to notify affected individuals, and requires business associates to notify covered entities following the discovery of a breach of unsecured PHI. The notification requirement is only triggered if the breach poses a significant risk of financial, reputational, or other harm to the affected individual. The HITECH Act authorizes each state's attorney general to file lawsuits, on behalf of their residents, to enforce HIPAA's privacy and security protections, and imposes increased civil monetary penalties for security breaches.

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA) Public Law. 106-102 of 1999, partially repealed the Glass–Steagall Act of 1933, thereby removing barriers in the market among banking companies, securities companies and insurance companies that prohibited any one institution from acting as any combination of an investment bank, a commercial bank, and an insurance company, i.e., banks, and securities firms and insurance companies were allowed to consolidate. The act has two key provisions carrying significant privacy implications for "financial institutions": the Financial Privacy Rule and the Safeguards Rule. "Financial institutions" include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers, such as lending, brokering or servicing consumer loans, preparing individual tax returns, providing financial advice or credit counseling, and collecting consumer debts.

The Financial Privacy Rule requires financial institutions to provide each consumer with a privacy notice at the time the consumer relationship is established and annually thereafter. The privacy notice must explain the information collected about the consumer, where that information is shared, how that information is used, and how that information is protected. The notice must also identify the consumer's right to opt out of the information being shared with unaffiliated parties pursuant to the provisions of the Fair Credit Reporting Act. Should the privacy policy change at any point in time, the consumer must be notified again for acceptance.

PATRIOT Act

The USA PATRIOT Act Public Law 107-56 of 2001 extended in 2011 provides authority for law enforcement agencies to compel disclosure of virtually any document, including electronic documents held by email, social media and cloud providers.

- Section 215 of the Act permits the issuance of *ex parte* Magistrate Judge court orders
- Further, those who receive a Section 215 court order are severely restricted in their ability to reveal to others that they received such an order, or to alert the subject of the order that the order was received.
- So, those who use cloud providers to store or process their data may not even know that the government obtained their records.

Pursuant to Section 505 of the Act, the FBI may demand, through the use of National Security Letters (NSLs), personal customer records (including e-mails, financial records, and consumer reports) from financial institutions and wire or electronic communication service providers without any prior court approval. Because any electronic data stored in the United States is potentially subject to *ex parte* governmental disclosure, a few foreign governments (most notably the Canadian provinces of British Columbia and Nova Scotia) have enacted various restrictions and/or prohibitions regarding the cross-border transfer of information with U.S.-based cloud providers. Section 215 of the Patriot Act is set to expire on June 1, 2015.

New York State Information Security Breach and Notification Act

The NYS Information Security Breach and Notification Act is comprised of section 208 of the State Technology Law and section 899-aa of the General Business Law. State entities and persons or businesses conducting business in New York who own or license computerized data which includes private information must disclose any breach of the data to New York residents Additionally, under section 899-aa of the General Business Law or persons or corporations conducting business in New York must also notify three (3) NYS offices: the NYS Attorney General; the NYS Division of State Police; and the

Department of State's Division of Consumer Protection of any breach of the data concerning New York residents.

CONCLUSION

This article is a mere overview of the current state of information privacy. A seemingly endless stream of data flows freely in the cyber world of today. We need to be vigilant and aware of our personal data and ensure that those to whom we have entrusted that data are legally bound and proactive about protecting it. We must enact laws which enforce the practice of responsible data stewardship and hold the stewards accountable. We must empower and educate people to protect their privacy, control their digital footprint, and make the protection of privacy and personal data a major priority for all.

***

Joseph J. Bambara is currently In House Counsel and a VP of technology architecture at UCNY, Inc. His e-mail address is jbambara@ucny.com. For the last 10 years, he has been acting as Counsel for small to mid-size technology firms in the metro area. He has worked on outsourcing contracts, intellectual property as it pertains to mobile and enterprise software, SMS mobile marketing issues as well as trade/service marks. In addition to Lawline, he has done CLE's on law and technology for New York County and City Bar Association. He was named The New York Enterprise Report Technology Attorney of 2010. Prior entrepreneurial career included developing applications systems for the financial, brokerage, manufacturing, medical, and entertainment industries in New York, Los Angeles and western European community. These applications systems were implemented using Java for mobile, enterprise and database development. Mr. Bambara has a Bachelor's and a Master's degree in Computer Science. He holds a Juris Doctorate in Law and is admitted to the New York State Bar. He has taught various computer courses for CCNY's School of Engineering. He is member of the New York County Lawyers Association Cyberspace Committee and an active member in the International Technology Law Association. He has authored the following books: Sun Certified Enterprise Architect for J2EE Study Guide (Exam 310-051) (McGraw-Hill, 2007), J2EE Unleashed (SAMS 2001), PowerBuilder: A Guide To Developing Client/Server Applications (McGraw-Hill, 1995), Informix: Client/Server Application Development (McGraw-Hill, 1997), Informix: Universal Data Option (McGraw-Hill, 1998), SQL Server Developer's Guide (IDG, 2000). Over the past ten years, he has taught numerous courses and given many presentations on all aspects of the law and enterprise and mobile development in cities worldwide, including Los Angeles, Vienna, Paris, Berlin, Orlando, Nashville, New York, Copenhagen, Oslo, and Stockholm.

UC is an unified communications consulting and technology workforce acquisition firm, providing services to a global clientele since 1996.

Our list of clients includes: Standard and Poor's, McGraw-Hill, Bank of New York, CNA Insurance, Deutsche Bank, Federal Reserve Bank of New York, Forbes, Goldman Sachs, JP Morgan Chase, Lewco, The New York Stock Exchange, Nestlé Waters. NYC (Mayors office & HPD), Merck, Merrill Lynch, OSI Pharmaceutical, PurchaseSoft, Roche, Schroder & Co., Salomon Smith Barney, SIAC, and Sony Time/Warner.

Our company is comprised of highly qualified and experienced professionals. We combine industry know-how, expertise in new technologies and proven approaches in order to solve business problems fast.