September 18, 2014

Emerging Technologies Push the Boundaries of Privacy Law

Duane Cranston

As technology developers continue to push the envelope on services and applications affecting the daily lives of consumers, the intersection of technology and privacy is becoming increasingly fraught with legal implications for technology developers, users, and governmental regulatory and law enforcement agencies. Recent news on this front has included Apple's introduction of its "Apple Pay" mobile payment system, security breaches of numerous network security systems that hold individual user data including those of JPMorgan Chase, Home Depot, and Apple's iCloud service which resulted in the public posting of personal photos and other private content, and the declassification of correspondence between Yahoo! and the U.S. Department of Justice regarding subpoenas for information on Yahoo! users. Yet even as real-time developments continually demonstrate both the rapid expansion of such capabilities and the implicit risks associated with this technology, the legislative framework governing this area has remained relatively static.

These developments present an ever-evolving set of issues for companies impacted by these technological developments, as they attempt to conform their development and use of such technology to laws that did not necessarily contemplate this new technological frontier. Companies must be cognizant of laws, regulations and policies relating to: (i) their receipt, retention and use of personal user data; (ii) obligations to disclose security breaches relating to personal data; and (iii) disclosure obligations in response to governmental requests for such information. In addition to federal privacy laws, many states have also imposed a patch work of privacy regulations that expand the framework of privacy compliance. The limitless geographic scope of online transactions requires that U.S. companies not only be aware of federal laws and regulations, but that they pay close attention to local laws and international privacy directives which can often times be more rigorous than their federal counterparts. The following is a brief survey of some of the U.S. federal and state laws that apply to privacy and security issues for web technology, particularly in light of recent events.

The Gramm-Leach-Bliley Act

Following the Apple Pay announcement, Visa and MasterCard announced that they were developing a "token" payment security framework to support Apple's payment system. Financial

companies that receive personal data in connection with processing transactions, including through online and mobile payment systems, are subject to the provisions of the Gramm-Leach-Bliley Act of 1999 (the "GLBA") (15 U.S.C. §§ 6801, et seq.) which imposes numerous obligations on financial institutions with respect to their use of such data.. The act also applies to companies that provide personal financial services, including banks, insurance companies, mortgage brokers and financial advisors. The GLBA requires that these institutions "protect the security and confidentiality of those customers' nonpublic personal information," including any personally identifiable information "(i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution." The GLBA requires financial institutions to "insure the security and confidentiality of customer records and information … protect against any anticipated threats or hazards to the security or integrity of such records; and … protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."

The GLBA places restrictions on the use of such information, permitting their use for administrative purposes in connection with their provision of services, or for law enforcement purposes. The GLBA also imposes notice requirements on a financial institution's use of nonpublic personal information, including informing consumers of how their information may be used and allowing customers to "opt out" of having such information shared with unaffiliated third parties. Similarly, financial institutions are required to notify customers of their policies regarding the protection and disclosure of nonpublic personal information.

The Electronics Communications Privacy Act

The Electronics Communications Privacy Act (the "ECPA") similarly imposes a privacy obligation on telecommunications providers, providing that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication… to any person or entity other than an addressee or intended recipient of such communication." The provisions of the ECPA referred to as the "Stored Communications Act" (18 U.S.C. §§ 2701 et. seq.), include a private right of action for individuals and companies whose information has been unlawfully accessed, setting out penalties for violators that include fines and even imprisonment. Unlawful access to digital information is additionally prohibited under the Computer Fraud and Abuse Act (the "CFAA") , which provides an additional private right of action for information security breaches.

The ECPA and CFAA were enacted in 1986, and many technology developers and service providers have challenged their application to services that have emerged in the nearly two decades since their enactment. Accordingly, lawmakers and industry groups alike have made policy recommendations and

proposed new legislation to update the substantive provisions of the ECPA and CFAA and establish a more effective framework for the application and enforcement of their respective provisions, though none have yet been passed.

State Encryption and Security Standards

Certain state laws and regulations extend privacy obligations beyond financial institutions and telecommunications providers to other companies. Notably, Nevada and Massachusetts both apply heightened encryption standards to the processing of financial transactions. Nevada's encryption law, originally enacted in 2005 and amended in 2009 , requires companies doing business in the state to comply with certain encryption standards in their transmission of personal data, and also imposes certain technical requirements in accordance with the Payment Card Industry Data Security Standards for companies that accept debit or credit card payments. Case law on the issue of whether a company is doing business in Nevada indicates that this determination is heavily fact-dependent on a case-by-case basis. See Executive Mgmt. Ltd. v. Ticor Title Ins. Co., 38 P.3d 872 (Nev. 2002). Massachusetts has similarly set forth specific encryption standards relating to the transmission of personal data of Massachusetts residents under its regulation 201 CMR 17.00, which applies to any entity that holds such information regardless of where that entity is located.

State Data Breach Notification Laws

Even where companies have complied with applicable federal and state legal and regulatory requirements, additional legal obligations may be triggered by a data breach that occurs in spite of a company's best efforts. California has often taken the lead in enacting legislation to protect its citizens' privacy, enacting the first breach notification law in 2002 which went into effect in 2003. Today, 48 states and other U.S. territories have enacted their own breach notification laws. Following a 2012 report issued by the California Attorney General detailing security breaches in California, the state broadened the application of its breach notification law to require notification where any breach disclosed names and email addresses in combination with passwords or security questions. See Cal. Civ. Code § 1798.82. Other states could foreseeably follow suit by broadening the protections of their data breach notification laws in similar fashion, particularly given the impact of recent security breaches such as the "Heartbleed" internet security bug that was discovered around April of this year after it had exposed many of the largest websites to security penetration.

Disclosure of Personal Data in Response to a Governmental Request

Finally, in contrast to state and federal privacy and security laws and regulations, certain state and federal laws also require the disclosure of personal data in response to a governmental request. The Stored Communications Act (the "SCA") supplements the ECPA by providing that a governmental entity may require communications service providers (which would include internet service providers) to disclose the contents of communications that have been stored on their systems, with or without notice to service customers depending upon the length of time that such communications have been stored and the procedure required for obtaining a warrant or issuing a subpoena. A governmental entity may also request other information on these users, including a user's name, address, computer network address, and credit card and bank information relating to such user's payment for the use of the service provider's systems.

Record retention requirements under §§2703 and 2704 of the SCA are triggered upon the request of such information by a government agency. §2703 requires that service providers maintain records subject to a government request for a period of up to 180 days. §2704 provides that a service provider may be required to create backup copies of such records "as soon as practicable consistent with its regular business practices."

In addition to the SCA, government offices including those of the Attorney General and the Director of National Intelligence may request user records under the provisions of the Foreign Intelligence Surveillance Act of 1978 ("FISA") , which was amended by the FISA Amendments Act of 2008 (see H.R. 6304). FISA was previously amended by the Protect America Act of 2007 (see S. 1927), pursuant to which the Department of Justice issued subpoenas to Yahoo! for personal information regarding its users. The recent declassification and release of documents relating to these information requests illustrate the fact that companies that receive and retain user data should have internal data retention policies in place in order to comply with unforeseen information requests from a government agency.

Conclusion

As technological progress continues to encompass the convergence of personal and financial user information, companies that transmit, receive and utilize such data must be prepared to comply with privacy requirements imposed by numerous federal and state laws and regulations. Companies should be prepared to evaluate their protocols and internal policies in order to ensure compliance with these laws. Internal technical and legal safeguards should be consistent in order to ensure that notices to consumers accurately reflect the technical realities of their services, and to ensure full legal compliance with respect to their use of such technology.