Legal Update

Federal and State Laws Regulating Data Privacy and Security

As of September, 2011

Michele A. Whitham
Partner, Founding Co-Chair
Security & Privacy Practice Group

Foley Hoag LLP
155 Seaport Boulevard
Boston, MA 02210

I. An Overview of the Statutory Law Bearing on Data Breach[1]

In a world where people's lives are played out increasingly on line -- and their personal information is stored in far-flung electronic locations -- lawmakers in the United States have until recently largely focused their response on safeguarding the privacy and security of individuals' electronic data. The result is an array of overlapping statutes intended to protect personal information summarized below.

A. Federal Data Privacy Statutory Framework (see Exhibit A)

On the federal side, Congress has chosen to regulate data privacy and security by dividing the landscape by subject matter. For example, realms such as individuals' financial or health information, computers and personal communications are each separately protected by stand-alone federal statutes. Layered over these core protections are a number of more narrowly focused statutes which round out individual protections. The following is a brief overview of the statutes enacted in each protected niche.

1. Federal Statutes Protecting Financial Data

i. Electronic Funds Transfer Act (EFTA)

The EFTA (15 U.S.C. § 1693) applies to institutions offering direct debit electronic fund transfers from bank accounts, including pre-authorized automatic transfers. The Act requires financial institutions to make extensive disclosures to their customers detailing electronic fund transfer processes, error-reporting procedures, and notification details, including periodic statements in addition to time-of-transaction statements. The EFTA provides a private right of action, with remedies including both actual and statutory damages, attorneys' fees, and costs. In the case of an action filed by an individual, statutory damages range from $100 to $1,000.

ii. Fair Credit Reporting Act (FCRA)

FCRA (15 U.S.C. §1681), enacted in 1970, applies to data contained in consumer credit reports, including personal and financial data. The Act requires consumer reporting agencies to maintain reasonable procedures to ensure that information in consumer credit reports will be disclosed only for permissible reasons, including in response to court order / legal process, pursuant to written instructions of a consumer, to a person who intends to use the information in connection with a credit transaction, for employment purposes, for insurance underwriting services, or to obtain a government license or loan. Other permissible purposes include disclosure to a child support enforcement agency or, as a catch-all, to a person who has legitimate business need for the information.

---

[1] This overview is exclusive of unenacted data privacy and cyber-security legislative initiatives currently pending before the United States Senate or House of Representatives.

Only individual customers may seek to invoke FCRA's remedial provisions. Willful noncompliance can result in actual and punitive damages as well as costs and attorney's fees. Any person who knowingly and willfully obtains information on a consumer under false pretenses, or any credit reporting agency that provides information to a person not authorized to receive it, faces fines and/or imprisonment of up to two years.

iii. Fair and Accurate Credit Transactions Act (FACTA)

FACTA (Pub. L. No. 108-159 111 Stat. 1952), enacted in 2003 as an amendment to FCRA, *supra*, specifically concerns identity theft related to personal and financial data contained in consumer reports. Under FACTA, covered entities that hold customer accounts must implement identity theft prevention measures designed around recognizing and responding to various "red flags" which indicate suspicious account activity.

iv. Gramm-Leach-Bliley Act (GLBA)

GLBA (15 U.S.C. §§ 6801 *et seq.*), enacted in 1999, regulates personally identifiable, nonpublic financial information disclosed to non-affiliated third parties by financial institutions. The sensitive information at issue for these institutions includes credit card applications, account histories, names, addresses, and telephone numbers in conjunction with social security numbers, passwords, and account numbers. Under GLBA, financial institutions must give written or electronic notice of these categories of information collected from consumers, and the categories of entities to which the information will be disclosed. The Act creates a consumer opt-out right to disclosure *before* disclosure occurs.

GLBA further requires each institution to implement significant technical, physical, and administrative safeguards to maintain the security of this sensitive information. Enforcement of GLBA is left to the FTC, which is restricted to implementing the standards associated with the Act and seeking injunctions against those institutions that disclose information in violation of the Act.

v. Right to Financial Privacy Act (RFPA)

The RFPA (12 U.S.C. § 3401) requires federal agencies seeking customer records from financial institutions to obtain either a search warrant supported by probable cause, the customer's consent, or a specifically proscribed procedural device (such as a subpoena) before accessing these records. Under the Act, a customer has a right of action against either the agency *or* the institution, and civil penalties of at least $100, along with punitive damages, are available.

2. Federal Statutes Protecting Health Information

i. Health Insurance Portability and Accountability Act (HIPAA)

HIPPA (Pub. L. No. 104-191, 110 Stat. 1936), enacted in 1996, applies to three different types of entities: health plans, health care providers, and health care

clearinghouses, along with the "business associates" of any of these entities. Under the Act, these entities cannot disclose "protected health information" (PHI) to third parties without patient authorization. Further, the entities cannot even disclose the patient's PHI for treatment, payment or health care operations without the patient's signing a consent form.

For the purposes of HIPPA, PHI is defined as individually identifiable health information that is transmitted by electronic media, maintained in any electronic medium, or transmitted or maintained in any other form. Enforcement of HIPPA is left to the government, and an entity violating these privacy provisions is subject to civil fines, ranging from $100 per violation up to $50,000 per violation, with a total maximum penalty of $1,500,000 during a single calendar year. Criminal fines and even incarceration are available for egregious violations of the Act.

3. Federal Statutes Protecting Computer and Internet Data

i. Children's Online Privacy Protection Act (COPPA)

COPPA (15 U.S.C. § 6501 et seq.), enacted in 1998, mandates that a website or online service operator cannot collect or disclose personally identifying information from a child under thirteen years of age without obtaining requisite parental consent. Personal identifying information is defined in the Act as a name, address, email address or contact information, social security number, persistent identifier (cookie) or combination of name or photograph with other information that would permit physical or online contacting. Thus, even websites that give the child ability to have an email account without parental consent are subject to the Act. COPPA contains no private right of action. Rather, enforcement is carried out by the FTC, and the Act allows penalties of up to $11,000 per violation.

ii. Computer Fraud and Abuse Act (CFAA)

The CFAA (18 U.S.C. § 1030) prohibits accessing a protected computer, without authorization, in order to obtain information, affect use by the government involving an interstate or foreign transaction, further a fraud when value is obtained (over $5,000 in any one year period), intentionally or recklessly damage the computer, traffic in passwords, or exhort payment. The Act defines "protected computers" as those used by financial institutions, by the U.S. government, and those used (by *any* person or entity) in communications involving interstate or foreign commerce. Thus, the Act has a very broad scope.

The CFAA contains both civil and criminal remedies. On the civil side, in order to bring an action, the asserted damage or loss must fit into a strict set of categories: aggregated damage exceeding $5,000, potential modification or impairment of a medical diagnosis, examination, treatment or care of one or more persons, physical injury, a threat to public health or safety, or damage to a government computer that is used in furtherance

of the administration of justice, national defense, or national security. On the criminal side, violations of the CFAA are punishable by fine and/or imprisonment.

iii. Controlling the Assault of Non-Solicited Pornography and Marketing Act (CANSPAM)

CANSPAM (15 U.S.C. §§ 7701-13, 18 U.S.C. § 1037 and 28 U.S.C. § 994), enacted in 2003, targets commercial email messages whose primary purpose is the advertisement or promotion of a product or service. The sender of the email as well as the advertiser within the email are subject to CANSPAM. Under CANSPAM, a sender of these emails is permitted to send communications to a recipient unless and until that recipient has opted out from said communications. Further, every individual must be permitted to opt out, and thus, each message must contain a clear opt-out mechanism. A private right of action exists (injunctions and actual monetary damages are available) for internet service providers, and the FTC may also enforce the Act's provisions.

4. Federal Statutes Protecting Personal Communications

i. Electronic Communications Privacy Act (ECPA)

The ECPA is comprised of two Titles that provide different types of protection to individuals. Title I, otherwise known as the **Wiretap Act** (18 U.S.C. § 2510, et seq.; 47 U.S.C. § 605) prohibits intentionally intercepting or endeavoring to intercept protected communications (including through the use of electronic, mechanical, or other devices) as well as disclosing or using the intercepted information. Protected communications under Title I include electronic mail, radio communications, data transmission and telephone calls. Title II, otherwise known as the **Stored Communications Act** (18 U.S.C. et seq.), prohibits persons from tampering with computers or accessing computerized records while they are in electronic storage. Title II further prohibits providers of electronic communication services from disclosing the contents of stored communications. A private cause of action is available under both titles, and remedies include injunction, declaratory judgment, actual or statutory damages ($100 per day for each violation or $10,000, whichever is greater), punitive damages, reasonable attorneys' fees and costs. Under Title II, statutory damages are the greater of the actual damages and profits earned by a violator or $1,000.

ii. Telephone Consumer Protection Act

The Telephone Consumer Protection Act (47 U.S.C. § 227), enacted in 1991, is aimed at telemarketer phone calls. The Act requires that telemarketers cease calling an individual once a request to cease has been made, and for telemarketers to keep records of such requests for a period of ten years. Individuals can sue for damages under the Act, amounting to up to $500 for each call. Related is the Telemarketing and Consumer Fraud Abuse and Prevention Act (15 U.S.C. § 6101), which requires telemarketers to clearly inform consumers at the outset of a call of the identity of the seller, the purpose for the call, and what goods or services the telemarketer is offering.

5. Other Areas of Protection Offered by Federal Statutes

i. Cable Communications Policy Act (CCPA)

The CCPA (47 U.S.C. § 551), enacted in 1984, requires cable television operators to notify their subscribers about collection and use of personal information. Further, cable operators may not collect and disclose information about a subscriber's viewing habits without the subscriber's consent. A private right of action exists, and includes possible damage awards of at least $1,000, plus punitive damages, costs, and attorneys' fees.

ii. Driver's Privacy Protection Act (DPPA)

The DPPA (18 U.S.C. §2721), enacted in 1994, prohibits state DMV's from releasing personal information from drivers' license and motor vehicle registration records absent drivers' consent. The chief concern of the Act is drivers' information being disclosed to marketers desirous of such information. Both civil and criminal enforcement is possible under the Act. Civil penalties include damages not less than $2,500, punitive damages in cases of willful and reckless violation, and reasonable attorneys' fees and costs. On the criminal side, state DMV's can be fined up to $5,000 per day for each day of substantial noncompliance.

iii. Family Educational Rights and Privacy Act (FERPA)

FERPA (20 U.S.C. §1232g), enacted in 1974, concerns student records, defined by the Act as records which contain information directly related to students and which are kept by an educational agency or institution. FERPA mandates that the educational agency or institution cannot release student records without consent of the student or the parent of a minor student. No private right of action is provided; rather, the Department of Education may withhold federal funds if an institution is found to have violated the Act.

iv. Video Privacy Protection Act

The Video Privacy and Protection Act (18 U.S.C. § 2710), enacted in 1988, holds that videotape service providers cannot disclose customer names, addresses, and the subject matter of their purchases or rentals for marketing or other use without customers' consent. A private right of action to enforce the statute exists, and videotape service providers that violate the act may be liable for damage awards of at least $2,500, plus attorneys' fees and costs.

B. State Data Privacy Statutory Framework (see Exhibit B)

Forty-six (46) of the fifty states have statutes in place that address data privacy and security. (Only Alabama, Kentucky, New Mexico and South Dakota are currently holding out). At the state level, data privacy is statutorily safeguarded in a more general sense. Rather than carve out discrete areas to protect, as the federal statutes do, most states defer to Congress on this front, and rather seek to install guidelines for covered entities to adhere to when it comes to the preservation of sensitive private data and customer notification of security breaches when they happen to occur.

The typical state data security statute holds that in the event of a security breach, a business owning the compromised personal information must provide prompt notice to the affected individuals. *See e.g.* Cal. Civ. Code §§ 1798.80 *et seq.* (2011). Generally, state statutes are uniform in that they allow notice to be satisfied through electronic means or the mail. *Id.* In cases where a large number of state residents need to be notified and doing so individually would be prohibitively costly, website or news media publication is typically permitted. *Id.* Many state data privacy statutes also contain a provision allowing for relaxed notification standards where notification will impede criminal investigation. *See e.g.* 73 Pa. Cons. Stat. § 2304 (2011).

One of the more rigid statutory models exists in Massachusetts. In addition to having a breach notification similar to California's scheme, *supra*, Massachusetts takes the additional step of mandating that standards be set (by the department of consumer affairs) in connection with the initial safeguarding of personal information contained in paper and electronic records by "any person that owns or licenses personal information about a resident of the commonwealth." Mass. Gen. Laws ch. 93H § 2(a) (2011). Further, the statute mandates government branches and agencies to create and enforce similar standards. *Id.* at § 2(b)-(c). As a result of this statutory requirement, virtually every company doing business in Massachusetts is obligated to implement and maintain complex data security regimes, ranging from physical to sophisticated electronic security measures, and including requiring certifications from the entities with which they do business attesting to their implementation of similar measures.

Finally, it should be noted that several states have taken the forward-thinking step of creating a state executive office specifically governing data security in privacy. For example, New York has created the Office of Cyber Security and Critical Infrastructure Coordination, which focuses on threats to electronic information systems, California the Office of Privacy Protection (COPP), and Colorado the Office of Cyber Security. The step of creating state agencies could foreshadow similar measures taken in the future at the federal level, as data privacy issues jump to the forefront of both individual and national security.