Bloomberg BNA

Privacy and Security Law Report®

What Every General Counsel Needs to Know About Privacy and Cybersecurity Law: 10 Trends for 2015

BY REECE HIRSCH

There was a time, not so very long ago, when privacy and cybersecurity issues were the domain of the information technology department and security professionals. Relatively few companies had appointed privacy officers. Lawyers who specialized in privacy issues were focused on specific sectors, such as financial services, health care and e-commerce. That time is long past, and that fact was never clearer than in 2014, as major breaches involving Target Corp., Home Depot Inc. and Sony Pictures Entertainment Inc. grabbed headlines. In 2015, privacy and cybersecurity issues will be critical to every business that handles personal information, which is virtually every business.

Privacy and cybersecurity matters have emerged as bottom-line issues for corporate America for several reasons. First, privacy is personal and goes right to the heart of a consumer's (or an employee's) relationship with a company. Second, it is very easy to make mistakes given the complex patchwork of federal, state and international laws. Finally, privacy and security regulatory enforcement and litigation are on the rise.

This article will highlight and provide an overview of 10 trends in privacy and cybersecurity law that every general counsel should be aware of. The focus here is on topics of broad applicability, rather than industry-specific issues, such as health-care industry compliance with the Health Insurance Portability and Accountability Act (HIPAA). These are the overarching privacy and cybersecurity issues that touch nearly every company.

Reece Hirsch is a partner in the San Francisco office of Morgan, Lewis & Bockius LLP and co-head of the firm's Privacy and Cybersecurity practice. He is also a member of the Privacy & Security Law Report's advisory board. Hirsch can be reached at rhirsch@morganlewis.com or (415) 442-1422.

1. Do Your Mobile Apps Have Appropriate Privacy Policies?

The proliferation of mobile applications poses unique privacy concerns. The smartphones and tablets that we use every day collect enormous volumes of personal information, which can be tied to specific individuals through geolocation data. The picture is further complicated by the complex ecosystem of players, including operating systems, app developers and ad networks. Finally, providing robust privacy disclosures on a small mobile device screen is inherently challenging.

The Global Privacy Enforcement Network (GPEN), a network of privacy governing organizations from around the world, conducts an annual privacy sweep focusing on a particular issue—in 2014, it was mobile apps. The September 2014 report with GPEN's findings regarding the state of mobile app privacy were not encouraging.[1] Fifty-nine percent of apps did not provide enough information on user privacy prior to app installation. Forty-three percent of apps failed to tailor disclosures to the small screen. Thirty-one percent of apps sought ''excessive permissions,'' gathering data that exceeded what was necessary for the app's functionality.

As part of the GPEN sweep, the Federal Trade Commission announced in May 2014 a proposed settlement with Snapchat Inc. based on allegations that its privacy policy misrepresented its privacy practices, including how its mobile app worked. Snapchat portrayed its app as a service for sending ''disappearing'' photo and video messages, but allegedly failed to acknowledge possible circumvention techniques that would permit the messages to be retained.[2] Snapchat also allegedly collected geolocation data without privacy policy disclosures.

[1] Office of the Privacy Comm'r of Canada, *Backgrounder: Results of the 2014 Global Privacy Enforcement Network Sweep* (Sept. 2014), *available at* https://www.priv.gc.ca/media/nr-c/2014/bg_140910_e.asp (13 PVLR 1613, 9/15/14).

[2] Agreement Containing Consent Order, *In re Snapchat, Inc.*, File No. 132-3078 (FTC May 8, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140508snapchatorder.pdf (13 PVLR 832, 5/12/14). The final de-

So what can companies do to improve their mobile app privacy? Start by reading the FTC's February 2013 staff report ''Mobile Privacy Disclosures: Building Trust Through Transparency,'' which offers suggestions on privacy transparency for mobile platforms and app developers.[3] The FTC report recommends posting a privacy policy and making it available through the platform's app store, so consumers can review it before downloading an app. The agency also supports obtaining ''just in time'' disclosures and affirmative express consent when an app collects sensitive information (financial, health or children's data) outside the platform's application programming interface (API) or shares sensitive information with third parties.

2. Have You Adopted a Formal, Written Data Security Compliance Program?

Despite the uneven, patchwork approach to privacy and security regulation in the U.S., a growing number of companies are now subject to an obligation to adopt ''reasonable'' data security measures. Among the laws mandating some form of ''reasonable security'' are: (i) the HIPAA security regulations applicable to the healthcare industry;[4] (ii) the Gramm-Leach-Bliley Act (GLB Act) ''safeguards'' regulations for financial institutions;[5] (iii) state insurance law analogs to the GLB Act Safeguards Rule applicable to insurance companies;[6] and (iv) state laws governing businesses that maintain personal information of residents of Massachusetts, Nevada, California, Connecticut, Rhode Island, Oregon, Maryland, Arkansas, Texas and Utah.[7]

Since 2005, the FTC has applied the ''unfairness doctrine'' to assert that the failure to employ reasonable and appropriate security measures may constitute unfair and deceptive practices that harm consumers, even in the absence of specific representations by a company regarding its security practices. In closely watched cases, Wyndham Worldwide Corp. and LabMD Inc. have challenged the FTC's authority to apply the unfairness doctrine to enforce data security standards under Section 5(a) of the FTC Act.[8] In 2014, the FTC was allowed to proceed in both enforcement actions, suggesting that the FTC's use of the unfairness doctrine will be upheld.[9] However, the judge in the *FTC v. Wyndham Worldwide Corp.* case warned that this ''does not give the FTC a blank check to sustain a lawsuit against every business that has been hacked.''[10]

Further complicating the regulatory landscape, in October 2014 the Federal Communications Commission for the first time asserted its jurisdiction to regulate security with enforcement actions against TerraCom Inc. and YourTel America Inc.[11]

In its enforcement actions, which are often precipitated by security breaches, the FTC has frequently mandated comprehensive information security programs of up to 20 years accompanied by independent third-party audits. Companies are well-served to be proactive in implementing a formal, written data security compliance program, or regularly updating an existing program. In the wake of a high-profile security breach, it may not be sufficient to *implement* reasonable security practices; it is equally critical to thoroughly *document* those practices through policies, procedures and processes in order to effectively defend against regulatory enforcement actions and class action lawsuits.

3. Have You Implemented a Breach Response Plan?

A recent survey report from Experian Data Breach Resolution and the Ponemon Institute LLC listed data breaches ''among the top three occurrences that affect a company's reputation.''[12] However, in a recent FTI Consulting Inc. survey, 27 percent of directors said that their company did not have a written security breach response plan; 31 percent weren't sure.[13] These figures highlight that, while security breaches can pose a substantial risk to a company, that risk is often not adequately addressed.

A breach response plan is part of a company's formal security compliance program, but it merits special focus because, unlike other security policies, it is much more than a technical, systems-oriented document. A breach response plan implicates all facets of an organization, as reflected in the plan's appointed incident response team, which should include representatives from compliance, legal, human resources, public relations, investor relations (for public companies) and IT. If a company does not have an engaged and active incident response team that is primed to respond to a major breach, then its security breach response plan could probably be improved.

---

cision and order is available at http://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf (14 PVLR 69, 1/12/15).

[3] FTC Staff, *Mobile Privacy Disclosures: Building Trust Through Transparency* (Feb. 2013), *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf (12 PVLR 166, 2/4/13).

[4] 45 C.F.R. pts. 160, 162 and 164.

[5] 15 U.S.C. § § 6801–6809.

[6] *See e.g.*, Cal. Fin. Code § § 4050–4060.

[7] *See e.g.*, Ark. Code Ann. § § 4-110-101 to 4-110-108 (2009); Cal. Civ. Code § 1798.81.5 (2009); Conn. Gen. Stat. Ann. § 42-471 (2010); 201 Mass. Code Regs. § § 17.01-17.05 (2008); Md. Code Ann., Com. Law § § 144-3501 to 14-3503 (2009); Nev. Rev. Stat. § 603A.210 (2009); Or. Rev. Stat. § 646A.622 (2009); R.I. Gen. Laws § 11-49.2-2 (2008); Tex. Bus. & Com. Code Ann. § § 72.001-72.051 (2009); Utah Code Ann. § § 13-44-101 to 13-44-301 (2009).

[8] 15 U.S.C. § 45(a).

[9] *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-JAD, 2014 BL 94785 (D.N.J. Apr. 7, 2014) (13 PVLR 619, 4/14/14); *LabMD, Inc. v. FTC*, No. 13-15267 (11th Cir. Feb. 18, 2014), *available at* http://www.bloomberglaw.com/public/document/LabMD_Inc_v_Federal_Trade_Commission_Docket_No_1315267_11th_Cir_N (13 PVLR 337, 2/24/14); *LabMD, Inc. v. FTC*, No. 1:14-cv-00810-WSD (N.D. Ga. May 12, 2014), *available at* http://www.bloomberglaw.com/public/document/LabMD_Inc_v_Federal_Trade_Commission_Docket_No_114cv00810_ND_Ga_M/3 (13 PVLR 884, 5/19/14).

[10] *Wyndham Worldwide Corp.*, 2014 BL 94785, at *4.

[11] Notice of Apparent Liability for Forfeiture, *In re TerraCom, Inc. and YourTel Am., Inc.*, No. FCC 14-173 (F.C.C. Oct. 24, 2014), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-173A1.pdf (13 PVLR 1898, 11/3/14).

[12] Ben DiPietro, *Survey Roundup: Compliance Burden, Reputation Breaches*, Wall St. J., May 16, 2014, *available at* http://blogs.wsj.com/riskandcompliance/2014/05/16/survey-roundup-growing-compliance-burden-data-breaches-and-reputation/.

[13] Megan Stride, *Data Security Now a Top Worry for GCs, Directors: Report*, Law360, Aug. 15, 2012.

  PVLR ISSN 1538-3423

Incident response teams should consider guidance such as the October 2014 report issued by the California Attorney General's Office analyzing 2013 breaches in that state.[14] The California attorney general report includes the following key recommendations for retailers: (i) update point-of-sale terminals so that they are chip-enabled, (ii) encrypt payment card data from point of capture until transaction authorization and (iii) implement tokenization solutions to devalue payment card data. Companies should also keep an eye on the progress of the Personal Data Notification & Protection Act, called for by President Barack Obama Jan. 12, which would create a single national standard for security breach notification.[15]

No organization's security is perfect, and security breaches are inevitable. However, when a severe breach occurs, companies are judged by the reasonableness of their efforts to prevent and mitigate incidents, as demonstrated by a thoughtfully implemented breach response plan.

4. Is 'Privacy by Design' Part of Your Product Development Process?

In March 2012, the FTC released a set of recommendations for business and Congress regarding the collection and use of consumer personal information (the ''Privacy Framework'').[16] A central tenet in the Privacy Framework is the notion of ''privacy by design,'' which is the philosophy of embedding privacy from the outset into the design specifications of information technologies, accountable business processes, physical spaces and network infrastructures.

Recent FTC enforcement actions have made it clear that privacy by design is more than a recommendation. In February 2013, the FTC settled charges with mobile device manufacturer HTC America Inc. that it had failed to take reasonable steps to secure the software it developed for smartphones and tablet computers.[17] The FTC cited HTC America for ''permission re-delegation'' issues, which can arise when a user consents to an app's use of geolocation data, but the data are then shared with another app without user permission.

Companies that design and market products capable of collecting, storing, accessing or transmitting personal information should incorporate privacy by design principles by carefully reviewing data flows. Consider whether your data flows are consistent with product descriptions, legal requirements, user expectations and posted privacy policies. It is also vital to involve legal counsel in the early stages of product development to ensure that privacy and security considerations are ''baked in,'' rather than tacked on prior to rollout or, worse still, re-engineered in response to a negative consumer or regulatory response.

5. Have You Applied the NIST Cybersecurity Framework?

In February 2014, the Obama administration released the final version of a much-anticipated *voluntary* cybersecurity framework developed by the National Institute of Standards and Technology (NIST) in collaboration with stakeholders (the ''NIST Framework'').[18] The NIST Framework focuses on protection of the nation's critical infrastructure, defined as ''[s]ystems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets could have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.''[19]

The NIST Framework clearly applies to sectors such as transportation, financial services, energy and utilities, government and the public Internet, but any company experiencing a cybersecurity event will want to be able to demonstrate that its security practices are consistent with the framework—regardless of industry sector. It is likely that plaintiffs' attorneys and perhaps insurers will seek to utilize the NIST Framework as a general standard of care for cybersecurity.

The NIST Framework dovetails with other legal trends supporting the adoption of formal security compliance programs. It borrows from existing industry security standards and encourages organizations in the critical infrastructure sector to:

- map out a ''current profile'' of cyberattack readiness;
- pinpoint a ''target profile'' that reflects readiness based on an analysis of the likelihood and impact of a cybersecurity event;
- identify ''gaps'' between the profiles; and
- implement an action plan to address those gaps.

At present there are no incentives for compliance with the NIST Framework, but there has been discussion about tying the framework to benefits such as liability protections, grants, cyber insurance and government contracts. Regardless of whether such incentives are created, companies are likely to feel mounting pressure to implement the NIST Framework in 2015 and beyond.

6. Is Your Board of Directors Engaged in Managing Cyber Liability Risk?

Boards of directors have a duty to protect corporate assets and, increasingly, those assets take the form of information. Several recent security breaches have been followed by shareholder derivative lawsuits against directors and officers, alleging that failure of

[14] Cal. Office of the Attorney Gen., *California Data Breach Report* (Oct. 2014), *available at* https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf (13 PVLR 1912, 11/3/14).

[15] Personal Data Notification & Protection Act (2015), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf (14 PVLR 87, 1/19/15).

[16] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012), *available at* http://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers (11 PVLR 590, 4/2/12).

[17] Proposed Agreement Containing Consent Order, *In re HTC America Inc.*, File No. 122 3049 (F.T.C. Feb. 22, 2013), (12 PVLR 377, 3/4/13). The final decision and order is available at http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htcdo.pdf.

[18] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (13 PVLR 281, 2/17/14).

[19] *Id.* at 3.

oversight and inadequate cybersecurity systems led to breaches. Proxy advisory services have also questioned board conduct following certain security breaches.

In a June 2014 speech to the New York Stock Exchange on ''Cyber Risks and the Boardroom,'' Securities and Exchange Commission Commissioner Luis A. Aguilar stated, ''Given the significant cyber-attacks that are occurring with disturbing frequency, and the mounting evidence that companies of all shapes and sizes are increasingly under a constant threat of potentially disastrous cyber-attacks, ensuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director's risk-oversight responsibilities.''[20]

This does not mean that directors are required to become cybersecurity experts, but they should develop a high-level understanding of cyber risks through briefings from management and others. Discussions about cyber risk management should be given regular, adequate time on the board agenda.

The board's risk oversight function often either lies with the full board or is delegated to the audit committee. Unfortunately, in many organizations both bodies lack the technical expertise to adequately manage cyber liability risks. Aguilar cited another approach—the creation of a separate enterprise risk committee on the board charged with developing a ''big picture'' approach to cybersecurity and other companywide risks. Whatever approach a company adopts, Aguilar warned, ''Boards that choose to ignore, or minimize, the importance of cybersecurity oversight do so at their own peril.''[21]

7. Are You Properly Insured Against Cyber Liability Damages?

Cyber liability insurance is the crucial last step in an effective security breach risk management strategy. Cyber liability policies typically cover ''first-party losses,'' such as: hiring a security forensics firm; notification mailing costs; public relations; credit monitoring services; call centers; identity theft resolution services; legal services; data restoration and security remediation costs; and e-extortion (payments to a hacker to recover data). The policies vary widely with respect to coverage of ''third-party losses,'' such as: third-party claims based on the failure to protect confidential information; defense costs; data loss; fines and penalties; and media liability (such as libel, slander and copyright infringement).

In the past, many companies relied upon their commercial general liability (CGL) insurance to address cyber liability, but that window has largely closed. In 2013, Insurance Services Office Ltd. filed several data breach exclusionary endorsements for use with standard-form CGL policies, and those endorsements became effective in most states in 2014.[22] Going forward, it will be increasingly difficult to rely on CGL policies to cover data breach liabilities.

Cyber liability policies sometimes provide that ''interrelated claims'' or ''interrelated wrongful acts'' will be deemed to have commenced for coverage purposes on the date in which either the claim was made or the insurer receives notice from the insured that a wrongful act took place. These provisions can be either helpful or problematic, depending upon the circumstances. For example, if interrelated wrongful acts resulting in a breach occurred prior to the ''retroactive date'' (the first date of coverage), then they can cause claims to not be covered—even if the acts that resulted in those claims happened *after* the retroactive date. Companies should strongly consider cyber liability insurance and take care to understand how the coverage works because the devil truly is in the details.

8. Are You Prepared for Economic Espionage and New Cyberthreats?

The Sony hack brought state-sponsored hacking into the national spotlight, but, just as significantly, 2014 marked the first economic espionage case brought against state actors by the Department of Justice (DOJ). In *United States v. Liew*, the DOJ charged members of the Chinese military with conspiracy to steal trade secrets concerning chloride-route titanium dioxide production technology with the intent to benefit state-owned companies of the People's Republic of China.[23] The lead defendant was sentenced to 15 years in prison, forfeiture of $27.8 million and $511,667 in restitution.

Former National Security Agency Director General Keith B. Alexander referred to the thefts of intellectual property of U.S. companies by hackers in recent years as ''the greatest transfer of wealth in history.''[24] While that statement may have been hyperbolic, it underscores the breadth of the problem. Companies must be cognizant of current cyberthreats and harden their defenses accordingly, with a particular focus on safeguarding critical intellectual property and trade secrets. Public companies that have been victimized by these sorts of hacks also need to consider whether the events are sufficiently material to require disclosure in SEC filings.

Another trend in cyberthreats is represented by the April 2014 breach involving the hospital operator Community Health Systems Inc., which likely originated from China and focused on valuable nonclinical, nonmedical data, such as patient names, addresses, birth dates, telephone numbers and Social Security num-

[20] Speech, Luis A. Aguilar, Commissioner, SEC, Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus (June 10, 2014) (13 PVLR 1063, 6/16/14).

[21] *Id.*

[22] Matt Dunning, *Insurers Prepare for Implementation of New Cyber Liability Exclusions*, Bus. Ins. (Jan. 19, 2014), *available at* http://www.businessinsurance.com/article/20140119/NEWS04/301199978/insurers-prepare-for-implementation-of-new-cyber-liability-exclusions.

[23] *United States v. Liew*, No. 3:11-cr-00573 (N.D. Cal. 2014); *see also* Karen Gullo, *California Man Guilty of Stealing DuPont Trade Secrets*, Bloomberg, Mar. 5, 2014, *available at* http://www.bloomberg.com/news/2014-03-05/california-man-guilty-of-stealing-dupont-trade-secrets.html (13 PVLR 1239, 7/14/14).

[24] *Trade Secrets: Promoting and Protecting American Innovation, Competitiveness, and Market Access in Foreign Markets: Hearing Before the Subcomm. on Courts, Intellectual Property, and the Internet of the H. Comm. on the Judiciary*, 113th Cong. 2d (June 24, 2014) (statement of Rep. Jerrold Nadler, Ranking Member of the Subcomm.), *available at* http://judiciary.house.gov/_cache/files/5311b6c1-9a4f-49e5-a477-451a3ee228bf/113-97-88436.pdf.

   ISSN 1538-3423

bers.[25] The incident is notable because it is a departure from typical health-care industry security breaches that involve employee mishandling or misappropriation of data. The Community Health Systems breach indicates that the health-care industry is not immune to sophisticated hacks originating outside the U.S.

Another trend in cyberthreats is exemplified by the so-called ''FIN4'' hacks, a U.S.-based hacking ring that targeted law firms in successfully gathering information on nearly 100 U.S. publicly traded health-care and pharmaceutical companies.[26] The goal of the FIN4 hacks appears to have been gathering information on mergers and acquisitions (M&A) deals and other nonpublic, market-moving events that could be used to inform stock sales. Cyberthreats are constantly evolving, making it important for companies to stay abreast of the latest trends in order to implement appropriate countermeasures.

9. Does Your Privacy Policy Address New California Requirements?

For the privacy officers of national companies, California is often the tail that wags the dog, setting a *de facto* national standard by being the first state to implement new forms of privacy regulation. One important example of California's first-mover status is the California Online Privacy Protection Act (CalOPPA). CalOPPA is a unique state law that requires operators of commercial websites and online services that collect personally identifiable information of California residents to post a privacy policy containing certain required elements.[27] The privacy policy must be ''conspicuously'' posted.

Effective Jan. 1, 2015, CalOPPA was amended to give California minors (under 18) the right to remove information that they post online.[28] Website operators must provide notice of the ''delete'' option and the fact that it does not guarantee complete removal of the content. The new law, known as S.B. 568, also prohibits certain types of marketing and advertising to minors, including ads for firearms, tobacco and dietary supplements. S.B. 568 complicates online minor privacy compliance efforts because the standard is very different from the federal Children's Online Privacy Protection Act (COPPA).[29]

The privacy policies of companies collecting personal information of California residents online must also include a provision explaining whether they process do not track signals sent from Internet browsers.[30] That amendment to CalOPPA became effective on Jan. 1, 2014. Companies should regularly review their online privacy policies to confirm compliance with these and other new laws. It is even more important to regularly review an online privacy policy to confirm that it is reasonably complete and accurate in describing the company's current practices in collecting, using and disclosing personal information online. Failure to be less than fully transparent about privacy practices may subject a company to an FTC enforcement action for an ''unfair or deceptive act or practice'' violating Section 5(a) of the FTC Act.

10. Are You Embracing the Possibilities, and Avoiding the Pitfalls, of Big Data?

''Big data'' has become such a popular catch phrase that the term has nearly lost its meaning. Big data typically refers to the application of emerging techniques in data analytics, such as machine learning and other artificial intelligence tools, to enormous new stores of personal information. Vast amounts of data from sources such as smartphone GPS data, Web browsing data, social networking activity and biometric data are being pooled and analyzed to assemble powerful and often surprisingly granular information about individual behavior. Big data poses challenges for regulators because privacy laws generally regulate how a business shares information with third parties and bar uses of information that are inconsistent with stated business purposes. Privacy laws are less well-suited to addressing a consumer's discomfort when, in the course of providing its services, a company comes to know more about the consumer than he or she could have imagined.

2014 saw the first steps to consider regulation of big data. In May 2014, the White House released a report on big data, and a parallel report was issued by the President's Council of Advisors on Science and Technology.[31] The President's Council report recommends that new policies should focus on how data are used, rather than technical aspects of data collection. Some form of regulation of big data seems likely, but at this point it is difficult to say what form it might take.

Even in the absence of regulation, companies seeking to leverage the power of big data in developing new products and services should be sensitive to consumer perceptions. Just because a particular use of data is legal does not mean that it won't draw criticism. The power of big data has also brought new focus on securing the rights to use customer or other data for big data analytics purposes. It is impossible to anticipate all of the potential future uses a company may have for big data when entering into a customer agreement, but data use provisions should be carefully drafted and negotiated with an eye toward those potential future uses. The stakes can be high because, if data rights are properly granted, big data often provides the key to new products, services and even new lines of business.

---

[25] *Data Breach Notification*, Cmty. Health Sys., http://www.chs.net/media-notice/ (last visited Jan. 21, 2015) (13 PVLR 1504, 9/1/14).

[26] Gail Sullivan, *Report: ''FIN4'' Hackers Are Gaming Markets by Stealing Insider Info*, Wash. Post, Dec. 2, 2014, *available at* http://www.washingtonpost.com/news/morning-mix/wp/2014/12/02/report-hackers-are-gaming-markets-by-stealing-insider-info/.

[27] Cal. Bus. & Prof. Code § 22575(a).

[28] *Id.* § § 22580–22582; *see also* S.B. 568 (Cal. 2013), *available at* http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_0551-0600/sb_568_bill_20130923_chaptered.pdf (12 PVLR 1685, 9/30/13).

[29] 15 U.S.C. § § 6501–6506.

[30] Cal. Bus. & Prof. Code § 22575(b)(5) (12 PVLR 1720, 10/7/13).

[31] White House, *Big Data: Seizing Opportunities, Preserving Values* (May 2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf; President's Council of Advisors on Science and Tech., *Big Data and Privacy: A Technological Perspective* (May 2014), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf (13 PVLR 761, 5/5/14).