Bloomberg BNA

Privacy and Security Law Report®

Regulators and Plaintiffs' Lawyers Are Ready to Pounce on Privacy and Data Security Missteps: A Guide to Limiting Corporate Risk



By Des Hogan, Michelle Kisloff, Christopher Wolf, and James Denvil

The past decade has witnessed a revolution in technology employing personal data to provide new ways for people to communicate, to receive services and to be connected. Ten years ago, the ''smart phone'' was in its infancy; today, iPhones and Android phones are everywhere. Ten years ago, social networks were just getting launched. Today, Facebook has over a billion users. Ten years ago, no one had heard of ''apps.'' Today, apps, or mobile device applications, are the way people access a staggering array of information and services tailored to who they are and where they are. Ten years ago, the first data security breach notification law in the nation was passed in California; today nearly every state has a notification law.

And ten years ago, privacy and data security class actions were not a real threat to businesses. Today, they are a threat, along with the growing possibility of regulatory enforcement for privacy and data security missteps.

The increasing collection and use of personal data, sometimes in ways that are unexpected by the average consumer, have put privacy and data security onto the national agenda. The Federal Trade Commission (FTC) and state attorneys general devote substantial resources to investigate privacy and data security practices. Also, as the media and academic researchers uncover perceived privacy issues, and as data security breaches are made public as a result of the notification laws, plaintiffs' lawyers have set their sights on technology companies and their deep pockets to attempt class action litigation.

Despite national attention on privacy and data security, for several years plaintiffs' firms struggled to gain traction in privacy-related cases, with courts often dismissing purported class actions at the initial pleading stage due to the absence of cognizable financial harm resulting from the complained-of activity. Regulators initially focused on ''low hanging fruit''—violations that were obvious, like promising one thing with respect to the use of personal information and doing another, or failing to use basic data security techniques.

Times have changed. The plaintiffs' bar has won a string of recent victories in privacy class actions, which could light a path for others seeking to bring similar cases. And both the FTC and National Association of Attorneys General (NAAG) have, in the past year, significantly increased the resources they will focus on this area and have expanded the scope of their enforcement beyond ''low hanging fruit.'' Companies that ignore the risk of privacy-related litigation and investigations—perhaps thinking hopefully, outside of the high-tech industry, ''it won't happen to us''—do so at their peril.

This changing and more perilous environment comes as the collection and use of customer and other personal data increase. Personal information fills employee records, customer lists, consumer profiles, sales receipts, credit reports, marketing surveys, and myriad other records. And businesses collect personal information to comply with legal obligations, evaluate employees, secure company facilities, develop and implement marketing strategies, and sometimes, to sell the information to others. In light of this new reality, it is an appropriate time to consider some recent developments in the law and to discuss steps companies can take to re-

 ISSN 1538-3423

duce their exposure to such lawsuits and enforcement actions.

Privacy Class Action—A Changing Tide

Recently, there have been some highly visible class action settlements.[1] But those headline-grabbing settlements belie the fact that most privacy class actions have been dismissed because the plaintiffs failed to establish standing to sue (with the requisite ''injury-in-fact'') or because the plaintiffs failed to state a claim (because they could not allege real damages). Over the years, dozens of attempted class actions were thrown out of court for lack of standing or failure to state a claim. For example, in *LaCourt v. Specific Media Inc.*, a case involving an ad network's placement of flash cookies to circumvent users' privacy settings, the district court dismissed the complaint because the plaintiffs failed to adequately plead that the collection of their personal information caused economic harm.[2] In several cases in which plaintiffs sued for failing to adequately protect personal information, purportedly creating an increased risk of future identity theft, the courts ruled that the plaintiffs lacked Article III standing because the increased risk of future harm did not constitute an injury-in-fact.[3]

Recent Developments

Recently, however, federal courts have issued a string of decisions refusing to dismiss plaintiffs' complaints and allowing cases to move forward into discovery and class proceedings. And in one recent, important case, the U.S. Court of Appeals for the Eleventh Circuit reversed the dismissal of a privacy class action complaint. Specifically, in *Resnick v. AvMed Inc.*, the plaintiffs alleged that two laptops containing unencrypted sensitive information were stolen from a health plan.[4] Within fourteen months, two of the health plan's customers were victims of identity theft. Those customers claimed that their personal information had never been compromised other than when the laptops were stolen, and thus they had stated an injury fairly traceable to the laptop thefts. The Eleventh Circuit held that the plaintiffs had standing because their allegations sufficiently established that they suffered an injury-in-fact that was fairly traceable to the defendant's actions and they stated several common law claims.

Perhaps most importantly, in *Resnick* the Eleventh Circuit also held that, with respect to plaintiffs' unjust enrichment claim, the plaintiffs stated a claim because the insurer allegedly did not properly secure its customers' data and thus ''cannot equitably retain their monthly premiums—part of which were intended to pay for the administrative cost of data security.''[5] The Eleventh Circuit's holding that subscriber fees inherently contain a portion that is intended to keep data safe from exposure, if followed, potentially could provide a theory on which plaintiffs could rely to try to establish standing and a viable common law cause of action anytime customer data are exposed.[6]

In another important recent decision, *Cousineau v. Microsoft Corp.*, the class representative plaintiff alleged that she denied the defendant access to her location information, but Microsoft collected it anyway through the camera application on her Windows phone.[7] In holding that the plaintiffs had standing and allowing her Stored Communications Act[8] claim to go forward, the court found that the ''loss of location data'' and the potential of linking location information to a specific consumer constituted a concrete injury.[9] Having survived a motion to dismiss and a petition for interlocutory appeal, the plaintiffs are scheduled to move for class certification in July 2013.

Similarly, in *Dunstan v. comScore Inc.*,[10] the class plaintiffs alleged that comScore surreptitiously collected private information from their computers in violation of the Electronic Communications Privacy Act.[11] The complaint alleged that comScore offered free items and, when a consumer accepted, without warning it downloaded and installed tracking software, collecting online activity information, which could be aggregated and resold. Rejecting defendants' lack of standing argument, the court held that the mere collection of this private information was a cognizable injury and that the plaintiffs had stated a claim.[12] On April 2, the U.S. District for the Northern District of California granted the plaintiffs' motion for class certification in part.[13]

---

[1] *E.g.*, *Lane v. Facebook, Inc.*, No. C 08-3845 RS, 2010 WL 9013059 (N.D. Cal. Mar. 17, 2010), *aff'd,* 696 F.3d 811 (9th Cir. 2012), *available at* http://op.bna.com/pl.nsf/r?Open=dapn-83n3ht ($9.5 million to establish a privacy foundation with $2.3 million going to the plaintiffs' lawyers) (9 PVLR 432, 3/22/10); *In re Google Buzz User Privacy Litig.*, No. C 10-00672 JW, 2011 WL 7460099 (N.D. Cal. June 2, 2011), *available at* http://epic.org/privacy/ftc/googlebuzz/EPIC_Google_Buzz_Settlement.pdf (up to 30 percent of the $8.5 million settlement went to the plaintiffs' lawyers and the remainder was dedicated to consumer education and privacy organizations).

[2] *LaCourt v. Specific Media, Inc.*, No. SACV 10-1256-GW, 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011).

[3] *Katz v. Pershing, LLC*, 672 F.3d 64 (1st Cir. 2012), *available at* http://op.bna.com/pl.nsf/r?Open=kjon-8rwpzc (11 PVLR 421, 3/5/12); *Reilly v. Ceridian Corp.,* 664 F.3d 38 (3d Cir. 2011), *available at* http://pub.bna.com/eclr/11cv1738_121211.pdf (10 PVLR 1859, 12/19/11); *Amburgy v. Express Scripts, Inc.* 671 F. Supp. 2d 1046 (E.D. Mo. 2009), *available at* http://op.bna.com/pl.nsf/r?Open=dapn-7ye7gb (8 PVLR 1713, 12/7/09).

[4] *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012), *available at* http://op.bna.com/hl.nsf/r?Open=mapi-8xzpsx (11 PVLR 1413, 9/17/12).

[5] *Id.* at 1328.

[6] Although the issue does not seem to have been considered by the Eleventh Circuit, the applicability of the court's decision could be limited in some circumstances by the Filed Rate Doctrine. In a case involving similar allegations that involves a company whose regulator approved its rates, the Filed Rate Doctrine could serve as a defense to a *Resnick*-type class action.

[7] *Cousineau v. Microsoft Corp.*, No. C11-1438-JCC (W.D. Wash. June 22, 2012), *available at* http://newsandinsight.thomsonreuters.com/uploadedFiles/Reuters_Content/2012/06_-_June/gibson_microsoft.pdf.

[8] 18 U.S.C. §§ 2701–2712.

[9] *Cousineau*, at *9.

[10] Complaint, *Harris v. comScore, Inc.*, No. 1:11-cv-05807 (N.D. Ill. Aug. 23, 2011), *available at* http://pub.bna.com/eclr/11cv5807_082311.pdf (10 PVLR 1250, 9/5/11).

[11] *See* 18 U.S.C. §§ 2510–22, 2701–11, 3121–26.

[12] Transcript of Proceedings, *Dunstan v. comScore, Inc.*, No. 1:11-cv-05807 (N.D. Ill. Nov. 30, 2011).

[13] *Harris v. comScore, Inc.*, No. 1:11-cv-05807 (N.D. Ill. Apr. 2, 2013), *available at* http://www.bloomberglaw.com/public/document/Dunstan_et_al_v_comScore_Inc_Docket_No_111cv05807_ND_Ill_Aug_23_2 (*see related report*).

  PVLR ISSN 1538-3423

These cases join others over the past several years that make potential privacy-based class actions more likely. In *In re iPhone Application Litigation*, the court ruled that the consumption of bandwidth, storage space, and battery life by applications transmitting personal information from mobile devices constituted an injury-in-fact sufficient to establish standing.[14] Another judge in same district allowed a putative class action alleging violations of California's computer crime law and consumer protection statutes and a variety of common law theories to proceed, based in large part on the named plaintiff's allegation that it would cost $12,250 to remove a social media app and its tracking software.[15]

And the risk of this type of litigation is not limited to ''high tech'' companies. A putative class action against a grocery chain has been allowed to proceed after hackers breached the store's electronic payment processing system; the U.S. Court of Appeals for the First Circuit held that a customer's reasonable efforts to mitigate risks of identity theft constituted a basis for cognizable damages under Maine's negligence and breach of implied contract laws.[16] The *Resnick* case mentioned above was brought against a health care plan, and class actions against retailers and financial service companies based on purportedly improper marketing messages have also survived motions to dismiss.[17]

The U.S. Supreme Court Weighs In

Important developments in standing jurisprudence are not limited to federal district and circuit courts. In February, the U.S. Supreme Court issued a ruling that affects the arguments of plaintiffs seeking to establish Article III standing to sue for alleged privacy violations. In *Clapper v. Amnesty International USA*,[18] the Supreme Court held that plaintiffs did not have standing to challenge the constitutionality of the Foreign Intelligence Surveillance Act of 1978 (FISA) Amendments Act, which allows the government to monitor the electronic communications of non-U.S. persons overseas without obtaining a warrant.[19] In a 5-4 decision, the court held that neither the plaintiffs' fears that their future communications with likely targets of surveillance might be monitored nor the costs the plaintiffs incurred to avoid monitoring satisfied the constitutional requirement that they have suffered an actual or imminent injury fairly traceable to the challenged action. Under *Clapper*, plaintiffs relying on the risk of future harm to establish standing must show that the risk is ''certainly impending.''[20]

The U.S. Supreme Court's *Clapper* ruling does not spell the end of privacy class-actions.

This ruling does not spell the end of privacy class-actions. The *Clapper* plaintiffs did not allege that their communications were intercepted. They attempted to establish their standing to sue based on speculation that their communications would likely be intercepted and on the measures they took to avoid being monitored. The plaintiffs in *Resnick*, *Cousineau*, and *Dunstan*, on the other hand, claimed that their personal information was accessed without authorization. *Clapper* will likely make it more difficult for plaintiffs to survive motions to dismiss when the harms alleged are based on speculations about access to personal information. But *Clapper* may not have a significant effect on cases in which plaintiffs allege that their personal information was actually accessed or otherwise compromised.

Is the Tide Really Shifting?

The bottom line is that the plaintiffs' attorneys have become more creative, standing requirements may be relaxed, and courts have become more willing to allow privacy-related class actions to proceed past the initial pleading stage and into time- and resource-draining class discovery and proceedings. Nonetheless, we still have not seen many privacy class actions procure windfall damages awards for plaintiffs. So, the valid question remains, is there a significant risk over the horizon? The answer seems to be yes.

As plaintiffs' lawyers learn to navigate the hurdles in seeking damages for alleged violations of their clients' privacy rights, the incentives to bring these suits increase. This is especially so because many state laws include nominal damages clauses in their data breach and privacy laws, making the proof of liability easier.[21] Michigan's Video Rental Privacy Act (VRPA) provides statutory damages of the greater of $5,000 or actual damages for improperly disclosing video rental records.[22] If class action plaintiffs, for example, were to succeed in showing that Pandora violated the VRPA by

[14] *In re iPhone Application Litigation*, 844 F. Supp. 2d 1040, 1055 (N.D. Cal. 2012), *available at* http://op.bna.com/pl.nsf/r?Open=kjon-8vflql (11 PVLR 1000, 6/25/12).

[15] *Hernandez v. Path, Inc.*, No. 12-CV-01515-YGR, 2012 WL 5194120 (N.D. Cal. Oct 19, 2012), *available at* http://op.bna.com/pl.nsf/r?Open=dapn-8zcsja (11 PVLR 1586, 10/29/12); *see also Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855 (N.D. Cal. 2011), *available at* http://op.bna.com/pl.nsf/r?Open=dapn-8g348c (the plaintiff alleged a developer failed to adequately secure users' email addresses and login credentials, the court ruled the plaintiff's allegation that the breach caused some unidentified loss to the value of the plaintiff's personal information was sufficient to allow the case to go forward) (10 PVLR 620, 4/25/11).

[16] *Anderson v. Hannaford Bros.*, 659 F.3d 151, 166–67 (1st Cir. 2011), *available at* http://op.bna.com/pl.nsf/r?Open=dapn-8mukuq (10 PVLR 1519, 10/24/11).

[17] *E.g.*, *Mims v. Arrow Fin. Servs., LLC*, 132 S. Ct. 740 (2012), *available at* http://pub.bna.com/lw/101195.pdf (holding that federal and state courts have concurrent jurisdiction over private suits arising under the Telephone Consumer Protection Act) (11 PVLR 159, 1/23/12); *Chesbro v. Best Buy Stores, L.P.*, 705 F.3d 913 (9th Cir. 2012), *available at* http://pub.bna.com/eclr/11cv35784_101712.pdf (reversing the lower court's grant of summary judgment to Best Buy LP) (11 PVLR 1557, 10/22/12).

[18] *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013), *available at* http://pub.bna.com/lw/111025.pdf (12 PVLR 350, 3/4/13).

[19] 50 U.S.C. § 1881a.

[20] *Id.* at 1147.

[21] *See., e.g.*, Cal. Civ. Code § 56.36 (West 2012) ($1,000 per affected patient in a health data breach); Cal. Civ. Code § 1747.08 (West 2012) (up to $1,000 per instance of recording personal information on a credit card transaction form absent specified exceptions); Mich. Comp. Laws § 445.1715 (2012) (greater of $5,000 or actual damages for wrongful disclosure of information regarding purchase, lease, rental, or borrowing of books, sound recordings, or videos).

[22] Mich. Comp. Laws § 445.1715.

disclosing the listening history of approximately 5 million Michigan Pandora users, the minimum award would be $25 billion.[23] Similarly, California's Confidentiality of Medical Information Act includes a nominal damages clause of $1,000 per affected patient.[24] St. Joseph Health is currently facing multiple data breach lawsuits, one of them for $31.8 million because an alleged breach involved 31,800 California residents.[25]

Some federal laws also provide significant statutory damages. For example, the Telephone Consumer Protection Act of 1991 (TCPA)[26] traditionally used by plaintiffs to bringing ''junk fax'' class actions, has been reinvigorated in response to mobile text marketing. The TCPA provides a $500 per violation penalty (which can be trebled to $1,500 per violation), to which every customer who receives the offending text is entitled.[27] The U.S. Court of Appeals for the Ninth Circuit recently reversed a summary judgment finding for Best Buy LP in a TCPA class action, and the case was remanded for trial.[28] And, in another TCPA case, the U.S. District Court for the Northern District of California in February certified a class of 60,000 consumers against a life insurance company and a marketing firm that purportedly sent text messages to attract customers to the insurer.[29] These state and federal statutes and others like them provide all the incentive the plaintiffs' bar needs to pursue these types of actions.

And it seems certain that they will have opportunities to do so. According to Verizon's *2012 Data Breach Investigations Report*, hundreds of millions of records were breached in 2011.[30] Likewise, according to Navigant Consulting Inc.'s *Information Security & Data Breach Report June 2012 Update*, in the six-month period between October 2011 and June 2012, there were 122 reported breaches in the United States involving thousands of potentially exposed records.[31] And the Ponemon Institute's *Third Annual Benchmark Study on Patient Privacy & Data Security* found that 94 percent of health care organizations participating in the survey have had at least one data breach in the past two years.[32] Forty-five percent of those organizations have had more than five.

Federal and state laws that include statutory damages provide all the incentive the plaintiffs' bar needs to pursue class actions.

As individuals disclose and companies collect ever-increasing amounts of personal information, there will no doubt be more and more incidents in which personal information will be misused, mishandled, misappropriated, or otherwise compromised. And those breaches may generate privacy class actions.

Increased Government Oversight

Federal Government

As if increased litigation risk were not enough, it appears that both the federal and state governments are going to become more expansive in enforcing data privacy and security laws and regulations. The FTC trumpets its ''ongoing efforts to protect the security and confidentiality of consumers' sensitive health and financial information.''[33] And the FTC recently stated that it ''can and will take action to make sure that companies live up to the privacy promises they make to consumers.''[34]

The public record also suggests that the FTC's promised enforcement activity is well under way. Last year, the FTC aggressively pursued and reached settlement with companies that allegedly violated consumers' privacy. For example, Google Inc. agreed to pay $22.5 million to settle charges that it misrepresented privacy practices to Safari browser users.[35] Spokeo Inc. paid $800,000 to settle allegations that it violated the Fair Credit Reporting Act[36] by marketing consumer information for employee screening purposes.[37] In February, the FTC announced that Path Inc. has agreed to pay $800,000 to settle charges that its mobile social networking app collected personal information from children under 13 without parental consent.[38] And in finalizing its recent settlement with the FTC, Facebook Inc. promised that it would obtain consumer consent before sharing information beyond established privacy settings.[39]

---

[23] *See Deacon v. Pandora Media, Inc.*, No. C 11-04674 SBA, 2012 WL 4497796 (N.D. Cal. Sept. 28, 2012), *available at* http://op.bna.com/pl.nsf/r?Open=kjon-8yptc3 (11 PVLR 1498, 10/8/12).

[24] Cal. Civ. Code §§ 56.36.

[25] *See* Complaint at 10–12, *DeBaeke v. St. Joseph Health Sys.*, No. 2012-251417 (Cal. Super. Ct., Sonoma Cty. Apr. 2, 2012).

[26] 47 U.S.C. § 227 (2006).

[27] *Id.*

[28] *Chesbro*, 705 F.3d at 913.

[29] *Lee v. Stonebridge Life Ins. Co.*, No. C-11-0043-RS, 2013 WL 542854 (N.D. Cal Feb. 12, 2013), *available at* http://www.bloomberglaw.com/public/document/Lee_v_Stonebridge_Life_Insurance_Company_Docket_No_311cv00043_ND_ (12 PVLR 327, 2/25/13).

[30] Verizon, *2012 Data Breach Investigations Report* (October 2012), *available at* http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf.

[31] Navigant Consulting Inc., *Information Security & Data Breach Report June 2012 Update* (June 2012).

[32] Ponemon Institute, *Third Annual Benchmark Study on Patient Privacy & Data Security* (December 2012), *available at* http://lp.idexpertscorp.com/ponemon-2012/?gclid=CMb1_qrkhrQCFQ-f4AodJgoATQ (11 PVLR 1772, 12/10/12).

[33] Press Release, FTC, Cord Blood Bank Settles FTC Charges That It Failed to Protect Consumers' Sensitive Personal Information (Jan. 28, 2013), *available at* http://ftc.gov/opa/2013/01/cbr.shtm (12 PVLR 195, 2/4/13).

[34] *Id.*

[35] *United States v. Google Inc.*, No. CV-12-04177, 2012 WL 5833994 (N.D. Cal. Nov. 16, 2012), *available at* http://op.bna.com/pl.nsf/r?Open=kjon-927pey (11 PVLR 1727, 12/3/12).

[36] 15 U.S.C. §§ 1681–1681x.

[37] *United States v. Spokeo, Inc.* No. CV-12-05001, 2012 WL 3247483 (C.D. Cal. June 7, 2012), *available at* http://www.ftc.gov/os/caselist/1023163/120612spokeoorder.pdf (11 PVLR 955, 6/18/12).

[38] *United States v. Path, Inc.*, No. 13-cv-00448-RS, (N.D. Cal. Feb. 8, 2013), *available at* http://www.ftc.gov/os/caselist/1223158/130201pathincdo.pdf (12 PVLR 188, 2/4/13).

[39] *Facebook, Inc.*, No. 92-3184 (FTC July 27, 2012), *available at* http://www.ftc.gov/os/caselist/0923184/120810facebookdo.pdf (11 PVLR 1312, 8/20/12).

  PVLR ISSN 1538-3423

In addition to enforcement activity, the FTC has recently implemented significant policy initiatives addressing privacy issues. Late in 2012, the FTC released an updated Children's Online Privacy Protection Act Rule.[40] The new Rule increases the regulatory burdens on websites and online services directed to children under thirteen, making operators of those services strictly liable for the collection of under-13 children's personal information from their services, even by third-party ad networks and plug-in providers. On Feb. 1, the commission released a report containing recommendations for the mobile app industry.[41] Although the report does not impose new rules on industry, the FTC ''strongly encourages'' the mobile app industry to implement the report's recommendations.[42] And the FTC has ordered nine data brokers to provide details about how they collect, use and share consumer data.[43] The commission will use that information as the basis of a future report containing recommendations for the data broker industry.

Additionally, although it is beyond the scope of this article, the Department of Health and Human Services (HHS) dramatically rewrote how the Health Insurance Portability and Accountability Act (HIPAA) will be enforced, recently issuing omnibus HIPAA regulations which will require substantial operational changes for HIPAA-covered entities and their business associates.[44] These regulations made substantial changes to the data breach notification requirements and signaled a new era of HHS enforcement.

State Attorneys General

The federal government is not alone in increasing enforcement activity. Realizing the increasing scope and consumer demand for data security and privacy protection, state authorities have also increased their efforts at privacy enforcement. For example, the NAAG adopted ''Privacy in the Digital Age'' as a 2012–2013 initiative.[45] That initiative will focus on creating transparency in data collection and dissemination practices; empowering consumers with controls over data practices; ensuring that consumer are protected against data breaches; confronting financial privacy and mobile payment issues; and bringing attention to location privacy. And in 2012, California's attorney general established the Privacy Enforcement and Protection Unit, the mission of which is to enforce state and federal privacy laws; teach Californians how to control their personal information; promote smart online behavior; advise the attorney general on privacy issues; and offer best practice guidance to companies.[46] Shortly after the unit was established, the California Attorney General filed a high-profile complaint against Delta Air Lines Inc. for its alleged failure to attach a privacy policy to its mobile app.[47]

EU Activity

Moreover, this increased enforcement activity and regulation is not limited to the United States. Europe has been fertile ground for privacy developments. Recently, European regulators launched formal investigations into the privacy practices of Facebook, Google, and Microsoft Corp. The proposed EU General Data Protection Regulation—which is designed to replace the current patchwork of European data protection laws with a single set of laws governing the processing of personal data across the European Union—will likely create compliance issues for U.S. businesses that collect information about EU data subjects.[48] The regulation's jurisdiction may extend to entities that offer goods or services to or monitor the behavior of EU data subjects, even if the entities have no establishments in the European Union. EU data subjects could have the right to delete their data if there are no legitimate grounds for an entity to retain it. Consent to processing personal data would have to be informed and explicit. Data subjects would have the right to move their personal data to rival firms. And the regulation's strict rules on international transfers may prohibit transfers of personal data to the United States, even if those data are subject to discovery obligations and orders from courts in the United States. Violations of the regulation would subject organizations to fines of up to 2 percent of their global revenue.

What Can Companies Do?

The first step for companies to avoid privacy-related class actions and regulatory enforcement is nearly self-evident. First, they need to take stock of what personal information they collect, how they use it, with whom they share it, and how they secure it. Then, they must implement appropriate physical, administrative, and

[40] Children's Online Privacy Protection Rule; Final Rule, 78 Fed. Reg. 3971 (Jan. 17, 2013) (to be codified at 16 C.F.R. pt. 312), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-01-17/pdf/2012-31341.pdf (11 PVLR 1833, 12/24/12).

[41] FTC Staff, *Mobile Privacy Disclosures: Building Trust Through Transparency* (February 2013), *available at* http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf (12 PVLR 166, 2/4/13).

[42] *Id.* at 29.

[43] Press Release, FTC, FTC to Study Data Broker Industry's Collection and Use of Consumer Data (Dec. 18, 2012), *available at* http://www.ftc.gov/opa/2012/12/databrokers.shtm (11 PVLR 1845, 12/24/12).

[44] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 78 Fed. Reg. 5565 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts 160, 164), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf (12 PVLR 123, 1/28/13).

[45] Press Release, NAAG, New NAAG President Is Maryland Attorney General (June 22, 2012), *available at* http://www.naag.org/new-naag-president-is-maryland-attorney-general.php (11 PVLR 1122, 7/9/12).

[46] Press Release, Cal. Office of the Attorney Gen., Attorney General Kamala D. Harris Announces Privacy Enforcement and Protection Unit (July 19, 2012), *available at* http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-privacy-enforcement-and-protection (11 PVLR 1174, 7/23/12).

[47] Complaint, *People v. Delta Air Lines, Inc.*, No. CGC-12-526741 (Cal. Super. Ct. Dec. 6, 2012), *available at* http://op.bna.com/pl.nsf/r?Open=kjon-92rkaa (11 PVLR 1776, 12/10/12).

[48] European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (11 PVLR 178, 1/30/12).

technical protections for personal information. Workforces should be trained on and kept aware of the importance of privacy and security

But even with the best security and compliance program in place, an external agent's nefarious determination or an employee's misstep may result in the wrongful disclosure of personal information. That is why companies should take specific steps to mitigate the risks of, or reduce the liability in, privacy litigation and enforcement actions. Because the reasonableness of a security program is often a factor in both litigation and how regulatory agencies look at breaches and other data security and privacy issues, companies should implement comprehensive documentation of the steps they take to protect the personal data they hold. In addition, there are liability-limiting devices that are available in many circumstances: arbitration clauses in user agreements can minimize the risk that breaches will result in costly class actions; well drafted limitation-of-liability clauses can reduce or eliminate damages; and risk-shifting contractual provisions can allocate risk to third parties. In short, companies should prepare for the coming lawsuit before it is filed or investigation before it is initiated—coordinating their business practices with litigation counsel to ensure they can be best prepared to avoid liability.

These and other steps can significantly reduce a company's financial and reputational exposure. In light of the new reality of increased litigation risk and regulatory scrutiny, prudent companies should implement all available protections before they are served with a class action complaint or an access letter or civil investigative demand from a regulator

Most of all, businesses are well-advised to inform themselves of the evolving legal requirements for the collection, use, and safeguarding of personal information, especially highly regulated personal data like children's, financial, and health data.

Des Hogan is a Hogan Lovells partner whose practice focuses on high-stakes class action litigation and governmental investigations, including privacy-related litigation, investigations, and regulatory compliance matters. Michelle Kisloff, a partner in the firm's litigation and privacy practices, focuses on commercial litigation and investigations involving consumer protection and privacy, data breaches, directors' and officers' liability, and insurance matters. Christopher Wolf leads the Privacy and Information Management practice at Hogan Lovells and is founder and co-chair of the Future of Privacy Forum, a think tank focused on advancing privacy. James Denvil is an associate in the Privacy and Information Management group with experience handling issues involving electronic contracting and U.S. and EU privacy laws. All are based in the firm's Washington office.

Updates on developments in privacy and data security law are available at www.hldataprotection.com, the Hogan Lovells privacy blog.

  PVLR ISSN 1538-3423