THOMSON REUTERS

Westlaw®

Major cybersecurity and data privacy trends and issues to anticipate in 2018

By Natasha G. Kohne, Esq., and Diana Schaffner, Esq., *Akin, Gump, Strauss, Hauer & Feld* *

MARCH 19, 2018

This is set to be a benchmark year for cybersecurity and data privacy litigation and regulation in many ways, from the rollout of the European Union's General Data Protection Regulation to decisions by U.S. courts in several key cases.

Internationally, data privacy and security regulations will continue to develop with an emphasis on protecting each nation's own citizens. The year should also reveal how new U.S. and international laws will be interpreted.

As the year progresses, we should see how landmark laws such as the GDPR and the New York Department of Financial Services' cybersecurity regulation will impact businesses and the enforcement appetite of regulators.

We expect 2018 to be no less active than prior years with respect to court activity, regulatory enforcement, and the continuing development and clarification of legislation.

ATTORNEY-CLIENT PRIVILEGE, WORK PRODUCT PROTECTION

We expect U.S. courts to continue to grapple with the applicability of the attorney-client privilege and work product protection in the context of a cyberincident. Recent case law generally supports the theory that privilege protections exist within certain parameters so long as outside counsel and companies carefully structure the retention of forensic firms and take other precautionary actions.

In *In re Experian Data Breach Litigation*, No. 15-cv-1592, 2017 WL 4325583 (C.D. Cal. May 18, 2017), a California federal judge held that the work product doctrine protected a report produced by a forensic firm that was engaged by outside counsel in anticipation of litigation.

The plaintiffs argued that the report in question was not work product because Experian had independent business duties to investigate, unrelated to litigation. The court disagreed.

Overall, the evidence showed that outside counsel instructed the forensic firm and, but for the anticipated litigation, the report would not have been prepared in the same manner or had the same content.

The court weighed factors including the timing of the retention of the forensic firm and supportive evidence in the engagement letter. It rejected the plaintiffs' claim that they had a "substantial need" for the report that justified disclosure, finding that the materials the forensic firm relied upon could be sought in discovery.

In October the U.S. District Court for the District of Oregon reached a different conclusion and ordered Premera Blue Cross to produce a range of post-breach materials that were initially withheld as privileged or protected. *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, No. 15-md-2633, 2017 WL 4857596 (D. Or. Oct. 27, 2017).

Premera first engaged a forensic firm to assist in investigating its systems generally. Only after the forensic firm suspected a potential cyberincident did Premera hire outside counsel and amend the engagement letter to have counsel supervise the investigation. No amendments were made to the preexisting scope of the engagement.

> This year looks poised to continue a trend in which local governments seek to expand the reach of their cybersecurity and privacy statutes beyond strict geographic limitations.

The court rejected Premera's claim that documents prepared at the direction of counsel or that incorporated the advice of counsel, but were not prepared by or sent to counsel, were automatically covered by the attorney-client privilege or work product doctrine.

With regard to documents related to the forensic firm's work, the court concluded that the materials were not covered by the work product doctrine because the forensic firm was engaged by Premera before litigation was anticipated and the scope of the engagement was never amended.

In January, in denying a petition for a writ of mandamus to vacate two prior district court decisions, the 6th U.S. Circuit Court of Appeals concluded that United Shore Financial Services implicitly waived any privilege protection over documents prepared by a forensic firm retained by outside counsel when it included the report's conclusions in discovery responses. *In re United Shore Fin.*

Servs. LLC, No. 17-2290, *petition for mandamus denied* (6th Cir. Jan. 3, 2018).

The court noted that United Shore initially disclosed some of the report's conclusions in support of its affirmative defense in discovery that sought to shift liability to its vendor. Citing attorney-client privilege, United Shore then withheld the report and related documents.

The 6th Circuit condemned United Shore's attempt to use privilege as both a shield and sword.

The following steps may help limit the inadvertent waiver of privilege or protection in the context of a cyberincident:

- Involve counsel in any breach investigation from the outset. Direct communications related to reports and the investigation through counsel.
- Outside counsel should directly engage any forensic firms. Engagement letters should be clear that the work is intended to assist counsel in providing legal advice.
- If the forensic firm was previously engaged by the company, be sure to update the scope of the agreement to reflect the new purpose and goals of the investigation.
- Limit any disclosures related to the investigation to facts alone.
- Anticipate plaintiffs' potential use of a "substantial need" argument. Preserve potential source materials that can later be produced instead of providing a forensic firm's work product.

KEY DEVELOPMENTS IN CONSUMER PRIVACY LITIGATION

We have seen a steady growth of activity among consumers and individuals seeking to enforce individual privacy rights both in cases related to data breaches and in cases alleging general misuse of data.

Two developments in the U.S. and the EU will continue to shape — and in the case of the EU likely increase — consumer-focused data privacy litigation moving forward.

Circuit split regarding harm, standing in data breach cases

Since the ruling in *Spokeo Inc. v. Robins*, 136 U.S. 1540 (2016), federal courts have struggled to implement the Supreme Court's holding in the data breach context that, in order to have Article III standing, a plaintiff must show an injury in fact that is fairly traceable to the defendant's conduct and that is concrete and particularized.

In the context of data breach claims, decisions out of the 3rd, 6th, 7th, 9th and D.C. circuits could be interpreted to suggest that victims of a data breach have suffered a concrete harm if certain types of personal data is stolen (i.e., through increased risk of identity theft).

In contrast, the 2nd, 4th and 8th circuits suggest that more harm is required — such as proof of fraudulent charges to a credit card — particularly if time has passed between the breach and the case filing.

The Supreme Court recently denied review in a case that would have offered the opportunity to reconsider its approach to harm in this context, but other opportunities for the high court to review its approach are likely to arise.[1]

Potential spread of class-action-type privacy cases to the EU

Article 80 of the GDPR includes a provision that permits individual data subjects to mandate a not-for-profit consumer protection body to exercise rights and bring claims on their behalf. This right empowers privacy rights groups and others to bring claims on behalf of many data subjects at once.

States are collaborating both on cases and enforcement actions, as well as policy measures with regard to cybersecurity and data privacy.

Max Schrems, an Austrian privacy activist who successfully attacked the safe harbor agreement, recently founded a group called NYOB (none of your business), which is set to go into action the day the GDPR takes effect. The goal of NYOB is to collectively enforce data protection and privacy laws. Schrems raised 59,222 euros (about $73,000) within his first 24 hours of fundraising.

Federal regulators continue work, with more focused enforcement

We expect a sharper and more select focus on enforcement in 2018 as some federal government agencies restructure how they tackle cybersecurity and data privacy issues. These reorganization efforts are partially reflected in President Donald Trump's proposed fiscal year 2019 budget, which seeks to shift spending in accordance with administration goals.

The Commodity Futures Trading Commission has shown a renewed interest in cybersecurity and data privacy issues in 2018, after issuing rules and guidance that went into effect in 2016.

Little concrete enforcement was seen in this area until Feb. 12, when the CFTC announced it had settled charges against a registered futures commission merchant for a failure to diligently supervise the implementation of key provisions in its information systems security program that enabled a third party to access and copy customer information.[2] The settlement imposed a $100,000 fine and reporting requirements.

Energy Secretary Rick Perry recently announced the establishment of a new Office of Cybersecurity, Energy

Security and Emergency Response within the Energy Department. Trump's proposed fiscal year 2019 budget requested $96 million in funding for the project.

The new office will focus on protecting infrastructure from cyberattacks and foreign attacks. It will also help to protect critical energy infrastructure from natural threats.

The past year witnessed a dramatic reset in relations between the Federal Communications Commission and the Federal Trade Commission in terms of each agency's role in policing privacy and data security issues, particularly with regard to broadband internet service providers.

In 2015 the FCC reclassified broadband internet access service as a common carrier service (removing ISPs from the FTC's reach), adopted net neutrality rules and settled multiple enforcement actions. In 2016 the FCC passed groundbreaking privacy rules. These actions were reversed beginning in 2017.

In April 2017 Trump signed legislation repealing the 2016 privacy rules. The FCC and FTC later signed a memorandum of understanding regarding division of labor between the two that tasked the FTC with privacy oversight.

In January the FCC repealed its net neutrality order and its 2015 determination that broadband internet service access is a common carrier service. This action effectively restored the FTC's authority over ISPs.

After operating with just two commissioners (out of five) since February 2017, the FTC is set to be at full capacity should the Senate confirm Trump's four recent nominees, as expected.

The effect of these members on the FTC remains to be seen. Only one of the nominees has a consumer advocacy background. There is some suggestion that the agency will begin to focus more on antitrust issues because the nominee for chairman is an antitrust attorney.

The Securities and Exchange Commission continues to make cybersecurity compliance a priority, although the pace of its data security enforcement actions did slow down for some time.

In August 2017 the SEC explicitly indicated that cybersecurity compliance procedures and controls would be a focus of agency examinations . Cybersecurity is one of the SEC's top examination priorities for 2018, and covered areas include risk assessments, access rights and controls, vendor management, and incident response and training.

In addition to its examination priorities, the SEC has also shown an interest in matters related to cryptocurrencies, including initial coin offerings. On Feb. 21 the agency issued interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents.

The guidance indicates, among other things, that companies should reveal to investors cybersecurity risks even if they have not yet been the target of a cyberattack. It also says company executives must not trade in a company's securities if they possess nonpublic information regarding cyberincidents.

LOCAL REGULATIONS, INCREASED DATA LOCALIZATION

This year looks poised to continue a trend in which local governments seek to expand the reach of their cybersecurity and privacy statutes beyond strict geographic limitations. National governments are increasingly willing to regulate data (wherever it is stored) to the extent it is interpreted as affecting local residents or markets.

Navigating this maze requires an understanding of what data your company collects, about whom it collects that data and where it stores that data.

Microsoft decision, reach of U.S. law enforcement

The Supreme Court heard oral arguments Feb. 27 in a key privacy case. The issue in the case is whether the U.S. government can compel Microsoft, through use of a U.S. subpoena under the federal Stored Communications Act, to produce data stored in servers located in Ireland.

The Justice Department sought Supreme Court review after the 2nd U.S. Circuit Court of Appeals concluded that the SCA does not apply extraterritorially. *United States v. Microsoft*, 829 F.3d 197 (2d Cir. 2016).

The decision in this case could greatly expand the U.S. government's ability to seek information on a global scale.

Brazilian court upholds law enforcement's access to data stored in U.S.

A case raising similar issues to those raised in the Microsoft action appears to have been recently decided by the Brazilian Superior Court of Justice. On Feb. 7 the court purportedly ordered Yahoo Inc.'s Brazilian unit to either give to a Brazilian criminal court customer emails stored on Yahoo servers located in the U.S. or face daily fines of $15,000.

Yahoo Brazil had apparently refused to comply on the ground that the emails were stored in servers in the U.S. and could be provided only by its U.S. parent company. The decision may be a foretaste of similar cases to come granting local law enforcement greater access to data.

Implementation of the GDPR, reach of EU regulators

The GDPR, which is set to go into effect in May, applies to data controllers and processors both inside and outside the EU when they process data from individuals in the EU for specific goals.[3] It considers both the location of data (it applies to all data in the EU) and the location of the individual whose data is being processed (it applies when EU residents' data is affected).

Non-EU organizations can fall within the scope of the GDPR by offering goods or services to individuals in the EU or by monitoring the behavior of individuals within the EU market. It remains to be seen just how far the EU will push the bounds of its jurisdiction under the GDPR.

Data localization, government access requirements in China

China's cybersecurity law forces network operators and businesses in critical sectors to store within mainland China data that is gathered or produced by the network operator in China.

It also requires that business information and data on Chinese citizens gathered in China be stored domestically and prohibits its transfer abroad without permission.[4] How broadly the Chinese government will seek to apply the law's provisions remains to be seen.

States remain active, may step up to counterbalance federal activity

Some state regulators and attorneys general remained active in 2017 with regard to promoting new legislation and regulations and pursuing enforcement actions and cases connected with cybersecurity and data privacy issues. We expect this level of engagement to continue in 2018.

It is not yet clear whether states will move to counterbalance federal activity as some federal regulators narrow their enforcement focus and reorganize.

NYDFS cybersecurity regulation

The majority of the provisions of the New York Department of Financial Services' first-of-its-kind cybersecurity regulation went into effect March 1, 2017. Additional provisions take effect this year, and full compliance is required by March 1, 2019.

The regulation covers all entities regulated by the NYDFS. It is fast becoming the standard by which some companies may be judged in terms of best practices for cybersecurity and privacy issues. Given its history of active enforcement, the NYDFS may begin to flex its muscles with regard to enforcement of the regulation in 2018.

Companies that fall within one of the regulation's three limited exemptions should keep in mind that those exemptions apply only to certain provisions and not the entire regulation.

Collaboration between states

States are collaborating on cases, enforcement actions and policy measures with regard to cybersecurity and data privacy. In 2017 numerous states collaborated to settle cases related to major data breaches affecting citizens of multiple states, including via joint settlements concerning the Target, Nationwide and Lenovo breaches. This trend will likely continue in 2018.

There is also collaboration with regard to wider policy. For example, 38 state governors signed a compact in 2017 and pledged to make cybersecurity a top priority.5 The effort was led by then-Virginia Gov. Terry McAuliffe, a Democrat, who has called on states to take a more active leadership role in the face of federal inaction.

New and updated state data breach laws

States have continued to adopt new data breach notification laws and revise existing ones. In 2017 New Mexico became the 48th state to pass a similar law. The only states without such laws — South Dakota and Alabama — both have legislation pending.[6]

Multiple states also updated notification laws in 2017 or are considering doing so. Delaware, like several other states, now requires entities conducting business in the state to implement reasonable security measures to safeguard protected information.

Some states expanded their definitions of personally identifiable information to include, among other things, biometric information.

CONCLUSION

2018 is likely to be an active year in the evolution of cybersecurity and data privacy law. As new legislation takes effect, judicial interpretation should help us improve compliance and readiness and mitigate risks.

NOTES

[1] *Attias v. CareFirst Inc.*, 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, 2018 WL 942459 (U.S. Feb. 20, 2018).

[2] Press Release, U.S. Commodity Futures Trading Comm'n, CFTC Orders AMP Global Clearing LLC to Pay $100,000 for Supervision Failures Related to Cybersecurity of its Customers' Records and Information (Feb. 12, 2018), http://bit.ly/2FXWeEs.

[3] *See* Council Regulation 2016/679, arts. 4 & 6, 2016 O.J. (L119) 11.

[4] *See* Network Security Law (P.R.C.) (adopted Nov. 7, 2016, effective as of June 1, 2017), Art. 37.

[5] *See* Nat'l Governors Ass'n, A Compact to Improve State Cybersecurity, http://bit.ly/2Du70Np.

[6] *See* S.B. 318, 2018 Reg. Sess. (Ala. 2018), H.B. 410, 2018 Reg. Sess. (Ala. 2018); S.B. 62, Leg. Assemb., 93d Sess. (S.D. 2018).

This article first appeared in the March 19, 2018, edition of Westlaw Journal Corporate Officers and Directors.

ABOUT THE AUTHORS

Natasha G. Kohne (L) serves as a co-leader of **Akin, Gump, Strauss, Hauer & Feld**'s cybersecurity, privacy and data protection practice, which was named among the top cybersecurity practices in 2017 by BTI Consulting. She splits her time between the firm's San Francisco and Abu Dhabi offices and serves on the firm's management and innovation committees. Kohne's practice also focuses on investigations, litigation and international arbitration often involving complex multijurisdictional and international problems. **Diana Schaffner** (R) s a counsel in the firm's litigation practice in the San Francisco office. She focuses on complex commercial litigation and business disputes involving a variety of issues on behalf of clients in the insurance, financial services and energy industries. She also counsels clients on regulatory matters and provides representation in government investigations and enforcement actions. A member of the firm's cybersecurity and data privacy practice, Schaffner advises on related compliance matters and litigation.

Thomson Reuters develops and delivers intelligent information and solutions for professionals, connecting and empowering global markets. We enable professionals to make the decisions that matter most, all powered by the world's most trusted news organization.