ALERT MEMORANDUM

Cybersecurity and Data Privacy Developments: A Look Back on 2017, and Ahead to 2018

January 18, 2018

Over the last year, the existential risk posed by cyberattacks and data security vulnerabilities has become one of the top concerns for boards of directors, management, government agencies, and the public. 2017 was punctuated by a series of headline-grabbing breaches affecting scores of companies and hundreds of millions of individuals. At the same time, there were fast-moving changes in the regulatory landscape as regulators across the globe tried to respond to the systemic threats and protect their constituents, while not imposing crippling costs on businesses. Of particular note, the New York Department of Financial Services ("DFS") cybersecurity regulations went into effect in 2017 and many companies spent significant resources preparing for the implementation of the European Union's General Data Protection Regulation ("GDPR"), which goes into effect in May 2018. There were also other important legal developments, including record-breaking civil and regulatory settlements by companies that had suffered major breaches, while U.S. courts have been grappling with unique standing and privilege issues raised in the context of cyber-related litigation.

This memo surveys some of the key cybersecurity and data privacy developments of 2017, including the major data breaches and cyberattacks, regulatory and legislative actions, and notable settlements and court decisions, with an eye towards what may be in store in 2018.

For additional insights and updates relating to cybersecurity and data privacy, please visit and subscribe to the Cleary Cybersecurity and Privacy Watch blog.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors.

NEW YORK

Jonathan Kolodner
+1 212 225 2690
jkolodner@cgsh.com

Daniel Ilan
+1 212 225 2415
dilan@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

NEW YORK
One Liberty Plaza
New York, NY 10006-1470
T: +1 212 225 2000
F: +1 212 225 3999

Major Cyberattacks and Big Settlements in 2017: The New Norm?

2017 will likely be remembered as the year that the worst-case cyberattacks, which experts have been warning about for several years, came closer to reality than ever before. These mega-attacks drove the conversation among cybersecurity experts and were looming in the background of actions taken by the private sector, regulators, and courts. Some of the year's more notable incidents included:

— The WannaCry and Petya ransomware attacks, which affected hundreds of thousands of computers in over 150 countries, blocking user access to data systems unless users made ransom payments. The attacks disrupted thousands of businesses and government services worldwide, including, perhaps most unnervingly, large portions of the National Health Service ("NHS") in England.

— The Equifax breach, in which approximately 145.5 million U.S. consumers—over 40% of the country—had their personal identifying information compromised. In the wake of the breach, Equifax saw its stock drop more than 30% and lost more than $5 billion in its market cap. The company also faced Congressional hearings, federal and state investigations, and dozens of consumer and shareholder class actions, and it suffered enormous reputational harm as a result.[1]

— The same month that the Equifax breach was announced, the SEC—which has been pushing regulated entities to address cybersecurity risk—announced that its own EDGAR filing system had been breached, potentially leading to the exposure of securities data and illicit gain through insider trading.[2]

— Finally, in November, Uber announced that hackers had stolen personal information of 57 million drivers and passengers worldwide in October 2016. Uber further disclosed that it had paid the hackers to delete the data instead of disclosing the breach to the affected individuals and regulators. Uber is now facing several investigations in the U.S. and Europe, as well as sprawling class action litigation.[3]

Other major breach announcements in 2017 included Verizon, Yahoo!, K-Mart, and Whole Foods, among others. If one can make any safe predictions for 2018, it is that this trend of serial breaches will unfortunately continue and even potentially accelerate.

In addition to the data breaches that took place last year, earlier data breaches continued to make waves in 2017, as companies reached substantial settlements with private litigants and government authorities:

— Anthem Inc. agreed to pay $115 million to settle consumer class action claims over a 2015 cyberattack, which compromised data affecting 78.8 million people, in the largest data breach settlement to date.[4] If the proposed settlement is approved by the court, Anthem will be required to implement changes to its data security practices for a period of three years, including annual assessments of IT security risks to be conducted by an outside party, mandatory training for all associates, and minimum annual expenditures to be designated for information security.

— Home Depot agreed to pay $25 million to resolve a putative class action brought by financial institutions relating to its 2014 data breach (on top

[1] For Cleary Gottlieb's previous blog post discussing agencies that initiated probes into the Equifax breach in the immediate wake of its announcement, see https://www.clearycyberwatch.com/2017/09/multiple-agencies-announce-probes-equifax-breach/.

[2] For Cleary Gottlieb's previous blog post discussing the EDGAR breach, see https://www.clearycyberwatch.com/2017/09/sec-issues-statement-following-cyberbreach-edgar-systems/.

[3] For Cleary Gottlieb's previous blog post discussing the regulatory responses to the Uber breach in the U.S. and EU, see https://www.clearycyberwatch.com/2017/12/eu-u-s-regulators-respond-uber-breach/.

[4] *In re Anthem, Inc. Data Breach Litig.*, No. 5:15-md-02617-LHK (N.D. Cal. filed June 12, 2015).

of the almost $20 million that Home Depot agreed to pay to consumers based on the same incident). The settlement also requires Home Depot to implement enhanced data security measures to protect against a future breach, including safeguards to manage risks identified through a risk exception process involving Home Depot's leadership, use of vendors capable of maintaining adequate security practices, and adoption of an industry recognized security control framework.[5]

— Target reached an $18.5 million settlement with the Attorneys General of 47 states and the District of Columbia, resolving their investigation into Target's 2013 data breach and bringing the total amount paid by Target to settle legal claims arising out of the breach to over $130 million, including claims brought by private litigants.[6] The settlement further requires Target to adopt comprehensive data security measures, including enhanced data encryption, two-factor authentication, data segmentation policies, the appointment of an executive to oversee information security, and the hiring of outside consultants to conduct security assessments.

— The owner of the Ashley Madison website agreed to pay $11.2 million to settle U.S. litigation brought on behalf of roughly 37 million users whose personal details were exposed in a July 2015 data breach.[7] Although the settlement agreement does not impose obligatory cybersecurity measures, it details the changes and actions taken in response to the data breach, including, for example, a comprehensive third party review of the website's data protections, implementation of an enhanced information security program, creation of a Chief Information Security Officer position, and enhanced mandatory security training for employees.

— Nationwide Mutual Insurance Co. ("Nationwide") agreed to a $5.5 million settlement with the Attorneys General of 32 states and the District of Columbia in connection with a 2012 data breach that exposed the personal information of over 1.2 million individuals. As part of the settlement, Nationwide agreed to take steps to strengthen its security practices in the next three years, including by updating its policies and procedures related to maintaining and storing personal data, conducting regular inventories of its systems used to maintain personal information, performing internal assessments, and hiring an outside independent provider to perform an annual audit of its practices.

While these settlements were significantly larger than those in prior years, the litigation growing out of the massive breaches that took place in 2017 is likely to eclipse these settlements both in terms of dollar value and the additional data security requirements imposed on the companies that were breached.

U.S. Regulators Make Their Mark

2017 was also the year that the first comprehensive cybersecurity regulations made their debut.

The DFS cybersecurity regulations went into effect on March 1, 2017. Among other things, the regulations require institutions regulated by DFS to maintain a cybersecurity program, design an incident response plan, appoint a Chief Information Security Officer, conduct risk and vulnerability assessments, employ appropriate encryption, and certify compliance on an annual basis. Compliance with several of the requirements was mandated by August 2017 and there are additional upcoming transition deadlines for several other requirements in March 2018, September 2018, and March 2019.[8] In addition to being mandatory for covered entities, the DFS regulations

[5] *In re The Home Depot, Inc., Customer Data Sec. Breach Litig.*, No. 1:14-md-02583-TWT (N.D. Ga. Sept. 22, 2017).
[6] For Cleary Gottlieb's Alert Memorandum discussing the Target settlement, see https://www.clearygottlieb.com/~/media/organize-archive/cgsh/files/2017/publications/alert-memos/recent-developments-highlight-measures-to-mitigate-litigation-and-regulatory-exposure-from-cyberattacks.pdf.
[7] *In re Ashley Madison Customer Data Sec. Breach Litig.*, No. 4:15-md-02669-JAR (E.D. Mo. filed Dec. 9, 2015).
[8] For Cleary Gottlieb's Alert Memorandum discussing the DFS regulations and transition periods, see

have quickly become a reference point for other regulators and private entities in determining best practices in managing cybersecurity risk.

Other U.S. and state regulators were also active on the cybersecurity front in 2017:

— Following the announcement of its own data breach in September, the SEC announced the creation of the Cyber Unit in its Enforcement Division, which will target cyber-related misconduct and filed its first enforcement action in December.[9] In addition, the SEC's Director of Corporation Finance announced in November that companies will receive new guidelines for disclosing cybersecurity risk and breaches to investors, updating the existing guidelines, which were issued in October 2011.[10]

— At the Congressional level, the House and Senate have introduced numerous bills in response to the recent data breaches. For example, the Active Cyber Defense Certainty Act was proposed to protect and empower private actors to use certain offensive and defensive measures against cyber intrusions.[11] Other proposals include the Cyber Breach Notification Act of 2017[12] and the Data Security and Breach Notification Act,[13] proposed by the House and Senate respectively, to establish nationwide notification requirements in the event of a breach (as opposed to the current hodgepodge of state laws), as well as the House and Senate versions of the Cyber Shield Act of 2017, which aim to establish a program to identify and promote cybersecurity standards for internet-connected products.[14]

— At the U.S. state level, at least 30 states proposed or considered cybersecurity legislation in 2017.[15] Delaware, for example, enacted legislation in August, requiring companies to comply with additional data security obligations if they do business in Delaware or maintain personal information on Delaware residents.[16] In November, New York State Attorney General Eric T. Schneiderman proposed stricter data security legislation through the Stop Hacks and Improve Electronic Data Security ("SHIELD") Act, which would (1) require all companies holding sensitive data of New York residents to implement protective measures, whether or not the companies do business in New York, (2) broaden the information covered as compared with current New York state law, and (3) increase potential penalties for failure to comply.[17] Further, in response to the Equifax breach, Governor Cuomo proposed a regulation that would extend the DFS's

https://www.clearygottlieb.com/-/media/organize-archive/cgsh/files/2017/publications/alert-memos/nydfs-cybersecurity-regulations-take-effect-8-21-17.pdf.

[9] For Cleary Gottlieb's previous blog post discussing the charges, see https://www.clearycyberwatch.com/2017/12/newly-created-sec-cyber-unit-takes-first-action-allegedly-fraudulent-ico/.

[10] Ezequiel Minaya, *SEC Says Companies Can Expect New Guidelines on Reporting Cybersecurity Breaches*, Wall St. J. (Nov. 9, 2017, 5:40 PM), https://www.wsj.com/articles/sec-says-companies-can-expect-new-guidelines-on-reporting-cybersecurity-breaches-1510267201.

[11] For Cleary Gottlieb's previous blog post discussing the Active Cyber Defense Certainty Act, see https://www.clearycyberwatch.com/2017/11/active-cyber-defense-act-congress-considers-authorizing-companies-use-offensive-measures-cybercriminals/.

[12] H.R. 3975, 115th Cong. (2017).

[13] For Cleary Gottlieb's previous blog post discussing the Data Security and Breach Notification Act, see https://www.clearycyberwatch.com/2018/01/2018-brings-continued-calls-federal-data-protection-breach-statute/.

[14] H.R. 4163, 115th Cong. (2017); S. 2020, 115th Cong. (2017).

[15] National Conference of State Legislatures, *2017 Security Breach Legislation* (Oct. 16, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/2017-security-breach-legislation.aspx.

[16] For Cleary Gottlieb's previous blog post discussing the Delaware legislation, see https://www.clearycyberwatch.com/2017/08/delaware-strengthens-cyber-breach-obligations/.

[17] For Cleary Gottlieb's previous blog post discussing the SHIELD Act, see https://www.clearycyberwatch.com/2017/11/wake-equifax-breach-new-yorks-attorney-general-proposes-new-stricter-data-privacy-law/.

coverage to credit reporting agencies, in addition to financial institutions and insurance companies.[18]

Developments Outside of the U.S.: The GDPR and Other New Cybersecurity Regulations

Companies within and outside of the EU spent 2017 preparing for the new data security and privacy rules under the GDPR, which becomes effective on May 25, 2018. As we have previously discussed,[19] the GDPR imposes strict and far-reaching data protection and breach notification obligations, and grants broad enforcement powers to supervisory authorities. Regulated entities—which include those that operate both within and outside of the EU to the extent they process EU citizen data—are subject to potentially staggering fines, up to 4% of global revenue.

Throughout 2017, the Article 29 Working Party (an advisory group consisting of representatives from EU national data protection authorities together with the European Commission) published waves of guidance for implementing the GDPR, including on risk assessments, administrative fines, the use of profiling and automated decision-making, and data breach notifications.[20] In addition, the European Commission issued guidance in September for implementation of the Network and Information Security Directive ("NISD"),[21] which will operate in parallel with the GDPR to govern certain "operators of essential services" and "digital service providers," and requires compliance by May 9, 2018.[22]

Outside of the EU, countries across the globe also ramped up their cybersecurity regulations in the face of ongoing challenges, many of which set deadlines for compliance and implementation in 2018. Some notable examples include the following:

— China's Cybersecurity Law ("CCL")[23] took effect on June 1, 2017, and aims to protect Chinese "cyberspace sovereignty" and ensure network security within China by imposing comprehensive obligations on "network operators." Both domestic and foreign companies are covered by the CCL, so long as they operate or use networks to provide services to customers in China, and have until December 31, 2018 to ensure compliance with cross-border data flow requirements. In addition, the Cyberspace Administration of China ("CAC") issued several regulations in 2017 to implement the CCL.[24]

— Russia passed additional cybersecurity legislation in 2017, including legislation prohibiting the use

[18] For Cleary Gottlieb's previous blog post discussing Governor Cuomo's proposal, see https://www.clearycyberwatch.com/2017/09/ny-governor-seeks-regulate-credit-reporting-agencies-following-equifax-breach/.

[19] For Cleary Gottlieb's previous Alert Memoranda discussing the GDPR, see https://www.clearygottlieb.com/-/media/organize-archive/cgsh/files/publication-pdfs/alert-memos/alert-memo-pdf-version-201650.pdf and https://www.clearygottlieb.com/-/media/organize-archive/cgsh/files/publication-pdfs/alert-memos/2017/cybersecurity-in-the-eu--the-new-regime-under-the-gdpr-and-nisd-5-5-17.pdf.

[20] For Cleary Gottlieb's previous blog posts discussing the Working Party's guidance to the GDPR, see https://www.clearycyberwatch.com/2017/11/preparing-gdpr-guidance-article-29-working-party/ and https://www.clearycyberwatch.com/2017/12/administrative-fines-gdpr/.

[21] Eur. Comm'n Corrigendum, Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (Oct. 4, 2017), https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-476-F1-EN-MAIN-PART-1.PDF.

[22] For Cleary Gottlieb's Alert Memorandum discussing the GDPR and NISD, see https://www.clearygottlieb.com/~/media/organize-archive/cgsh/files/publication-pdfs/alert-memos/2017/cybersecurity-in-the-eu--the-new-regime-under-the-gdpr-and-nisd-5-5-17.pdf.

[23] PRC Cybersecurity Law (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017) China L. & Prac., Jan. 19, 2017.

[24] For Cleary Gottlieb's Alert Memorandum discussing the CCL and CAC's regulations, see https://www.clearygottlieb.com/~/media/organize-archive/cgsh/files/2017/publications/alert-memos/understanding-the-impact-of-chinas-far-reaching-new-cybersecurity-law-10-5-17.pdf.

of internet proxy servers, banning certain websites, and imposing obligations on internet service providers and operators to cooperate with the government in blocking access to those websites.[25] In addition, the recent legislation bans the use of anonymous instant messaging, requiring instant messaging services to identify users by their subscriber numbers.[26] Certain Russian organizations and individuals are also required to notify the government of any cyberattacks, to cooperate in the government's cybersecurity efforts, and to implement protective measures.[27]

— The Hong Kong Securities and Futures Commission ("SFC") issued Guidelines for Reducing and Mitigating Hacking Risks Associated With Internet Trading ("Guidelines")[28] in October, requiring the implementation of baseline cybersecurity measures for all persons licensed or registered with the SFC and engaged in internet trading. On the same day, the Hong Kong Monetary Authority ("HKMA") issued a letter[29] to all registered institutions, directing them to implement the requirements set forth in the Guidelines.[30]

— Several Latin American countries also took steps this year to bolster their data protection laws. For example, in early 2017, the Argentine Data Protection Authority ("DPA") proposed a draft law heavily based on the GDPR,[31] Mexico published a law setting forth general principles and procedures for the protection of personal data held by government and other public entities,[32] and the Chilean government considered draft legislation that would introduce new data privacy principles and establish new requirements for use of sensitive data, international data transfers, data security, and notification in the event of a breach.[33]

These are just some examples of the global explosion of cybersecurity and data privacy laws and regulations. This trend will no doubt continue in 2018 and companies will increasingly find themselves navigating overlapping—and, at times, potentially conflicting—data security, breach notification, and privacy obligations in multiple jurisdictions.

[25] Federal Law No. 276-FZ of July 29, 2017, "On Amendments to the Federal Law on Information, Information Technologies, and Information Protection."
[26] Federal Law No. 241-FZ of July 29, 2017, "On Amendments to Articles 10(1) and 15(4) of the Federal Law on Information, Information Technology and Information Protection."
[27] Federal Law No. 187-FZ of July 26, 2017, "On Security of Critical Information Infrastructure of the Russian Federation."
[28] H.K. Sec. and Futures Comm'n Circular, Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading (Oct. 27, 2017), http://www.sfc.hk/web/EN/assets/components/codes/files-current/web/guidelines/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading.pdf.
[29] H.K. Monetary Auth. Circular, Security Controls for Internet Trading Services (Oct. 27, 2017), http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2017/20171027e1.pdf.
[30] For Cleary Gottlieb's Alert Memorandum discussing the SFC and HKMA's guidelines, see https://www.clearygottlieb.com/~/media/organize-archive/cgsh/files/2017/publications/alert-memos/hong-kong-sfc-and-hkma-issue-new-guidelines-for-reducing-and-mitigating-hacking-risks.pdf.
[31] Dirección Nacional de Protección de Datos Personales, Anteproyecto de la Ley de Protección de los Datos Personales ("Draft Law on the Protection of Personal Data") (May 17, 2017), http://www.jus.gob.ar/media/3223892/anteproyecto_mayo2017.pdf.
[32] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados ("General Law on the Protection of Personal Data Held by Obligated Parties"), Diario Oficial de la Federación [DOF] 26-01-2017.
[33] Camara de Diputados de Chile, Boletín No. 11144-07, Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales ("Regulates the Protection and Treatment of Personal Data and Creates the Data Protection Agency") (March 15, 2017), https://www.camara.cl/pley/pley_detalle.aspx?prmID=11661&prmBoletin=11144-07.

Court Decisions

Courts also shaped the cybersecurity legal landscape in 2017, setting important parameters for future actions by private litigants, as well as government agencies.

— *Privilege and Attorney Work-Product.* The application of the attorney-client privilege and work-product doctrines in the context of a company's response to a data breach has been a hotly contested issue. Earlier this year, two U.S. district court decisions highlighted how actions taken in response to a data breach may have significant consequences for litigation down the road. First, in a consumer class action following a breach at a health insurance company, a federal judge in Oregon ordered the production of certain remediation-related documents created by the company's forensic firm in response to the breach, finding that the documents were created for a business purpose, rather than to obtain legal advice or in anticipation of litigation, and therefore, were not protected by privilege or work-product protections.[34] In contrast, a California federal judge found in the Experian data breach litigation that an investigation report and related documents created by a forensic firm, hired by outside counsel in response to a data breach, were protected under the work-product doctrine, on the basis that the forensic firm conducted the investigation and prepared the report for outside counsel in anticipation of litigation.[35] The application of the attorney-client privilege and work-product protections will continue to be of utmost concern to companies that suffer breaches as post-breach litigation continues to proliferate.

— *Standing.* As circuit courts have continued to grapple with the application of the Supreme Court's decision in *Spokeo v. Robins*[36] to the data breach and privacy contexts, a circuit split emerged in 2017 regarding the "concrete injury" requirement to confer standing to sue. The D.C. and Third Circuits joined the majority of circuit courts to rule on this issue, holding that a showing of *potential* harm following a data breach can meet the requirements for standing.[37] In contrast, the Second, Fourth, and Eighth Circuits held that a substantial risk of future injury was not sufficient to confer standing in data breach cases.[38] In addition, the Second Circuit issued a string of decisions in 2017, holding that technical statutory violations alone were insufficient to confer standing,[39] whereas the Ninth Circuit decided on remand from the Supreme Court in *Spokeo* that the statutory violation at issue was sufficient.[40] Heading into 2018, the split shows no signs of abating, absent intervention by the Supreme Court.

— *FTC Jurisdiction.* Meanwhile in the regulatory context, the Eleventh Circuit heard oral argument in June regarding the FTC's enforcement authority under Section 5(n) of the Federal Trade Commission Act ("FTCA"), centering on whether

[34] *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, No. 3:15-md-2633-SI, 2017 WL 4857596 (D. Or. Oct. 27, 2017).
[35] *In re Experian Data Breach Litig.*, No. 8:15-cv-01592, 2017 WL 4325583 (C.D. Cal. May 18, 2017).
[36] 136 S. Ct. 1540 (2016), *as revised* (May 24, 2016).
[37] For Cleary Gottlieb's Alert Memorandum discussing the D.C. Circuit's ruling and the circuit split, see https://www.clearygottlieb.com/~/media/organize-archive/cgsh/files/2017/publications/alert-memos/dc-court-issues-significant-data-breach-decision-8-7-17.pdf.
[38] *See In re SuperValu, Inc., Customer Data Sec. Breach Litig.*, 870 F.3d 763 (8th Cir. 2017); *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89 (2d Cir. 2017); *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017), *cert. denied sub nom. Beck v. Shulkin*, 137 S. Ct. 2307 (2017). For Cleary Gottlieb's Alert Memorandum discussing additional cases contributing to the circuit split, see https://www.clearygottlieb.com/~/media/organize-archive/cgsh/files/2017/publications/alert-memos/with-equifax-looming-split-on-standing-in-data-breach-cases-grows-with-recent-decisions-10-4-17.pdf.
[39] *See Santana v. Take-Two Interactive Software, Inc.*, No. 17-303, 2017 WL 5592589 (2d Cir. Nov. 21, 2017); *Katz v. Donna Karan Co.*, 872 F.3d 114 (2d Cir. 2017); *Crupar-Weinmann v. Paris Baguette Am., Inc.*, 861 F.3d 76 (2d Cir. 2017). For Cleary Gottlieb's previous blog post discussing the Second Circuit's rulings, see https://www.clearycyberwatch.com/2018/01/second-circuit-issues-order-affirming-dismissal-data-privacy-class-action-suit/#more-2037.
[40] *Robins v. Spokeo, Inc.*, 867 F.3d 1108 (9th Cir. 2017).

the FTC must establish a concrete consumer injury in order to bring an enforcement action for "unfair" practices.[41] If the Eleventh Circuit rules against the FTC—which would be in significant tension with the Third Circuit's prior holding in the *Wyndham* decision, upholding the FTC's enforcement authority over cybersecurity issues in that case under the same section of the FTCA[42]—it would be a major setback for the agency and set up potential Supreme Court review. If the FTC prevails, on the other hand, it would likely only further embolden the FTC's cybersecurity enforcement activity under the theory that lax data security may constitute an "unfair" trade practice.

— *Supreme Court.* Two cases currently pending before the Supreme Court have the potential to set critical parameters for government access to digitally stored information. In October, the Supreme Court granted certiorari in the *Microsoft* case on the issue of whether the Stored Communications Act allows law enforcement to access consumer email data stored outside the U.S.[43] In addition, the Supreme Court heard oral argument in November on the issue of whether law enforcement must obtain a warrant to access an individual's cell phone location information.[44] However the Court rules on these issues, it will have wide-ranging effects on the ability of law enforcement to obtain data in the digital age and the privacy rights of potentially millions of individuals.

— *Decisions Abroad.* Meanwhile, on the other side of the Atlantic, private litigants continue to challenge the lawfulness of transfers of personal data outside of the EU. In October, the Irish High Court cast fresh doubt on the legitimacy of so-called Standard Contractual Clauses ("SCCs", also commonly referred to as Model Contracts) as an approved method of ensuring lawful personal data transfers from the European Economic Area ("EEA") to the U.S. The Irish High Court agreed with the "well-founded" concerns that U.S. law enforcement "surveillance" programs, such as the Foreign Intelligence Surveillance Act ("FISA") and those leaked in 2013 by Edward Snowden, jeopardize EU citizens' privacy rights upon transfer of data to the U.S. The Irish High Court has now called on the Court of Justice of the European Union ("CJEU") for a preliminary ruling on the validity of SCCs for such transfers. An adverse ruling could lead to a crisis in international data flows as an overwhelming majority of EEA companies use SCCs as their basis for ensuring compliant personal data transfers not only to the U.S. but also to other countries outside of the EEA. The uncertainty created by such an outcome would also come at a time when the GDPR becomes effective and is being fully enforced.[45]

Looking Ahead to 2018

Looking ahead, we expect to see the key developments of 2017, from increasing cyberattacks to the growing regulatory response, to continue in the coming year. The unprecedented reach of the recent cyberattacks has sparked a renewed focus on addressing cyber threats prophylactically, through issuance of voluntary guidelines and mandatory regulations, while at the same time recognizing, as the SEC recently noted, that "even the most diligent cybersecurity efforts will not address all cyber risks that enterprises face."[46] Thus, 2018 will likely continue to see a dual emphasis on preemptive and remedial measures, as well as

[41] *LabMD, Inc. v. Fed. Trade Comm'n*, No. 16-16270 (11th Cir. argued June 21, 2017).
[42] *Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).
[43] *United States v. Microsoft Corp.*, No. 17-2 (U.S. filed June 23, 2017).
[44] *Carpenter v. United States*, No. 16-402 (U.S. argued Nov. 29, 2017).
[45] For Cleary Gottlieb's blog post on the decision, see https://www.clearycyberwatch.com/2017/10/schrems-ruling-renewed-scrutiny-standard-contractual-clauses-eu-us-personal-data-flows/.
[46] Chairman Jay Clayton, SEC, Statement on Cybersecurity (Sept. 20, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20.

disclosure requirements. In particular, the SEC is poised to issue new guidelines for the first time since 2011, and the Cyber Unit is primed to bring additional enforcement actions, including, potentially, the SEC's long-anticipated first cybersecurity disclosure case.

In addition, there appears to be a strong impetus for further legislative action at both the U.S. state and federal level in 2018, with several proposals in the queue. Countries abroad will similarly continue to face ongoing data protection challenges as they introduce and implement cybersecurity measures, which will likely impact companies in the U.S. as well.

Moreover, the settlements reached with private litigants and regulators, in tandem with the regulations and guidance promulgated by government authorities, continue to build on the emerging set of standards for best practices in the cybersecurity context. It further remains to be seen whether any cybersecurity litigation will reach the merits stages, which may, in turn, provide further guidance on preventive and remedial measures.

From a data privacy perspective, the critical issue is how companies respond to the implementation of the GDPR, and how the EU ultimately enforces it. The first enforcement actions, and the accompanying penalties, will clearly set the tone.

Finally, several pending and potentially blockbuster court decisions will have significant implications for the standing to pursue cybersecurity actions, the scope of the government's enforcement authority, and the privacy rights of individuals.

In sum, while 2017 was a year in cybersecurity like never before, 2018 promises to bring even more dramatic developments that could surpass last year's high bar.[47]

…

CLEARY GOTTLIEB

[47] This Alert Memorandum was prepared with the assistance of Alanna B. Newman and Guilherme Duraes.