ALERT MEMORANDUM

2020 Cybersecurity and Privacy Developments: A Year in Review

January 25, 2021

Cybersecurity and data privacy, topics that were already top of mind for companies at the start of 2020, were pushed even further to the forefront due to the COVID-19 pandemic, significant data security enforcement actions, and the SolarWinds breach discovered in December. The increased prevalence of remote work made it all the more critical for companies to manage cybersecurity risk. In a recent survey of business and technology executives, 96% of respondents said that they will shift their cybersecurity strategy due to COVID-19 and 50% say that they are more likely to consider cybersecurity in *every* business decision (up from 25% last year).[1] While cyber and privacy risks were continuing to grow, 2020 also saw new legislation and regulations that increased both the cost and complexity of compliance and the penalties for failing to do so. And, on top of everything, cyber and privacy enforcement and litigation, already at high levels, were more active than ever.

In this Year in Review, we highlight the most significant cybersecurity and privacy developments of 2020 and predict key challenges and areas of focus for the coming year.

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

WASHINGTON

Katherine Mooney Carroll
+1 202 974 1584
kcarroll@cgsh.com

Alexis Collins
+1 202 974 1519
alcollins@cgsh.com

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

Daniel Montgomery
+1 212 225 2614
dmontgomery@cgsh.com

LONDON

Natalie Farmer
+44 20 7614 2309
nfarmer@cgsh.com

PARIS

Emmanuel Ronco
+33 1 40 74 69 06
eronco@cgsh.com

[1] *Cybersecurity coming of age*, PwC (Oct. 5, 2020), https://www.pwc.com/gx/en/news-room/press-releases/2020/global-digital-trust-insights-survey-2021.html.

Data Breaches and Other Cyberattacks

A number of significant data breaches and other cyberattacks, including ransomware incidents, occurred in 2020, driving the conversation on cybersecurity risk. Some of the notable incidents included:

— In January, Travelex, the foreign-exchange company, was hit with a ransomware attack that damaged its operations for several weeks.
— In March, Marriott announced a breach of the personal information of approximately 5.2 million guests, including names, contact details and addresses. This follows the previous high-profile incident involving data acquired in Marriott's Starwood acquisition that the company disclosed in 2018.
— In May, EasyJet announced that hackers had improperly accessed the email addresses and travel details of approximately 9 million customers, including over 2,000 customers' credit card numbers and security codes.
— In July, the Twitter accounts of many high-profile figures, including Joe Biden, Bill Gates and Kanye West were hacked in a bitcoin scam.
— In December, it was reported that upward of 250 U.S. federal agencies and private businesses had been hacked for at least nine months, likely by Russian intelligence services, through a network management software called SolarWinds. The extent and ramifications of the breach are still being understood, although the apparent inability of domestic intelligence agencies and others to detect the hack earlier suggest potential significant and ongoing weaknesses in private and public cybersecurity infrastructures.

While these are some of the more significant examples, many companies dealt with cybersecurity incidents on a smaller scale, resulting in exposed data, locked systems or other harm.

U.S. Enforcement

In the face of continuing significant data breaches and other security incidents, U.S. regulators were increasingly active in bringing cybersecurity enforcement actions against companies that suffered security incidents or otherwise allegedly failed to maintain required data security programs.

— In July, New York's Department of Financial Services ("DFS") brought its first ever enforcement action for the alleged breach of its cybersecurity regulations, which had been in force as of 2019. DFS alleged that First American Title Insurance Company was aware of a vulnerability of its website that allowed tens of millions of documents containing personal information to be publicly accessed, but, because of a "cascade of errors," First American allegedly did not remedy the vulnerability for six months.
— In August, the Department of Justice ("DOJ") charged Uber's former Chief Security Officer with obstruction of justice and misprision of a felony for allegedly attempting to cover up a 2016 data breach during the course of an investigation by the Federal Trade Commission.[2] The prosecution represents an aggressive step by federal authorities in bringing charges under the obstruction and felony misprision statutes, the latter of which is relatively rarely-used in white-collar cases.
— In September, Anthem, Inc. entered into a $39.5 million settlement with a multi-state coalition of state attorneys general arising out of a cyber-attack in 2014, and agreed to a series of data security and governance provisions designed to strengthen its cybersecurity practices going forward.
— The Office of the Comptroller of the Currency ("OCC") brought two enforcement actions in 2020 that included civil money penalties related to data security incidents, marking the agency's first significant penalties imposed on banks in connection with a data breach or an alleged failure

[2] For further information, see the Cleary Gottlieb "DOJ Charges Former Uber Executive for Alleged Role in Attempted Cover-Up of 2016 Data Breach" publication at https://www.clearycyberwatch.com/2020/09/doj-charges-former-uber-executive-for-alleged-role-in-attempted-cover-up-of-2016-data-breach/.

to comply with the OCC's guidelines relating to information security.

- In August, the OCC assessed an $80 million civil money penalty and entered into a cease-and-desist order with the bank subsidiaries of Capital One, following a 2019 cyber-attack.[3]
- In October, the OCC assessed a $60 million civil money penalty against two bank subsidiaries of Morgan Stanley for allegedly failing to comply with the OCC's information security guidelines in connection with the decommissioning of two data centers and certain network devices.

— In November, the Federal Trade Commission announced a settlement with Zoom Video Communications, Inc. ("Zoom") relating to allegations about the level of encryption it offered for users' communications, as well as an allegation that Zoom secretly installed software that bypassed an Apple Safari browser security safeguard. In connection with the settlement, Zoom agreed to establish and implement a comprehensive security program that requires it, among other things, to regularly review software updates for security flaws.

— On December 30, the DOJ charged Ticketmaster L.L.C. with violating the Computer Fraud and Abuse Act ("CFAA") and committing wire fraud, based on allegations that Ticketmaster employees repeatedly used stolen passwords from a competitor to conduct business intelligence.[4] As part of Ticketmaster's deferred prosecution agreement it agreed to (i) pay a $10 million fine; (ii) maintain a compliance and ethics program designed to prevent and detect violations of the CFAA and other applicable laws, and to prevent the unauthorized and unlawful acquisition of confidential information belonging to its competitors; and (iii) report annually to the government regarding its compliance.

New U.S. Legislation and Regulations

California Privacy Rights Act

In the November 2020 election, Californians passed the California Privacy Rights Act ("CPRA") via ballot initiative, amending the California Consumer Privacy Act (the "CCPA"), that itself only came into effect in the beginning of 2020. The CPRA, which goes into effect on January 1, 2023, both clarifies certain ambiguities in the CCPA and introduces new complexities and uncertainties.

Some of the notable changes under the CPRA include:

— *Additional Obligations regarding Sharing of Personal Information.* The CPRA includes new rights and obligations regarding the practice of a business "sharing" (not only selling) personal information. The act's broad definition of "sharing" includes providing a third party with consumer personal information for the purpose of cross-context behavioral advertising. The CPRA provides consumers with a new right to opt-out of the sharing of their data for this purpose and, as a result, businesses will have to modify their websites and business practices to allow consumers to exercise this right.

— *Reasonable Security Practices and Contracts with Third Parties.* The CPRA contains an affirmative requirement for covered businesses to implement reasonable security procedures and practices to protect all covered categories of personal information. Further, when a covered business shares personal information with certain third parties, service providers, or contractors, the CPRA requires that the covered business's contracts with those third parties require the third party to provide the same level of privacy

[3] For further information, see the Cleary Gottlieb "OCC Imposes $80 Million Penalty in Connection with Bank Data Breach" publication at https://www.clearycyberwatch.com/2020/08/occ-imposes-80-million-penalty-in-connection-with-bank-data-breach/.

[4] *United States v. Ticketmaster L.L.C.*, No. 1:20-cr-563-MKB-1 (E.D.N.Y. Dec. 30, 2020), ECF No. 7.

protection as the covered business provides under the CPRA.

— *New Rights relating to Sensitive Personal Information.* The CPRA creates a new concept of "sensitive personal information" ("SPI") which, among other things, includes information that reveals a consumer's precise geolocation, race, ethnicity, religious or philosophical beliefs, and account log-in, financial account, debit card, or credit card number in connection with any required security or access code. Consumers may direct businesses collecting SPI to limit the use of their SPI to those uses "necessary to perform the services or provide the goods reasonably expected by an average consumer" of such goods or services.

— *New GDPR-Inspired Principles*. The CPRA adopts principles that are akin to those under the EU General Data Protection Regulation ("GDPR")—specifically, the right to correct personal information and the requirement of "data minimization," meaning covered businesses may only collect, use, retain and share a consumer's personal information to the extent that it is "reasonably necessary and proportionate" to either (1) the purpose for which it was collected or processed or (2) another disclosed purpose that is compatible with the context in which it was collected.

— *Enforcement*. The CPRA establishes a "California Privacy Protection Agency," the first agency of its kind in the United States, that will be able to enforce the CCPA and CPRA beginning July 1, 2023.

Other Data Security and Privacy Legislation, Regulations, and Guidance

— *New York.* In March 2020, the compliance provisions of New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act)—which was passed in 2019—came into effect. The SHIELD Act affirmatively requires businesses that own or license computerized data which includes private information of New York residents to develop, implement, and maintain "reasonable" data security safeguards.[5]

— *Other U.S. State Laws*. Throughout 2020, data privacy bills were introduced in at least 30 states and Puerto Rico. However, the COVID-19 pandemic shifted legislative attention and, aside from California, no other prominent state privacy legislation was enacted.

— *Federal Ransomware Attack Advisories.* In October, the U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCEN) issued a pair of advisories to assist in efforts to combat the increasing threat of ransomware attacks and comply with sanctions and anti-money laundering requirements. Both advisories share common themes relating to the development of adequate risk-based compliance programs and the reporting of ransomware attacks and suspicious activity to authorities. The OFAC advisory describes how U.S. economic sanctions can apply to ransomware payments and offers guidance on OFAC's compliance expectations and enforcement considerations relating to ransomware payments; similarly, the FinCEN advisory warns that certain activities by companies regularly engaged with victims of ransomware could constitute money transmissions such that the companies must register as "money services businesses" and be subject to Bank Secrecy Act obligations.[6]

— *OCC Proposed Rule.* Also in the federal regulatory space, on December 15, 2020, the OCC, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation issued a notice of proposed rulemaking regarding "Computer-Security

[5] For further information, see the Cleary Gottlieb "New York Passes Expansive New Cybersecurity Law" publication at https://www.clearygottlieb.com/-/media/files/alert-memos-2019/new-york-passes-expansive-new-cybersecurity-law.pdf.

[6] For further information, see the Cleary Gottlieb "OFAC and FinCEN Issue Advisories on Cyber Ransom Payments" publication at https://www.clearycyberwatch.com/2020/10/ofac-and-fincen-issue-advisories-on-cyber-ransom-payments.

Incident Notification Requirements for Banking Organizations and Their Bank Service Providers." If implemented as proposed, the rule would require (i) a banking organization to notify its primary federal regulator within 36 hours whenever the banking organization believes in good faith that a significant "computer-security incident" has occurred; and (ii) a bank service provider to immediately notify its banking organization customers when it believes in good faith that it has suffered a computer-security incident that could disrupt, degrade, or impair its provision of services for at least four hours.

— *IoT Cybersecurity Improvement Act of 2020.* In December, the federal IoT (Internet of Things) Cybersecurity Improvement Act of 2020 was signed into law after receiving bipartisan support. Among other things, the law requires the National Institute of Standards and Technology to develop standards and guidelines for federal agencies regarding their use of certain IoT devices, related vulnerability disclosure, and the resolution of such disclosed vulnerabilities. Beginning December 5, 2022, federal agencies will be prohibited from entering into or renewing contracts involving the use of IoT devices if doing so would prevent them from complying with security standards or disclosure guidelines.

— *Other U.S. Federal Legislation.* There was no substantial progress towards comprehensive federal data security and privacy legislation, although in September, Republican Senators introduced new proposed legislation—the Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act. Democrats and Republicans remain split on the key issues of preemption (which Republicans favor) and private rights of action (which Democrats favor). Whether comprehensive legislation becomes a priority of the Biden administration is yet to be seen. However, in light of the COVID-19 pandemic, there is a possibility of renewed attention to federal data privacy law, particularly related to health information.

Litigation Developments

There were also significant developments in litigation related to cybersecurity and data privacy in 2020.

— In February, in largely denying Marriott's motion to dismiss litigation arising out of the 2018 breach of Starwood Hotels & Resorts (which Marriott acquired in 2016), a Maryland federal district court rejected Marriott's standing arguments and held that plaintiffs can establish injury-in-fact based on the non-speculative "imminent threat" of identity theft.[7] The decision is one of a potentially developing trend of companies facing increasing difficulty in obtaining dismissals of data breach litigation at early stages based on the argument that consumers were not injured by exposure of their personal information, particularly when such information is arguably sensitive. Other examples in 2020 include:

  - The Ninth Circuit in *In re Facebook, Inc. Internet Tracking Litigation* permitted plaintiffs' privacy claims to proceed past the motion to dismiss stage, finding that the company's alleged use of cookies to track users even after they have logged out of the platform constituted a concrete injury for standing purposes.[8]
  - The Seventh Circuit in *Bryant v. Compass Group USA, Inc*. found that defendant's failure to provide plaintiff with informed consent to the collection of her biometric data caused plaintiff to suffer a concrete injury and allowed certain of her Illinois Biometric Information Privacy Act claims to proceed in federal court.[9]

— In May, in class action litigation against Capital One arising out of its 2019 data breach, the bank was ordered by a federal Magistrate Judge in Virginia to produce to plaintiffs a digital forensic

[7] *In re: Marriott Int'l, Inc., Customer Data Security Breach Litig.*, 440 F. Supp. 3d 447 (D. Md. 2020).

[8] 956 F.3d 589 (9th Cir. 2020).

[9] 958 F.3d 617 (7th Cir. 2020).

investigation report, finding that such report was not protected from disclosure by the attorney work product doctrine.[10] The court determined that the report was not produced primarily in anticipation of litigation based on several factors, including the similarity of the report to past business-related work product by the investigator and the bank's subsequent use and dissemination of the report. The decision was later affirmed by the District Judge.

— The CCPA gave California residents a private right of action in the event of data breaches. The first such lawsuits have already been filed, such as *Atkinson v. Minted, Inc.*, an action arising out of an alleged data breach of the account information of millions of customers of an online stationery and craft company.[11] CCPA litigation is likely to proliferate, particularly with the passage of the CPRA, which added to the list of data types that are actionable in the event of a breach.

Cybersecurity and Data Privacy Outside of the U.S.

Outside the U.S., there were a number of significant judicial, legislative, and enforcement actions in 2020.

— *EU–U.S. Privacy Shield Invalidated.* In a highly-anticipated landmark judgment handed down on July 16, 2020, the Court of Justice of the European Union (the "CJEU") in *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* ("*Schrems II*") invalidated the EU-U.S. Data Protection Shield (the "Privacy Shield") as a means for legal transfer of personal data from the EU to the United States.[12] Businesses that transfer personal data from the EU to the United States can no longer rely on the Privacy Shield framework to transfer such data in compliance with the GDPR.

- The CJEU's judgment confirmed that "Standard Contractual Clauses" or "SCCs"—which are a set of contractual clauses provided by the European Commission that set forth the rights and obligations of the parties to a data transfer—remain a valid mechanism for the transfer of personal data to "third countries" (including, but not limited to, the United States). However, the *Schrems II* judgment confirmed that primary responsibility for determining SCCs' efficacy on a case-by-case basis, by reference to the laws applicable in the recipient country, remains with the data exporter. The data exporter must ascertain, in collaboration with the data importer, that the laws of the recipient country would not cause the parties to be incapable of complying with the SCCs or take efficient supplementary measures to protect the transferred data. In particular, the existence of laws permitting surveillance of, or access to, personal data by public authorities (where such access goes beyond what is "*necessary in a democratic society*") will preclude the ability to rely solely on the SCCs as a means to transfer the data in compliance with the GDPR unless technical, contractual or organizational measures (such as encryption or pseudonymisation) are taken to remedy the risk of unauthorized access.

[10] *In re: Capital One Consumer Data Security Breach Litig.*, No. 1:19-md-2915, 2020 WL 2731238 (E.D. Va. May 26, 2020), *aff'd*, 2020 WL 3470261 (E.D. Va. June 25, 2020). For further information, see the Cleary Gottlieb "Federal Court Compels Production of Data Breach Forensic Investigation Report" publication at https://www.clearycyberwatch.com/2020/07/federal-court-compels-production-of-data-breach-forensic-investigation-report/.

[11] No. 3:20-cv-03869-VC (N.D. Cal. June 11, 2020), ECF No. 1.

[12] For further information, see the Cleary Gottlieb "*Schrems II*: The CJEU Declares EU-U.S. Privacy Shield Invalid, Upholds the SCCs And Calls On 27 Supervisory Authorities to Ensure Their Compliance" publication at https://www.clearycyberwatch.com/2020/07/schrems-ii-the-cjeu-declares-eu-u-s-privacy-shield-invalid-upholds-the-sccs-and-calls-on-27-supervisory-authorities-to-ensure-their-compliance/, and the "*Schrems II*: A Global Update" publication at https://www.clearycyberwatch.com/2020/10/schrems-ii-a-global-update/.

— *Enforcement Activity.* In October, the United Kingdom's Information Commissioner's Office ("ICO") issued fines against British Airways and Marriott Hotels for violations of the GDPR that occurred in connection with their previously-disclosed data breaches.

  - In 2019, the ICO had announced its intent to fine British Airways and Marriott £183 million and £99 million, respectively, but the final fines as imposed were reduced to £20 million and £18.4 million. In cutting the imposed fines, the ICO apparently took into account financial hardship and economic circumstances caused by the COVID-19 pandemic on these companies, whose industries (airline and hospitality) were arguably among the worst affected.[13]

— *Litigation in Europe and the U.K.* Litigation arising out of data breaches or privacy violations is increasing across jurisdictions outside of the U.S. The European Union and United Kingdom are seeing a rise in representative or class-action type suits—with class-actions filed in the Netherlands against Oracle and Salesforce.com for alleged GDPR violations, as well in the UK against British Airways and Marriott in connection with their personal data breaches. In 2021, the U.K. Supreme Court is set to hear the final appeal in the *Lloyd v Google* representative action which could open the door to representative actions in the U.K. for damages associated with the "loss of control" of personal data. Currently, class actions under the GDPR are limited by member-state laws governing class actions, but this could change in light of a new directive agreed in June 2020 that, if adopted, would create a right of collective class action across the entire EU for data privacy violations.

— *Data Privacy Legislation Outside of Europe*. In 2020, a data privacy law in Brazil modeled off of the GDPR came into effect, making it the first comprehensive general data protection law in Latin America. Although implementation of Thailand's data protection law was delayed from 2020 until 2021, the Thai government imposed interim requirements for certain data controllers. The Indian government introduced a draft framework for the regulation of data for public comment, and South Korea passed amendments to its major data privacy laws.

Key Takeaways

— Increased regulatory action and recent regulatory guidance related to cybersecurity issues portends the continued shift away from regulators viewing hacked companies as only victims and toward potentially holding them responsible for perceived deficiencies in their cybersecurity programs and other implicated internal controls, or for their actions taken in response to a cybersecurity incident such as a ransomware attack.

— Data privacy risks are also more acute than ever. The GDPR and CCPA/CPRA continue to lead the way, and active European regulators and the eventual launch of a new California enforcement agency mean that other jurisdictions have an increasingly well-worn roadmap to follow suit.

— Private litigation arising out of data breaches and data privacy issues continues to proliferate and U.S. courts have recently handed down plaintiff-friendly decisions on standing and discovery issues, which may make the cases even more expensive to litigate. In Europe and the U.K., data breach and privacy class action risks are also becoming more significant for companies operating in those jurisdictions.

— The trend of increased cybersecurity and data privacy legislation will likely continue into 2021, both in the U.S. and globally, requiring companies to continue to monitor the evolving legal landscape.

[13] For further information, see the Cleary Gottlieb "UK ICO Data Breach Fines – What Can We Learn From British Airways and Marriott?" publication at https://www.clearycyberwatch.com/2020/12/uk-ico-data-breach-fines-what-can-we-learn-from-british-airways-and-marriott/.

— A new administration in the U.S. may mean increased focus on enforcement and potentially federal data security and privacy legislation that has eluded lawmakers for years. President Biden has nominated several agency leaders with cybersecurity experience, including his nominee for the Secretary of Homeland Security and a newly created cybersecurity advisor position on the National Security Council. Particularly in light of the SolarWinds breach discovered in December, expect the Biden administration to consider advocating for additional cyber and privacy regulations, alongside public-private cooperation efforts.

In a year marked by the COVID-19 pandemic and other monumental world events, 2020 also saw a number of significant cybersecurity and privacy developments. We expect these ongoing risks to continue to be a top concern for in-house counsel, management, and boards of directors for the next year and beyond.

…

CLEARY GOTTLIEB