O'Melveny | omm.com

What's Next in Data Security and Privacy?

6 Trends to Watch in 2020

The world of data security and privacy is rapidly becoming more complex and dynamic. The increased integration of new technology into our lives is expanding horizons, while rendering us ever more vulnerable to exploitation by sophisticated cyber actors. As regulators and legislators endeavor to tackle these difficult issues, companies will need to contend with a new slate of laws and regulatory actions. Here are the legal trends we are watching in 2020.

1 NEW PRIVACY LEGISLATION AND REGULATION

With California leading the way, the states will continue to be the main event when it comes to privacy legislation in 2020, contributing to a growing patchwork of laws that give consumers greater rights to, and control over, their personal information. Bills are pending in Massachusetts, Washington, Pennsylvania, New Jersey, and New York, among other states.

The coming year will also see continued efforts at the federal level to create a comprehensive nationwide data privacy law, but whether a federal privacy law has a realistic chance at enactment is uncertain. Lawmakers have fundamental disagreements on several key issues, including whether consumers should have a private right of action to enforce their rights (rather than just leaving enforcement to a regulator, such as the Federal Trade Commission) and whether the federal law would preempt state laws like the California Consumer Privacy Act (CCPA).

Indeed, CCPA compliance must be a major focus of companies in 2020, given its breadth and scope.[1] The California Attorney General plans to issue final regulations in the first quarter of 2020, which companies hope will clarify how they can comply with the law and resolve ambiguities in the current legislation. Forceful statements made by the Attorney General suggest that California plans to begin aggressively enforcing the CCPA in the second half of the year.

Industry and privacy advocates have already begun a push to revise and amend the CCPA in 2020. The most significant of these efforts is the California Privacy Rights and Enforcement Act of 2020, a proposed ballot measure that would create a new agency to enforce privacy rights, require additional transparency on how collected data is used, and give consumers the right to opt-out of certain types of targeted advertising.

[1] O'Melveny's CCPA Toolkit explains the law's requirements, helps companies make an initial assessment as to whether they are affected by the law, and lays out eight steps for compliance.

2 STRICTER STANDARDS FOR THE INTERNET OF THINGS

2020 will see exponential growth in the number and types of Internet of Things (IoT) devices, particularly in the manufacturing and healthcare sectors. As exploitation of flaws in connected devices makes headlines—the hacking of home security cameras being the latest example—legislators and regulators are stepping up efforts to set privacy and security standards that go beyond the protections for personal information.

At the state level, California's and Oregon's IoT-specific laws went into effect on January 1, and a number of other states are developing their own IoT legislation. The California and Oregon laws both require manufacturers to develop products that implement "reasonable security" measures that are appropriate to the nature and function of the particular device, although the Oregon law covers a narrower scope of devices. Like the current patchwork of state privacy laws, state IoT security laws will feature subtle but significant differences in scope and compliance requirements. It will also be important to follow judicial and regulatory actions that are expected to clarify the meaning of "reasonable security" in various contexts.

At the federal level, there have been a number of legislative proposals focusing on IoT, including the Cyber Shield Act, the Protecting Privacy in Our Homes Act, the Automatic Listening Exploitation Act, and the Internet of Things Cybersecurity Improvement Act. Like their state counterparts, these proposals push for baseline security measures and encourage regulators to focus on IoT security. It is not clear whether IoT-focused legislation will get traction in Congress independent of federal privacy legislation, but look for additional proposals to be introduced responding to the latest round of media attention on IoT vulnerabilities.

Even without new legislation, regulators have begun to look specifically at IoT issues themselves. For instance, the Federal Trade Commission reached a settlement earlier in 2019 with smart home products manufacturer D-Link over alleged software security deficiencies in routers and internet-connected cameras. With the public attention on recent hacking of internet-enabled home security cameras, and the likelihood that there will be similar incidents in the future, security requirements for connected devices will continue to be a priority for legislators and regulators in 2020.

3 MORE TARGETED AND DESTRUCTIVE RANSOMWARE ATTACKS

From small towns to big cities, from hospitals to schools, there was a steady stream of ransomware reports in 2019. But while the profile and impact of ransomware attacks is increasing, the overall number of attacks has decreased in the years since WannaCry and NotPetya. Ransomware has become more targeted and more costly to victims and insurers. Cyber criminals are moving away from broad-based, indiscriminant phishing campaigns as an entry point, and instead are developing customized malware designed to target a specific organization's vulnerabilities and unique data sets. This evolution has led to larger monetary ransom demands and greater vulnerability of organizations' critical data.

In 2020, the trend of more targeted, destructive attacks will continue as attackers become ever more sophisticated. Concurrently, more "traditional" ransomware victims like hospitals, critical infrastructure, and local government are likely to remain the prime targets; they provide critical services to citizens, and often face greater pressure to pay the ransom.

Because ransomware attacks are high-profile and affect the provision of basic services, Congress has sought to find ways to help victims. The House and Senate both passed legislation in 2019 intended to provide technical assistance to critical infrastructure operators in the event of a ransomware attack, and reconciliation and ultimate enactment of the legislation is expected in 2020.

4 SHARPER FOCUS ON SUPPLY CHAIN ISSUES

2020 will be a significant year for technology supply chain issues. The Department of Commerce is in the process of implementing President Trump's May 2019 executive order on Securing the Information and Communications Technology and Services Supply Chain, which grants the Secretary of Commerce the authority to prohibit, require mitigation measures, or unwind particular technology transactions. The comment period on Commerce's proposed rule closed on January 10, 2020, and there is no public deadline for issuance of the final rule. Whether Commerce makes wholesale changes to the review process outlined in the proposed rule and how Commerce chooses to wield the extraordinarily broad authority on a "case by case basis" merits close industry attention.

The federal government has been particularly aggressive in addressing supply chain issues in procurement, which may have secondary impacts in the private sector. In August 2019, the federal government issued a rule prohibiting agencies from procuring certain telecommunications equipment or services from Huawei, ZTE, and certain other Chinese companies. The scope of the federal ban becomes broader in August 2020, when agencies will be prohibited from contracting with any entity that merely uses prohibited telecommunications technology or services, even if that technology is not part of the service being provided to the government. The Federal Communications Commission, which, in 2019, prohibited Universal Service Funds from being used to buy Huawei equipment, will likely continue its focus on promoting technology it views as secure and trustworthy. With these efforts, as well as export controls and foreign investment restrictions, inextricably linked with the outcome of ongoing trade negotiations with China, 2020 promises to be an eventful year for supply chain issues.

5 TOUGHER ENFORCEMENT OF CRYPTOCURRENCY STANDARDS AND RISKS FROM DIGITAL PAYMENTS

In Spring 2019, FinCEN issued a significant guidance document intended to synthesize its previous interpretive guidance on how principles applicable to "traditional" money services businesses (MSB) under the Bank Secrecy Act (BSA) apply to conduct involving blockchain and cryptocurrency. Shortly thereafter, the Financial Action Task Force (FATF)—an intergovernmental organization tasked with recommending international standards for combatting money laundering and terrorist financing (AML/CFT)—released a recommendation on standards governing virtual assets (VAs) and virtual asset service providers (VASPs) (entities that exchange, transfer, store, and issue or underwrite virtual assets), which is particularly relevant to companies doing business internationally. By the end of the year, financial regulators across the federal government had come together to emphasize their joint commitment to aggressive enforcement of AML/CFT rules against businesses conducting digital asset-related activities.

In the coming year, regulators are poised to begin putting these standards and commitments to the test through enforcement actions. Meanwhile, blockchain and digital asset businesses will continue to grapple with how to comply with requirements written for traditional banks that do not easily fit the blockchain ecosystem. FinCEN's recent guidance on cryptocurrency businesses, for instance, emphasizes the requirement that MSBs (including hosted wallets) comply with the "Funds Travel Rule" when transmitting digital assets—a regulation originally designed to require banks to collect and forward certain identifying information as part of wire transactions. While compliance with that rule is routine for banks using SWIFT or similar messaging systems to capture and send information from fiat transfers, the rule poses a major regulatory problem for businesses engaged in blockchain transactions, where no similar messaging mechanism for sending the required information yet exists. In 2020, industry players will expand coordinated efforts to respond to this and other compliance challenges through initiatives like "OpenVASP," a recently proposed protocol aimed at facilitating the transmission of Travel Rule information in blockchain transactions.

As 2020 promises fintech innovation, so too does it portend new risks. The proliferation of blockchain and digital asset services, including mobile payment services, will offer cyber criminals and state-sponsored hackers new opportunities to target financial institutions for cybercrime, including through increasingly sophisticated email compromise fraud schemes. These schemes—in which cyber criminals attempt to misappropriate funds by sending fraudulent payment instructions using compromised email accounts—are on the rise, accounting for almost US$9 billion in attempted theft since 2016. As financial institutions contend with an increasing number of these and other attacks, it is worth remembering that FinCEN and other

regulators—such as the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (FRB), and the Federal Deposit Insurance Corporation (FDIC)—continue to expect that cyber-events and cyber-enabled crimes are closely tracked and reported to regulators, including through mandatory and voluntary Suspicious Activity Reports (SARs). In 2020, as regulators race to stay one step ahead of rapidly changing technology, financial institutions innovating in the blockchain and cryptocurrency space must be increasingly nimble to effectively comply with evolving regulatory reporting regimes.

6 THE DISRUPTIVE FORCE OF ARTIFICIAL INTELLIGENCE

As Artificial Intelligence (AI) continues to provide tremendous business and investment opportunities across all industry sectors, it is also disrupting legacy technologies and challenging business leaders to consider the principles and ethical questions raised by its use. For all these reasons, 2020 will bring increased attention to the regulation of AI. Several companies have laid the groundwork for these discussions by articulating preliminary principles for the use of AI and are taking steps to align their AI practices with these principles.

In response to changing public expectations, regulators and legislators have started to shift their attention towards specific industries and applications involving AI. For example, the US Department of Housing and Urban Development sued Facebook for using algorithms that enabled advertisers to discriminate based on gender and race. Various efforts to deploy facial recognition technology have drawn the ire of privacy and civil rights advocates who point to flawed machine learning models as the cause for the mislabeling and profiling of people based on race and gender. Motivated in part by these concerns, in 2019, California passed a three-year moratorium on the use of facial recognition by law enforcement agencies, while San Francisco completely banned facial recognition systems for its agencies. Other US cities, including Somerville and Brookline, Massachusetts, followed suit — a trend that will likely continue in 2020.

In healthcare, the Food and Drug Administration (FDA) announced that it is considering a new regulatory framework for the use of AI in medical devices, to ensure that safety and efficacy is maintained. This framework would address the FDA's approach to determining when it will require premarket review of AI or machine-learning software modifications to medical devices. The New York Department of Financial Services is also focused on the healthcare sector, as demonstrated by its recent inquiry into potential bias in algorithms used by healthcare providers.

Finally, as its capabilities grow, AI is certain to remain a top military and national security issue in 2020. Recently, for instance, the Bureau of Industry and Security, a part of the Department of Commerce, issued an interim final rule restricting the export of certain AI software designed to analyze satellite imagery. Similarly, it is likely that non-US companies seeking to invest in US companies working on similar technologies may be required to obtain approval from the Committee on Foreign Investment in the United States.

Whether at the federal or state level, 2020 will feature continued engagement by regulators and legislators seeking to address the proliferation and rapid evolution of AI-based technologies.

KEY CONTACTS

Steve Bunnell
Co-Chair,
Data Security and Privacy Practice
Washington, DC
+1 202 383 5399
sbunnell@omm.com

Lisa Monaco
Co-Chair,
Data Security and Privacy Practice
Washington, DC: +1 202 383 5413
New York: +1 212 326 2000
lmonaco@omm.com

Michael Dreeben
Partner
Washington, DC
+1 202 383 5400
mdreeben@omm.com

Randall Edwards
Partner
San Francisco
+1 415 984 8716
redwards@omm.com

Laurel Loomis Rimon
Partner
Washington, DC
D +1 202 383 5335
lrimon@omm.com

Scott Pink
Special Counsel
Silicon Valley
+1 650 473 2629
spink@omm.com

John Dermody
Counsel
Washington, DC
+1 202 383 5306
jdermody@omm.com

Evan Schlom
Associate
Washington, DC
+1 202 383 5512
eschlom@omm.com

For more on our team and capabilities, visit omm.com/data-security-and-privacy.