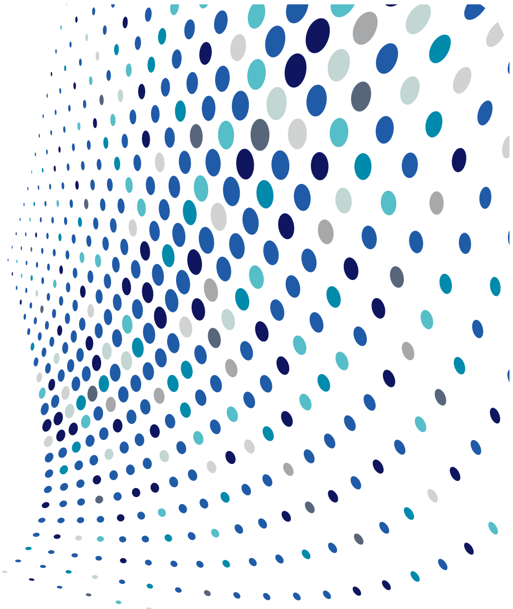
O'Melveny | omm.com



Data Security and Privacy Predictions for 2021

6 Issues to Watch

2020 was unprecedented. With the COVID-19 pandemic, large-scale nation-state cyber intrusions, and tensions with China over technology, new data security and privacy issues emerged rapidly. With a new administration, there undoubtedly will be new approaches to addressing these issues in the coming year. Here are six trends you can expect in 2021.

1 CONSOLIDATION AND COORDINATION OF DISPARATE TECHNOLOGY SECURITY EFFORTS

The Trump Administration took steps to address concerns with cyber and telecommunications security. These efforts, which grabbed headlines and leveraged federal authority in novel ways, included the May 2019 Telecommunications Supply Chain executive order, the placement of Chinese technology companies on the Department of Commerce's entity list, and the aggressive use of the Committee on the Foreign Investment in the United States ("CFIUS") to force the divestment of social media companies. Implementation of these policies, however, was fraught and lacked coordination, leaving many outstanding issues for the incoming administration.

There will be pressure on the Biden Administration to maintain some level of continuity with the prior administration on issues related to technology and China. We expect the Biden Administration to invest the time and political capital to adopt a more coordinated and deliberate approach to addressing cyber and telecommunications security, something that will be helped by Congress's creation of the National Cyber Director position in the White House.

The Biden Administration will face challenges in implementing supply chain restrictions in the telecommunications and energy sectors, as well as congressionally mandated restrictions on federal acquisitions of Chinese technology. There likely will be heightened coordination of cybersecurity requirements in federal procurement through the Federal Acquisition Security Council, including the expansion beyond the Department of Defense of the Cybersecurity Maturity Model Certification ("CMMC"). Responding to the SolarWinds incident and countering the technological ambitions of China will require the Biden Administration to cooperate significantly with the private sector.

2 TACKLING THE EU DATA PROBLEM

With Brexit and the July 2020 *Schrems II* case, reconfiguration of transatlantic data flows will begin in 2021. In *Schrems II*, the Court of Justice for the EU invalidated the EU-US Privacy Shield and called into question whether standard contractual clauses can survive in practice when companies are ordered to provide information to US intelligence agencies. Regarding Brexit, although an agreement was reached on the negotiated exit of the UK from the EU, the European Commission put off a decision on whether the UK provides adequate data protections. Now that the UK is a third country for purposes of the General Data Protection Regulation ("GDPR"), the UK may be in the same boat as the US when it comes to whether its surveillance laws run afoul of *Schrems II*.

US and EU negotiators are currently negotiating a successor to the Privacy Shield, but the sweeping scope of the *Schrems II* decision is a massive impediment to overcome. Meanwhile, European data protection authorities, which issued a number of high-profile fines in 2020, will examine uses of standard contractual clauses by electronic communications service providers in the US. The UK may face similar challenges.

Until there is an adequacy decision and a renegotiated EU-US data transfer agreement, companies transferring data to the US from the UK and the EU will be in limbo as to legal certainty. Alternative data transfer mechanisms, such as binding corporate rules, may prove inefficient, forcing companies to evaluate the compliance risk posed by European regulators.

3 REGULATION OF AI

Artificial intelligence ("AI") will continue to be a focus of regulators in 2021, as innovators unveil new technologies and stakeholders voice increased concerns of AI bias and potential misuses. Throughout 2020, concerns about misuses of AI technology gained traction. The sale of Clearview AI's facial recognition technology to numerous law enforcement agencies and private companies sparked an international debate, legal threats, and lawsuits about the use of facial recognition technologies.[1]

As we discussed in our June 2020 Survey of Global Artificial Intelligence Regulation, several states and localities have banned the use of facial recognition software by certain actors, and we expect additional restrictions will be imposed in 2021. Reports indicate that the Biden Administration will seek increased regulation of AI,[2] and Vice President Kamala Harris has voiced her support for protections to ensure technology does not further racial disparities or other biases.[3]

The Biden Administration will be building on an existing foundation of government efforts to regulate AI. In November 2020, the White House Office of Science and Technology Policy ("OSTP") finalized principles for governmental agencies to consider when proposing AI regulations for the private sector. The principles encourage agencies to, *inter alia*, promote reliable, robust, and trustworthy AI applications; provide ample opportunities for public input on AI regulation; leverage scientific and technical information and processes; and consider how AI applications may promote discrimination. Under the final guidance, agencies must submit plans to implement these principles by May 17, 2021. Additionally, OSTP recently established the National AI Initiative Office, which is charged with overseeing the US national AI strategy and coordinating AI research and policymaking across various stakeholders.

In the FY2021 National Defense Authorization Act ("NDAA"), Congress directed the National Institute of Standards and Technology ("NIST") to consult with industry to develop a voluntary, risk management framework containing best practices and standards for trustworthy AI. By the end of 2021, NIST must also issue guidance designed to help industry and the government broker voluntary AI data sharing arrangements. In addition to carrying out these directives, we expect that NIST will also issue guidance and standards pursuant to its August 2019 Plan for Federal Engagement in Developing Technical Standards and Related Tools, including final guidance regarding its principles to ensure AI algorithms yield explainable outcomes and conclusions (*see* draft guidance here).

[1] https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement; https://www.aclu.org/legal-document/aclu-v-clearview-ai-complaint.

[2] https://www.rollcall.com/2020/12/08/advocates-to-press-biden-congress-on-facial-recognition-curbs/.

[3] https://kamalaharris.medium.com/kamalas-plan-to-transform-the-criminal-justice-system-and-re-envision-public-safety-in-america-f83a3d739bae.

Finally, across the Atlantic, the European Commission is expected to propose new AI regulations "within the first quarter of 2021" following its February 2020 White Paper on Artificial Intelligence.[4] In the White Paper, the European Commission proposed creating a unique "ecosystem of trust" surrounding AI technology and a policy framework that will mobilize resources across Europe to achieve an "ecosystem of excellence" along the entire AI value chain. (*See* more in a previous client alert.) Regulations are currently being drafted, guided by input received during the public consultation period that ended last summer.

4 RANSOMWARE REACHING A BREAKING POINT

Our prediction that ransomware would be a significant trend in 2020 was unfortunately prescient. 2020 saw an enormous increase in the number and cost of ransomware attacks. Some of that increase is attributable to the pandemic, which led to new phishing techniques and remote work vulnerabilities. But the bigger, more troubling factors are the maturation of the ransomware market and the evolution of Ransomware as a Service ("RaaS").

The price of ransomware payments steadily increased over the year, and one estimate suggested that the global damage from ransomware in 2020 was US$20 billion. Because cyber actors have successfully extracted payments from affected entities, the market for ransomware has increased, the ransoms have increased, and cyber actors have developed new techniques to incentivize victims to pay. One such technique is combining data exfiltration with the ransomware attack, which offers attackers an additional and potentially repeatable avenue for exploitation.

Critical to the explosion of these attacks has been RaaS. RaaS allows sophisticated cyber threat actors to provide low-grade but effective malware to a broad range of customers while simultaneously allocating their resources to develop more sophisticated tools and services. RaaS now features leases for pre-packaged malware, customer service help lines, and services focused specifically on monetizing illicit access. This has lowered the cost and technical sophistication needed to deploy ransomware and increased the ability of illicit actors to successfully scale-up and monetize their activities.

All of this has increased the pressure on the US government to approach ransomware as a systemic problem. In response, the Department of the Treasury has made forceful statements regarding payments to sanctioned entities, creating additional dangers for entities responding to a ransomware attack. The Biden Administration has highlighted cyber issues as a priority and is likely to explore novel, proactive solutions to take on cyber threat actors and improve cybersecurity resilience. Further, the rise in ransomware payments under cyber insurance policies may impact how insurance carriers price, define, and determine what is covered by cyber insurance policies.

5 PRIVACY LAWS - BIOMETRICS IN THE SPOTLIGHT

With the Democrats in control of Congress and the White House, the likelihood of a federal privacy law has increased significantly. There is already bipartisan support for a nationwide privacy standard and for increasing privacy protections, but a sharp divergence remains between Democrats and Republicans over two key issues: (a) whether individuals will have a private right of action for privacy violations and (b) whether federal law will preempt state laws (such as the California Consumer Privacy Act) or merely provide a floor for privacy protections.

Biometric privacy will also remain a hot issue for state and federal regulators. 2021 started with the Federal Trade Commission ("FTC") announcing a settlement and consent order with SF-based Everalbum over claims that it deceived users about the use of their photos to develop and train its facial recognition technology. The FTC alleged that Everalbum, the maker of the now-defunct Ever app, made false promises and statements that users could opt out of the use of personal photos for facial recognition technology. The FTC also alleged that Everalbum falsely assured users that deactivating their accounts would delete their images and biometric information.

[4] https://ec.europa.eu/digital-single-market/en/artificial-intelligence.

The settlement and consent order required Everalbum not only to delete the ill-gotten photos and biometric data based thereon, but also all facial recognition technologies, algorithms, and models enhanced by the improperly obtained photos and data. This shows the willingness of regulators to ensure that companies do not retain any benefits from improperly used data. The order mandates that the company provide notice and receive consent for the collection of biometric information and prohibits Everalbum from making any further misrepresentations around such data. The FTC also noted that Everalbum had taken a different approach to notice and consent for residents of states with biometric laws—Illinois, Washington, and Texas—than those from other states. The FTC called for federal legislation to preempt the multi-front approach to regulating the use of biometric data.

In early January, a bipartisan slate of New York state legislators introduced Assembly Bill 27, which would grant consumers a private right of action for the misuse of their biometric identifiers or information. The proposed legislation is very similar to Illinois's Biometric Information Privacy Act ("BIPA") in that it requires notice and consent for the collection and use of biometric data and prohibits the sale, lease, trade, or "otherwise profiting" from such information. The proposed law allows for consumers to recover the greater of actual damages or liquidated damages per violation of up to $1,000 for a negligent violation and up to $5,000 for an intentional or reckless violation. Attorneys' fees and costs would also be recoverable and there is no bar on aggregated or class claims.

The increased privacy enforcement by state and federal regulators, along with the narrow Democratic majority, may provide the momentum and opportunity for Congress to finally pass national privacy legislation.

6 CHINA PRIVACY LAW DEVELOPMENTS

2021 promises to be an important year for the development of China privacy and security laws. The Civil Code, which defines the scope of privacy for the first time and enumerates infringing activities (e.g., disturbing others' private, peaceful life by phone calls and processing others' private information), took effect on January 1, 2021. Based on the trailblazing work done by the Cybersecurity Law, the Civil Code also solidifies personal information protection rules. We expect that this will increase enforcement actions as individuals seek relief under the Civil Code. To avoid being subject to such actions, companies may need to adjust their data collection activities.

Companies also should monitor the progress of the draft Personal Information Protection Law ("PIPL Draft"), which the Standing Committee of the National People's Congress issued on October 21, 2020. With seven sections and 70 provisions, the PIPL Draft sets out the first comprehensive set of principles and rules for processing of personal information in China. Similar to the GDPR, the PIPL Draft establishes: (a) the legal bases and principles for processing of personal information; (b) basic rules for processing, including notice requirements and cross border transfers; (c) data subject rights such as the right to access and delete personal information; and (d) the obligations of personal information processors.

A 12-department's joint promulgation, the Measures for Cybersecurity Review (the "Measures"), effective as of June 1, 2020, finalized rules for cybersecurity review over the purchase of network products and services[5] by critical information infrastructures operators ("CIIOs"). Prior to procurement of network products or services, a CIIO must assess potential national security risk exposure and apply for an official cybersecurity review if it determines such a procurement presents national security risks. The Measures do not define the scope of CIIOs, but leaves the identification to administrative authorities for the protection of critical information infrastructures. This means the Measures will only apply to entities that have been identified as CIIOs by relevant authorities.

The National Information Security Standardization Technical Committee also released new guidance for data security in 2020, including: (1) the Personal Information Security Specification, which focuses on the security issues of personal information and aims to standardize personal information controllers' conduct at various stages of information processing and (2) a Guidance for Personal Information Security Impact Assessment, which will go into effect on June 1, 2021, and provide a framework, methods, and procedures for companies to refer to when performing security impact assessments, along with guidance for the supervision, inspection, and evaluation of personal information security by administrative authorities and third-party evaluation agencies.

[5] Such as core network equipment, high performance computers and servers, large capacity storage equipment, large database and application software, network security equipment, cloud computing services, and other network products and services that have important impacts on the security of critical information infrastructures.

KEY CONTACTS

Tod Cohen
Partner
Washington, DC
+1 202 383 5348
tcohen@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

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
Counsel
Washington, DC
+1 202 383 5512
eschlom@omm.com

Bo Li
Associate
Beijing
+86 10 6563 4248
bli@omm.com

Kristin Marshall
Associate
Washington, DC
+1 202 383 5202
kmarshall@omm.com

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

Century City • Los Angeles • Newport Beach • New York • San Francisco • Silicon Valley • Washington, DC
Beijing • Brussels • Hong Kong • London • Seoul • Shanghai • Singapore • Tokyo
omm.com

Portions of this communication may contain attorney advertising. Prior results do not guarantee a similar outcome. Please direct all inquiries regarding New York’s Rules of Professional Conduct to O’Melveny & Myers LLP, Times Square Tower, 7 Times Square, New York, NY, 10036. T: +1 212 326 2000.