O'Melveny | omm.com

Data Security and Privacy Predictions for 2022

6 Issues to Watch

Are we here again? Although there were many developments over the last year, including a new administration in the White House, the start of 2022 sees us in a familiar place: enduring another phase of the pandemic, reading reports and warnings of major cyber incidents, and waiting for Congress to clarify privacy law in the United States.

Our predictions for 2022 are variations on enduring data security and privacy themes. Whether maturation of US state privacy laws, increased privacy and cybersecurity activity from China, or continued cyber incidents leading to federal government attention, this year will bring new challenges to businesses.

1 CONTINUED CYBER INCIDENTS WILL PROMPT INCREASED REGULATION

It is a new year and we are again facing a massive new cyber vulnerability. In 2021, we wrestled with the fallout from SolarWinds, and this year the Log4j vulnerability is occupying the attention of IT security professionals and government officials. The Log4j vulnerability relates to an open-source logging library that is used by millions of computers worldwide and could be exploited by threat actors to gain access and deploy malware. So far there has been limited public reporting of significant exploitations by cyber threat actors, but these types of vulnerabilities often have a long tail.

These large-scale incidents add fuel to the US federal government's push for new and expanded cybersecurity regulation. During the last month, the White House convened representatives from major tech companies and government agencies to discuss the national security threat posed by Log4j. However, such industry-government collaboration is unlikely to stave off increased regulation. Although cybersecurity legislation has not yet been enacted, the continued push for action by the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency, and the Federal Bureau of Investigation, as well as the stand-up of the Office of the National Cyber Director, means greater regulation through existing mechanisms should be expected this year.

2 THE UK WILL EMERGE AS A PREFERRED DESTINATION FOR PRIVACY-CENTRIC BUSINESS

Now that the UK has extricated itself from the EU, will there be a new approach to some transatlantic transfers of personal data? Although the UK has incorporated the substantive provision of the General Data Protection Regulation into its own law, and the EU has determined that this provides adequate privacy protections under EU law, there is a growing divide between the UK and EU over international transfers of personal data. When the EU implemented new Standard Contractual Clauses ("SCCs") for the international transfer of personal data in June 2020—in part to address the concern with US surveillance practices expressed in the *Schrems* II case—the UK declined to adopt those clauses. Instead the UK proposed its own framework that should be finalized sometime this year.

In contrast to the some of their European counterparts, such as Ireland and Germany, the UK may adopt a more pragmatic approach to international data transfers, since the UK has fewer concerns about US intelligence practices due to the UK-US close national security partnership. Consequently, the UK SCCs may be more business-friendly and call for less scrutiny from data protection authorities. This would make the UK a more appealing jurisdiction to conduct data-heavy operations, potentially altering the privacy and business landscape in Europe.

3 CRYPTO WILL BE REGULATED THROUGH PRIVACY

As regulators address an ever expanding market of cryptocurrencies, including decentralized financial applications, privacy considerations will become a major concern for cryptocurrency exchanges. Due in part to cryptocurrencies' central role in facilitating ransomware payments, financial regulators are increasing the pressure on cryptocurrency exchanges to comply with anti-money laundering requirements, including know your customer ("KYC") rules, and submitting civil investigative requests to cryptocurrency exchanges for customer information. This creates potential problems for exchanges with customers in jurisdictions that have rigid requirements on the use and transfer of personal information, such as the EU and China.

Likewise, those jurisdictions with active or emerging cryptocurrency markets may seek to leverage data localization laws to retain control over those markets. Cryptocurrency exchanges may find themselves stuck between US financial regulators and the obligations to provide privacy protections to customers. Acquiring customer consent to share personal information with US regulators may be a tall order for some exchanges. Either way, in 2022 cryptocurrency exchanges will need to become privacy experts.

4 CHINA WILL LEVERAGE NEW PRIVACY AND CYBERSECURITY LAWS

China is suddenly the epicenter for privacy and cybersecurity-related restrictions. In August 2020, China enacted the Personal Information Protection Law of the People's Republic of China ("PIPL"), which was modeled after the EU's GDPR. In addition to imposing familiar data handling principles, notice and consent requirements, and individual rights to correct information, the PIPL imposes novel requirements on cross-border transfers. Companies seeking to transfer personal data out of China must go through a personal information protection certification conducted by regulators and pass a security assessment implemented by the Chinese cybersecurity authority.

The new law, in addition to existing cybersecurity law and regulations, allows Chinese authorities increased power to exert significant pressure on international companies. Indeed, we have reports of the Chinese government investigating international companies and many of these and other companies proactively adjusting operations to minimize exposure. GDPR established the potential power of regulating data flows, and 2022 will reveal how China will wield that power to its advantage.

In addition, local government authorities are increasingly getting involved in privacy. Two of China's main economic hubs, Shanghai and Shenzen, implemented data regulations in January, 2022 that address the obligations of data controllers in connection with the processing of personal information. While generally consistent with PIPL, businesses operating in these area will need to take account of local regulations. This is a trend that is likely to continue.

5 THE FTC WILL INCREASE EFFORTS TO PROTECT DATA PRIVACY

New FTC Chair Lina Khan is looking to flex the FTC's data privacy muscles and the Biden Administration has given the agency the green light. In October, Chair Khan outlined her expansive vision for the agency's role in protecting consumer data privacy. Khan is leveraging a "cross-disciplinary" approach deploying competition and consumer protection laws to increase competition and protect consumers from unfair business practices. Under Khan's proposal, the FTC will "prioritize" investigating predatory or exclusionary practices by "walled garden" adtech advertising companies. In addition the FTC will investigate discriminatory, deceptive, or unfair data practices relating to biometric or other sensitive data, and reinvigorate COPPA (Children's Online Privacy Protection Act) enforcement.

Beyond enforcement, Khan wants the FTC to pursue rulemaking authority to set new limits on the way companies may interact with consumer data. This approach was backed by President Biden in Executive Order 14036, in which he encouraged the FTC to use its rulemaking authority to target "unfair data collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy." At the end of 2021, the agency was given a prime opportunity to pursue this goal when Accountable Tech petitioned the FTC to ban all "surveillance advertising" as an unfair method of competition. The petition was opened to the public for comment until the end of January.

While an outright ban on surveillance advertising is unlikely, there is no doubt that the FTC under Chair Khan will push for limiting certain digital privacy and security practices.

6 US STATE PRIVACY LAWS EVOLVE AND COME ONLINE

With federal privacy legislation still up in the air, the momentum behind state efforts to regulate personal data will accelerate in 2022, increasing the odds that privacy landscape will grow more complex. In 2021, 23 state legislatures saw comprehensive privacy bills introduced, with Virginia and Colorado enacting statutes that take effect in 2023. Adding to this momentum, the Uniform Law Commission adopted the Uniform Personal Data Protection Act in summer 2021, which could serve as model privacy laws for states to readily adopt. Bills are being actively considered in Kentucky, Massachusetts, Minnesota, New York, North Carolina, Ohio, and Pennsylvania. Although consensus has developed around some trends, including rights of access, correction, and portability, no uniform approach to privacy regulation has emerged.

Some states such as Virginia and Colorado take cues from the GDPR, requiring entities to perform data protection assessments and assigning enforcement responsibilities to the state. Others, including Massachusetts and New York, are weighing a partial or robust private right of action. Meanwhile, California's new Privacy Protection Agency has indicated it will unveil final regulations that implement the California Privacy Rights Act ("CPRA") by July 1, 2022, a full year in advance of the statute's July 1, 2023 effective date. The Agency is the first concrete deliverable of the CPRA and will share concurrent enforcement authority with the California Attorney General.

As more and differing state privacy laws come online, businesses will need to pay close attention to variations in each of these frameworks as substantive differences will require a thorough understanding of how, where, and what information a business collects and processes. And because the laws don't always adopt the same framework, merely applying the "strictest" set of rules may not be an option. As the value of data to the US economy continues to grow in 2022, state efforts to regulate privacy will likewise grow, forcing companies to pay close attention so as not to be caught off guard by new compliance requirements or enforcement actions.

KEY CONTACTS

Tod Cohen
Partner
Silicon Valley
+1 650 473 2610
tcohen@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

Lorenzo d'Aubert
Associate
Washington, DC
+1 202 383 5323
ldaubert@omm.com

Joshua Goode
Law Clerk
Washington, DC
+1 202 383 5332
jgoode@omm.com

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