Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Privacy And Cybersecurity Developments That Shaped 2020

By **Allison Grande**

Law360 (December 21, 2020, 6:34 PM EST) -- The past year has delivered big changes in the privacy and cybersecurity world, from the COVID-19 pandemic spurring a spike in ransomware attacks to an uptick in data collection questions to voters in California backing changes to enhance the state's landmark privacy law.

The U.S. Supreme Court is set to clarify the scope of a pair of decades-old laws regulating autodialers and computer crimes, and the European Union's top court cut down a popular transatlantic data transfer mechanism in a decision known as Schrems II.

"Around the world, the privacy landscape has shifted considerably in the last 12 months, from big legal changes — such as the implementation of the California Consumer Privacy Act and the Schrems II decision in the EU, which further complicated cross-border data transfers to novel privacy issues related to sharing of medical data related to COVID," said Sherrese Smith, vice chair of the data privacy and cybersecurity practice at Paul Hastings LLP.

And through it all, attorneys have kept busy "advising and providing practical guidance to clients on a daily basis as they navigate these complex changes that have significantly increased the importance of strong global privacy programs," Smith said.

Here, attorneys reflect on some of the major privacy and cybersecurity developments from a busy 2020.

COVID-19 Brings Ransomware, Data Privacy Issues to Forefront

While the effects of the COVID-19 pandemic left some attorneys worrying about the long-term viability of their practice areas, cybersecurity and privacy work continued to flourish, largely due to an increase in online attacks during the crisis and a sharpened focus on thorny questions about how to handle health and location data.

"The biggest development of 2020 was really just this dramatic shift to virtual life and e-commerce, which was already happening but that COVID-19 made happen more quickly," said Brian Kint, a member at Cozen O'Connor.

As more aspects of life went fully virtual, bad actors took advantage. Scores of lawyers and cybersecurity firms reported dramatic increases in the number of phishing emails, ransomware hits and other types of

online attacks, as employees are distracted, information-technology departments stretched thin and work being routed through less secure home networks.

State actors also stepped up their activities, zeroing in on targets that included companies and institutions working to develop vaccines and treatments for COVID-19.

"Once a lot of people shifted to working from home, there was in particular a significant increase in hackers being able to go in and lock up devices," said Arent Fox LLP partner Eva Pulliam. She said this was particularly a concern for businesses like hospitals that handle "mission-critical data" and whose takedown could put lives in danger.

These attackers primarily turned to ransomware, locking organizations out of their own systems and demand digital currency in exchange for regaining access. But attorneys began noticing an alarming twist: instead of just locking down systems, attackers were increasingly moving to filch personal data, trade secrets and other valuable information from systems before they shut them down.

"In many instances, companies have had backups available, and they've disregarded the threat," said Mark Krotoski, co-head of the privacy and cybersecurity practice at Morgan Lewis & Bockius LLP. "So it appears that the threat actors are trying to maximize the likelihood of getting a payment by saying that if companies don't pay, they can post the data they've exfiltrated on the dark web too."

As incidents continued to rise, the U.S. Department of Treasury's Office of Foreign Assets Control notably stepped in with an October warning that ransomware victims and the third-party companies that negotiate on their behalf may be penalized for paying criminals that are listed on the U.S. government's sanctions list.

"Ransomware is becoming a big and expensive enough a problem that the federal government is seeing the need to throw more resources at stopping it, and one of the only ways to stamp it out is to make it harder for [targets] to pay ransoms," said Laura Jehl, who heads the privacy and cybersecurity practice at McDermott Will & Emery LLP.

The COVID-19 pandemic also unleashed an influx of questions about how to handle the medical information that businesses suddenly found themselves having to collect and how to keep track of the virus's spread without compromising personal privacy.

"The COVID-19 pandemic changed the way we do almost everything, including accelerating the use of new technology like contact-tracing apps and creating vast troves of sensitive personal information about employees and individuals, such as temperature checks and symptom and travel histories," said Amy Pimentel of McDermott.

"That's prompted a lot of questions about what are the best practices for collecting, using and sharing this data, and how can that be done in a way that balances the need to protect employees' privacy with the need to protect the workforce," she said.

Attorneys expect to continue fielding these types of data privacy questions in 2021, especially as vaccines are rolled out and businesses consider whether to require proof of vaccination to enter places like offices, stores and public venues.

"One question that's going to arise is whether a tracking system for who's been vaccinated is going to be

developed and if that's going to somehow be associated with biometrics," said Melinda McLellan, a partner at BakerHostetler. "And if that's the case, that's likely to raise questions about what's being collected, who it's being shared with, and what kinds of notices or disclosures should be given to individuals."

California Voters Strengthen Privacy Regime

Companies kicked off the year with a Jan. 1 deadline to comply with the California Consumer Privacy Act, the first law in the U.S. to allow individuals to find out what data companies hold about them, to have that information deleted and to opt out of its sale.

As the year unfolded, businesses closely tracked several rounds of updates to regulations the state attorney general was charged with crafting to help companies comply with their new obligations.

Those rules were finalized in August, more than a month after the attorney general's office began enforcing the statute by sending out warning letters to companies that had failed to post required privacy notices or a mechanism to enable consumers to opt out of the sale of their personal data.

"A good chunk of the past year has been spent dealing with the CCPA and uncertainty around what the regulations mean for businesses, especially those in the advertising ecosystem," said Jessica Lee, co-chair of the privacy and security practice at Loeb & Loeb LLP.

Then in November, less than a year after the CCPA took effect, voters approved the California Privacy Rights Act, a ballot initiative that "ratchets up the CCPA's privacy protections and will bring a whole new stage of compliance," said Reece Hirsch, the other co-head of the privacy and cybersecurity practice at Morgan Lewis.

The CPRA, which takes effect in January 2023, creates a new agency dedicated to data privacy and handing consumers the right to limit the use and disclosure of a new category of "sensitive" personal information, which includes health, financial, racial and precise geolocation data.

The measure also empowers individuals to opt out of the sharing of their data and to correct inaccurate data, and it triples fines for the unlawful collection or sale of children's personal information.

"The bar got raised a few more notches with the CPRA, so if you're a company that was already behind and struggling to get into compliance with the CCPA in 2020, now you've got even more work to do," said Morrison & Foerster LLP partner Nathan Taylor.

Supreme Court Tackles Computer Crimes, Robocall Laws

The Supreme Court is examining whether it is a federal crime under the Computer Fraud and Abuse Act to use one's authorized access to a computer for inappropriate purposes, in a test of a key computer crimes law criticized as being dangerously broad.

In Van Buren v. U.S., the high court will have a chance to resolve a circuit split among appeals courts that have reached different conclusions on whether employees, or anyone else authorized to access a computer, face criminal or civil liability for abusing that authorization to access information for improper purposes under the CFAA, which dates back to 1984.

"It's a recurring scenario where people are told they can only use their access for one purpose and not for other purposes, so if the Supreme Court reverses Van Buren's conviction [for exceeding his authorized access], then that recurring scenario likely won't have a remedy under federal law," said Krotoski, who is also a former federal cybercrimes prosecutor and national coordinator for the computer hacking and intellectual property program in the U.S. Department of Justice's Criminal Division.

During oral arguments in late November, several justices appeared open to former police officer Nathan Van Buren's claims that the CFAA is "dangerously vague" and could criminalize innocuous online activity that may only technically violate employers' policies, websites' terms of service and other third-party restrictions.

"The court seemed to be trying to find a way to say it's not appropriate for individuals to misuse a system that they happen to have access to for their own purposes versus punishing everyone who comes to a website and violates terms of use they may have never seen before, and it's likely that the court will ultimately try to come up with a commonsense idea of what 'without authorization' means under the statute," said Aaron Charfoos, a partner in the privacy and cybersecurity practice at Paul Hastings LLP.

The Supreme Court is slated to decide the Van Buren case in the coming months, along with another high-profile privacy case that could determine whether litigation will dry up or continue to boom under the popular Telephone Consumer Protection Act.

The justices agreed to take up the dispute in Facebook v. Duguid over what qualifies as an automatic telephone dialing system, or autodialer, under the TCPA less than a week after it handed down a ruling in a separate case that upheld the statute's sweeping ban on autodialed calls to cellphones while striking down an exemption that permitted such calls to be made to collect federally backed debts.

Facebook has argued that defining the law broadly to encompass all devices with the mere capacity to automatically dial numbers, as the Ninth Circuit did, would expose users of virtually any modern smartphone to hefty liability under the statute.

Noah Duguid and his backers, meanwhile, have countered that interpreting the term narrowly to exclude equipment that dials from preexisting lists of numbers would result in companies being given the unfettered ability to bombard consumers with automated calls and texts without consequences.

During oral arguments in early December, several justices appeared receptive to Facebook's argument that the TCPA, which was enacted in 1991, narrowly prohibits only random-fired automated calls and texts to cellphones, a development that Jaszczuk PC founder Martin Jaszczuk said "portends, at long last, welcome relief for America's businesses from the TCPA's draconian reach."

"Recognizing the logical limits of the ATDS definition, many of the justices' questions appeared to indicate a clear recognition that, on both statutory construction and policy grounds, the ATDS definition simply cannot be stretched to encompass calls that do not include a random or sequential dialing component," Jaszczuk said.

The cases are Van Buren v. U.S., case number 19-783, and Facebook Inc. v. Duguid, case number 19-511, in the Supreme Court of the United States.

EU High Court Deals Major Blow to Transatlantic Data Flows

The European Court of Justice also made waves in July when it threw a wrench in transatlantic data flows by invalidating the popular Privacy Shield mechanism that more than 5,300 companies relied on to transfer personal data from the European Union to the U.S.

"The decision looms very large and casts significant doubt over companies' ability to move data from Europe to the U.S.," said Jeremy Feigelson, co-chair of the data strategy and security practice at Debevoise & Plimpton LLP.

The court cut down Privacy Shield on the grounds that it failed to provide Europeans with effective redress rights or adequately protect them from having their data intercepted by U.S. intelligence authorities.

It also directed companies and national data protection authorities to more carefully scrutinize data transfers to anywhere outside the EU using standard contractual clauses, another widely used mechanism, and to shut down those exchanges when the laws of the receiving country didn't provide adequate protections for this information.

"The decision requires companies using Privacy Shield to go back to the drawing board and those relying on standard contractual clause to do an assessment" to ensure that EU citizens' transferred data is being adequately protected, said McDermott's Pimentel.

U.S. and EU officials have already confirmed they're in talks to replace Privacy Shield, and attorneys say they'll be watching to see if the more diplomatic approach that the incoming Biden administration is expected to take to international relations has any impact on the speed or success of these negotiations.

The European Commission in November also took the long-awaited step of issuing a draft proposal to modernize standard contractual clauses, which companies will need to implement starting in early 2021.

"These new clauses will make cross-border data transfers from the EU to the U.S. even more complex, requiring a lot of additional due diligence on third parties and on the countries where the data will be transferred," said Paul Hastings' Smith.

Congress Makes Move on Cybersecurity Regulation

While the COVID-19 pandemic derailed most nonurgent lawmaking efforts in 2020, Congress was able to agree on some important measures designed to boost info security efforts in both the public and private sectors.

"We've seen across the board the issue of protected and critical infrastructure, whether its schools or local governments, being hit by cyberattacks, and now it's getting the attention of federal lawmakers," said Foley & Lardner LLP partner Aaron Tantleff.

In early December, President Donald Trump signed a bipartisan bill to mandate security standards for federal purchases of internet-connected devices that are part of the growing "internet of things" market.

The legislation requires the National Institute of Standards and Technology to develop minimum security

standards for any internet-connected device the federal government purchases, from thermostats to vehicles. Vendors also would have to create vulnerability disclosure policies so federal officials learn of security flaws as soon as they're uncovered.

Congress also inserted dozens of cybersecurity-related clauses in the sweeping annual defense policy and budget bill it sent to President Trump in December, many of which stemmed from the final report of the congressionally mandated Cyberspace Solarium Commission released in March.

Those provisions included the creation of a national cyber director position within the president's office, a Senate-confirmed position that would direct and coordinate federal cybersecurity policies.

"There's a lot of duplication across federal agencies that are studying problems from different angles and aren't necessarily coordinating or having a coherent policy on cyber issues, so the hope is that the national cyber director will help bring some unity and continuity to those work streams and how these agencies approach cyber issues," said Sam Kaplan, special counsel at Wiley Rein LLP and former assistant secretary for cyber, infrastructure, risk and resilience policy at the U.S. Department of Homeland Security.

The push to install a cyber director within the executive branch was spurred by the Cyberspace Solarium Commission's finding that a primary reason the U.S. hasn't been highly effective at defending against online attacks in both the public and private sectors was a lack of leadership at the federal level.

Having a high-level point cybersecurity person in the administration is expected to benefit not only federal agencies, many of which were swept up in a sprawling attack that was uncovered in December, but also private-sector companies that are facing mounting pressure to exchange cyberthreat information with the government, according to attorneys.

"The private sector is getting hammered by criminal cyberattacks," said Colleen Brown, a privacy and cybersecurity partner at Sidley Austin LLP. "There's no easy solution, but it's clear that there's an urgent and vital need for leadership on these cybersecurity issues."

--Additional reporting by Ben Kochman and Daniel Wilson. Editing by Philip Shea and Brian Baresch.