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

5 Cybersecurity & Privacy Predictions For 2020

By **Allison Grande**

Law360 (January 1, 2020, 12:04 PM EST) -- The expectations for companies handling personal information will continue to evolve as a new decade begins, while mounting ransomware threats, the use of facial recognition technology and the growth of insurance disputes over emerging privacy issues also will attract significant attention.

Here are five predictions attorneys expect to be the hottest topics and trends in the privacy and cybersecurity arena in 2020.

Privacy Perceptions Will Continue to Evolve

With the recent passage of California's landmark Consumer Privacy Act and the European Union's groundbreaking General Data Protection Regulation — both of which give individuals more control over how their personal information is handled and shared — companies, consumers and regulators are paying more attention to data privacy than ever.

"In general, we've gone from privacy being a specialty issue for a limited range of companies to it being a first-tier issue in almost every industry around the world," said Kirk Nahra, co-chair of the privacy and cybersecurity group at WilmerHale.

As a result, the way that data is viewed and valued is beginning to change, attorneys say.

Mary J. Hildebrand, the founder and chair of the privacy and cybersecurity team at Lowenstein Sandler LLP, observed that while companies have traditionally viewed personal information as "almost a form of intellectual property" over which they exercised complete control, this data is starting to become a "separate asset class with a new and rapidly emerging legal framework around it."

"With laws like the CCPA and GDPR, companies' ability to use and disclose data is going to be determined by the nature of the rights granted to them by the user or owner of the data, and that's a big deal," Hildebrand said.

The price tag that should be attached to this data will also be a question that resonates throughout 2020, according to attorneys.

California's new privacy law, which took effect Jan. 1, only allows companies to offer services such as loyalty programs that require consumers to waive their rights only if the offer is "reasonably related to

the value of consumers' data." That requires companies to calculate the value of this data. State and federal lawmakers have recently floated the idea of compensating consumers for the use of their valuable personal information, a push that attorneys believe will take firmer hold in the new year.

"Fueled by the acknowledgment that businesses can 'sell' personal information under various state laws, consumers will be attracted to the idea that they themselves should be paid for the use of their information," said Adrienne Ehrhardt, the chair of Michael Best & Friedrich LLP's privacy and cybersecurity practice group.

These changes have prompted regulators to train a closer eye on how tech giants' data gathering activities align with antitrust law. The U.S. Department of Justice, the Federal Trade Commission, nearly every state attorney general and officials in the U.K. and Australia are among those that have signaled that they are investigating Facebook, Google, Amazon and other major technology platforms over their market dominance, and these probes will only continue to gain steam in 2020.

"As data continues to be monetized and priced by big companies, it wouldn't be surprising to see Europe lead the way, as they have in so many antitrust actions, and for there to be more of an appetite for serious investigations along antitrust lines about what companies are doing with consumers' data," said Robins Kaplan LLP principal Michael Reif.

Ransomware Scourge to Intensify

Ransomware attacks — where cybercriminals use malicious software typically sent as an email attachment or link to seize control of a target network and lock users out — expanded in both frequency and prevalence in 2019, and the threat is expected to grow as the new decade dawns, attorneys say.

"Ransomware continues to be a real scourge and it's gradually increasing, since you don't need insider credentials to spread it and even with a tiny hit rate, hackers can get a good amount of money," said Joseph Moreno, a former federal prosecutor and partner in Cadwalader Wickersham & Taft LLP's white collar defense and investigations group.

Government officials and private researchers have warned that cybercriminals are increasingly using ransomware to specifically target vulnerable entities like hospitals and municipalities, which often have weaker IT defenses and a higher incentive to cave to ransom demands in order to quickly regain access to the data that has been locked during the attack.

Recent victims include several school districts and government agencies in Louisiana, where during the past year, two statewide emergencies have been issued by the state's governor and one by the mayor of New Orleans following ransomware attacks. Hackensack Meridian Health in New Jersey also confirmed in December that it had been forced to pay an undisclosed ransom to unlock its systems.

"What we're likely going to continue to see is a trend in ransomware attacks moving away from giant spray or splatter attacks that just hit everyone large and small and ask for a small ransom to more attacks that are really intended to target particular entities like health care companies and municipalities, on the theory that it'll be cheaper for that company to pay the ransom than attempt to recover on their own," said Seth Berman, the leader of Nutter McClennen & Fish LLP's privacy and data security group.

As a result, hospitals and other particularly vulnerable entities will move to "funnel a lot more money into this area to create more secure systems and increase employee training," Moses & Singer LLP partner Jason Johnson said.

Ransomware won't be the only major cyberthreat facing companies in the new year.

Business email compromise schemes — in which hackers trick targets into wiring them money or sharing sensitive data by pretending to be a company executive or other high-ranking official — also are expected to spread. And they're likely to get more sophisticated as hackers take advantage of artificial intelligence technologies to spoof employees by using actual audio recordings or voice manipulation to make the request seem more authentic, attorneys say.

"There was one publicly known attack that used deepfake simulation software to make it sound like the boss had called and ordered someone on the phone to follow through on an email that he had allegedly sent, and we're likely to see even more of that," Berman said.

The past few years have been punctuated by several major breaches apparently orchestrated by nation states against companies such as Equifax, Marriott and Sony, and attorneys say we'll likely continue to see big incidents like these in the headlines.

"Unfortunately, it's difficult to rule out the possibility of another major breach," said Sunil Shenoi, a partner at Kirkland & Ellis LLP. "Given how important data is to all kinds of companies, there's always a risk of such an incident."

And with high-stakes presidential and congressional elections looming in November, both election security and scrutiny of what social media companies are doing to clamp down on the spread of disinformation will be in the spotlight as well, attorneys say.

"The sophistication of threat actors and the level of cyber risks are only going to increase, especially considering the politics in the Western world right now, whether it's the general election in the U.S., or Brexit in the U.K., that provide fertile ground for these kinds of activities," said Scott Lashway, co-leader of the privacy and data security group at Manatt Phelps & Phillips LLP.

Facial Recognition Technology Regulation Will Take Center Stage

As the use of facial recognition technology by companies and the government to automate services and conduct surveillance continues to rise, state and federal policymakers are increasingly inclined to set barriers around the emerging technologies' deployment, attorneys say.

"New technologies like facial recognition have the potential to offer considerable positive benefits for society, but they can also become unduly intrusive if not subject to reasonable constraints, oversight and regulation," said Alan Charles Raul, the leader of the privacy and cybersecurity practice at Sidley Austin LLP. "The question really will be what oversight and regulatory model will develop to reassure the public that this very powerful technology will be used only pursuant to reasonable limitations and oversight."

Local governments have stepped up during the past year in response to concerns over police use of the sensitive data. The San Francisco Board of Supervisors passed an ordinance in May that would prohibit city departments, including the police department, from using facial recognition technology, and the

Massachusetts city of Somerville and Oakland, California, followed in those footsteps in July by enacting similar bans of their own.

Congress has also shown an interest in the issue, with Sens. Chris Coons, D-Del., and Mike Lee, R-Utah, floating a legislative proposal in November that would require federal law enforcement to get a warrant to track people using facial recognition technology for longer than 72 hours.

"Consumers want to feel comfortable being out in public, but at the same time effective, safeguards need to be put in place to ensure that biometric information is being used properly and with people's consent," said plaintiffs' attorney Amy Keller of DiCello Levitt Gutzler LLC.

Policymakers in the U.S. and abroad have also moved to set limits on the use of facial recognition technology in the commercial context to help companies automate their services and track consumers' behaviors.

Illinois, Texas and Washington State have laws on the books regulating the collection and retention of biometric data— with Illinois being the only one to include a private right of action, which has set off a flood of litigation —and France's data protection regulator in late December released a discussion paper exploring the technical, legal and ethical aspects of facial recognition technology and the regulator's role in ensuring its responsible use.

"In the next year, what we're likely to see is a continued and increasing focus on regulating the collection of biometric identifiers and the use of biometric information on a number of fronts," said Melinda McLellan, a BakerHostetler partner.

Andy Gandhi, a managing director with Alvarez & Marsal's disputes and investigations practice, noted that regulation of the tracking of behavioral attributes is likely to be a particular target, given mounting concerns over the ability of companies and governments to profile individuals without their knowledge.

"States are likely to drive that effort, because there's a smaller ship to turn there and more understanding of these issues, and federal lawmakers are likely to follow," Gandhi said.

Raul added that these proposals likely will be more refined and nuanced over time, as these issues become better understood and the contours of the technology become clearer. He floated the idea of creating an independent government body like Privacy and Civil Liberties Oversight Board, on which he previously served. The board is charged with considering the implications of counter-terrorism, and a similar oversight board could be useful for reviewing emerging technologies, such as facial recognition.

Attorneys also anticipate that states will continue to act to amend their data breach notification statutes to add a range of biometric data, including face scans, to the types of information whose disclosure would trigger reporting obligations.

"This is the new frontier of data collection, and it will be important to watch how sates define biometric information and whether they decide to include biometric information in their existing statutes or create additional laws to regulate this technology," said Mark Krotoski, co-head of Morgan Lewis & Bockius LLP's privacy and cybersecurity practice.

And biometrics is unlikely to be the only emerging technology to catch the attention of policymakers and regulators in 2020, attorneys say.

Facebook's move to launch the digital currency Libra attracted a wide array of regulatory scrutiny in 2019, and this heat is unlikely to die down in the new year, attorneys say.

"Libra was kind of the sacrificial lamb going out there and being piled on by regulators," said Philip Berg, chair of Otterbourg PC's privacy and cybersecurity practice. "That started a conversation and put attention on the issue, but little regulatory clarity emerged in 2019, and it's still unclear how this will all shake out."

Insurance Disputes Will Heat Up

As the insurance landscape for cybersecurity and privacy-related claims has matured, attorneys say they are seeing more coverage disputes hit the courts, and they don't anticipate any slowdown in the new year.

"As cyber incidents continue to become more diverse and frequent, and expand beyond the classic breach of credit card information, there's likely going to be continuing disputes and a growth in those disputes about coverage under relevant policies," said Mayer Brown LLP partner Stephen Lilley.

This movement is being largely fueled by the natural progression of the insurance market, with insurers beginning to be more selective in the claims they honor as they get a better grasp of the market for emerging cybersecurity and privacy risks, attorneys say.

"With these issues becoming more prevalent, insurance companies are thinking carefully about denying claims and those who bought the coverage are asking hard questions, and that's leading to more litigation," said Reif, the Robins Kaplan principal.

Attorneys say they're seeing a particular uptick in disputes involving coverage for claims arising from Illinois' unique Biometric Information Privacy Act, which has been on the books since 2008 but only recently began to prompt a wave of litigation that has raised thorny legal questions.

"In 2020, we're likely to see insurance carriers start to be even more aggressive in terms of implementing greater exceptions or increasing premiums significantly in order for companies to be protected specifically from biometric claims," said Winston & Strawn LLP partner Sean Wieber.

International Data Transfers Will Get Stickier

The free flow of information between the U.S. and European Union is vital to both companies and law enforcement, and experts foresee several important developments materializing on this front in 2020.

For one, the scores of multinationals that rely on the Privacy Shield data transfer mechanism and standard contractual clauses to shuttle data from the EU to the U.S. are waiting with baited breath for the European Court of Justice to rule on a challenge mounted by Austrian privacy activist Max Schrems, who successfully swayed the high court to invalidate Privacy Shield's predecessor in 2015.

Hopes are high that Privacy Shield and standard contractual clauses will avoid a similar fate, and companies gained some measure of assurance when one of the court's advocate generals issued an advisory opinion in December recommending that both tools be preserved while continuing to give regulators broad leeway to halt transfers on a case-by-case basis.

But the opinion is nonbinding, leaving companies looking toward the coming weeks when the Court of Justice is expected to issue its formal decision on the validity of the mechanisms.

"There's some fear around whether the Court of Justice will decide to blow up the entire data transfer scheme again," said Lisa Sotto, chair of Hunton Andrews Kurth LLP's privacy and cybersecurity practice.

Companies will also be watching for the type of deals that the U.S. continues to hammer out with foreign governments under the CLOUD Act, which was enacted in 2018 to ease the cross-border sharing of user data for law enforcement purposes after Microsoft mounted a challenge to the government's ability to access such data stored overseas.

"So far, the U.K. is the only country in the EU having signed such an agreement with the U.S.," said Ahmed Baladi, who is based in Paris and co-chairs Gibson Dunn & Crutcher LLP's global privacy, cybersecurity and consumer protection practice group. "The CLOUD Act has raised significant concern in the EU, and it would be surprising if the EU Commission does not address it in the course of 2020."

The U.K.'s planned departure from the European Union early next year also has the potential to wreak havoc on the data transfer landscape if the U.K. crashes out of the bloc without a formal agreement in place.

"Brexit in an orderly fashion would have relatively low implications at least in the short term for data protection," said Eduardo Ustaran, who is based in the U.K. and serves as global co-head of the privacy and cybersecurity practice at Hogan Lovells. "But if the U.K. ends up leaving the EU with no deal, that would be quite catastrophic, as U.K. companies wouldn't be able to benefit from the current data transfer system and it would require a lot more work to transfer data."

--Additional reporting by Ben Kochman. Editing by Rebecca Flanagan.