CYBERSECURITY 2019

DATA PRIVACY TRENDS

THE LATEST NEWS & INSIGHTS IN CYBERSECURITY

Security Privacy and the Law Blog

www.securityprivacyandthelaw.com

FOLEY HOAG LLP

Table of Contents

Introduction

By Christopher Escobedo Hart

In 2018, privacy and data security crossed a number of thresholds. In the public mind, through high-profile data breaches and revelations about unexpected uses of personal information, questions of privacy became much more salient. In the legal and regulatory arena, both the GDPR and the California Consumer Privacy Act became clear catalysts for a global transformation in the coming years of privacy practices. Finally, new technologies suggest that flux and complexity we are currently experiencing will continue, as we face new challenges and new threats to privacy.

This collection of essays addresses each of these issues. The essays collected here were each originally published as a series of posts on Foley Hoag's *Security, Privacy, and the Law* as part of the blog's 2019 "Year in Preview" series. Collected here together, they provide a holistic overview of trends affecting organizations managing personal information (and the regulations surrounding them) in 2019 and beyond.

On the enforcement side, Colin Zick, who leads the firm's Privacy and Data Security practice, provides an overview of the trends in the Health Insurance Portability and Accountability Act (HIPAA), including increased use and exchange of health data, increased sophisticated use of such data, and increased enforcement when health data is mismanaged. Michael Licker gives an overview of the enforcement trends in the hot cryptocurrency and blockchain space, noting that enforcement trends are beginning to create discernable rules of the road in the absence of clearly applicable regulations. Jeremy Meisinger takes a close look at how children's online privacy is protected, comparing and contrasting the Children's Online Privacy Protection Act (COPPA) with the GDPR's protection of minors. And Stephen Bartlett examines trends among state attorney general enforcement, where much of the governmental action has been and continues to be.

Looking at the impact of new technologies and threats, Scott Bloomberg tackles elections and political advertising, noting especially how social media companies are responding to the continuing fallout of the 2016 election. Vivek Krishnamurthy examines artificial intelligence and emerging threats, demonstrating that there are significant privacy questions yet unanswered at the same time that AI is becoming ubiquitous. And Carol Holahan analyzes, specifically digging into the Federal Energy Regulatory Commission's issuance of a final rule to modify the North American Electric Reliability Corporation's Reliability Standards to cyber security incidents.

It is not an overstatement to say that we seem to be entering a new era in privacy and data security, where we think of privacy and security differently and where potentially revolutionary new technologies force us to engage in increasingly more difficult questions. Our hope is that this collection helps you navigate this continuously evolving area.

HIPAA

By Colin Zick

HIPAA was signed into law on August 21, 1996, over 22 years ago. As a 22 year-old, HIPAA is no longer a child, but not quite a full-fledged adult. And, as a 22 year-old, it could be considered a part of the Millennial generation. As we look to the year ahead for HIPAA, what can its status as a Millennial tell us about what is to come?

Wikipedia says Millennials are characterized by "increased use and familiarity with communications, media, and digital technologies," That sounds like the current issues that are challenging HIPAA covered entities: communications (e.g., the growing use of email and testing by patients); media (e.g., the impact of social media on the provision of health care); and digital technologies (e.g., EHRs, blockchain). Of course, Millennials also like craft beer and poke bowls, so this analogy does have some limits.

What else is in store for HIPAA in 2019?

- **More data from non-HIPAA regulated data sources** (e.g., remote monitoring devices and wearables), which will challenging HIPAA's goal of greater interoperability and creating more concerns about privacy and data security.
- Nevertheless, there will be **more data exchange and more sophisticated uses of data** (as Cigna's merger with Express Scripts and CVS's merger with Aetna start to be effectuated).
- **More methods of accessing and moving data**:
  - **Telemedicine** (a Baby Boomer) **will finally start to fulfill its promise**, but along the way will bring more concerns about data privacy and security
  - As more patient-accessible gateways and portals for health information are created, privacy and security solutions will struggle to keep up.
- Increasing state privacy regulation (e.g., California Consumer Privacy Act) and a Democratic House of Representatives will drive a push for revisions and updated to the HIPAA statute and regulations:
  - **We're already seeing more guidance on what HIPAA means, with HHS's December 28, 2018 release of voluntary cybersecurity practices** to the healthcare industry in an effort to move organizations "towards consistency" in mitigating cyber threats; expect these "voluntary" practices to become industry standard in short order.
  - **And the Office for Civil Rights issued a request for information in December 2018 about existing HIPAA provisions** that may limit or discourage information sharing ("Request for Information on Modifying HIPAA Rules To Improve Coordinated Care").
- **State attorneys general will take a larger role in enforcing HIPAA**, as the ones from Arizona, Arkansas, Florida, Indiana, Iowa, Kansas, Kentucky, Louisiana, Minnesota, Nebraska, North Carolina, and Wisconsin did in December 2018, when they sued Medical Informatics Engineering, Inc., operating as Enterprise Health, LLC and K&L Holdings, and NoMoreClipboard, LLC, and joined an existing civil suit over a HIPAA breach impacting 3.9 million individuals.
- **More and bigger breaches will occur** (because there's more data, more uses of data, more movement of data, and more value to data).
- **More and bigger efforts by the plaintiff's class action bar to turn HIPAA breaches into $$$.**

Cryptocurrencies and SEC Enforcement

By Michael Licker

In our 2018 SEC year in preview post, we called attention to an expected increase in SEC cybersecurity enforcement action. The SEC has certainly lived up to the billing throughout 2018, which was the first full year in existence for the SEC's new Cyber Unit. In particular, the Cyber Unit and the SEC's Enforcement Division focused on three types of enforcement actions: (1) stopping unregistered and/or fraudulent trading of digital assets, including initial coin offerings (ICOs); (2) the safeguarding of customer information by registered entities; and (3) public company disclosures and controls.

Digital Assets/Initial Coin Offerings

The SEC made clear in 2018 that one of its top priorities is stopping the unlawful sales of unregistered digital assets. In mid-November, the SEC Divisions of Corporation Finance, Investment Management, and Trading and Markets jointly released a statement highlighting enforcement actions "involving the intersection of long-standing applications of our federal securities laws and new technologies." The release covered three types of issues that have been top of mind for the SEC in 2018: (1) initial offers and sales of digital asset securities (including ICOs); (2) investment vehicles investing in digital asset securities and those who advise others about such investments; and (3) secondary marketing trading of digital asset securities.

While one purpose of the release was to highlight areas of concern for the SEC, the Commission also made clear that it is willing to permit previously unregistered issuers to register under the appropriate circumstances. In this regard, the SEC settled two matters involving unregistered offerings of tokens on the same day it issued the release. In both cases, the issuers agreed to pay a $250,000 civil penalty, but also agreed to register with the SEC so that they could continue operating. The SEC intended these matters to demonstrate that there is a path of compliance going forward, even where issuers have already violated the law by conducting an unregistered offering of digital asset securities.

The SEC has also targeted investment vehicles that improperly fail to register as an investment company. Crypto Asset Management LP offered an unregistered hedge fund that the SEC claimed was falsely marketed as the "first regulated crypto asset fund in the United States." The fund also claimed, according to the SEC, that it was regulated by the SEC and had filed a registration statement with the SEC. However, by engaging in a non-exempt public offering and investing more than 40 percent of the fund's assets in digital asset securities, the SEC claimed that CAM caused the fund to operate as an unregistered investment company. The SEC also found that the fund's manager was an investment adviser, and had violated the antifraud provisions of the Investment Advisers Act of 1940 by making misleading statements to investors in the fund.

Third, the SEC has made clear that a platform that offers trading in digital asset securities and operates as an "exchange" must either register with the SEC as a national securities exchange or qualify for an exemption from registration. Under Exchange Act Rule 3b-16, the SEC uses a functional approach to determine whether a system constitutes an exchange, regardless of how an entity may characterize itself. The analysis focusses on an assessment of the totality of the activities and technology used to bring together orders of multiple buyers and sellers for securities using "established non-discretionary methods" under which such orders interact. This area has become a primary concern for the SEC as advancements in blockchain and distributed ledger technology have led to new methods for facilitating electronic trading in digital asset securities. These concerns led to the SEC's first case based on findings that a digital token trading platform, EtherDelta, operated as an unregistered national securities exchange. EtherDelta operated as an online platform

for secondary market trading of ERC20 tokens, which is a type of blockchain-based token commonly issued in ICOs. Because EtherDelta's platform offered trading of securities, the SEC stated that it was required to register as an exchange or operate pursuant to an exemption, which it failed to do.

In addition to the types of enforcement actions highlighted in the release, the SEC continued to focus on the making of false representations in the sale of digital asset securities. For example, the SEC halted an ICO run by Dallas-based AriseBank, which claimed to be the world's first "decentralized bank." AriseBank allegedly used other common tactics, including social media and a celebrity endorsement to raise what it claims to be $600 million of their $1 billion goal in just two months. The SEC claimed that it also falsely stated that it purchased an FDIC-insured bank, which allowed it to offer customers FDIC-insured accounts. Additionally, in May 2018, the SEC obtained a court order halting an ICO run by a self-described "blockchain evangelist." Titanium Blockchain Infrastructure Services, Inc. allegedly lied about business relationships with the Federal Reserve, PayPal, Verizon, Boeing and The Walt Disney Company, among others.

One of the key underpinnings of the SEC's digital asset securities enforcement activity is that digital tokens do in fact qualify as "securities" under the federal securities laws. The SEC, applying the traditional "Howey test," has readily concluded that they do. This view dates back at least to 2017 when the SEC issued an investigative report, known as the DAO Report, which concluded that that issuers of distributed ledger or blockchain technology-based securities must register offers and sales of such securities unless a valid exemption applies. This view, which is of course fundamental to much of the SEC's enforcement activity in this area, took a bit of a hit in late 2017 when a federal judge in the Southern District of California denied an SEC request for a preliminary injunction to stop an ICO because the court could not determine whether certain tokens qualified as securities. While the decision did not go so far as to conclude that the tokens are not securities, it paused to consider the issue in a way that the SEC's internal administrative decisions have not. It also signals a willingness of federal courts to consider that some token offerings may not involve a "security." This issue will merit close watching by industry participants in 2019.

Safeguarding Customer Information

The maintenance of appropriate cybersecurity policies and procedures also continues to be a top SEC priority. In September 2018, the SEC fined a broker-dealer and investment adviser $1 million related to a cyber intrusion that compromised personal information of thousands of customers. In doing so, the SEC charged Voya Financial Advisors Inc. with violating both the Safeguards Rule and Identity Theft Red Flags Rule. The Safeguards Rule, which is Rule 30(a) of Regulation S-P, requires every broker-dealer and investment adviser registered with the SEC to adopt written policies and procedures that address safeguards for the protection of customer records and information. The Identity Theft Red Flags Rule, which is Rule 201 of Regulation S-ID, requires broker-dealers and investment advisers registered with the SEC to develop and implement a written Identify Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of certain covered accounts.

In the VFA case, cyber intruders impersonated contractors employed by VFA over six days by calling VFA's support line and requesting that contractors' passwords be reset. The intruders used the new passwords to access the contractors' accounts and gain access to personal information of 5,600 VFA customers. The intrusion continued for several days, and the SEC claimed that VFA's security staff failed to take action such as blocking the intruders' IP addresses or freezing the compromised representatives' work sessions.

This marked the first SEC enforcement action charging violations of the Identity Theft Red Flags Rule. While VFA had a written Identity Theft Prevention Program pursuant to the rule, it did not review or update the program in response to changes in risks to its customers or provide adequate training to its employees. The SEC has repeatedly emphasized the importance of maintaining adequate cybersecurity policies and procedures, both through examinations and enforcement actions, and this is yet another reminder that simply having policies in place is not good enough. The policies must regularly reviewed and adhered to, and employees must be trained on them.

Public Company Disclosures

In 2017, the SEC previewed that the failure of a public company to make appropriate disclosures about a cyber event could lead to an enforcement action. In 2018, it followed through on the warning, assessing Altaba (formerly known as Yahoo!) a $35 million penalty based

on its alleged failure to disclose a massive data breach in which hackers obtained personal data relating to hundreds of millions of user accounts. According to the SEC, within days of a 2014 intrusion, Yahoo's information security team knew that hackers had stolen personal data of millions of customers that Yahoo internally referred to as the company's "crown jewels." However, according to the SEC, the breach was not disclosed to the public until more than two years later when Yahoo was in the process of closing the acquisition of its operating business by Verizon. During these two years, Yahoo's SEC filings stated that it faced the risk of data breaches, but from the SEC's perspective never disclosed that a large breach had occurred.

The SEC has also attempted to provide the market with guidance on when an issuer should disclose a data breach. The Commission's February 2018 guidance was its second effort (its first was in 2011) in this regard. The guidance focused on the materiality of a particular cyber risk or breach, and stressed that the need to make a disclosure must be analyzed on a case-by-case basis, depending on the nature, extent and potential magnitude of the risk or breach. In assessing whether disclosure is required, a company should consider the range of harm that an incident could cause, including to a company's reputation, financial performance, and customer or vendor relationships, along with the possibility of litigation or regulatory actions. By and large, this guidance did not provide much clarity beyond what the SEC had previously advised. In a new twist, however, the guidance also touched on insider trading and made clear that material, non-public information regarding cyber events should be treated no differently than any other material, non-public information. Officers, directors and other executives cannot trade on such information, and companies should have policies and procedures in place to guard against them doing so and also to help ensure the company makes timely disclosure of such information.

COPPA, the GDPR, and Protecting Children's Data

By Jeremy Meisinger

Since the General Data Protection Regulation (GDPR) came into effect in May 2018, one of the most common questions for practitioners is what the GDPR means for children.

As with many provisions of the GDPR, the text itself says relatively little, and precise guidance for businesses – both those intentionally directing online services to children and those that offer more general services that may be used by children – has not yet clarified all of the ambiguities created by the GDPR.

This is to be expected, because the regulatory build-out of the GDPR – in terms of guidance documents, precedents, and other helpful materials – is not yet at the same stage of interpretive and enforcement maturity as the Children's Online Privacy Protection Act (COPPA) in the United States, for which the Federal Trade Commission has had years to provide explicit regulatory standards and lengthy guidance, and for which there is an abundance of enforcement precedents. I compare below some of the key concepts under both laws because COPPA, though it differs from the GDPR, is conceptually useful in thinking about how online services can approach GDPR compliance.

What does the GDPR require with respect to children?

Article 8 of the GDPR states that processing a child's data by an online service offered "directly to a child" without parental consent is not permitted, unless "the child is at least 16 years old."[1] Where a child is below 16, "processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child." Data controllers are required to "make reasonable efforts to verify […] that consent is given or authorized by the holder of parental responsibility over the child, taking into account available technology." Recital 38 echoes that children can be expected to be "less aware of the risks, consequences, and safeguards" of using online services and so merit extra care when "us[ing] personal data of children for the purposes of marketing or creating personality or user profiles."

Many of these terms are familiar to anyone who is also familiar with the analogous COPPA Rule, which requires that "[i]t shall be the obligation of the [online service] operator to provide notice and obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children." 16 CFR 312.4(a). The difference from COPPA, however, is that under COPPA there are elaborate explanations of when a service is offered to a child, who may consent, and by what methods consent can be obtained.

When is an online service offered "directly to a child"?

Asking whether an online service is offered "directly to a child" under the GDPR is similar to asking under COPPA whether a service is "directed to a child," but with an important difference. As with COPPA, for a generally-available website, a service may be considered to be offered "directly to a child" when it is "made available to all users without any age restrictions" and where the site may reasonably be understood to target children, taking into account such factors as "site content" and "marketing plans."

But the GDPR parts ways from COPPA in applying only to online services that are in fact "directly" offered. The UK data protection authority, the Information Commissioner's Office (ICO) has flatly stated than a service "offered through an intermediary, such as a school," is not offered "directly" to a child.[2] COPPA

does not draw this distinction; rather, it applies to any service used by children, but creates special rules around services used by schools and, importantly, allows a school to stand in for a parent in providing consent for a child to use a service in an educational context.

What are "reasonable efforts" to obtain consent?

The GDPR does not define "reasonable efforts" with the specificity that COPPA does. More importantly, UK ICO guidance suggests that the term "reasonable efforts" does not have a static definition; rather, what is "reasonable" depends on the risk of failing properly to identify the individual giving consent. The UK ICO states that "subscrib[ing] to a band's e-newsletter" is a much lower risk proposition than allowing a child "to post personal data via an unmonitored chat room," and that the latter calls for "more stringent means to verify the consent." Interestingly, the UK ICO acknowledges on this point that "[c]ollecting excessive information" for the purposes of consent "is unlikely to comply with the data protection by design approach in the GDPR." In other words, a data service must collect just enough information to verify consent in light of the risk, but not so much that attempting to verify itself creates a risk of over-intrusion.

So how does a business thread that needle? The answer is not clear. Some companies are understandably re-purposing the same verification methods they use under COPPA, such as requiring a credit or debit card verification. Others are taking less intrusive approaches, which involve less certainty in terms of verification, but also less potentially "excessive" gathering of information. Ultimately, there is no one-size-fits-all solution under the GDPR.

What does "consent" mean?

Consent under both the GDPR and COPPA specifically means informed consent. Under COPPA, this means that the giver of consent must be provided with a direct notice of the online service's privacy practices, the contents of which are built out by 16 CFR 312.4(c). The GDPR does not provide this level of specificity, but does elaborate on the requisite conditions for consent-based data processing in Article 7, which itself references Recital 32. Recital 32 calls for "specific, informed, and unambiguous" consent from a data subject, following provision of "clear, concise, and not unnecessarily disruptive" notice of what data is to be collected and how it will be processed.

Thus, here too COPPA provides an imperfect, but usable, guide. The basic principles used to develop privacy policies and direct notices under COPPA can also be used to inform consents obtained for GDPR purposes. Both must focus on the important questions of (1) what information is collected, (2) how such information is used, (3) when such information may be disclosed, (4) how a data subject may access or change such information, and (5) how such information is protected. The GDPR is actually more specific in certain regards (for example, as to (4), the data subject must be given a specific set of rights to change and delete data as those obligations are laid out in the GDPR), but in thinking about GDPR compliance, COPPA compliance is not a bad place to start.

What other key differences exist between GDPR and COPPA?

The most important distinction between the GDPR and COPPA is that COPPA is a self-contained regulatory approach to children's data (although certain states, such as California, do have additional child-focused protections in particular contexts). Article 8 of the GDPR, by contrast, contains special provisions that are peculiar to children, but children are also covered by every other protection of the GDPR as well as member state-level legislation that governs child privacy. This means that, in thinking about GDPR compliance, Article 8 is only one piece of the puzzle. While COPPA provides some useful guideposts and analogies, offering internet services to children resident in the EU calls for a comprehensive approach to privacy that both takes account of the ways that children differ from other data subjects but also the ways that the GDPR protects all data subjects in common.

[1] The GDPR permits member states to lower this age to 13.

[2] https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf.

New Attorney General and Trends in State Data Privacy Laws

By Stephen Bartlett

Whether it was a Blue Wave or a "Big Victory," the midterm elections unequivocally transformed state regulatory and enforcement landscapes by sweeping in four new Democratic Attorneys General and earning Democrats a majority of those key policymaking positions. The Democrats flipped four offices with Aaron Ford (NV), Phil Weiser (CO), Dana Nessel (MI) and Josh Kaul (WI) each claiming victory over GOP opponents. Ford and Kaul each unseated GOP incumbents. While these new AGs will face a host of common issues in their home states – the opioid epidemic, criminal justice reform, and LGBTQ+ discrimination, to name a few – their greatest opportunity to effect meaningful reform may present itself at the national level.

In recent years, state AGs have become the primary line of defense in the cybersecurity universe, filling the void left by the federal government's reluctance to introduce comprehensive data privacy reforms and to aggressively combat cybercrimes. Indeed, a recent GAO report trumpeted the need for urgent action at the federal level to address the multiplying cybersecurity threats facing the nation. That report identified 4 major cybersecurity "challenges" and 10 critical actions that the federal government and other entities should take in response. The challenges included: 1) establishing a comprehensive cybersecurity strategy and performing effective oversight; 2) securing federal systems and information; 3) protecting cyber critical infrastructure; and 4) protecting privacy and sensitive data. It would be a surprise to many if the feds suddenly stirred from their slumber to address the laundry list of vulnerabilities identified by the GAO. It is far more likely that the daunting task of protecting consumers from cyber threats will remain squarely on the shoulders of state AGs.

Post-election, the Democratic AGs may feel increasingly emboldened to homogenize the existing patchwork of state cybersecurity regulations. Now holding a majority – 27 – of state AG posts, the Democrats certainly have the strength in numbers to inspire broad reform across the nation.

Are the newbies up to the challenge?

Of the four, Aaron Ford brandishes the most impressive cybersecurity CV. Ford showed his mettle while serving in the Nevada legislature by co-sponsoring a progressive cybersecurity bill, which was signed into law this past June. The law's enactment made Nevada only the third state in the nation to require website operators to inform consumers about data collection and use practices. The law requires "operators" – defined to include entities that operate a website, collect or maintain personally identifiable information from Nevada residents, or conduct activities within the state – to: 1) identify the categories of personally identifiable information being collected from consumers; 2) describe the process for consumers to review and request changes to any information collected; 3) identify the categories of third parties with whom the operator may share such personally identifiable information; and 4) disclose whether a third party may collect personally identifiable information about the consumer's online activities over time and across different internet websites. Coming full circle, Ford will now be charged with enforcing the law he pushed through the Nevada legislature. The Nevada Attorney General's Office is authorized to initiate legal proceedings if it has reason to believe that an operator is violating the above-enumerated disclosure requirements.

Ford's overarching purpose in sponsoring the bill was to ensure that "Nevada's privacy laws reflect that we are all conducting more of our lives online." But the law was also a direct rebuke of federal government's scale-back of Obama-era FCC privacy rules. Then-Senator Ford called out Congress and the President in characterizing the unraveling of FCC internet privacy protections as a grave mistake. According to Ford, continuation of the

FCC internet privacy scheme "would have been a big leap forward to help us in this digital age, but they rolled it back." Although proud of the Nevada cybersecurity law, Ford lamented that it was only an incremental step and called for Congress to do more: "We're hoping that Congress is going to make a move to reconsider some of these rules that they have not done, but in the meantime, at a minimum, we can require the disclosure component."

Although he may not have the same meaty credentials as Ford, Phil Weiser's rhetoric at least suggests acute awareness of the issues and acknowledgment that the federal government is asleep at the wheel. Weiser put Washington in the crosshairs while campaigning for Colorado Attorney General in declaring that "[w]e must be prepared to protect our consumers when the federal government is turning its back on consumer protection, privacy, and antitrust enforcement. We need a state Attorney General who can fight for us and act as a national leader on these issue." Perhaps foreshadowing collective-AG action in the data privacy realm, Weiser has condemned the Trump administration's evisceration of the Consumer Financial Protection Board and highlighted the need to "act together with other states to protect Coloradans from forces that exploit the vulnerable every day." With experience in the DOJ, academia, and the Obama White House, Weiser may be key figure in bringing together Democratic AGs to spur national advancement in cybersecurity and consumer internet protection.

In contrast, Dana Nessel and Josh Kaul have, at least in their proclamations of priority initiatives, been relatively silent on cybersecurity. Nessel, a former prosecutor in Wayne Co., Michigan and criminal defense attorney, has earmarked consumer protection as a critical initiative for her office. But, the breadth of Nessel's consumer protection focus does not, at least to this point, include attention to cyber threats and data privacy issues. Rather, Nessel has vowed to protect Michigan's seniors from fraud and abuse. Nessel has expressed desire to "do more to make certain that this epidemic of abuse and neglect and economic exploitation of seniors [is brought] to an end and that somebody is there to advocate on behalf of the elderly in this state."

Similarly, Josh Kaul, who traced his mother's footsteps in ascending to the position of Wisconsin Attorney General, campaigned on a consumer protection platform which made little mention of the grave cybersecurity issues facing his state and the nation. Promisingly, though, like his first-term counterparts, Kaul has also signaled the need for state collaboration to better protect the nation's consumers: "The federal government has rolled back some important consumer protections. Some states have stood up to take action, but Wisconsin has not." Under Kaul's leadership, it would not be surprising to see Wisconsin band together with other states on data privacy issues.

If Attorney General-elects Nessel and Kaul may lag somewhat behind their Nevada and Colorado peers in cybersecurity dexterity, they will need to get up to speed quickly. Cyber threats already outpace existing regulatory and enforcement schemes, and consumers need sophisticated regulators at the helm. As the GAO report made abundantly clear, cybersecurity issues continue to proliferate as the emergence of new technologies can potentially introduce security vulnerabilities in those technologies which were previously unknown. Until Washington decides to act, consumers will need state Attorneys General to remain steadfast in combating cyber threats and protecting personal data. As these four new AGs take office, we will monitor for any important cybersecurity initiatives and keep you informed.

Elections and Political Advertising

By Scott Bloomberg

Social media companies' and search engines' revenue models are based on creating valuable advertising platforms for marketers.

These platforms allow advertisers to reach a broad and engaged user-base at a fraction of the cost of traditional advertising, and allow them to do so on highly targeted bases. Advertisers can market their products based on users' search terms, demographics, location, affiliations, interests, and much more. The extensive amount of personal data utilized by online advertising platforms creates attendant data-privacy concerns for users and lawmakers.

Data-privacy concerns are heightened in the context of political advertising. As a result of the foreign interference in the 2016 U.S. Presidential election, users are not only wary about who is funding and organizing the political advertisements interspersed in their social media feeds, but also how much personal data those advertisers have access to, and how that data can be used. Since the 2016 election, online advertising platforms such as Facebook, Twitter, and Google have responded to these (and other) concerns by adopting comprehensive political advertising policies. While federal lawmakers have yet to act, some states have enacted online political advertising regulatory regimes.

In 2019, a few more states may enact online political advertising reforms, but with a divided government, federal legislation is unlikely to come to fruition. Accordingly, the most consequential changes to online political advertising regulations in 2019 will likely come in the form of self-regulation. And evolving social and community norms surrounding data privacy will contribute to any such changes.

Post-2016 Election Regulation of Online Political Advertising

In the wake of the 2016 election, several states enacted laws to regulate online political advertising. These laws generally impose disclosure requirements on online advertising platforms, and obligate large platforms to maintain a database of political advertisements. For example, California's 2018 Social Media DISCLOSE Act requires online platforms to include "paid for by" disclaimers or hyperlinks to payers' identifying information in certain California political advertisements. It also requires platforms to maintain publicly-available databases of political advertisements, including information about the payer's identity, the cost of the ad, and the reach of the ad. New York's Democracy Protection Act similarly institutes disclosure and disclaimer requirements for online political advertisements. The law also obligates platforms to create databases for independent-expenditure advertisements, and requires platforms to verify that independent-expenditure advertisers are registered with the state board of elections. Washington State and Maryland have also implemented online political advertising disclosure reforms.

A handful of state reforms notwithstanding, most of the post-2016 regulation of online political advertisements has come in the form of self-regulation. The largest online advertising platforms – Twitter, Facebook, and Google – have developed (and are continuously modifying) robust policies that involve disclosure requirements, public databases of political advertisements, advertiser-identity verification processes, and, for Google, some ad-targeting restrictions.

Twitter's policy requires advertisers who want to air "political content" ads in the U.S. to complete a certification process, which varies depending on the type of political content ad. An individual who wants to air an issue ad – an ad that "refer[s] to an election or a clearly identified candidate," or "that advocate[s] for legislative issues of national importance" – must provide Twitter with a U.S. government-issued photo ID and a U.S. mailing address. An organization must supply its EIN or Tax ID number and a U.S. mailing address. For "political campaigning ads" – in relevant part, those "that advocate for or against a clearly identified candidate for Federal office" – individuals must provide a U.S. passport, a government-issued photo ID with a U.S. mailing

address, and a notarized form affirming the accuracy of the submitted information. An organization that is not registered with the FEC and that wants to run a political campaigning ad must have a natural person submit his or her passport number, other identifying information, and a U.S. mailing address. Once this identifying information is submitted, Twitter sends a paper form to the provided mailing address to verify its legitimacy.

For Facebook, any advertiser that wants to run an "election-related or issue ad" must comply with an authorization process that includes identity and location confirmation. To confirm that the advertiser has a U.S. location, Facebook requires the advertiser to enter its address, then sends a letter to the address. The letter directs advertisers to a URL where it must enter a code included in the letter. To confirm the advertiser's identity, Facebook requires advertisers to upload an image of her U.S. driver's license, state identification card, or passport, to enter her zip code, and to enter the last four digits of her social security number.

Google's political advertising policy also requires verification through the submission of individual or organizational identifying information for certain types of political advertising. Uniquely, Google also requires advertisers to complete this verification process before they can target users based on users' political affiliations, ideologies, and opinions. If John Doe wants to market his political rally by advertising to Republicans on Google, he will first have to verify his identity and location in the U.S. For that matter, if ACME Corp. wants to market its widgets to pro-choice advocates, it will have to do the same.

Forecasting 2019: Industry Self-Regulation & Evolving Data Privacy Norms

For social media companies (and other online advertising platforms), 2019 will likely be an important and challenging year when it comes to online political advertising. As an initial matter, the status of state-level regulation is in flux. Recent Democratic pick-ups in Maine, Colorado, New Mexico, Nevada, Connecticut, and Illinois make those states possible candidates for online political advertising reforms. New regulatory regimes may prompt platforms to adopt special advertising rules for some jurisdictions, or to forego advertising in some state elections altogether. At the same time, a Maryland lawsuit calls into question the constitutionality of state disclosure regimes, as applied to media organizations.

On the federal level, social media companies such as Facebook have expressed support for the Honest Ads Act, which would increase disclosure requirements, mandate political advertisement databases, and require platforms to make reasonable efforts to ensure that foreigners do not buy political advertisements. While Congressional Democrats will almost certainly shepherd the Act through the House, it is exceedingly unlikely to survive in the Republican-controlled Senate.

With a lack of federal regulation and only minimal state regulation, changes in online political advertising regulation in 2019 will likely come in the form of self-regulation. Whether and how social media companies (and other online advertising platforms) change their political advertising policies will depend on how social and community norms evolve along a number of fronts. Most relevantly for present purposes, this includes data privacy norms.

Social media companies' self-regulation of political advertising requires a difficult balancing act. On the one hand, the companies' revenue models revolve around advertising; and more particularly, an advertising product that allows marketers to reach highly targeted audiences. On the other hand, social media companies must ensure that their advertising policies conform to social and community norms, lest their user bases become disaffected, causing a drop in user numbers or user engagement, and, correspondingly, a less desirable audience for advertisers. Further, social media companies may tailor their policies to address concerns raised by lawmakers, so as to not invite more stringent regulation. These factors create an incentive to restrict political advertising practices in some situations.

While there are several ingredients that go in to this chemistry of pro- and anti- self-regulatory incentives, evolving data-privacy norms play an important role in forecasting industry self-regulation of political advertising in 2019. In the coming year, data-privacy regimes in Europe and California will frequently be in the news, and public scrutiny of data policies will surely persist. Furthermore, campaign finance and political advertising practices are likely to be at the center of a Democratic presidential primary in which several candidates will be pushing for democratic reforms. As these inputs cause social and community norms to evolve, online political advertising policies may need to evolve along with them.

In particular, data-privacy norms related to online political advertising could shift based on what personal data should be utilized for political advertising purposes and who should be allowed to use that personal data for political advertising. As to the former, online advertisers are allowed to microtarget their ads based on a host of highly-specific user information. Community and social norms may evolve to become less tolerant of microtargeting when advertisements include political messaging or are targeted based on political affiliations or beliefs. This may prompt platforms to institute restrictions surrounding what personal data can be used to target political advertising, and how political personal data can be used in advertising.

As to who users will tolerate receiving targeted political advertisements from, lawmakers and users have thus far been mostly concerned with foreign actors exploiting social media to interfere in our democracy. That is why platforms have taken steps to attempt to verify that political advertisers are U.S. persons. But as norms around money-in-politics continue to shift in 2019, lawmakers and users may also grow weary of how domestic organizations – often anonymously – utilize user data for political messaging. These changed norms could prompt platforms to restrict the targeting capabilities of certain types of political organizations; namely, so-called "Dark Money" groups or "SuperPACs."

Conclusion

In sum, evolving norms surrounding data privacy and money-in-politics may intersect in 2019 to prompt significant changes in online political advertising policies. The precise nature and extent of these changes are difficult to predict; however, online advertising platforms should be attuned to these evolving norms in order to respond with appropriate policy changes.

AI, Security, and Emerging Threats

By Vivek Krishnamurthy

Predicting the future is always a bit of a mug's game, given that today's bold claims about what is coming next often end up being served as tomorrow's "claim chowder," to use John Gruber's memorable phrase. Despite the risks in doing so, here are a trio of emerging privacy and cybersecurity threats that seem likely to create headlines (and billable hours for attorneys) in the year to come.

Hardware Security Flaws, By Accident and By Design

2018 was the year that concerns about security vulnerabilities in hardware really came to the fore. It was the year that the world learned of the Spectre and Meltdown design flaws afflicting nearly every microprocessor manufactured in the last 20 years, but also the year that we seriously confronted the possibility that global electronic supply chains are vulnerable to state-level actors introducing security flaws into equipment during the manufacturing process. The accuracy of the Bloomberg News story alleging that Chinese spies implanted chips onto motherboards manufactured in that country by U.S.-based Supermicro has been hotly contested, yet the story demonstrates how easy it would be for an adversary possessing privileged access to the supply chain to introduce hardware flaws into devices. Indeed, the concern that devices and equipment manufactured by Chinese telecommunications companies such as Huawei and ZTE contain vulnerabilities is the key reason why several Western governments—including the United States and Australia—have imposed bans on the use of these companies' products in various parts of their networks.

Given the central role China plays in global electronic supply chains and the growing mistrust of the products manufactured by its "national champions" in much of the world, 2019 might well be the year that we see substantial efforts to secure these supply chains against malicious interference. Interestingly, there is much scope for such efforts to leverage the work that has been done over the last 20 years to audit, assess, and address the social and environmental impacts of supply chains. Such assurance systems could be leveraged for new purposes, though it will take a great deal of cooperation between competitors who use the same suppliers and components to develop effective measures.

A key question will be how the Chinese government reacts to this growing problem and any efforts to solve it. Will the Chinese leadership view it in their strategic interest to be a trusted supplier of products and services to the global market? Or will they find that their geopolitical aims (from their "Made in China 2025" policy to the "One Belt, One Road" initiative) are better served by exploiting their current position as the "world's factory," regardless of the long-term costs?

Encryption Policy: From Bad to Worse

Another major looming risk on the horizon comes from understandable yet ultimately ill-advised government moves to regulate encryption—such as by mandating the inclusion of backdoors into encrypted systems to permit lawful access. For the better part of the last five years, some version of the "Going Dark" debate has been raging, wherein law enforcement and intelligence officials complain about their investigative efforts being stymied by the growing prevalence of encrypted devices and services. This debate reached a fever pitch here in the U.S. back in 2016 when the Obama Administration sought to compel Apple to help it decrypt an iPhone belonging to the perpetrator of a mass shooting pursuant to the authority of the 1791 All Writs Act. In that case, as in many others, governments were ultimately able to find a way into the encrypted device because security software, like everything else produced by human hands, inherently contains flaws and imperfections that can be exploited.

Yet it is the fact that all software contains security flaws that points to the dangers of legislative proposals—such as the one recently enacted by the Australian Parliament—that would require technology companies to provide government agencies with access to encrypted communications. No reasonable person would deny that security threats need to be detected, that crimes need to be investigated, and more generally that no one and nothing should be beyond the reach of fair and just legal process. That said, the notion that we can improve our security against crime, terrorism, and other threats by weakening or restricting encryption fails to understand the security risk inherent in doing so. To paraphrase Bruce Schneier, the trade-off in weakening or restricting encryption is not between security and privacy, but rather between more or less security against different kinds of threats. While it is clear that the pervasiveness of encryption in our society has some very significant negative consequences, the threat posed by weakening encryption is far worse—given that so many mission-critical systems in our society (from healthcare to utilities to defense) all operate using the same commodity hardware and software.

Even so, pressure has been building in a number of jurisdictions to enact regulations to restrict or limit the use of encryption, or to require the providers of encryption technologies to provide governments with various forms of assistance to decrypt encrypted data—from best efforts assistance to the mandating of backdoors. Now that Australia has enacted legislation, 2019 may well be the year that efforts in other leading industrialized countries begin to gain ground—with serious consequences for us all.

AI and Privacy

2018 was also the year that hype about AI reached fever pitch. There are breathless predictions everywhere about how AI will transform society. Many of these predictions are dystopian, from the potential of killer robots to run amok to the possibility that automation will put millions of people out of work, but there is the occasional glimmer of hope, such as in stories of how AI systems are routinely beating the best doctors in diagnosing certain diseases.

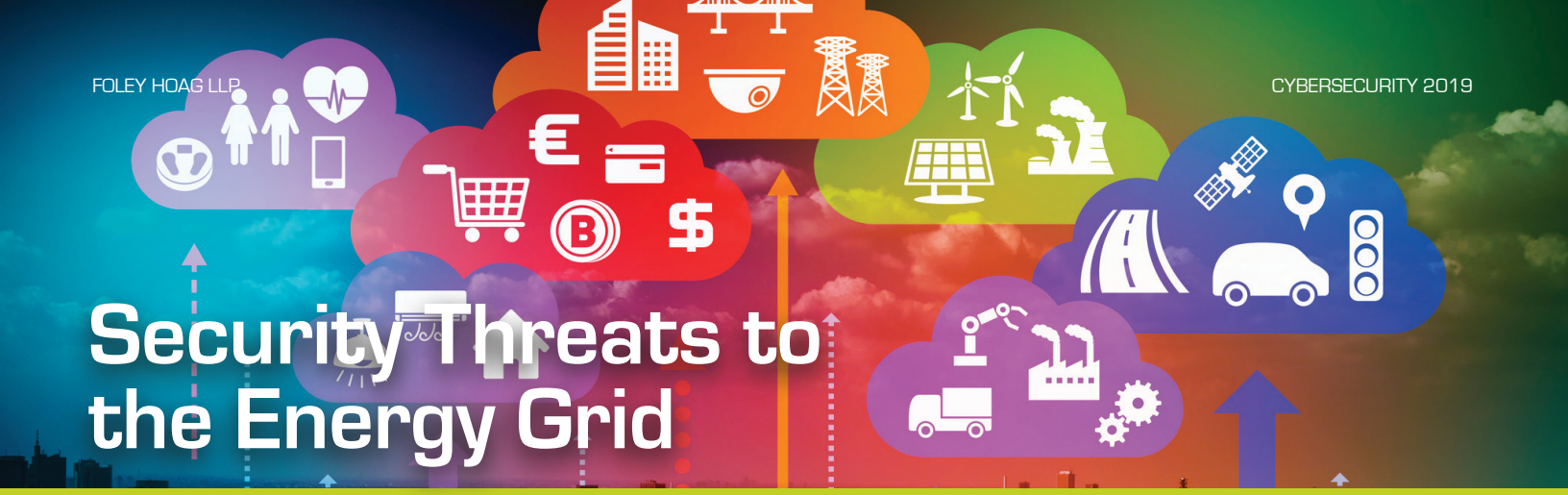
Regardless of whether you're an AI optimist or a pessimist, there's no getting around the fact that AI is a data-hungry technology. Current machine learning techniques are premised on feeding algorithms vast sums of data from which they identify patterns and correlations that are used to make predictions. This is true of everything from the algorithms that power autonomous vehicles (which learn to decide how to drive the car based on petabytes of training data), to those underlying credit scoring models (which look at an array of financial data points to judge your credit-worthiness).

There are obvious challenges associated with ensuring that existing privacy laws are respected when data subject to these laws is fed into an AI system—whether for training or for analysis. What is much more difficult to deal with, however, is the manner in which AI-powered techniques can take data in which an individual has no privacy rights to generate powerful predictions about them.

The capture of the "Golden State Killer" in California last year exemplifies the challenge. By running DNA samples that had been collected at crime scenes nearly a quarter-century ago against online genealogical databases, the police were able to determine that the suspect bore specific degrees of consanguinity with other individuals in those databases. This allowed the police to narrow down the pool of potential suspects down to the individual who was ultimately arrested.

What is not yet widely appreciated is that the same techniques used to nab the Golden State Killer can be used to generate powerful predictions about other aspects of our lives from data belonging to the people around us. Much can be predicted about my health, my finances, and a multitude of other characteristics by looking at data from my spouse, my children, my close relatives, or my good friends. Since the data being used to generate predictions and insights about me fundamentally pertains to other people, however, existing privacy laws offer me few protections against such uses.

These are emerging challenges that current data privacy frameworks are simply not equipped to handle. In the long run, government regulation might be required to provide individuals with privacy protections in information pertaining to others that nonetheless reveals something fundamental about us. In the meanwhile, however, companies operating in this space would do well to seek wise counsel on how to do so in a socially responsible manner, so as to avoid problems later.



Security Threats to the Energy Grid

By Carol Holahan

While 2018 has been a year of unprecedented and escalating cyber-related threats generally, such has certainly been the case with respect to attacks on the nation's domestic energy facilities.

For example, a media report from earlier this year describes hackers' successful infiltration of the control rooms of multiple electric utilities. According to the article, and many others like it, attacks by both independent and state-sponsored hackers pose an on-going and constant threat to the security of the nation's bulk power system. Agency oversight of the industry has focused on fortifying infrastructure against physical intrusion, erecting firewalls and other barriers to prevent electronic entry, and developing effective detection, monitoring, and reporting systems.

In response to the rising number of cyberattacks, the Federal Energy Regulatory Commission ("FERC"), pursuant to its authority under the Federal Power Act, issued a final rule earlier this year directing the North American Electric Reliability Corporation ("NERC") to develop modifications to NERC's Reliability Standards related to cyber security incidents. FERC's new rule requires NERC to "augment the mandatory reporting of cyber security incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the bulk electric system." In a statement accompanying the new rule, then FERC Chairman Kevin McIntyre voiced FERC's growing concern with respect to cyber threats stating, "Industry must be alert to developing and emerging threats, and a modified standard will improve awareness of existing and future cyber security threats…Cyber threats to the bulk power system are ever changing, and they are a matter that commands constant vigilance."

FERC's new rule addresses NERC's Critical Infrastructure Protection Standards, which apply to responsible entities comprising the nation's bulk power system, including large utilities, transmission systems and generation facilities. Importantly, the new rule lowers the threshold for a "reportable cyber event." Not only is this change aimed at creating consistency in reporting, but also will ultimately result in better data collection for assessing the true scope and scale of cyber-related threats. These minimum reporting attributes include: 1) the functional impact of the attempted or achieved incident; 2) the attack vector of the attempted or achieved incident; and 3) the level of intrusion of the attempted or achieved incident. FERC expressly left to NERC the discretion to augment the list "should it determine that additional information would benefit situational awareness of cyber threats." Moreover, whereas NERC's current standards obligate responsible entities to report a cyber incident only when it has successfully "compromised or disrupted" one or more "reliability tasks," FERC's new rule requires NERC to adopt standards that include not only successful incidents, but also any "attempt to compromise" an entity's electronic security perimeter or associated electronic access control systems.

Perhaps equally as important, however, the rule directs NERC to change its current reporting requirements to ensure that information related to cyber events is also shared with the Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). In discussing the reporting discrepancies and deficits in information sharing by various federal agencies, FERC noted that in December of 2017, NERC reported zero reportable cyber security incidents in 2016, the Department of Energy reported four cyber security incidents for the same period, and ICS-CERT reported that it had responded to 59 incidents in the energy sector in 2016. Based on this data, FERC correctly concluded that, "the current reporting

threshold in [the NERC Reliability Standard] may not reflect the true scope and scale of cyber-related threats facing responsible entities."

FERC's rule change mandating a lower reporting threshold and greater information sharing should help eliminate at least some of the reporting disparities highlighted by FERC. While this may shed some additional light on the true extent of cyber threats on energy facilities, all indications already demonstrate that the bulk power system is and will remain vulnerable to cyberattacks. Both the energy industry and the federal government, however, have taken a proactive approach to dealing with current and emerging threats by taking critical steps towards identifying and reducing vulnerability. Continued vigilance and a commitment to sharing information can only help to insulate the country's domestic energy resources from a successful cyberattack.

About the Authors

Christopher Escobedo Hart
Counsel *- Boston*
p: 617 832 1232
e: chart@foleyhoag.com

Colin Zick
Partner, Chair, Privacy & Data Security Practice *- Boston*
p: 617 832 1275
e: czick@foleyhoag.com

Michael Licker
Partner *- Boston*
p: 617 832 1197
e: mlicker@foleyhoag.com

Jeremy Meisinger
Associate *- Boston*
p: 617 832 3029
e: jmeisinger@foleyhoag.com

Stephen Bartlett
Associate *- Boston*
p: 617 832 3007
e: sbartlett@foleyhoag.com

Scott Bloomberg
Associate *- Boston*
p: 617 832 1242
e: sbloomberg@foleyhoag.com

Vivek Krishnamurthy
Counsel *- Boston*
p: 617 832 1711
e: vkrishnamurthy@foleyhoag.com

Carol Holahan
Counsel *- Boston*
p: 617 832 1125
e: cholahan@foleyhoag.com