Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | August 2019

Advancements in technology continue to push privacy laws and regulations in new directions. Policymakers and regulators are being challenged to deal with privacy issues raised by developments in big data, mass communications, and internet connectedness – to say nothing of artificial intelligence (AI). In this issue, we start by discussing new litigation that highlights the challenges – and risks – of de-identification in a world of big data, in an article by Antonio Reynolds, Dot Powell-Woodson, and Boyd Garriott. Next, Lee Goodman discusses the legal issues raised by tech-driven dissemination of government-mandated political disclosures.

From there, Kevin Rupy delves into the latest government efforts to protect consumers from invasive illegal robocalls. Jackie Ruff and I discuss the coming phase of regulation of AI, which will include close scrutiny of privacy issues. And Megan Brown, Kat Scott, and Boyd Garriott explain NIST's draft IoT cybersecurity baseline, which will play a critical role in IoT security going forward.

As always, please reach out with suggestions or feedback. And watch out for more in the coming months on the latest developments in California's privacy law, slated to go into effect at the beginning of next year. I can be reached at 202.719.4533 or dpozza@wileyrein.com. Thank you as always for reading.

-Duane Pozza, Partner, Privacy & Cybersecurity Practice

ALSO IN THIS ISSUE:

New Litigation Brings De-Identification of Health Care Information Back Into the Spotlight

By Antonio Reynolds, Dorthula Powell-Woodson, and Boyd Garriott

Significant advances in technology have resulted in the development of an increasing number of connected medical devices, software applications, and online health systems. However, these innovations have raised new and challenging questions about the protection of health information by, among others, health care providers, health plans, and technology companies handling health information.

Dinerstein v. Google

On June 26, 2019, a proposed class action – *Dinerstein v. Google, the University of Chicago Medical Center, and the University of Chicago*, Civil Action No. 1:19-CV-04311 – was **filed** in the U.S. District Court for the Northern District of Illinois. In the complaint, the plaintiff alleges that the University of Chicago Medical Center,

continued on page 2

New Litigation Brings De-Identification of Health Care Information Back Into the Spotlight

Continued from page 1

in contravention of HIPAA, unlawfully shared the Electronic Health Record (EHR) of "nearly every patient from the University of Chicago Medical Center from 2009 to 2016." These records, according to the plaintiff, were shared without patient authorization to assist Google in designing its own proprietary and commercial EHR system.

The University has denied the claims through a spokesperson, as a responsive pleading has not yet been filed. According to the spokesperson: "The Medical Center entered into a research partnership with Google as part of the Medical Center's continuing efforts to improve the lives of its patients. That research partnership was appropriate and legal, and the claims asserted in this case are baseless and a disservice to the Medical Center's fundamental mission of improving the lives of its patients."

De-Identification Requirements Under HIPAA

Under HIPAA, health care providers and other covered entities generally may not disclose EHRs to third parties for commercial purposes without written patient authorization. They may, however, use or disclose the information without authorization if the information is "de-identified." At the heart of the dispute between plaintiff and defendants is de-identification and what steps must be taken to reasonably de-identify health information that is furnished to third parties.

HIPAA's long-standing **de-identification standard** provides two methods of de-identification that are sufficient for compliance with the statute. U.S. Department of Health and Human Services (HHS) **guidance** calls them the "expert determination" method and the "safe harbor" method. *First*, the "expert determination" method provides that an expert statistician may certify that the risk of re-identification is "very small" for a given data set.

Second, the "safe harbor" method is applicable if a provider removes 18 enumerated identifiers, including "names," "email addresses," "Social Security numbers," and others. The wrinkle, however, is that removal of the 18 identifiers is insufficient if one has "actual knowledge that the information could be used alone or in conjunction with other information to identify an individual who is a subject of the information."

In addition to the two de-identification methods above, HIPAA rules also **provide** for the sharing of a "limited data set ... only for the purposes of research, public health, or health care operations." This rule allows for the sharing of health data with *some* direct identifiers – but still precludes sharing names, Social Security numbers, etc. – in tandem with a "data use agreement" that requires, among other things, specific and limited use of the data and "appropriate safeguards" to prevent use or disclosure of such data. Finally, this method requires the disclosing party to take "reasonable steps to cure" if it becomes aware that the recipient is in violation of the data use agreement.

Looking Forward

The exception to the safe harbor – where information could be used "in conjunction with other information" to re-identify an individual – presents a thorny issue in the world of big data. As the *Dinerstein* plaintiff put it: "Google has access to nearly unlimited information capable of re-identifying medical records." If that is true – and only time will tell if it is – the exception could swallow the rule, as there is an argument to be made that big technology companies have the capability to re-identify most "de-identified" data by using troves of complex consumer profiles in tandem with advanced machine learning.

These kinds of issues were probably not on HHS' radar when it promulgated its de-identification standard nearly a decade ago. But they are a reality now. As a result, the question increasingly becomes how a company will credibly maintain that it does not

continued on page 3

The Downside of Government-Compelled Exposure Needs Scrutiny

By Lee E. Goodman

The U.S. Supreme Court ruled in *NAACP v. Alabama* in 1958 that the First Amendment protects the privacy of political associations and donations. The State of Alabama had sought to compel the NAACP to disclose the names of its members and donors in order to establish that the NAACP had been doing business in Alabama without registering over several years. The NAACP resisted the disclosure because government officials would make the information public, thereby exposing NAACP members and donors to harassment, loss of employment, and even threats of physical harm. The Supreme Court ruled that government exposure policy is responsible when it triggers private retaliation and harassment against the citizens who are exposed. It struck down the disclosure requirement under the First Amendment, thus protecting the political privacy of NAACP members and donors. This landmark case recently was analyzed in ***Privacy in Focus***.

The Supreme Court subsequently protected the right to associational privacy in many contexts following its holding in *NAACP v. Alabama*. However, two decades later, in its 1976 *Buckley v. Valeo* decision, the Court made an exception, upholding a law requiring the disclosure of contributors to election campaign committees. The government argued that people making contributions to campaigns for public office presented a unique need for public exposure. Such exposure was necessary, the government posited, to combat the corruption of politicians. So long as contributors were publicly disclosed, it reasoned, the public could hold candidates and elected officials accountable, thereby reducing the chances of politicians doing improper favors for contributors.

The government did not argue – indeed denied – that other candidates or public officials would weaponize public disclosure of campaign contributors to retaliate against them, harass them, or hold them out to public ridicule, economic loss or perhaps worse. But that happened recently when U.S. Rep. Joaquin Castro **published** the names of 44 Trump campaign contributors (some of whom ironically were Castro contributors too), accusing them of responsibility for the President's rhetoric about immigration that Castro found objectionable. He also identified their businesses. This was publicly interpreted by many as a shaming or "doxing" exercise intended to invite retaliation against the disclosed individuals. The Castro event has renewed legal and popular debate over the proper and improper uses of government-compelled exposure of private associations. The Castro event also has underscored the inherent

continued on page 4

New Litigation Brings De-Identification of Health Care Information Back Into the Spotlight

Continued from page 2

have "actual knowledge" that de-identified information it provides a tech company could be re-identified. Simply complying with the "safe harbor" might not be enough, and additional contractual commitments beyond HIPAA may become warranted. ■

For more information on these and other de-identification issues, please contact:

Antonio J. Reynolds
202.719.4603 | areynolds@wileyrein.com

Dorthula H. Powell-Woodson
202.719.7150 | dpowell-woodson@wileyrein.com

Boyd Garriott
202.719.4487 | bgarriott@wileyrein.com

The Downside of Government-Compelled Exposure Needs Scrutiny

Continued from 3

dangers and potential misuses of government-compelled exposure.

Since the *Buckley* decision, the lower federal courts have blithely extended the public exposure rules tailored for campaign finance and upheld mandatory public disclosure requirements in far-flung contexts such as speakers and associations engaged in issue advocacy, public policy discussions, nonprofit solicitations, and state ballot measure advocacy. Many of these scenarios involve little risk of corrupting politicians but do enable doxing designed to silence speakers. Although the Supreme Court has reiterated its endorsement of compelled exposure of donors in the campaign finance context in a number of cases (*see, e.g.*, *Citizens United v. FEC* in 2010), the Court has been reticent to clarify the First Amendment limits for compelled exposure in other contexts. However, after the Third Circuit upheld a Delaware law requiring the disclosure of donors to groups that post public officials' voting records on the internet, in *Delaware Strong Families v. Attorney General of Delaware* (2015), two Justices – Justice Thomas and Justice Alito – voted in favor of granting certiorari. Observers are watching closely to see if the two new Justices, Justice Gorsuch and Justice Kavanaugh, will join them to provide the four votes needed to grant Supreme Court review of government-compelled exposure in such other contexts and, at least, delimit *Buckley* to campaign finance and the corruption of politicians.

A handful of cases are pending in lower courts that could make their way to the Supreme Court for review and offer the opportunity for the Court to provide needed clarification. They include two cases in the Ninth Circuit, *Center for Competitive Politics v. Harris* and *Americans for Prosperity Foundation v. Becerra,* which require disclosure of donors to certain nonprofits. A petition for certiorari is expected in *Becerra* by August 26. Another potential review vehicle is *The Washington Post v. McManus,* pending in the Fourth Circuit, which involves *The Washington Post*'s challenge to Maryland's law requiring internet-based advertising platforms to collect and publish extensive detailed information about political advertisers. So, stay tuned.

For more detail on the First Amendment political privacy issues in need of clarification by the Supreme Court, see the recent article by Lee Goodman in ***Privacy in Focus***. ■

For additional information on the right of political privacy generally, please contact:

Lee E. Goodman
202.719.7378 | lgoodman@wileyrein.com

Targeting Voice Providers That Encourage Illegal Robocalls

By Kevin G. Rupy

Since the beginning of this year, industry, regulators, and elected officials have made significant strides in their collective efforts to address the tide of illegal robocalls flooding consumer phones. These collective efforts have generally focused on three components: 1) empowering consumers with tools to block or restrict illegal and unwanted robocalls; 2) strengthening caller ID authentication; and 3) increased enforcement against illegal robocallers. A recently emerging – and potentially significant – additional component involves identifying and targeting voice providers that are actively and deliberately engaged in the generation of illegal robocalls.

Expanding the Holistic Approach: Identifying and Targeting Bad Actors

While no single component can independently solve the robocall problem, there is increased focus on identifying and targeting the service providers that are actively facilitating illegal robocall traffic. In a pending rulemaking proceeding at the Federal Communications Commission (FCC), the agency specifically seeks comment on how best to target "those voice service providers that are most likely to facilitate unlawful robocallers." The most meaningful aspect of such an approach is that it effectively stops illegal robocalls at the source. While consumer tools can mitigate some – but not all – of this traffic on the terminating end of a call, removing such traffic at the source stops it from ever originating in the first place.

Even illegal robocallers themselves agree that such providers should be identified and targeted. In his 2018 Senate testimony, Adrian Abramovich – who was fined $240 million by the FCC for robocall violations – noted that the VoIP providers that actively solicit customers for "short duration calls" are critical to the proliferation of illegal robocalls. He said that companies advertising for such traffic will accept "all the calls you can throw at them," and "never ask" about the caller ID information used by their customers. Abramovich was undoubtedly correct when he stated that such providers are "fueling" illegal robocall traffic, and that it would be a "good idea" to focus on the "five or six companies" responsible.

Facilitators of Illegal Robocall Traffic Are Easier to Find

While the exact number of voice providers responsible for generating such traffic may currently be unknown, the ability to identify them has substantially improved due to the increasing capabilities of industry traceback efforts. In recent years, the time needed to trace back illegal robocalls has been reduced from weeks to days – sometimes even hours. These traceback efforts will be further enhanced as SHAKEN/STIR deployments become more widespread, and the true origin of illegal robocall traffic can be even more rapidly identified.

Industry is actively sharing the results of its traceback investigations with various enforcement agencies, to include the FCC and the Federal Trade Commission (FTC). Indeed, in a recent Senate hearing this year, FTC Chairman Joseph Simons acknowledged that his agency was aware of specific voice providers that are in the business of facilitating illegal robocalls (**this link**).

For its part, while the FCC has not yet taken enforcement action against voice providers facilitating illegal robocalls, it has expressed a willingness to publicly identify those that have not supported industry traceback efforts. In November 2017, the FCC's Enforcement Bureau and Chief Information Officer issued letters to eight voice providers that were not supportive of industry traceback efforts. Notably, four of those letters sought information from voice providers pursuant to the Section 403 of the Communications Act, which provides the FCC with the authority to pursue an inquiry on its own motion.

continued on page 6

Targeting Voice Providers That Encourage Illegal Robocalls

Continued from 5

To Abramovich's point about company advertising, the Section 403 letters sought information about the "marketing materials" used by the companies to advertise their services to wholesale and retail customers.

Remediation Measures for Illegal Robocallers

The docket in the FCC's current rulemaking proceeding includes various stakeholder proposals for frameworks to address the activities of voice providers facilitating illegal robocall traffic. Some of these proposals are more regulatory in nature, while others propose a more industry-centric approach. For example, one approach would establish a registration and best practices framework analogous to the one established by the FCC in its Rural Call Completion proceeding. Whereas the Rural Call Completion framework is designed to ensure the termination of calls, the framework proposed in the robocall proceeding focuses on ensuring the integrity of calls on the origination end.

Another proposed framework is less prescriptive in nature. It would have the FCC publicly identify "particularly egregious providers that facilitate illegal robocalls," such as those that repeatedly appear in industry tracebacks but decline to identify the source of their traffic. Once the provider is publicly identified by the FCC, additional administrative processes would be triggered that would "culminate in the provider's eligibility for blocking by other providers." The approaches may vary, but there is growing consensus that identifying and targeting such providers could advance meaningful reductions in illegal robocall traffic.

The Need to Proceed Cautiously

While the value in identifying and acting against providers facilitating illegal robocall traffic could be significant, any established framework should be cautiously implemented. Due to the interconnected nature of the telephony network, and the scale of many voice providers, no service provider can ensure that *none* of its customers will engage in illegal conduct. Even providers that aggressively monitor and remove illegal traffic from their networks will nevertheless unknowingly be the source of such traffic. Given these realities, the implementation of any such framework should be carefully structured to ensure that only the most egregious of providers are subject to its implications.

Conclusion

Adrian Abramovich's testimony acknowledged the existence of a seemingly small universe of voice providers that are knowingly facilitating substantial volumes of illegal robocall traffic. Identifying and targeting such providers could be an additional tool that industry and government stakeholders can deploy in their battle against illegal robocalls. ■

For more information on this initiative and efforts to address the problem of illegal robocalls in general, please contact:

Kevin G. Rupy
202.719.4510 | krupy@wileyrein.com

What's the Next Phase of AI Regulation in the U.S. and Abroad?

By Duane Pozza and Jacquelynn Ruff

Recent developments in the United States and on the international stage suggest we're moving into a new phase in regulatory approaches to artificial intelligence (AI) – one where countries are moving forward on determining whether and how AI will be regulated within and across sectors.

AI can be broadly used in a range of applications, from voice assistants to autonomous vehicles to medical diagnoses to credit and other financial decisions, and one big question is whether countries will adopt a "one size fits all" approach or one tailored to individual sectors. Despite the differences among AI applications, both the U.S. and other countries have shown openness to adopting principles and standards across sectors. At the same time, in certain areas – like AI-powered facial recognition – lawmakers and regulators have pushed for more swift and sector-specific action.

Below we recap the current developments in AI regulation, and look at what is coming next. This includes international efforts that – as we have seen with the EU's General Data Protection Regulation (GDPR) – can directly affect American companies and drive U.S. federal and state regulatory approaches. For further information, check out our latest **podcast**, in which we discuss these developments in more detail.

International Efforts

Internationally, over the past few months, leading global intergovernmental organizations have issued public policy frameworks for AI, typically with input from a range of experts and stakeholders. These are intended to be models for use by governments and other parties around the world. The Organization for Economic Cooperation and Development (OECD) adopted principles for "trustworthy" AI, first released in March and finalized at highest levels in May. These establish expectations for *all* actors who participate in the AI system life cycle. The OECD is also developing practical guidance on ways to act consistently with these principles. And in June, the G20 adopted the OECD framework with some variations on details.

Regional and national initiatives are also underway. The European Commission (EC) has conducted an extensive effort to develop ethics guidelines for AI that were released in April. Their implementation guidance is occurring through a pilot, using an assessment list in which participants report on 130+ detailed questions as to their practices in this area. Just a few weeks ago, the expert group advising the EC on AI published a report on policy recommendations that includes a section on possible legislative changes to address AI.

Notably, against this backdrop, German Chancellor Angela Merkel recently called for "regulation" of AI along the lines of the GDPR. And the newly elected President of the European Commission, Ursula von der Leyen, has announced her intention to propose legislation on the "human and ethical implications" of AI within her first 100 days in office. The OECD and EC frameworks could provide road maps for national regulators intent on taking such action. AI is also an area in which many countries follow the lead of – or at least draw ideas from – the first countries to approach regulation. Indeed, information-sharing and other collaboration among countries on AI is already occurring regularly. At a hearing on international engagement and emerging technologies conducted by the Federal Trade Commission (FTC) in March, the FTC used AI as a timely case study, with panelists that included experts from other countries who expressed interest in heightened collaboration.

U.S. Efforts

In the United States, the National Institute of Standards and Technologies (NIST) at the Department of Commerce recently issued a federal AI engagement **plan** that calls for federal agencies to

continued on page 8

What's the Next Phase of AI Regulation in the U.S. and Abroad?

Continued from 7

move forward on a range of AI standards, including some that can form the basis of a regulatory approach. The Administration's Executive Order on AI, released in February, had required NIST to develop a plan for federal engagement on AI standards based on public input. The plan, which was submitted on August 9, calls for development and use of standards to support deployment of "reliable, robust, and trustworthy systems that use AI technologies."

While the NIST plan discusses a number of technical standards, it also sees a role for standards development being used to address substantive concerns around AI, such as safety, data quality, and explainability of AI decisions – though the plan is cautious about moving too quickly and not achieving sufficient consensus. In the category of standards "more primed" for development, it includes (among various relatively technical standards) standards for data, which encompass data analytics, data quality, and data privacy. And other standards it considers to be at "formative stages" are AI safety, risk management, explainability, and security. It also suggests that ethical considerations may be incorporated into standards "tied tightly to the type, likelihood, degree, and consequence of risk to humans."

Who will drive standards development? The NIST plan proposes that most of the domestic engagement on AI standard-setting will be driven by individual agencies, with a central coordinator at the National Science and Technology Council. And it heavily emphasizes the role of public-private partnerships, encouraging agencies and industry to work together where they can.

Beyond NIST, one area that has received significant scrutiny by a wide range of lawmakers is the use of AI in facial recognition. In May, the San Francisco Board of Supervisors voted to ban the use of facial recognition software by the police and other agencies. The city of Somerville, Massachusetts followed suit last month. On the federal level, Senators Roy Blunt (R-MO) and Brian Schatz (D-HI) released **proposed legislation** in March that generally would require notice and affirmative consent for collection and sharing of commercial facial recognition data, and require meaningful human review of decisions based on facial recognition technology in some circumstances. The draft legislation would also require companies making facial recognition technology available as an online service to set up an API to enable independent testing for accuracy and bias. Lawmakers continue to look at regulatory approaches to facial recognition that presage an approach to other technologies that use AI.

Overall, we expect AI regulatory approaches to advance on both the domestic and international fronts in the coming months. Stakeholder participation is key as lawmakers and regulators continue their discussions – and move beyond discussing to proposing potential laws or regulations. As with privacy law, input by industry participants before laws or regulations are passed will be critical in avoiding unintended consequences that can stifle beneficial AI innovation. ■

For additional information on AI regulation and legal issues, please contact:

Duane C. Pozza
202.719.4533 | dpozza@wileyrein.com

Jacquelynn Ruff
202.719.7224 | jruff@wileyrein.com

How to Protect IoT Devices: NIST Issues Key Draft Cybersecurity Guidance

By Megan Brown, Kathleen Scott, and Boyd Garriott.

The National Institute of Standards and Technology (NIST) released in late July **NISTIR 8259**, a draft of the long awaited[1] "Core Cybersecurity Feature Baseline for Securable IoT Devices." The publication (the baseline draft) proposes a voluntary, flexible, minimum "baseline of cybersecurity features based on common cybersecurity risk management approaches as a starting point for manufacturers." (p. 1). We expect it to shape standards of care and regulatory expectations for manufacturers and sellers of all connected devices. For stakeholders, and others, NIST provided multiple opportunities for engagement. NIST held a **workshop** on the baseline on August 13. Comments on the baseline draft are due September 30.

NIST's baseline draft is part of **NIST's longstanding and ongoing work** on IoT device security. These federal efforts are increasingly important, given that states — **California** and **Oregon** thus far — have enacted legislation to require IoT device manufacturers to equip such devices with reasonable security features. Both of those laws reference, and give various levels of deference to, federal IoT requirements. All of these efforts come amidst global regulatory interest in IoT security, from the European Union's certification requirements to evolving industry best practices.

NIST's document is primarily targeted at IoT device manufacturers and secondarily at individuals and entities that purchase such devices.

This article will tell you what you need to know about: (1) the scope of the draft; (2) the features included in the baseline itself; and (3) NIST's guidance about implementation.

NIST focuses on manufacturers and consumers of IoT devices

NIST defines the audience for the baseline draft as (1) "IoT device manufacturers seeking a better understanding of how to identify the appropriate cybersecurity features for their IoT devices, or wanting a common language for communicating with others regarding these features;" and (2) a "secondary audience" of "IoT device customers (i.e., individuals and organizations) that want to specify which cybersecurity features they need from IoT devices during their evaluation and acquisition process." (p. iii).

The draft covers only devices with the following characteristics: (1) at least one transducer "for interacting with the physical world;" and (2) "at least one network interface (e.g., Ethernet, WiFi, Bluetooth, Long-Term Evolution [LTE], ZigBee); and (3) "are not conventional IT devices . . . (e.g., smartphone, laptop)." (p. 1).

Finally, the baseline is a starting point that "addresses general cybersecurity risks faced by a generic consumer." (p. ii). NIST explains that the baseline should be the "default for minimally securable devices" but recognizes that "cybersecurity features will often need to be *added* or *removed* from an IoT device's design to take into account the manufacturer's understanding of customers' likely cybersecurity risks." (p. 9). The baseline also does not say how a feature must be achieved, providing manufacturers with "considerable flexibility in implement[ation] . . ." (p. 9).

The Draft Offers Six Baseline Features and Dozens of Elements it Suggests for Security By Design

The baseline contains six features for IoT devices. However, each "feature" is comprised of multiple "key elements," with a total of 22 such elements. These "features" and "key elements" are reproduced below:

continued on page 10

Continued from 9

Feature	Key Elements
Device Identification: The IoT device can be uniquely identified logically and physically.	1. A unique logical identifier 2. A unique physical identifier on it at an external or internal location authorized entities can access
Device Configuration: The IoT device's software and firmware configuration can be changed, and such changes can be performed by authorized entities only.	1. The ability to change the device's software and firmware configuration settings 2. The ability to restrict configuration changes to authorized entities only 3. The ability for authorized entities to restore the device to a secure default configuration defined by an authorized entity
Data Protection: The IoT device can protect the data it stores and transmits from unauthorized access and modification.	1. The ability to use accepted cryptographic modules for standardized cryptographic algorithms (e.g., encryption with authentication, cryptographic hashes, digital signature validation) to prevent the confidentiality and integrity of the device's stored and transmitted data from being compromised 2. The ability for authorized entities to configure the cryptography use itself when applicable, such as choosing a key length 3. The ability for authorized entities to render all data on the device inaccessible by all entities, whether previously authorized or not (e.g., through a wipe of internal storage, destruction of cryptographic keys for encrypted data)
Logical Access to Interfaces: The IoT device can limit logical access to its local and network interfaces to authorized entities only.	1. The ability to logically or physically disable any local and network interfaces that are not necessary for the core functionality of the device 2. The ability to logically restrict access to each network interface (e.g., device authentication, user authentication) 3. The ability to enable, disable, and adjust thresholds for any ability the device might have to lock or disable an account or to delay additional authentication attempts after too many failed authentication attempts
Software and Firmware Update: The IoT device's software and firmware can be updated by authorized entities only using a secure and configurable mechanism.	1. The ability to update all the device's software and firmware through remote (e.g., network download) and/or local means (e.g., removable media) 2. The ability to confirm the validity of any update before installing it 3. The ability to restrict updating actions to authorized entities only 4. The ability to enable or disable updating 5. The ability to set remote update mechanisms to be either automatically or manually initiated for update downloads and installations 6. The ability to enable or disable notification when an update is available and specify who or what is to be notified

continued on page 11

Continued from 10

Cybersecurity Event Logging: The IoT device can log cybersecurity events and make the logs accessible to authorized entities only.	1. The ability to log cybersecurity events across the device's software and firmware 2. The ability to record sufficient details for each event to facilitate an authorized entity examining the log and determining what happened 3. The ability to restrict access to the logs so only authorized entities can view them 4. The ability to prevent any entities (authorized or unauthorized) from editing the logs 5. The ability to make the logs available to a logging service on another device, such as a log server

Each feature references "existing sources of IoT device cybersecurity guidance specifying a similar or related cybersecurity feature." (pp. 9-12). These references include publications from both private and public entities, such as **CTIA's Cybersecurity Certification Test Plan for IoT Devices** and the **European Union Agency for Network and Information Security's Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures**.

Lastly, each feature also contains NIST's rationale for its inclusion in the baseline. Under "data protection," for example, NIST explained that "[c]ustomers often want the confidentiality of their data protected so unauthorized entities cannot access their data and misuse it." (p. 11).

Implementation Is Voluntary But Encouraged

Implementation of the baselines is voluntary. NIST explains that "manufacturers may *voluntarily* adopt [the baseline] for IoT devices they produce." (p. ii). And the "overall objective of this publication is to provide *voluntary guidance* for IoT device manufacturers . . ." (p. iv).

As noted above, this voluntary implementation of the baseline is intended to be flexible. Nevertheless, NIST provides four general categories of guidance for implementation of both the baseline and ancillary activities (e.g., customer disclosure).

First, NIST provides a non-comprehensive list of considerations for device manufacturers regarding *provisioning cybersecurity features*. (pp. 14-15). At a high level, these include the following recommendations:

- Select or build a device with sufficient hardware, firmware, and software resources to support desired features.
- "Be forward-looking and size hardware resources for potential future use."
- "Use hardware-based cybersecurity features."
- "Do not include unneeded features . . ."
- "Do not force the use of features that may negatively impact operations."
- "[C]onsider using an established IoT platform instead of acquiring and integrating hardware, firmware, and supporting software components (e.g., operating system)."

Second, NIST encourages IoT manufacturers to consider the context in which IoT devices will be used in order to recognize opportunities for "cybersecurity feature inheritance." (pp. 15-16). As an example, NIST notes that "if an IoT device is intended for use in an environment with stringent physical security controls in place, a manufacturer might be able to omit restricting access to the device's local interfaces because the facility's physical security can take care of it." (p. 15).

Third, NIST recommends that manufacturers provide cybersecurity information to customers. It provides specific examples under the rubric

continued on page 12

How to Protect IoT Devices: NIST Issues Key Draft Cybersecurity Guidance

Continued from 11

of five main categories: (1) device cybersecurity features; (2) device transparency; (3) software and firmware update transparency; (4) support and lifespan expectations; and (5) decommissioning. For example, under device cybersecurity features, NIST recommends "[c]ommunicating to customers which cybersecurity features the device provides, especially using common terminology (e.g., the feature names from the core baseline) . . ." (p. 17).

Fourth, NIST provides resources to manufacturers looking for information on secure software development practices for IoT devices. (pp. 20-21). Rather than diving into specifics, NIST points manufacturers to a number of white papers that lay out these best practices.

Next Steps

NIST wants feedback! They can change the draft before it is finalized, so IoT stakeholders should review it and determine whether they want to provide feedback.

Manufacturers should have their design and engineering teams review the baselines to see how reasonably they could implement NIST's suggestions.

Any company selling a connected device to the government should pay particularly close attention to this document because of ever-increasing attention being paid to IoT by procurement officials.

Policymakers should consider NIST's extensive treatment of the complexity and variety in IoT ecosystems, recognizing that when it comes to IoT security, one size does not fit all. ■

For additional information, please contact:

Megan Brown
202.719.7579/mbrown@wileyrein.com

Kathleen Scott
202.719.7577/kscott@wileyrein.com

Boyd Garriott
202.719.4487/bgarriott@wileyrein.com

Endnotes

[1] NIST had initially included a precursor to this baseline in its **NISTIR 8228** draft but ultimately decided to remove it, explaining in the **final draft** that the baseline would be "refined and released in a separate publication." Additionally, NIST explains in the current baseline draft that the baseline is part of the larger **Botnet Road Map** published by the Departments of Commerce and Homeland Security in November 2018. (pp. iv-v).

Events & Speeches

When Congress Investigates: Breaking Down the Nuts and Bolts of Congressional Investigations
2019 FBA Annual Meeting & Convention
Peter S. Hyun, Panelist
September 5, 2019 | Tampa, FL

Understanding Smart Contracts & How They Work
2019 SCG Legal Annual Meeting & 30th Anniversary Celebration
Duane C. Pozza, Speaker
September 6, 2019 | Washington, DC

5G, Huawei, and National Security
Wiley Rein National Security Webinar + Podcast Series
Megan L. Brown, Speaker
September 12, 2019

Webinar and Podcast Library

July 18, 2019
The Latest Regulatory Developments in AI
Wiley Connected
Duane C. Pozza, Jacquelynn Ruff

July 17, 2019
Latest Update on State Privacy and Security Laws: California and Beyond
Wiley Rein Webinars
Duane C. Pozza, Matthew J. Gardner, Joan Stewart, Kathleen E. Scott

March 26, 2019
Biometrics News
Wiley Rein Webinars
Duane C. Pozza, Kathleen E. Scott

March 20, 2019
Mobile World Congress: A Discussion on 5G and the Future of the Mobile Industry
Wiley Connected
Scott D. Delacourt, Jacquelynn Ruff

March 19, 2019
What to Watch: FTC Forecast for 2019
Wiley Rein Webinars
Megan L. Brown, Scott D. Delacourt, Duane C. Pozza

March 13, 2019
California Consumer Privacy Act (CCPA) Briefing
Wiley Rein Webinars
Matthew J. Gardner, Kathleen E. Scott, Joan Stewart

March 4, 2019
Federal Privacy Update: Congress, NIST & More
Wiley Rein Webinars
Megan L. Brown, Duane C. Pozza, Kathleen E. Scott

January 7, 2019
Blockchain, Trust, and Regulation: A Conversation with Wharton Professor Kevin Werbach
Wiley Connected
Duane C. Pozza

November 30, 2018
Advanced Persistent Chats: DHS's Cybersecurity and Infrastructure Security Agency Podcast
Wiley Connected
Megan L. Brown, Michael L. Diakiwski

October 30, 2018
Podcast: How Much Do You Know About Blockchain Policy? An Interview with the Blockchain Association's Director of External Affairs, Kristin Smith
Wiley Connected
Matthew J. Gardner

Privacy and Cybersecurity at Wiley Rein

Rachel A. Alexander	202.719.7371	ralexander@wileyrein.com
Daniel P. Brooks	202.719.4183	dbrooks@wileyrein.com
Megan L. Brown	202.719. 7579	mbrown@wileyrein.com
Moshe B. Broder	202.719.4186	mbroder@wileyrein.com
Jon W. Burd	202.719.7172	jburd@wileyrein.com
Scott D. Delacourt	202.719.7549	sdelacourt@wileyrein.com
Michael L. Diakiwski	202.719.4081	mdiakiwski@wileyrein.com
Matthew J. Gardner	202.719.4108	mgardner@wileyrein.com
Boyd Garriott	202.719.4487	bgarriott@wileyrein.com
Lee E. Goodman	202.719.7378	lgoodman@wileyrein.com
Peter S. Hyun*	202.719.4499	phyun@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Dorthula H. Powell-Woodson	202.719.7150	dpowell-woodson@wileyrein.com
Duane C. Pozza	202.719.4533	dpozza@wileyrein.com
Antonio J. Reynolds	202.719.4603	areynolds@wileyrein.com
Kevin G. Rupy	202.719.4510	krupy@wileyrein.com
Kathleen E. Scott	202.719.7577	kscott@wileyrein.com
Joan Stewart	202.719.7438	jstewart@wileyrein.com

*Not admitted to the District of Columbia Bar. Supervised by principals of the firm who are members of the District of Columbia Bar.