Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | May 2018

This month, Scott Delacourt explores issues related to abusive robocalls and how we can stop them, while Megan Brown, Katy Ross, and Matthew Gardner assess the most recent update by the National Institute of Standards and Technology (NIST) to its Framework for Improving Critical Infrastructure Cybersecurity.

As always, please let me know if you have questions or comments on any of these topics. Also, if there are topics you would like to see addressed in future issues of *Privacy in Focus* – or if you have a need for a privacy or data security speaker at your event – please let me know. I can be reached at 202.719.7335 or knahra@wileyrein.com. Thank you for reading. ■

— Kirk Nahra, Privacy & Cybersecurity Practice Chair

Abusive Robocalls and How We Can Stop Them

By Scott D. Delacourt

ALSO IN THIS ISSUE

This article reflects Scott's April 18 testimony before the Senate Commerce Committee on behalf of the U.S. Chamber Institute for Legal Reform. His full statement is available here.

Illegal and abusive robocalls continue to be a menace and a top complaint of consumers across the U.S. These calls originate with bad actors, and responsible American businesses share consumers' concern. Customers are the life-blood of commerce, and successful businesses avoid practices that customers revile. Responsible U.S. businesses have no interest in engaging in abusive practices. Indeed, businesses fear the brand and customer relationship damage of being cast as an illegal and abusive robocaller.

On the other hand, businesses are concerned about being able to communicate with their customers through the use of modern technology, in an efficient and cost-effective manner, while consumers desire and expect timely, contemporary communications from the companies

continued on page 2

NIST Releases Version 1.1 of Its Cybersecurity Framework with Important Changes

By Megan L. Brown, Katy M. Ross, and Matthew J. Gardner

On April 16, 2018, the National Institute of Standards and Technology (NIST) released an updated version of its **Framework for Improving Critical Infrastructure Cybersecurity** (Framework). The Framework Version 1.1 is intended to refine, clarify, and enhance the original **Framework Version 1.0** released in February 2014. The Framework is voluntary guidance to guide cybersecurity activities and help organizations manage cybersecurity risks.

While the Framework was developed to improve cybersecurity risk management in critical infrastructure, the Framework can be used by organizations in any sector or community.

Companies have been using the Framework for years in various ways. U.S. agencies use it, and international regulators look to and build their approaches on it. As a result, many urged NIST not to make major structural changes to the Framework, lest it foster fragmentation on cybersecurity best practices. Industry commenters filed

continued on page 6

Abusive Robocalls and How We Can Stop Them

continued from page 1

with whom they choose to do business. Unfortunately, the Telephone Consumer Protection Act (TCPA) has become an obstacle, preventing legitimate and lawful communications between businesses—large and small—and their customers and has placed businesses in the crosshairs of potential litigation each time they pick up the phone or send a text message.

The TCPA prohibits making phone calls to wireless telephone numbers "using any automatic telephone dialing system" (ATDS) without the prior express consent of the called party. The Act focuses on technology, not bad conduct such as harassment or fraud. Ambiguity over the technology used or what constitutes an ATDS has become a source of unnecessary and sometimes abusive class-action litigation, burdening how businesses reach their customers, while doing little to stop truly abusive robocalls. Indeed, the number of TCPA case filings exploded to 4,860 in 2016, and TCPA litigation grew 31.8% between 2015 and 2016. Much of this litigation targets legitimate companies – many of which are well-known brands – that have committed marginal or unavoidable violations, instead of the true bad actors: scam telemarketers, offshore operations, and fraudsters who operate through thinly-capitalized and disappearing shell companies. These latter activities are of little interest to class-action lawyers.

Abusive litigation targeting legitimate companies has devastating effects, as the TCPA's uncapped statutory damages can lead to multi-million-dollar judgments. Often consumers do not even collect from the judgment funds established to remediate harm, making class-action lawyers the only

continued on page 3

winners. Ironically, such litigation ultimately hurts the consumers it is intended to protect as the costs are passed along in the form of increased prices for goods and services.

The Federal Communications Commission's (FCC) implementation of the TCPA, to some degree, has contributed to this problem. In its 2015 *Omnibus Order*, the FCC expanded the types of devices that are considered ATDS to include equipment with computing capability or to which computing capability might be added—an expansive reading that potentially sweeps in everyday devices like smart phones and tablets, creating major uncertainty for businesses. Indeed, the FCC's *Omnibus Order* contributed to a 46% increase in TCPA litigation.

The D.C. Circuit's March 16 decision in *ACA Int'l v. FCC* (No. 15-1211) overturned certain key provisions of the FCC's *Omnibus Order*, including the agency's definition of an automated telephone dialing system (ATDS), which the court described as "utterly unreasonable." The decision includes a sensible roadmap for how the FCC might interpret the TCPA in a manner that is clear and understandable, significantly reducing frivolous class-action litigation. This decision provides an opportunity for the FCC to revisit and clarify its approach to the TCPA. Following the D.C. Circuit's approach would provide guidance and clarity to businesses, and allow regulators, law enforcement, and courts to focus on the bad actors who are the source of the robocalling problem.

Uncertainty and Unnecessary Litigation

Congress enacted the TCPA in 1991 to stop abusive cold-call telemarketing and fax-blast spamming. In promulgating its initial rules implementing the Act, the Commission acknowledged the TCPA's goal of "restrict[ing] the most abusive telemarketing practices." The Supreme Court recognized that "Congress determined that federal legislation was needed because *telemarketers*, by operating interstate, were escaping state-law prohibitions on *intrusive nuisance calls*." Unfortunately, the Commission's implementation of the Act over many years has fostered a whirlwind of litigation. Interpretations by courts and the FCC have strayed far from the statute's text, Congressional intent, and common sense, turning the TCPA into a breeding ground for frivolous lawsuits brought by serial plaintiffs and their lawyers, who have made lucrative businesses out of targeting U.S. companies. The number of TCPA case filings exploded to 4,860 in 2016, and TCPA litigation grew 31.8% between 2015 and 2016. The focus of these lawsuits is often legitimate companies and well-known brands who have committed accidental or unavoidable violations. As then-Commissioner Ajit Pai highlighted, the Los Angeles Lakers were hit with a class-action lawsuit from fans who received text messages confirming receipt of fan-originated texts. Similarly, a ride-sharing service was sued for texts confirming receipt of ride requests. And Mammoth Mountain Ski Area was sued for calling a group of litigants who had previously provided consent.

TCPA litigation has even gone so far as to subject nonprofit organizations to frivolous lawsuits. A blood bank, a state chapter of the Special Olympics, and the Breast Cancer Society have all faced TCPA suits. Recently, the American Heart Association was handed a "victory" when a court in Louisiana found the plaintiff consented to the text messages she received and that the content of the messages was informational, not promotional. As a result, the TCPA is forcing such organizations to

continued on page 4

continued from page 3

utilize and waste precious staff and monetary resources to handle needless litigation rather than devoting those resources to life-saving research.

Because the TCPA provides for uncapped statutory damages, defendants in these lawsuits face multi-million-dollar judgments. Outcome Health recently agreed to a $2.9 million settlement to end a class-action lawsuit over daily automated nutrition tips it texted to recipients who had signed up to receive such information. In another case, Lake City Industrial Products, Inc., a small, family-owned company from Michigan, faced over $5 million in statutory damages for faxes it sent believing they were legal. Other well-known companies, like Capital One Bank, AT&T, MetLife, Papa John's Pizza and Walgreens Pharmacy, have faced settlements of over ten million dollars, the largest of which was $75 million. TCPA lawsuits filed in the 17-month period after the 2015 FCC Omnibus Declaratory Ruling reached approximately 40 different industries.

Compliance with the TCPA has been frustrated by uncertain and shifting standards as the FCC's interpretations have evolved over decades, leaving a tangled web of obligations. Businesses making good-faith efforts to comply may nevertheless be subject to crippling litigation. Regulatory uncertainty and enormous settlements enriching class-action lawyers benefit neither consumers nor the economy. As FCC Commissioner Michael O'Rielly has observed, needless "enforcement actions or lawsuits" chill efforts by "good actors and innovators" to develop "new consumer-friendly communications services."

The FCC's *Omnibus Order* added to the uncertainty. The TCPA prohibits making a call "using any automatic telephone dialing system" without the prior express consent of the called party. The Act defines "automatic telephone dialing system" as "equipment which has the capacity to store or produce telephone numbers to be called, using a random or sequential number generator; and to dial such numbers." Uncertainty over the meaning of "capacity" led the FCC to adopt an order construing the term. Rather than providing clarity, however, the FCC adopted a sweeping interpretation including devices that have both the present and *potential* capacity to store or produce telephone numbers to be called, while also including devices that can generate random or sequential numbers and those that cannot. This baffling interpretation raised the prospect that everyday devices like smart phones and tablets could be ATDS subject to the TCPA's prohibitions because of their potential capacity to store or produce telephone numbers to be called. This construction conflicted with the text, history, and purpose of the TCPA, and contributed to a 46% increase in TCPA litigation, with class actions comprising approximately one-third of those filings.

The D.C. Circuit Decision - Roadmap

Numerous petitioners sought judicial review of the *Omnibus Order*'s unjustifiable expansion of the TCPA, arguing that the regime was unreasonable, impractical, and inconsistent with the statute's text. The D.C. Circuit largely agreed and vacated portions of the Omnibus Order in *ACA Int'l v. FCC*. Significantly, the court unanimously set aside the Commission's interpretation of ATDS, holding that the interpretation of capacity was "utterly unreasonable," "incompatible with" the statute's goals, and "impermissibly" expansive. The interpretation was so unreasonable, it was "considerably beyond the agency's zone of

continued on page 5

continued from page 4

delegated authority." The court also found unanimously that the Commission had offered an inconsistent and "inadequa[te]" explanation of what features constitute an [ATDS], "fall[ing] short of reasoned decision making."

The opinion also provided a roadmap for how the FCC should proceed. The court pointed to the interpretation of "make any call . . . using" offered by Commissioner Michael O'Rielly in his *Omnibus Order* dissent, which would require that dialing equipment "*be used as an [ATDS]* to make the calls." In other words, the calling equipment must actually use ATDS capabilities to make the call. Although the court did not explicitly endorse this approach, as the issue was not raised in the appeal, it noted that this construction would "substantially diminish the practical significance of the Commission's expansive understanding of 'capacity' in the [ATDS] definition." This is a significant signal to the FCC and the courts about the best reading of the TCPA.

Focus on Bad Actors

The D.C. Circuit's decision provides an opportunity for the FCC to rethink its approach to the TCPA. Confusing regulations and interpretations of the statutory text have contributed to a rise in TCPA litigation while doing little to reduce illegal and abusive robocalling. At the same time, increased liability exposure and compliance costs have deterred businesses from reaching out to their customers. A renewed focus on the TCPA's statutory text offers a path forward to better protect consumers and businesses that operate in good faith.

Adopting the D.C. Circuit's suggested approach on what constitutes an ATDS would realign the interpretation of the TCPA to its text and purpose. This straightforward reading will ensure that liability attaches only when ATDS capabilities are used to make a call, rather than sweeping in calls made using smartphones, tablets, and other devices that conceivably could be modified to support autodialing at some point in the future. Significantly, it would provide businesses with clear guidance on the type of equipment they can use to contact their customers. A device's theoretical or potential capabilities would not be relevant to determining whether it is an ATDS. Instead, the inquiry should focus only on the functions used to make the call or calls in question. This clarification will help businesses avoid unnecessary litigation over whether they used an ATDS and help consumers differentiate whether they are targets of an illegal robocall campaign or receiving a routine business communication. Reducing the amount of TCPA litigation will also free up resources to focus on the actual bad actors who are the source of abusive robocalls. With fewer complaints, enforcement resources will not be wasted on investigating legitimate business communications and can be used to find and punish illegal robocallers.

The TCPA was never intended to make all mass calling illegal. The legislative history reflects that the Act was intended to achieve a balance between the need for legitimate businesses to lawfully communicate with their customers and protecting consumers from certain abusive uses of the telephone system. There are bad actors who abuse the openness of our communications infrastructure, including through Caller ID spoofing and other illegal activities. The TCPA sought to prevent the use of specific equipment to engage in illegal and abusive

continued on page 6

Abusive Robocalls and How We Can Stop Them

continued from page 5

conduct—random or sequential cold calling that tied up telephone networks, including emergency lines, and harassed consumers. The construction of ATDS suggested by the D.C. Circuit would categorically prohibit those abuses. At the same time, it would provide clear guidance to businesses on how they may lawfully communicate with their customers.

The fact that the D.C. Circuit's preferred definition of ATDS does not cover as much equipment as the definition the court struck down in no way means that consumers are unprotected, or even less protected. The TCPA contains within itself the means of protection: the Do Not Call list. Any consumer lawfully contacted by a business using equipment that is not an ATDS and who does not desire to be called may ask the caller to be placed on the caller's company-specific Do Not Call list. Those consumers who proactively decide they do not want to receive calls—whether from an ATDS or not—may subscribe to the National Do Not Call List. Tens of millions of Americans already have.

Conclusion

As Congress and the FCC look for ways to reduce abusive robocalls, reforming the TCPA is an important step. Reducing the amount of unnecessary litigation plaguing legitimate businesses will shift the focus of enforcement to the actual bad actors who are the root cause of illegal robocalls. In this regard, the FCC is to be commended for taking action to give telephone companies the authority to use innovative solutions to block illegal robocalls. The D.C. Circuit has provided both an opportunity and a roadmap to further the FCC's work of focusing resources at the root of the robocalling problem. Following that guidance will help businesses avoid burdensome litigation, restore the TCPA to its original purpose, and redirect resources and attention towards reducing abusive robocalls. ■

For more information, please contact:

Scott D. Delacourt
202.719.7459
sdelacourt@wileyrein.com

NIST Releases Version 1.1 of Its Cybersecurity Framework with Important Changes

continued from page 2

several rounds of comments and participated in meetings with NIST as the revisions were considered. The new version addresses many of those comments and retains some of the more substantial additions, like vulnerability disclosure programs and supply chain protocols. It also explicitly addresses the Internet of Things.

Overall, Version 1.1 wisely retains the core features that made the original Framework a success. NIST emphasizes throughout Version 1.1 that there are a variety of ways to use the Framework and the decision about how to apply it is left to the implementing organization. The update clarifies that "compliance with the Framework" will have different meanings to different stakeholders, and that the Framework has utility as a structure and language for organizing cyber activities.

continued on page 7

NIST Releases Version 1.1 of Its Cybersecurity Framework with Important Changes

continued from page 6

Version 1.1 makes several key updates, including:

- Updating the scope of technologies covered by the Framework, noting that the Framework is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on "information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), or connected devices more generally, including the Internet of Things (IoT)."
- Adding language to Section 2.2 to better explain how to use Framework Tiers in Framework implementation.
- Creating a new subcategory related to the vulnerability disclosure life cycle. There are increasing expectations for companies to have methods to identify and manage vulnerabilities. These may not be right for all companies, but with the addition to NIST's Framework, they are something prudent companies should consider.
- Greatly expanding Section 3.3 to add discussion of supply chain risk management (SCRM). NIST emphasizes communication among stakeholders up and down supply chains, identifies examples of cyber SCRM activities, and notes that cyber SCRM encompasses technology suppliers and buyers as well as non-technology suppliers and buyers. The update also adds a Supply Chain Risk Management category to the Framework Core.
- Discussing "Buying Decisions" in a new Section 3.4, defining the objective as making the best buying decision among multiple suppliers, given a carefully determined list of cybersecurity requirements.
- Adding a new Section 4.0, "Self-Assessing Cybersecurity Risk with the Framework," describing how to use the Framework for self-assessing and demonstrating cybersecurity through measurements. NIST notes that the development of cybersecurity performance metrics is evolving and encourages organizations to innovate and customize how they incorporate measurements.
- Refining the language of the Access Control Category to better account for authentication, authorization, and identify proofing.

NIST held a **webcast** on April 27, 2018, discussing how the Framework was developed, describing the Framework's basic concepts, demonstrating how the Framework can be used by organizations, and highlighting the recent updates.

NIST has underway numerous other efforts that will affect the informative references in the Framework, and the tools for private sector companies. As those efforts unfold, organizations should consider adapting their approaches to stay up to speed with changing expectations.

Wiley Rein has been actively involved in shaping the original and new Frameworks, and helps clients across industries use and adapt it. We have also urged other countries to model their private sector cybersecurity strategies on it, in lieu of prescriptive

continued on page 8

continued from page 7

regulation. We are actively engaged on other NIST publications and work, as the agency continues to produce guidance on everything from IoT to privacy engineering. ■

For additional information on the Framework and related cybersecurity matters, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Katy M. Ross
202.719.7410
kmross@wileyrein.com

Matthew J. Gardner
202.719.4108
mgardner@wileyrein.com

Wiley Rein Awarded ISO 27001 Certification for Information Security Management

Wiley Rein LLP is proud to announce it has been awarded ISO 27001 certification as of May 1, 2018 – one of a select number of law firms to achieve this highly respected certification for information security management.

The certification reflects the firm's compliance with rigorous international standards and best practices, and its robust approach to protecting client data. Wiley Rein was granted the certification after an independent, comprehensive, year-long review of the firm's information security and risk management processes and procedures. The review process involved a multipronged audit by the British Standards Institute (BSI).

"We're proud to achieve the ISO 27001 certification, which demonstrates our ongoing commitment to the highest standards of information security," said Jim Goehrig, Chief Information Officer at Wiley Rein. "It is paramount that we protect the data of the firm, as well as the data entrusted to us by our clients."

ISO/IEC 27001 is an information security management standard, published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee. ISO/IEC 27001 specifies a management system that is intended to bring information security under management control. ■

For more information about Wiley Rein's ISO 27001 certification, please contact Jim Goehrig, Chief Information Officer (202.719.7050, jgoehrig@wileyrein.com) or Emmanuel Bot, Director of Information Security (202.719.4465, ebot@wileyrein.com).

Events & Speeches

Plenary Session 1: Success Stories in International Coordination – IoT

Megan L. Brown, Speaker

6th Annual Conference on Governance of Emerging Technologies and Science: Law, Policy and Ethics

May 16, 2018 | Washington, DC

Ready or Not, GDPR is Here.

Kirk J. Nahra, Panelist

Bloomberg Law Leadership Forum

May 23, 2018 | New York, NY

Gaps and Overlaps: Breaking Cover Down

Edward R. Brown, Speaker

2018 Cyber Risk Insights Conference

May 23, 2018 | Chicago, IL

Genetics: New Healthcare Opportunities New Legal Challenges

Kirk J. Nahra, Speaker

The Virginia Bar Association's 128th Summer Meeting

July 21, 2018 | Hot Springs, VA

FTC Guidance & Enforcement of Life Science Data Privacy & Security

Kirk J. Nahra, Speaker

Life Science Data Privacy Governance & GDPR Alignment Conference

July 26, 2018 | Philadelphia, PA

Privacy Bootcamp

Kirk J. Nahra, Speaker

IAPP Privacy. Security. Risk. 2018

October 17, 2018 | Austin, TX

I'm a Lawyer: How Can I Advise on Data Security Issues?

Kirk J. Nahra, Moderator

IAPP Privacy. Security. Risk. 2018

October 18-19, 2018 | Austin, TX

Mastering the Evolving Law of Data Analytics

Kirk J. Nahra, Speaker

AHIMA Data Institute: Making Information Meaningful

December 6, 2018 | Las Vegas, NV

Contributing Authors

Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Scott D. Delacourt	202.719.7459	sdelacourt@wileyrein.com
Matthew J. Gardner	202.719.4108	mgardner@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com
Katy M. Ross	202.719.7410	kmross@wileyrein.com