Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | June 2017

While much of Washington is focused on other topics, privacy and data security remain hot areas for regulatory and legislative developments. Shawn Chang and Hap Rigby look at the new proposed legislation to deal with internet privacy issues, following the recent Congressional steps to pull back on Federal Communications Commission (FCC) privacy rules. Katy Ross and Joshua Turner review some of the tricky issues related to the regulatory structure for flying cars. And Megan Brown, Matt Gardner, and Kat Scott analyze some of the possibilities in the ongoing review of the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

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

ALSO IN THIS ISSUE

Browsing the New Contours of the Online Privacy Debate

By Shawn H. Chang & Hap Rigby

Merely six weeks after Republicans in Congress successfully used the Congressional Review Act (CRA) to overturn the Federal Communications Commission's (FCC) 2016 Broadband Privacy Order, Representative Marsha Blackburn (R-TN), Chairman of the Communications and Technology Subcommittee and leader of the CRA effort in the House, introduced the Balancing the Rights of Web Surfers Equally and Responsibly Act of 2017, or the BROWSER Act, on May 18, 2017. The bill would establish uniform privacy rules governing how online service providers throughout the Internet ecosystem may use, disclose, or permit access to the consumer information they collect.

The bill's introduction caught stakeholders across the political spectrum and the Internet ecosystem by surprise. It challenges the conventional wisdom about the politics of the online privacy debate: that Republicans are satisfied with the Federal Trade Commission's (FTC) current privacy enforcement approach and that Democrats want to replace the FTC's privacy model with something similar to the FCC's 2016 Order and apply it to all stakeholders. It also

continued on page 2

‘Flying Cars’ Aren’t Cars. (And They Might Not Fly.)

By Katy M. Ross & Joshua S. Turner

Since the premiere of “The Jetsons” in 1962, we’ve all wondered when we can expect to see futuristic flying cars – pod-shaped vehicles that can float above traffic and safely deliver us to work and school – in real life. Momentum for the idea of flying cars has been building lately, leading industry watchers to speculate whether the future is now. Uber announced a new partnership with Dallas and Dubai to test a fleet of flying cars by 2020. Lilium is developing an electric aircraft capable of vertical takeoff and landing for on-demand air taxi and ridesharing. And Kitty Hawk, a startup backed by Google founder Larry Page, unveiled its prototype for an ultralight aircraft capable of vertical takeoff.

While these concepts are innovative, the term “flying car” is a misnomer for many of these vehicles. As currently envisioned, many of these flying cars probably won’t actually be designed to travel on roads like cars do. Companies are considering using aircraft

continued on page 3

Browsing the New Contours of the Online Privacy Debate *continued from page 1*

challenges how advocates have approached federal protection of online users’ private information: that businesses making money from using information collected about internet users will welcome the elimination of patchwork regulation at state and local levels, especially since such laws have proliferated in the wake of the passage of the CRA resolution, and that consumer advocates would support a federal privacy regime that not only meets, but arguably goes beyond, the standards created by the FCC’s 2016 Broadband Privacy Order, regardless of which agency is given the authority to enforce. The BROWSER Act appears to directly confront each of these conventional assumptions.

Whether the surprise it caused upon introduction was due to its sponsorship, its novel approach, or both, the BROWSER Act is now a significant – perhaps the most significant – contribution to the ongoing public policy debate about the appropriate framework for the privacy of internet user information in the digital age. Here are some of the reasons why.

The FTC Would Cover All Online Services Again

Republicans were already opposed to the Wheeler FCC’s reclassification of broadband internet access service (BIAS) as a common carriage service because they felt the prior light-touch information service classification had served all players of the internet economy, including internet users, well. In the privacy context, common carriage classification effectively prohibited the FTC from policing the practices of BIAS providers because of the FTC Act’s common carrier exception. When the Wheeler FCC adopted privacy rules for BIAS providers that did not completely reflect FTC’s approach to how information should be treated as sensitive or non-sensitive, Republicans felt the Commission created a second part to the already existing reclassification problem.

By repealing the FCC’s 2016 Broadband Privacy Order, the Trump Administration and Republican majorities in Congress took the initial step to return internet privacy regulation

continued on page 7

with vertical takeoff-and-landing systems, which would be more akin to a helicopter than a car. Those interested in a vehicle with the capability to both drive and fly might look instead to a concept like the Airbus Pop.Up vehicle, which is a "modular passenger capsule to switch between four-wheeled ground transport and quadcopter flight." But for now, this is just a concept.

Significant Obstacles

Whatever you call them, flying cars still face numerous obstacles before being put into everyday use.

- First, the Federal Aviation Administration (FAA) will have strong concerns about the safety of any airborne vehicle designed to carry humans, particularly vehicles that operate autonomously (without a pilot onboard). The FAA is going to be concerned about the safety of the passengers, as well as those people on the ground in case of a falling aircraft. While the FAA has loosened its restrictions on Unmanned Aircraft System (UAS, UAV, or drone) flights, the agency is proceeding cautiously. Indeed, the FAA currently does not permit commercial drones to fly over people – let alone carry people. The safety case for carrying humans will have to be airtight to get the FAA's signoff.
- Second, the FAA will have to consider airspace traffic management issues. If everyone has a flying car, the traffic in the air could quickly become as congested as the traffic on our roads. The FAA is currently looking at this issue with respect to drones and trying to create an integrated traffic management system that will bring some order to the airspace.
- Third, these vehicles will likely be quite costly. If a "flying car" is akin to a helicopter, it is easy to imagine that the cost of flight might be similar to the cost of chartering a helicopter – or at least somewhere between flying and driving. The price of owning your own flying car could also be exorbitant. That's not going to be an everyday mode of transportation for the average family.
- Finally, as with drones, members of the public may have privacy concerns about use of flying cars. In the drone context, the FAA and the industry are still grappling with the altitude at which a property owner's property ends and the public airspace begins. This tension will only be exacerbated when the aircraft at issue is a large vehicle carrying multiple people rather than a small drone.

Hurdles Overcome

Nevertheless, we are probably closer to having personal, flying transportation now than we ever have been in the past. That's because the biggest hurdles to "flying cars" have always been both technological and operational – and these hurdles are being addressed, out of necessity, as commercial UAS development continues. We thus may get "flying cars" purely as a byproduct of other developments in the UAV space.

For example, flying cars were never going to catch on as long as they required a pilot's license to operate. That's an expensive investment most Americans are unwilling to make. But a new generation of fully autonomous aircraft could make the pilot obsolete. And while the complexity of developing a functioning Unmanned Traffic Management (UTM) system remains

continued on page 4

daunting, those problems are going to have to be solved in order to deploy UAS, whether or not those aircraft are carrying passengers or cargo.

Finally, earlier flying car concepts like the Terrafugia were forced to be literally cars that could also fly because they had to be able to drive on the road in order to get to a runway and take off. That brings with it enormous compromises. All of the things that make a car safe to drive on the road add weight and complexity that make an airplane harder to fly. The development of the quadcopter UAV, however, has changed this paradigm completely. Further development of high-power, lightweight motors, batteries, and other associated technologies will be needed in order to make commercial UAV cargo delivery a reality – and this promises to deliver vehicles that can take off and land nearly anywhere, with useful payload and range capacities. A personal, autonomous, vertical takeoff aircraft does not need to drive on the roads, and thus can dispense with the redundant equipment needed to drive around safely.

The idea of an on-demand flying car has an enduring appeal. We may still be some time away from seeing flying cars become a viable means of transportation, but that day may finally be on the horizon. ■

For more information, please contact:

Katy M. Ross
202.719.7410
kross@wileyrein.com

Joshua S. Turner
202.719.4807
jturner@wileyrein.com

Cybersecurity Framework Updates Coming, Including on the Internet of Things

By Megan L. Brown, Matthew J. Gardner & Kathleen E. Scott

The National Institute of Standards and Technology (NIST) recently held a public workshop in Gaithersburg, MD, to discuss proposed updates to its highly lauded Cybersecurity Framework for Critical Infrastructure (CSF), which was released in 2014. CSF Draft Version 1.1 was released on January 10, 2017, and NIST has taken public comment. A summary by NIST of the comments received is available **here**.

One issue that NIST focused on during the workshop was the Internet of Things (IoT) – specifically, how the CSF can be applied to IoT. This discussion highlighted the vast IoT ecosystem, which is made up of many actors (e.g., device manufacturers, network providers, enterprises, consumers, etc.) across all sectors. With this context, discussion revolved around the intersection of the CSF with IoT. While there was general consensus that the CSF as a tool is applicable to IoT, there was much discussion about how best to use that tool. Suggestions included sector profiles, threat profiles, use cases, and including IoT into the CSF itself, among others. There was a suggestion that NIST might be able to add value to the IoT cyber effort at the consumer level, as there is little guidance/few standards regarding in-home and consumer IoT devices, as compared to enterprise IoT devices.

continued on page 5

Cybersecurity Framework Updates Coming, Including on the Internet of Things *continued from page 4*

Other major issues emerging for NIST and industry to tackle include whether and how to measure cyber success, whether to include "bug bounty" or coordinated vulnerability disclosures, and how to harmonize the CSF with the recent presidential Executive Order on Cybersecurity, which mandates federal agency use of the CSF.

A panel of private sector participants discussed their use of the CSF as a tool to discuss cybersecurity throughout their organizations and with their partners. It was seen as a positive contribution to the private sector broadly, which is increasingly using the CSF to shape internal risk management and evaluations. International commenters described non-U.S. governments' reactions to and reference to the CSF. They urged the United States to continue and increase its advocacy on the global stage to promote harmonization when it comes to cybersecurity best practices and expectations.

Below is a high-level readout on some of the key issues that NIST is working through for Version 1.1:

- **Metrics:** The workshop revealed nearly global consensus that the topic of metrics is critically important. However, workshop participants voiced concern about NIST's treatment of the topic in Version 1.1. Generally, participants urged NIST to simplify the metrics section and to reevaluate the level of detail that NIST provides regarding metrics. Workshop participants agreed that more work needs to be done with research around metrics, and that the final product needs to maintain flexibility.
- **Coordinated Vulnerability Disclosures:** Workshop participants affirmed that this is a mature topic that is ready for inclusion in the CSF. Participants also suggested additional research into the intersection between coordinated vulnerability disclosures and the CSF.
- **Law and Policy:** Participants noted that the CSF is widely used and may become a standard of care. They also expressed concern about the potential for regulation or misuse, which might be in tension with federal policy and law on cybersecurity. They highlighted that the voluntary nature of the CSF is what makes it successful, and suggested further engagement with regulators – at both the federal and the state level – to ensure that they understand the CSF's voluntary nature.
- **Supply Chain:** Participants agreed that clarifying language is needed at the beginning of the supply chain risk management (SCRM) section to further explain context and complexity. Although NIST was receptive to written comments urging it to not make SCRM its own category and to instead incorporate SCRM into the existing categories, it ultimately concluded at the workshop that such integration would be more appropriate for Version 2.0. For the current Version 1.1, NIST plans to keep SCRM as its own category.
- **Authentication:** Generally, workshop participants affirmed that the new authentication language proposed in Version 1.1 is appropriate and strengthens the overall category. Based on consensus from participants, NIST plans to add an authentication subcategory. With this

continued on page 6

continued from page 5

subcategory, NIST hopes to provide examples of authentication tools, but not drive organizations to certain solutions that may not make sense for their particular needs or risk profiles. To do this, NIST proposed identifying several authentication tools as options.

- **Threat Intelligence:** Participants suggested modifying the Core Framework language to make specific reference to threat intelligence.

Additionally, workshop panelists and attendees considered the application of the CSF to the Communications Sector. The Communications Sector panel and discussion group highlighted the Communications Security, Reliability, and Interoperability Council (CSRIC) mapping efforts, and focused mainly on metrics. The overall recommendation coming out of this discussion was that the metrics section in Version 1.1 should be streamlined at a higher level, and that additional work needs to be done looking at metrics that focus on organizations' internal risk management processes. The panel also warned that complex metrics may drive away potential users of the CSF. They highlighted that any metrics need to be understandable to the audience. Finally, the panel warned against tying metrics to CSF subcategories.

Going into the workshop, NIST had predicted that it would have the final version of 1.1 complete by the Fall of this year. Following the workshop, NIST introduced the idea that it may publish another draft before moving to a final version. We can expect a decision to be made public in June or July, along with a summary of the workshop.

Wiley Rein has been actively engaged with NIST on cybersecurity for years, including its previous implementation of President Obama's Executive Orders on cybersecurity. We have advised numerous companies on how evolving expectations about cyber will impact them, from regulatory obligations to consumer communications, and government contract provisions. ■

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Matthew J. Gardner
202.719.4108
mgardner@wileyrein.com

Kathleen E. Scott
202.719.7577
kscott@wileyrein.com

to the FTC-enforced framework that largely permits the collection, sharing, and use of internet users' personal information, so long as such information does not belong to narrow categories of "sensitive" personal information such as financial and health information. The next step to return the FTC cop to the privacy beat would be to have the Republican FCC majority, led by now-Chairman Ajit Pai, reverse the Wheeler FCC's classification of BIAS as a common carriage service. At that point, all would be well following conventional Republican wisdom. The introduction of the BROWSER Act, however, places a fork in that path for Republicans. In addition to removing the common carrier exception and restoring the FTC's authority over broadband service providers, the bill's introduction of a different regime for empowering consumer choice suggests that the FTC's current approach to privacy is insufficient to protect internet users.

Federal Privacy Regulations Would Increase

The BROWSER Act embraces much of the FCC regulation centered on principles of transparency and consumer choice. Despite removing the FCC's jurisdiction to police the privacy practices of broadband service providers and consolidating such authority with the FTC, the legislation mimics the "opt-in"-centric regime and scope of covered data favored by the Wheeler FCC's Democratic majority and treats browser history, app usage data, and the content of online communications as sensitive information requiring service providers to obtain "opt-in" consent from their customers in order to use, disclose, or permit access to such data. Furthermore, the bill would increase federal privacy regulations by extending these rules to all online service providers, including edge providers like Google and Facebook, thus addressing the lack of a level playing field caused by the FCC's 2016 rules.

Consumers Would Have More Control Over Their Information

The BROWSER Act is notable not only because of how it resembles the 2016 FCC broadband privacy rules, but also how it differs. Whether by accident or by design, the legislation does not contain several elements of the FCC's 2016 rules that would seem to alleviate online service providers' compliance burdens.

For example, the 2016 FCC rules permitted providers to use and disclose de-identified customer information without consent, following a fact-based three-part test. The FCC also sought to utilize its Consumer Advisory Committee's multi-stakeholder process to develop a standardized "safe harbor" privacy notice format providers could voluntarily use to inform customers about the collection, sharing, and use of their data. Neither of these features is part of the BROWSER Act, but will no doubt be considered should the bill move through the legislative process.

Instead, the legislation incorporates some of the more draconian aspects of the 2016 rules such as the prohibition on "take-it-or-leave-it" offers. Under the rule, a covered service provider cannot refuse to serve customers who do not consent to the use and sharing of their information for commercial purposes, even if the service is made available at no charge to the customer. While the provision may have limited application to an Internet service provider, the extension of such prohibition to edge providers under the BROWSER Act could fundamentally disrupt

continued on page 8

the very business model that drove the growth and adoption of the Internet: the provisioning of a free service paid for by the provider's ability to monetize the personal information of its customers.

Patchwork and Conflicting Privacy Rules Would Cease

The BROWSER Act explicitly preempts state and local laws related to online service providers and the privacy of internet user information, unlike the FCC's 2016 Order. BIAS providers and internet edge companies alike have long advocated for preemption of state and local privacy laws. Preemption has often been a sticking point in policy debates about any interstate commercial activity and consumer protection, and there may be no activity more interstate and consumer-centric in nature than modern internet usage. The question for traditional opponents of preemption will be whether privacy protections have been raised high enough by the BROWSER Act to give them a reason to accept a uniform federal regime in this case.

A New Baseline?

It is extremely difficult to successfully legislate these days on any matters, much less an issue as emotional and complex as online privacy, so it is unlikely that the BROWSER Act will arrive at the President's desk any time soon. Nevertheless, by including a bit of something for everyone as an initial position, the BROWSER Act has breathed new life into an otherwise stale privacy debate. Rep. Blackburn has provided the new contours of the privacy discussion – opt-in and opt-out control for consumers, uniform treatment of all online services, and general preemption of state, local, and FCC privacy activities. It remains to be seen whether the legislation will attract the support of Congressional Democrats or Senate Republicans, but it is possible that the BROWSER Act will serve as the new baseline to measure the strength or weakness of any future legislative efforts seeking to create a federal privacy regime for the digital economy. ■

For more information, please contact:

Shawn H. Chang
202.719.4456
schang@wileyrein.com

Hap Rigby
202.719.7461
hrigby@wileyrein.com

"Browsing the New Contours of the Online Privacy Debate" was first published by Bloomberg Law's *Privacy & Security Law Report* on June 19, 2017.

Events & Speeches

European Public Policy Trends – Cyber

Megan L. Brown, Panelist

1st Annual API-IOGP Cybersecurity Europe Conference for the Oil & Natural Gas Industry

June 22, 2017 | London, England

Privacy Regulation in the New Administration

Bennett L. Ross, Speaker

Law Seminars International

June 27, 2017 **| Telebriefing**

Events & Speeches (cont'd)

The New Era of Big Data for Health Care

Kirk J. Nahra, Speaker

American Health Lawyers Association Annual Meeting 2017

June 26 & 28, 2017 | San Francisco, CA

An Invitation to Hack: The Benefits and Risks of Vulnerability Disclosure or "Bug Bounty" Programs

Megan L. Brown, Matthew J. Gardner

Wiley Rein & HackerOne Webinar

July 13, 2017 | Webinar

Managing Data Security Contracts and Multiple Obligations

Kirk J. Nahra, Speaker

2017 Privacy & Security Forum

October 4-6, 2017 | Washington, DC

Privacy Bootcamp for Security Professionals

Kirk J. Nahra, Speaker

IAPP's Privacy. Security. Risk. 2017 Conference

October 16, 2017 | San Diego, CA

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

Kirk J. Nahra, Speaker

IAPP's Privacy. Security. Risk. 2017 Conference

October 17, 2017 | San Diego, CA

Contributing Authors

Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Shawn H. Chang	202.719.4456	schang@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
Hap Rigby *Senior Policy Advisor*	202.719.7461	hrigby@wileyrein.com
Katy M. Ross	202.719.7410	kmross@wileyrein.com
Kathleen E. Scott	202.719.7577	kscott@wileyrein.com
Joshua S. Turner	202.719.4807	jturner@wileyrein.com

To update your contact information or to cancel your subscription to this newsletter, visit:

www.wileyrein.com/newsroom-signup.html.

This is a publication of Wiley Rein LLP, intended to provide general news about recent legal developments and should not be construed as providing legal advice or legal opinions. You should consult an attorney for any specific legal questions.

Some of the content in this publication may be considered attorney advertising under applicable state laws. Prior results do not guarantee a similar outcome.