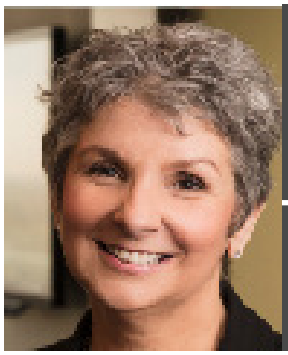


CRACKING THE CODE: RISK MITIGATION AND LITIGATION CONSIDERATIONS FOR THE SMART PRODUCT

Cheryl Bush
Bush Seyferth (Troy, MI)
248.822.7801 | bush@bsplaw.com

Cracking The Code: Risk Mitigation and Litigation Concerns for the Smart Product
Patrick G. Seyferth

Americans are increasingly reliant on Internet-equipped technology to perform a variety of tasks. Commonplace devices such as Amazon Echo, Google Home, and Apple HomePod allow the user to control a plethora of other devices in the house by voice. This is made possible by Apple and other electronics retailers whose devices connect not only to the Internet but also to one another. Traditional appliances have been overhauled and released to the public as digitally connected devices – baby monitors, ovens, even washers and dryers. Many homes are now integrated even more fully with the Internet through the proliferation of remote security systems, which typically take the form of cameras and microphones throughout the home that can be monitored anywhere from phones, tablets, or computers. Transportation has seen major leaps in connectivity, as well; from personal automobiles to passenger airliners, internet-connected technology is being leveraged to enhance safety and functionality. Innovations such as these provide benefits to the consumer. But they also introduce potential problems – such as hacking and malfunctions – that companies must manage to mitigate risk.

New Technological Horizons

The single biggest product liability story of this year has unquestionably been the saga of the Boeing 737 MAX, claimed to have been rushed through production to compete with chief rival Airbus' 320neo. It is alleged that the MAX was intentionally designed within the scope of the 737's original FAA certification to keep costs and turnaround time at a minimum. Reportedly, during testing Boeing found that under certain circumstances – albeit circumstances no passenger pilot would likely enter – the MAX was prone to stall where its predecessors were not. To avoid a lengthy and expensive re-certification, Boeing is alleged to have opted to add the Maneuvering Characteristics Augmentation System (MCAS), an automated stabilizer. MCAS worked so well in testing Boeing opted not to specify the program's existence to either the FAA or prospective MAX pilots. In the fatal crashes in Indonesia and Ethiopia, the ghost system allegedly activated to prevent a stall that was not there. MCAS could be counteracted by a skilled pilot familiar with the 737's systems and aerodynamics more generally. The night before the first crash in Indonesia, MCAS deployed on the same plane but was eventually deactivated by an unnamed person in the cockpit.[1] [2]

One fact often not emphasized is that these crashes also occurred in developing nations with a fraction of the flying hours required by the United States.[3] Smart products, as MCAS sadly shows, are only as smart as the users trained to handle them. The Boeing 737 was initially certified in 1968, fifty-one years ago. The U.S. Office of Special Counsel has recently aired allegations that the FAA itself was "misleading" in aspects of its reporting on pilot training and competency.[4] Whatever the eventual outcome of the Boeing investigation, and

1 https://www.nytimes.com/2019/09/18/magazine/boeing-737-max-crashes.html

2 https://www.wsj.com/articles/the-four-second-catastrophe-how-boeing-doomed-the-737-max-11565966629

3 https://www.usatoday.com/story/news/nation/2019/07/06/boeing-737-max-crash-grounded-problems-flight-training-pilots-faa/1641781001/

4 https://www.msn.com/en-au/money/company-news/faa-chief-invites-boeing-737-max-feedback-from-divided-world-regulators/ar-AAHJZzp

its import for the future of connected devices, it is clear that manufacturers, users, and regulators are susceptible to underestimating the import of today's boom in smart products.

Hackers are targeting similar connected devices faster than cybersecurity and legal professionals can keep up with. While some instances of hacking have involved relatively harmless gadgets such as virtual assistants, others have attacked machines with life-or-death implications such as automobiles and pacemakers. In one troubling instance, researchers were able to infiltrate an Amazon Echo with custom spyware and take full control of the device, including critical functions such as its microphone.[5] While this attack was executed by so-called "white-hat" hackers – those who race to find potential Achilles' heels before malicious, criminal hackers do – and the flaw was quickly patched by Amazon, in other instances "black-hat" hackers have beat the good guys to the punch. In South Carolina, one family found itself at the mercy of an unknown hacker who was controlling their baby monitor from afar – despite researchers agreeing that the infant's mother adhered to basic cybersecurity best practices.[6] Even more unsettling is the potential for hackers to literally stop a heartbeat at a keystroke. White-hat hackers last year engineered a way to place malware onto life-saving devices such as insulin pumps and pacemakers, raising a whole host of chilling possibilities.[7]

Another example is that of "connected vehicles" – an umbrella term for an array of features, one, some, or all of which may be in a particular vehicle – linked to the Internet and consequently vulnerable to Internet hacking. Starting with the advent of blind spot warnings in 2004, automakers have gradually instituted a raft of safety and convenience features administered by a computer. Automatic braking first found its way into cars as early as 2010; many technologies even more common in cars, like live traffic feeds on navigation systems such as have been around for much of the decade, create further openings for hackers. Mirroring the proliferation of virtual assistants in the home and in mobile phones, many cars now come equipped with not only Bluetooth but Siri, Alexa, or the like. Functions previously carried out by a physical key in proximity to the car – remote start, the panic button, even simple locking and unlocking – can often be activated from a mobile phone app.[8] Parking-assist cameras have been in cars a relatively long time; but now cameras have migrated from the exterior to the interior, enabling drivers to monitor their passengers and valets.[9] Cameras are also used to track head and eye placement and alert those who fail to keep their eyes on the road.[10] Some automakers are pushing past mere connectivity – new technologies like Nissan's "ProPILOT" and Volvo's "Pilot Assist" are being used to assess road conditions and drive the car accordingly.[11] [12] All these innovations, control-based and warning-based alike, are being incorporated into vehicles at unprecedented levels. Automakers totaling nearly 60% of U.S. market share have promised full-fleet connectivity by 2022 or earlier, to the point that the number of connected vehicles to be shipped in the year 2021 is projected at a staggering 94 million.[13] [14]

In recent years white-hat hackers have staged a number of successful intrusions into connected cars sold by a number of different companies. Tesla, for example, has encouraged white-hats to hack its vehicles and has to date paid out hundreds of thousands of dollars to those able to uncover vulnerabilities. The latest hack came at a Vancouver hacking conference in March 2019, following previous hacks of Tesla cars in 2016 and 2017.[15] Perhaps as a result of these and other high-profile incidents, a July 2019 survey found that only 36% of consumers expressed confidence in the future of self-driving vehicles. And this problem isn't even confined to connected automobiles, either; in that same month the Department of Homeland Security issued a warning explaining that connected systems also create a hacking vulnerability in small planes. Given physical access to the aircraft, a hacker could use a special device to gain access and manipulate flight instruments.[16] And NYU's Tandon School of Engineering has shown that "a data-driven attack strategy" has the near-future potential to use connected electric vehicle charging stations to bring down the entire power grid of Manhattan.[17]

Cyber-Litigation

Perhaps owing to cybersecurity's growing presence on governmental radar, investigation and/or legal action following hacking incidents or even suspicions of such

5 https://www.tomsguide.com/us/amazon-echo-spy-bug-defcon,news-27788.html

6 https://www.npr.org/sections/thetwo-way/2018/06/05/617196788/s-c-mom-says-baby-monitor-was-hacked-experts-say-many-devices-are-vulnerable

7 https://www.wired.com/story/pacemaker-hack-malware-black-hat/

8 https://www.theguardian.com/technology/2017/jul/31/tesla-model-3-electric-car-doesnt-have-key-things-we-learned-speedometer-battery-sleep

9 https://www.pcmag.com/news/326494/chevy-valet-mode-is-a-nanny-cam-for-your-car

10 http://www.motortrend.com/news/gm-super-cruise-2018-cadillac-ct6-with-auto-pilot/

11 https://www.sae.org/news/2018/01/nissans-propilot-assist-is-more-than-lane-keeping

12 https://www.autotrader.com/car-info/volvos-vision-2020-and-pilot-assist-254811

13 https://www.businessinsider.com/internet-of-things-connected-smart-cars-2016-10

14 https://www.forbes.com/sites/alanohnsman/2019/07/31/safety-group-says-a-50-cent-kill-switch-curbs-security-risk-of-hackable-cars/#677002fc3af1

15 https://electrek.co/2019/03/23/tesla-model-3-hacker-competition-crack/

16 https://www.bloomberg.com/news/articles/2019-07-30/apnewsbreak-us-issues-hacking-alert-for-small-planes

17 https://www.utilitydive.com/news/simultaneous-hack-of-ev-chargers-could-cause-manhattan-blackout-nyu-resear/560974/

risk to consumers is possible. For example, the FTC sued Wyndham Worldwide Corporation over allegations three of its franchised hotels neglected to secure the personally identifying information and payment data of its guests. The court ruled in the FTC's favor on the basis of a "common enterprise theory" which held the parent was liable for its subsidiaries' mistakes. Wyndham lost its appeal in the Third Circuit, which found that the Federal Trade Commission Act's ban on "unfair or deceptive acts or practices" gave the FTC remit to file suit against Wyndham.[18] The decision gives the FTC and other government agencies precedent to further pursue cybersecurity claims.

Management of cyber risk can be summarized via three main principles: choice, security, and accountability. The first strategy – consumer choice – is mandatory under Europe's General Data Protection Regulation (GDPR), a fact states are becoming more aware of. Consider Skuro v. BMW of North America, LLC, a class action in California in which the plaintiffs alleged that BMW taped its customer service helpline without prior disclosure that it was doing so.[19] Skuro exemplifies the extensive exposure businesses create without providing such notice; BMW was obliged to pay out $50 to every customer affected or to provide them 6 months free service. It is thus paramount that customers are given notice of and opportunity to consent to privacy policies. Security is another key facet of any good risk management strategy. With respect to connected vehicles, one study recommended that the addition of a simple, 50-cent 'kill switch' reduced security risks to a significant degree while consumers await more airtight and permanent cybersecurity precautions.[20] The final cornerstone is accountability. More and more governments are passing legislation aimed in part at holding businesses liable for security lapses in hopes of spurring security improvements; to date the European Union has been the leader on this, but the U.S. is gradually following suit.

Relevant Legislation

Passed in April 2016 and implemented in May 2018, the European Union's GDPR may be the most sweeping change to global privacy law in decades. Intended to synchronize data protection protocols across the EU, the legislation binds not only EU-based businesses but any entities that handle data within the Union. The GDPR endows individuals with an unprecedented package of consent rights; among these are the right to be informed, the right of access, the right of rectification, the right to erasure, the right to restrict processing, the right to data portability, and the right to object. Even more important to affected companies is the sheer robustness with which the law punishes non-compliant businesses; penalties are capped at 4% of global revenues or €20 million, whichever is higher.[21] What's more, China has moved to toughen up its own privacy laws to an extent that the Center for Strategic & International Studies pronounced "more far-reaching" and with "more onerous requirements" than the GDPR, "leading the United States to be more isolated with U.S. companies in reactive mode."[22] The increased rigor of these privacy rules will likely slow automakers' plans to monetize data, especially in the affected regions and with regard to the sale of analytics and information to third parties.

Washington D.C. has demonstrated a growing awareness of the cybersecurity menace – if not a sufficiently urgent one – and has kicked out a corresponding rise in bills drafted to combat it. Congress's first major passage of computer-related legislation occurred as early as 1986, when the Computer Fraud and Abuse Act first declared hacking to be a crime and provided hacking victims the ability to pursue a civil action against the hacker.[23] Interpreting connected vehicles as computers within the scope of the CFAA, it is thus a felony to hack a vehicle without permission. More recently, the Cybersecurity Information Sharing Act, passed in 2015, charges certain Cabinet departments with disclosing cybersecurity threat information to private and public entities under threat, and provides that "private entities may monitor and operate defensive measures on: (1) their own information systems; and (2) with written consent, the information systems of other private or government entities."[24] The Department of Homeland Security followed up the passage of CISA with a February 2016 memo detailing for businesses and other "non-federal entities" how they could benefit from the law's provisions.[25] Further cybersecurity legislation has been mired in committee. Among these is the Internet of Things Cybersecurity Improvement Act, which would prohibit hardcoded login credentials and require vendors to "ensure that their devices are patchable and are free from already known vulnerabilities when sold."[26] Another piece of proposed legislation in the current Congress, the SPY Car Act, aims to address the vulnerabilities of

18 https://harvardlawreview.org/2016/02/ftc-v-wyndham-worldwide-corp/

19 https://classactionlawsuitsinthenews.com/class-action-lawsuit-settlements/bmw-assist-class-action-settlement-of-bmw-assist-call-monitoring-or-recording-class-action-lawsuit/

20 https://www.forbes.com/sites/alanohnsman/2019/07/31/safety-group-says-a-50-cent-kill-switch-curbs-security-risk-of-hackable-cars/#677002fc3af1

21 https://gdpr.eu/what-is-gdpr/

22 https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr

23 18 U.S.C. § 1030(a)(2)(C)

24 S. 754; 114th Congress

25 https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf

26 H.R. 1668, S. 734; 116th Congress

connected vehicles specifically by directing the FTC and NHTSA to establish federal standards for driver privacy and cybersecurity. Under this legislation, any OEM found to have been hacked due to a lack of built-in security controls would face a fine of $5000 per car. Additionally, connected vehicles would be equipped with a "cyber dashboard", designed to provide consumers with an easily digestible overview of the OEM-installed security features.[27]

Certain states have been more successful than the federal government in terms of passing cybersecurity legislation. 2018's California Consumer Privacy Act, "America's GDPR" and the first such law in the nation, endows consumers with many of the same rights as the European original but stops short of a right to correction and defines most rights somewhat more narrowly. However, the CCPA does expand on some facets of the GDPR, most notably in not capping penalties for violators at all.[28] Nevada's even newer privacy law, SB 220, offers a relatively tamer counterpoint to neighboring California's CCPA. Unlike that law, and Europe's GDPR, Nevada does not give its consumers any right to access, portability, deletion, or non-discrimination. Nevada also does not require an "opt-in" to data selling or a "Do Not Sell" button as California mandates. Lastly, SB 220 contains a narrower definition of protected data than the CCPA.[29] Nevada shows, then, the extent to which cybersecurity laws will differ greatly as they are ratified in greater numbers of states. One thing is clear, however; disparities in privacy protections across state lines notwithstanding, there are more packages of legislation like California's and Nevada's on the way. As of 2019, all 50 states, the District of Columbia, Puerto Rico, and Guam had laws requiring consumers be alerted to a security breach of their personal data, and 21 state legislatures weighed action to alter those laws.[30]

Takeaways

There is a surplus of practical strategies businesses can pursue right now to bolster cybersecurity both in regard to connected vehicles and the digital sphere more generally. It is crucial to stay updated on relevant events in the news. Physical harm isn't the sole determinant of cost in a hacking incident; financial harm can alone be crippling. Getting in front of potential claims necessitates a well-trained consumer operations department; security hacks may very well be mistakes or oversights of a business's own making. A plan on dealing with hacks when they do arise is a must; coordinating such best practices will often involve complicated coordination between multiple departments. And when a potential threat does surface - speaking up is always the best policy.

Businesses can further secure their digital presences by exercising due care by design. Designing and building privacy and security protections into products from the outset is critical, as is integrating these same protections into everyday business practices. Companies can cultivate a top-to-bottom emphasis on security with executive-level commitment and employee training sessions. Such a reworking of the company culture creates efficiency, reduces risk, creates a competitive advantage, and reduces costs.

Despite the stringency of the GDPR and other beefed-up privacy standards, such laws are a boon to companies as well as consumers. An overwhelming consensus of consumers prefers to engage with companies which they trust to protect their personal information. 89% of American consumers surveyed said they would steer clear of businesses that they did not trust in this regard, giving businesses not only a legal but a financial incentive to take data protection seriously. What's more, 91% would do more business with those companies with independently verified privacy policies, and 68% of U.S. consumers take privacy into consideration before doing business at all. Regarding connected vehicles, a survey by KPMG found that 82% of respondents would "never" purchase a car from a carmaker affected by a vehicle hacking. [31] The takeaway is clear: requiring and upholding a high standard of privacy protection safeguards businesses and their reputations as well as their customers.

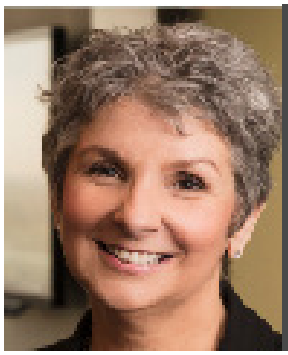
27 S. 2182; 116th Congress

28 https://www.pwc.com/us/en/services/consulting/cybersecurity/california-consumer-privacy-act.html

29 https://www.insideprivacy.com/united-states/state-legislatures/nevadas-new-consumer-privacy-law-departs-significantly-from-the-california-ccpa/

30 www.ncsl.org/research/telecommunications-and-information-technology/2019-security-breach-legislation.aspx

31 http://www.techrepublic.com/article/why-the-age-of-connected-cars-presents-a-very-real-threat-in-cybersecurity/



CHERYL A. BUSH

Founding Member
BUSH SEYFERTH (Troy, MI)

248.822.7801 | bush@bsplaw.com

Cheryl A. Bush has extensive first-chair trial experience and has obtained exceptionally positive results for her clients, including Fortune 500 companies, by winning 95.97% of her jury trials. She serves as National Counsel for a major automotive manufacturer, handling catastrophic air bag trials and coordinating discovery throughout the country. Her cases, which have spanned 30 states, often involve high-level nationwide media exposure.

Cheryl teaches regularly on trial advocacy, particularly in the area of automotive product liability. She is a Fellow in both the American College of Trial Lawyers and the International Society of Barristers. She is a member of the Product Liability Advisory Council and is engaged in the National Association of Minority & Women Owned Law Firms.

Related Services

- Advanced Technologies
- Business and Commercial
- Class Actions
- Product Liability
- Securities / Finance

Honors and Awards

- Michigan Lawyers Weekly, Hall of Fame, 2019
- Women Business Michigan Super Lawyers Top 25, 2018
- Crain's Detroit Notable Women Lawyers in Michigan, 2017
- Corp! Diversity Business Leader, 2017
- America's Top 100 Attorneys®, 2017
- America's Top 100 High Stakes Litigators® for Michigan, 2017
- Leading Lawyers, Member, 2014-present, Advisory Board Member, 2018
- Leon Hubbard Community Service Award, 2015
- Benchmark Litigation, Litigation Star, 2015
- Michigan Lawyers Weekly, Women in the Law, 2014
- Inclusion in The Best Lawyers in America©, Commercial Litigation and Product Liability Litigation – Defendants, 2012-present
- Michigan Super Lawyers, 2011-present
- U.S. News Best Lawyers®, 2010-present
- Michigan Lawyers Weekly, Leader in the Law, 2010
- DBusiness Top Lawyers, 2008-present
- National Association of Women Business Owners, Breakthrough Award
- Martindale Hubbel® AV Peer Review Rating

Education

- University of Michigan Law School, J.D., cum laude, 1984
- Wayne State University, B.A., magna cum laude, 1981