Title
Public Values, Private Infrastructure and the Internet of Things: The Case of Automobiles

Authors
Mulligan, Deirdre K
Bamberger, Kenneth A

Publication Date
2016-10-01

Peer reviewed

경제규제와 법 (Journal of Law & Economic Regulation)
제9권 제1호 (통권 제17호). (Vol. 9. No. 1). 2016. 5. pp.7~44

Special Issue Internet of Things : Legal Issues and Challenges towards a Hyperconnected World

Public Values, Private Infrastructure and the Internet of Things : The Case of Automobiles †

Deirdre K. Mulligan* · Kenneth A. Bamberger**

목차

〈ABSTRACT〉

In July 2015, two researchers gained control of a Jeep Cherokee by hacking wirelessly into its dashboard connectivity system. The resulting recall of over 1.4 million Fiat Chrysler vehicles marked the first-ever security-related automobile recall. In its wake, other researchers demonstrated the capacity for remote takeovers of automobiles. By September, it became public that GM had initiated a quiet over-the-air (OTA) update program to fix security vulnerabilities in millions of their vehicles.

These incidents reveal the critical security issues of modern automobiles, so-called "connected cars," and other Internet of Things (IoT) devices, and underscore the importance of regulatory structures that incentivize greater attention to security during production, and the management of security vulnerabilities discovered after connected devices are in circulation. In particular, it highlights the importance of incentivizing the development of OTA update systems to support safety and security critical updates to patch vulnerabilities. OTA update systems are essential to IoT security and the health and safety of humans who rely upon it.

Today's connected cars can have more than a 100 million lines of software code, and this code base is growing. This code plays a significant role in compliance with regulatory obligations, and a crucial role in automotive safety and security systems. Embedded sensors and algorithms trigger and modulate airbag deployment, seatbelt engagement, anti-skid systems, and anti-lock breaks, identify the size, weight, and position of people to inform airbag and seatbelt behavior, and inform parking assistance systems, anti-skid and anti-lock break systems, among others. Software's role in automotive safety is growing making the assumptions and calibrations of the code governing critical safety systems, as well as its security, increasingly

† 투고일자 2016. 4. 8, 게재확정일자 2016. 5. 30.

* Associate Professor, School of Information, University of California, Berkeley; Faculty Director, Berkeley Center for Law and Technology.

** Professor of Law, University of California, Berkeley; Faculty Director, Berkeley Center for Law and Technology.

important to saving lives. Addressing the vulnerabilities in automotive code — such as the ones exploited by the Jeep hackers — and specifically the capacity for remote exploits, are an essential element of the future of automotive safety and security.

The design of OTA update systems implicates crucial issues of governance, and the balance of a variety of values - both public and private. Developing systems intended to ensure automotive safety and security involves both choosing among competing visions of security, and determining how to protect other values in the process. The articulation of cybersecurity goals, and the way they are balanced against other values, must occur in a public participatory process beforehand that includes relevant public and private stakeholders.

This paper sets forth principles that should inform the agenda of regulatory agencies such as the National Highway Transportation (NHTSA) that play an essential role in ensuring that the IoT, and specifically the OTA update functionality it requires, responds to relevant cybersecurity and safety risks while attending to other public values. It explains the importance of OTA security and safety update functionality in the automotive industry, and barriers to its development. It explores challenges posed by the interaction between OTA update functionality, consumer protections — including repair rights and privacy — and competition. It proposes a set of principles to guide the regulatory approach to OTA updates, and automobile cybersecurity, in light of these challenges. The principles promote the development of cybersecurity expertise and shared cybersecurity objectives across relevant stakeholders, and ensure that respect for other values, such as competition and privacy is built into the design of OTA update technology. In conclusion, we suggest reforms to existing efforts to improve automotive cybersecurity.

Keywords: cybersecurity, privacy, administrative law, privacy by design, IoT

Ⅰ. Introduction

In July, 2015, two researchers gained control of a Jeep Cherokee by hacking wirelessly into its dashboard connectivity system.[1] The resulting recall of over 1.4 million Fiat Chrysler vehicles marked the first-ever security-related automobile recall.[2] In its wake, other researchers demonstrated the capacity for remote takeovers of automobiles via aftermarket telematics products used by the insurance industry; and by September, it became public that GM had initiated a quiet over-the-air update program to fix security vulnerabilities in millions of their vehicles — vulnerabilities identified by a team of computer scientists five years earlier.[3]

Together, these incidents reveal the critical security issues manifest specifically in modern vehicles, and the shortcomings of current policy and technology deployment to address them. In particular, they underscore the importance of assessing how best to incentivize greater attention to the security properties of on-board and after-market telematics, and to manage security vulnerabilities discovered after cars are in circulation.

1) Andy Greenberg, Hackers Remotely Kill a Jeep on the Highway—With Me in It, Wired (July 21, 2015), available at http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
2) Wright, Robert, and Andy Sharman, Cyber hack triggers mass Fiat Chrysler car recall, Financial Times (July 24, 2015), available at http://www.ft.com/cms/s/0/2bafe3e0-321f-11e5-8873-775ba7c2ea3d.html.
3) http://www.wired.com/2015/09/gm-took-5-years-fix-full-takeover-hack-millions-onstar-cars/.

More generally, these incidents highlight the security challenges created by the explosion in connected devices in a whole range of sectors. Indeed, the Internet of Things (IoT) has generally emerged without sufficient attention to the risks of embedding computation and connectivity in relatively unmanaged – and often unmanageable – devices over the long term. As a columnist recently penned, "If they can compromise credit card systems and NASA and even your car, how hard is it going to be to hack your toaster? Imagine the hell these nogoodniks could wreak by gaining access to all that juicy stuff your appliances know about you."[4)]

The question of how to address cyber security vulnerabilities identified after products are in circulation, such as the hacked automobiles already in widespread use, is of particular urgency.

Security experts have therefore pointed to the essential nature of update functionality in managing the security and safety risks posed by the Io T.[5)] Regulators have so far agreed in principle,[6)] and industry groups are considering a self-regulatory code for IoT devices that includes a requirement to remediate post product release design vulnerabilities either through remote updates or through actionable consumer notifications.[7)] Yet many sectors of the economy lack regulatory or market incentives to invest in update functionality. In particular, devices viewed as close-to-disposable, or low production, are often developed with scant attention to security, and are not upgradable. The risks posed by the proliferation of such increasingly powerful - yet un-updatable and unmanaged - connected devices are incalculable. Moreover, even where incentives exist to develop the capacity to patch security vulnerabilities, the sizeable technological challenges of making sure updates are effective, traceable, and secure, and the novel legal and policy questions of largely over-the-air (OTA) updates, remain largely unaddressed.

The automobile industry provides a guiding case study for these neglected questions, and the risks they reveal. Unlike other sectors in which IoT is being deployed, an institutional framework for addressing the public values implications of private infrastructure development already exists in the automotive context - an established network of administrative agencies already possesses regulatory authority over the transportation sector, and a longstanding regulatory framework addresses

4) http://theweek.com/articles/571728/why-internet-things-worse-than-zombie-apocalypse.

5) National Science Foundation, "Interdisciplinary Pathways towards a More Secure Internet", A report on the NSF-sponsored Cybersecurity Ideas Lab held in Arlington, Virginia, February 2014, http://www.nsf.gov/cise/news/CybersecurityIdeasLab_July2014.pdf (calling for the creation of a framework for managing software updates); RFC 7452 Architectural Considerations in Smart Object Networking March 2015, p.15 ("A solid software update mechanism is needed not only for dealing with the changing Internet communication environment and for interoperability improvements but also for adding new features and for fixing security bugs."); Hewlett Packard Enterprise, Internet of Things Research Study 2015 Report ("Updates to your product's software are extremely important and ensuring there is a robust system in place to support this is key.") p.6 http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

6) Federal Trade Commission Staff Report, Internet of Things: Privacy & Security in a Connected World, 2015 ("FTC IoT Report"). Available online: http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf ("companies should continue to monitor products throughout the life cycle and, to the extent feasible, patch known vulnerabilities") p.31; accord Article 29 Working Group IoT Opinion ("Device manufacturers should provide simple tools to notify users and to update devices when security vulnerabilities are discovered.").

7) Online Trust Alliance, IoT Trust Framework – Security, Privacy & Sustainability Release 11-6 https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework_11-6c.pdf.

safety recalls. Thus, as the safety and privacy threats of insecure devices spike more generally, the automobile sector provides a concrete context in which to address the question of how a public regulatory apparatus can catalyze the private sector's development of technological capacity for OTA update channels in a way that furthers and protects public cybersecurity goals.

Although the challenge of security vulnerabilities is now clearly important for manufacturers, drivers, regulators, and the general public alike, deciding how particular technological remedies for those vulnerabilities should be designed implicates crucial issues of governance, and the balance of a variety of values — both public and private — that those decisions require. Specifically, questions of who has input into setting the goals of such technological fixes, and how that input should be structured, will determine the meaning of the "security" that is, or is not, pursued as well as how other public values are vindicated by technological and regulatory choices.

To be sure, the writing of the code that powers automobile technology and OTA update channels will largely fall to the engineers within private corporations who possess the granular knowledge about the operations of the proprietary systems and products that their firms develop and manufacture, and are privy to proprietary designs and firm strategies. But the task of securing such systems cannot be left to private actors, guided by private incentives, technological mindsets, and firm-specific goals alone.[8] For as the development of the Internet of Things moves technology from a means to power products and services to a force that designs the very architecture of societal behavior, the reality that technological choices embody, and embed choices about, social values becomes increasingly salient.

Understood through this lens, then, developing systems intended to ensure automotive safety and security involves both choosing among competing visions of security, and determining how to protect other values in the process — a process that we have elsewhere called a "Design War."[9] Design, whether purposefully or inadvertently, makes determinations about the relative weight of an entire range of competing private, consumer, and more general public values, including cost, flexibility, marketability, interoperability, consumer protection, market power, safety and security — and even between competing notions of security itself. Technology, can no longer be viewed as a simply a neutral means of achieving firm outputs, guided by the metrics of engineers and business strategy, and shielded from public-policy attempts to look "under the hood" — until something goes awry.

Rather, an articulation of cybersecurity goals, and the way they are balanced against other values, must occur in a public participatory process beforehand that includes relevant public and private stakeholders. Despite the devastating risks posed by cybersecurity failures, to date there exists no framework for reaching agreement on cy-

8) Kenneth A. Bamberger, Technologies of Compliance: Risk and Regulation in a Digital Age, 88 Tex. L. Rev. 669, 677 (2010) (emphasizing "collaboration in the process of developing risk-management systems, drawing both on the granular expertise of firms and on the broader vantage of the administrative agency").

9) See Deirdre K. Mulligan & Kenneth A. Bamberger, *The Coming Design Wars* (forthcoming); Deirdre K. Mulligan & Kenneth A. Bamberger, *Apple v. FBI: Just One Battle in the 'Design Wars'* THE RECORDER (Monday, March 21, 2016), at 6 (available at http://www.law.com/sites/lawcomcontrib/2016/03/18/apple-v-fbi-just-one-battle-in-the-design-wars/?slreturn=20160303212714).

bersecurity goals in the automobile context let alone considering how to accommodate and preserve competing values such as competition and privacy in the process. We are proceeding in the dark, just as the threat of Design-War casualties escalates.

This paper begins to address this vacuum, setting forth principles that should inform the agenda of regulatory agencies such as NHTSA that play an essential role in ensuring that the IoT, and specifically the OTA update functionality it requires, responds to relevant cybersecurity and safety risks while attending to other public values. It articulates the case for OTA security and safety update functionality in the automotive industry. It explores the barriers to the development of such functionality, specifically the public good nature of cyber security, and the lack of robust sector specific cybersecurity expertise. It then discusses the additional challenges posed by the interaction between OTA update functionality, consumer protections – including repair rights and privacy – and competition. It then proposes a set of principles that should guide the regulatory approach to OTA updates, and automobile cybersecurity more generally, in light of these challenges. These principles aim both to promote the development of cybersecurity expertise and shared cybersecurity objectives across relevant stakeholders; and to ensure that respect for other values, such as competition and privacy, is built into the design of OTA update technology. In light of these goals, we then assess existing moves towards regulation and, finding them lacking, suggest important ways to move forward.

Legal frameworks differ across market sectors, but the automotive sector provides a rich case study for considering the implications of building out OTA update paths to manage cybersecurity and safety in the IoT. The case study highlights the range of potential consumer protection and competition issues raised by OTA security and safety updates across cyber-physical systems[10], and provides a launching point for a broader inquiry into the regulatory structures and technical investments required to address the novel privacy, security, physical safety, consumer protection, and competition challenges of the IoT environment. The development of OTA channels to support safety and security critical updates with appropriate protections for consumers and competition is essential to a healthy IoT ecosystem, and increasingly essential to the health and safety of humans who rely upon it. The development of OTA update systems that define and advance safety and security goals and are acceptable to all parties depends upon public processes that leverage industry knowledge, engage cybersecurity experts, and identify and resolve challenges OTA updates pose to other value commitments.

Ⅱ. Responding to the Cyber Security and Safety Risks of the Internet of Things: Over-the Air Updates and The Case of Automobiles

1. Code and Cars

Analysts predict that there will be as many as 250 million so-called “connected cars” – automobiles, like other IoT devices, connected to external networks - on the road by 2020. In the case of cars, the connection currently typically uses a

10) Cyber-physical systems (CPS) seamlessly integrate computational algorithms and physical components.

cellular network; however, technical standards are being developed to enable what some have called "talking cars"[11] – vehicle-to-vehicle networks ("V2V") that allow cars to communicate with one another on the highway. V2V communication is an essential piece of the self-driving car infrastructure; its development is reportedly being expedited at the request of the Obama Administration.[12] Complimentary work involves vehicle-to-infrastructure networks (V2I) using dedicated short-range communications (DSRC) protocols,[13] which support communications about road hazards, traffic flow, and accidents. V2I is already used to moderate traffic flow through applications such as on-ramp and traffic-maze metering, and researchers are encouraged about its potential to minimize accidents and congestion, and reduce the environmental impact of driving.[14]

Today's connected cars can have more than a 100 million lines of software code,[15] and this code base is growing as onboard computing and internal and external networking continue to expand.[16] The Volkswagen scandal underscored the extent to which this code is entwined with regulatory aims and public governance. Volkswagen used software code to alter automobile performance, in-real-time, under test conditions. Cars were designed to interpret their external environment and, when relevant, to alter behavior in a manner that brought emissions levels into conformance with regulatory requirements. On a more fundamental level, the scandal underscored the significant role software plays in compliance with regulatory obligations in the first instance.[17] In the automobile context, code governs, monitors and adjusts the timing, pressure, and mix of fuel and air flowing into the engine to optimize for fuel efficiency (or other attributes) within emission parameters set by government mandate.

Software today plays a crucial role in both preventative and responsive safety systems, as well as for security systems such as locks and alarms.[18] Embedded sensors and algorithms sense events that trigger and modulate airbag deployment, seatbelt engagement, anti-skid systems, and anti-lock breaks.[19] On the responsive safety side these systems identify the size, weight, and position of people to inform airbag and seatbelt

11) David Z. Morris, How Will Talking Cars Change Our Roads?, Fortune (January 8, 2016), available at http://fortune.com/2016/01/08/connected-vehicles-impact-cities/.

12) http://fortune.com/2015/05/14/v2v-communication-cars/.

13) V2I communications are also being developed that involve the wireless exchange of critical safety and operational data between vehicles (including brought-in devices) and highway infrastructure, intended primarily to avoid motor vehicle crashes while enabling a wide range of mobility and environmental benefits."

14) Bento, Luís Conde, Ricardo Parafita, and Urbano Nunes. "Intelligent traffic management at intersections supported by v2v and v2i communications." *Intelligent Transportation Systems (ITSC), 2012 15th International IEEE Conference on*. IEEE, 2012.

15) CHARETTE, Robert N. "This car runs on code. 2009." *IEEE Spectrum* (2013); http://blogs.wsj.com/digits/2013/11/11/chart-a-car-has-more-lines-of-code-than-vista/. For comparison the F-35 Joint Strike Fighter has 5.7 million lines and the Boeing 787 about 6.5 million lines http://www.redbend.com/data/upl/whitepapers/red_bend_update_car_ecu.pdf p.2.

16) Rick Merritt, "IBM tells story behind Chevy Volt design," EE Times, May 4, 2011, www.eetimes.com/document.asp?doc_id=1259444 (reporting that a 2011 Chevrolet Volt was estimated to use 10 million lines of code, up from a typical 2009 model which used 6 million lines of code and a 2005 model which used 2.4 million).

17) *See generally* Kenneth A. Bamberger, Technologies of Compliance: Risk and Regulation in a Digital Age, 88 Tex. L. Rev. 669, 670 (2010) (documenting "the increasingly pervasive reliance on technology … in complying with government regulation").

18) Gustafsson, Fredrik. "Automotive safety systems." *Signal Processing Magazine, IEEE* 26.4 (2009): 32-47. (discussing software in "active safety (driving safety) systems that prevent accidents and passive safety (crash protection) systems").

19) Id.

behavior.[20] On the preventative side they inform parking assistance systems, anti-skid and anti-lock break systems, among others.[21] As V2V and V2I standards and technology are adopted, moreover, the role of code in automotive safety will increase. The assumptions and calibrations of the code governing critical safety decisions will be increasingly important to saving lives. Identifying and addressing the vulnerabilities in such code, and the broader systems in which they are deployed will become an essential element of automotive safety and security.

2. The Challenge of Security and Safety Updates

As with the Volkswagen cars that now require software changes to achieve legal compliance (and in some instances hardware changes as well), safety and security critical code will need to be updated. A broad-based security critical update occurred in August, 2015, when General Motors changed software running its servers and the code in its OnStar RemoteLink iOS app to address a vulnerability that allowed a hacker to track, unlock, and trigger the horn and alarm through that remote-access system.[22] And the vulnerabilities discussed earlier that allowed hackers to remotely seize control over the brakes and acceleration on the Jeep, while not in the safety systems themselves had clear and critical ramifications for human safety.

The increasing reliance on code in all aspects of automotive experience – within the cars, on the highways, in tolls and other monitored areas – can improve driving safety. Software dependent safety systems have already been identified as making substantial contribution to safety improvements. However, code in cars, in their safety systems, and in the broader range of objects – such as cellular phones – that interact with them present new opportunities for failure, and for malfeasance. Reaping the benefits while minimizing the risk requires keen attention to the security of automotive software, and to the mechanisms available to patch, upgrade, and address vulnerabilities in such systems rapidly and ubiquitously. While the code base in cars may or may not grow, the increasing automation of both driving tasks – including the development of self-driving automobile capacity – and road infrastructure ensures that code will play an increasingly larger role in automotive safety.

3. The Technological Fix: The Case for Mandatory OTA Updates

a. Updating in the Software Context Generally

The reality that systems cannot be made impervious to future threats, and are often not built to withstand known threats, shapes understandings of software security across contexts. Sound security strategies require the capacity to update, and therefore demand both attention to the properties of the system, and an infrastructure to fix it as new vulnerabilities emerge.[23] In the desktop environment the ability to patch has been credited

20) Id.
21) Id.
22) Bill Howard, GM fixes, refixes OnStar RemoteLink hack, ExtremeTech (August 3, 2015), at http://www.extremetech.com/extreme/211483-gm-fixes-refixes-onstar-remotelink-hack.
23) Deirdre K. Mulligan and Fred B. Schneider. "Doctrine for Cybersecurity." *Daedalus* 140.4 (2011): 70-92.

with avoiding and containing serious security incidents.[24]

Despite the importance of updating software, however, the decision whether and when to update is generally not mandated in the desktop environment; it is left to the users' discretion. Many individuals do not apply patches, or delay doing so, and the failure to patch known vulnerabilities is a significant cause of computer compromise.

There are many reasons individuals and institutions delay or reject security software updates in the desktop and mobile environments. Reasons include concerns about: bandwidth limitations; the introduction of new vulnerabilities; incompatibility with other software, impact on business-essential features or functionality, difficulty restoring a prior state if patches are detrimental — or simply time and disruption, especially that caused by rebooting.[25]

Because of these behavioral realities, the absence of automatic updates results in unpatched vulnerabilities. Even where a vulnerability is widely disclosed and discussed in the media, and poses a significant security risk, patching can vary and remain incomplete.[26] Specialized search engines help bad guys (and others) to identify vulnerable devices.[27] Many exploits used to infect web sites rely on a small set of vulnerabilities for which patches are readily available.

Accordingly, firms are increasingly making security critical updates mandatory and automatic for some systems. With Windows 10, Microsoft moved to automate updates. Users are no longer able to manually select updates for installation. All updates are downloaded and installed automatically; however users can choose between an automatic reboot to install updates when the system is inactive, or a self-scheduled one. Similarly, in 2015, Google, Samsung, and LG began pushing security updates to Android devices.[28]

The externalities posed by unpatched systems have provided a rationale for forced updates in the desktop setting. Unpatched systems often end up conscripted into botnets and used to attack other machines, and a single security impoverished device can create vulnerabilities for the systems to which it connects. Update mechanisms will be particularly essential to address changing threat landscapes for Internet-enabled devices expected to have exceedingly long lifetimes,[29] as well as for semi-autonomous devices.

b. The Legacy System for Safety Issues in the Automobile Context

The general procedure for addressing safety risks in automobiles has developed differently.

24) Keizer, Gregg. (2008) Microsoft: We Took Out Storm Botnet. eWeek, April 22. Available at http://www.computerworld.com/s/article/9079653/Microsoft_We_took_out_Storm_botnet. (Microsoft's ability to remotely respond to Stormbot through a software update was a factor in reducing its impact).

25) Wash, Rick, et al. "Out of the Loop: How Automated Software Updates Cause Unintended Security Consequences." *Symposium on Usable Privacy and Security (SOUPS)*. 2014(discussing why humans must remain "in-the-loop").

26) For an example of patching behavior after Heartbleed — a high profile, high-impact vulnerability — see, Durumeric, Zakir, et al. "The matter of Heartbleed." *Proceedings of the 2014 Conference on Internet Measurement Conference*. ACM, 2014.

27) Article 29 Data Protection Working Party, Opinion 8/2014 on Recent Developments on the Internet of Things 19 (Sept. 16, 2014) ("Article 29 Working Group Opinion"), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

28) http://www.wired.com/2015/08/google-samsung-lg-roll-regular-android-security-updates/.

29) RFC 7452 Architectural Considerations in Smart Object Networking March 2015, p.17 ("It is anticipated that smart objects will be deployed with a long (e.g., 5-40 years) life cycle") http://tools.ietf.org/html/rfc7452.

Under the National Traffic and Motor Vehicle Safety Act[30] the Department of Transportation's National Highway Traffic Safety Administration (NHTSA) issues vehicle safety standards and rules requiring manufacturers to recall vehicles that fail to meet those standards or otherwise have safety-related defects. Safety standards and recalls apply to the physical design, mechanical design, and software of vehicles. Thus, as a legal matter, software-related safety risks can provide the trigger for voluntary or mandatory recalls.

Yet while the incidence of software-related safety-recalls has risen,[31] they have followed the automotive context norm, which largely requires owners proactively to bring their cars to dealers for patching.[32] The success of recalls structured in this fashion is haphazard, as recall notices frequently do not trigger the desired action. The Auto Alliance reported that only 75 percent of consumers respond to recall notices for new cars, and response rates decline precipitously with only 15 percent responding to recall notices for cars older than 10 years. Even where a safety issue is critical consumers may not avail themselves of the fix. In a consumer survey, a trade group found that lack of time to make the repair, distance to dealer, and inconvenience of scheduling and traveling to dealer were among the top reasons cited for not repairing vehicles.[33]

C. The Case for OTA Updates in the Automotive Context

This pattern of consumer behavior renders the dealer-based recall model inapposite for the particular risks raised by software vulnerabilities: the opportunity for remote attacks on vehicles, and the enhanced dangers that unpatched software may pose to other drivers and pedestrians. Unpatched vehicles pose not only a passive hazard, but a means for an active threat.

Software recalls, moreover, are economically ill-suited to the brick-and-mortar dealership model. They result in a significant loss of billable time, as cars receiving software updates occupy bays that could be used by cars needing hands-on repairs. The glut caused by large recalls can overwhelm dealers, particularly where the recall is software related. And the programming tools needed to complete software updates is expensive.

Only a system of forced OTA updates, then, can address software vulnerabilities to security and human safety both effectively and economically. OTA updates' capacity to respond quickly and completely to newly exposed vulnerabilities, with little burden on consumers' time and money, offers compelling safety and security benefits.[34] Such updates, moreover, can fix safety and security problems more conveniently and cheaply than can traditional repair methods. OTA channels permit the installation of updates in multiple vehicles simultaneously while they are at rest. They can increase the repair rate, removing the bottleneck caused by the requirement of a

30) Codified at 49 U.S.C. Chapter 301.

31) Thomson, J. R. *High Integrity Systems and Safety Management in Hazardous Industries*. Butterworth-Heinemann, 2015, p.83.

32) http://www.redbend.com/data/upl/whitepapers/red_bend_update_car_ecu.pdf, pp.2-3.

33) Auto Alliance and Global Automakers, Key Research Findings on Consumers and Auto Safety Recalls, October 7, 2015 ResearchFindings_ConsumersandRecalls07Octo 2015.pdf.

34) von Eitzen, Christopher. (2010) Google Uses Remote Delete to Remove Android Apps from Smartphones. The H Security. June 25. Available at http://www.h-online.com/security/news/item/Google-uses-remote-delete-to-remove-Android-apps-from-smartphones-Update-1029188.html. (Accessed October 2, 2012).

physical connection to the vehicle, allowing updates to occur at virtually any location or time. Limiting the inconvenience, time and other soft-costs of completing recalls, moreover, can in and of itself improve the rate of consumer response. Together, these variables make a compelling case for mandatory over-the-air safety and security software updates.

Ⅲ. The Governance Challenge: The Problem with Leaving Security Update Design to Private Actors Alone

Manufacturers will play a central role in the development of the update capacity necessary to address security vulnerabilities. Corporate managers, and the engineers who design the software that increasingly powers automobiles, possess unique granular knowledge about vulnerabilities, safeguards, response capacity, and network resiliency necessary for the identification and mitigation of security risks. They also have singular capacity to act on that information, and incentives to remedy vulnerabilities in ways that reduce corporate liability and reputational damage.

Yet, as this section explores, leaving private actors alone to address the social risks raised by software security in the increasingly pervasive footprint of the Internet of Things raises a variety of concerns, both about the effectiveness of security measures, and about the value choices that will guide, and be embedded in, the choices that they make. Most simply, the incentives driving security decisions by individual private firms will neither reliably produce optimal security decisions, nor ensure consideration of the range of public values implicated by security risk management. Such concerns are underscored by the security vulnerabilities in connected cars, the slow adoption of OTA update capacity itself, the questions of new vulnerabilities created by update capacity itself, and the resulting challenges for competition and consumer autonomy posed by reliance on proprietary software in risk remediation.

1. Baseline Concerns about the Mismatch Between Public Cyber Security Risk and Private Incentives

a. The Slow Adoption of OTA Updates

Attention to cyber security in the automotive sector has not kept pace with the increased risks of computation and connectivity.

To be sure, OTA has, in several notable instances, been used in telematics control units (TCUs) and onboard entertainment systems. For example, OnStar currently uses OTA updates for its telematics system. This feature, developed to address a vulnerability identified by researchers that allowed them to launch a complicated attack on the Chevy Impala's CAN bus – the collection of networked computers inside a vehicle that control everything from its windshield wipers to its brakes and transmission – by playing a song to the car's Generation 8 OnStar computer, was used to silently conduct an OTA update on millions of vulnerable vehicles. Tesla is an exception. The company has used over the air software updates to fix a fire hazard in nearly thirty thousand of its model S sedans,[35] as well as a ground clearance issue identified in collision reports by altering the

35) http://www.wired.com/insights/2014/02/teslas-air-fix-best-example-yet-internet-things/.

model S's suspension to improve ground clearance at high speeds.[36]

Yet despite the case for the effectiveness and cost benefits, OTA updates are still rare in the general automotive Electronics Control Unit (ECU) market. In 2006, researchers concluded that automotive ECUs provided only "low resistance to attacks of skilled adversaries" and that "[w]ith only minimal and easily obtainable equipment, an adversary can easily read out and install any software at will."[37] Five years later, things remained bleak; in 2010 and 2011 researchers demonstrated that vulnerabilities in telematics control units (TCUs) installed by car manufacturers in multiple automobiles allowed for both local and remote compromise and could be used to takeover virtually all onboard systems.[38] More recently, researchers demonstrated that aftermarket devices – such as dongles used for fleet management or insurance – that can be plugged into the On-Board Diagnostics port (OBD-II in the US) and often communicate wirelessly over the Internet are vulnerable to both local and remote attack.[39] Once compromised, these too can be used to interact with the automotive ECUs and seize remote control over core automotive safety systems.[40]

Summarizing the state of the field, Stefan Savage, the UCSD professor who led one of the two university teams working on the Impala hack, noted the continuing lack of robust security in the automotive sector. At the time of that hack, he explained, the manufacturers "just didn't have the capabilities we take for granted in the desktop and server world." "It's kind of sad," he concluded, "that the whole industry was not in a place to deal with this at the time, and that today, five years later, there still isn't a universal incident response and update system that exists."

The sluggishness of the auto manufacturers' response is not surprising, for a combination of reasons.

As an initial matter, a variety of economic factors suggest that individual firms by themselves will not secure the right investment in security. Because potential attacks can be directed in a way intended to trigger widespread damage extending far beyond the target, they create what scholars have termed "security externalities," which may not be reflected in a single manufacturer's cost-benefit analysis.[41] The increasingly networked nature of the information infrastructure under threat, moreover, diminishes the incentive to make the correct investment. Because a network is protected only if each of its elements is, collective action problems will shape security decisions; in-

36) http://www.reuters.com/article/2015/06/24/us-autos-gm-technology-idUSKBN0P42UY20150624#XOX87kMK8YXvkl2y.97.

37) Scheibel, Michael, Christian Stüble, and Marko Wolf. "Design and implementation of an architecture for vehicular software protection." *Embedded Security in Cars Workshop (ESCAR'06)*. 2006.

38) Koscher, A. Czeskis, F. Roesner, S. Patel,T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental security analysis of a modern automobile, In Proceedings of the IEEE Symposium and Security and Privacy, Oakland, CA, May 2010; Checkoway, D. McCoy, D. Anderson, B. Kantor, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. Comprehensive Experimental Analyses of Automotive Attack Surfaces, In Proceedings of the USENIX Security Symposium, San Francisco, CA, Aug. 2011.

39) Foster, I., Prudhomme, A., Koscher, K., & Savage, S. (2015). Fast and vulnerable: a story of telematic failures. In *9th USENIX Workshop on Offensive Technologies (WOOT 15)*.

40) Id.

41) *See* Kenneth A. Bamberger, *Global Terror, Private Infrastructure, and Domestic Governance* 211, in THE IMPACT OF GLOBALIZATION ON THE UNITED STATES: LAW AND GOVERNANCE, B. Crawford, ed., Vol. 2, 2008 ("Assessing the Market as an Accountability Mechanism: Economic and Cognitive Impediments to Effective Private Measures").

dividual actors will make security investments only if all do.[42] In one of its first reports, the Electronic Systems Safety Research (ERSR) division of NHTSA – created in 2012 to conduct research on the safety, security, and reliability of complex, interconnected, electronic vehicle systems – identified the perception that security did not have a clear return on investment as a recurring challenge to cybersecurity improvement in other industries in which incidents could jeopardize human safety.[43]

The lack of cybersecurity expertise in the automotive sector further complicates adoption. As a recent NHTSA study concluded, cybersecurity has not been a focus of the automotive industry, and to the extent pockets of expertise exist they are likely to be within the IT core competency and not within the developers of operations systems, hardware, and software.[44]

Finally, as discussed below, the OTA context in particular poses two additional barriers to adoption. First, updating thousands of lines of code requires robust connectivity and bandwidth.[45] Second, the security vulnerabilities created by OTA update channels themselves have been cited by at least one manufacturer as a reason for limiting the potential use of OTA updates for core car safety software.[46]

b. Challenges for Creating not Just OTA Capacity, but Secure Channels

The problem of private incentives is compounded by the costs, expertise, and technological barriers involved in addressing the increased risks created by update systems themselves. For while software updates are necessary to address emerging vulnerabilities, they raise security, safety, and privacy risks of their own.

Updates open a potential vector for attack,[47] whether they are offered OTA or through a wired connection. Indeed, analyses of multiple popular software update mechanisms found them susceptible to man-in-the-middle strikes.[48] Updates that patch or remove vulnerabilities are valuable, but only if the means to install them is itself secure – providing integrity checks, limiting access, ensuring compatibility, and ultimately doing no harm, or at least less harm than the unpatched version.[49] One examination of a popular aftermarket telematics control unit (TCU), which connects to a vehicle through the OBD-II port, found multiple security vulnerabilities in the security up-

42) See David Alderson and Kevin Soo Hoo, ''The Role of Economic Incentives in Securing Cyberspace,'' Stanford University Center for International Security and Cooperation, November 2004, 5 (discussing the literature on free-riders in information infrastructure security, perverse incentives in information insecurity, and cyber-security vulnerabilities arising from network dependencies).

43) McCarthy, C., Harnett, K., & Carter, A., *A summary of cybersecurity best practices*. (Report No. DOT HS 812 075). Washington, DC: National Highway Traffic Safety Administration, October, 2014. 28.

44) McCarthy, C., Harnett, K., & Carter, A., *A summary of cybersecurity best practices*. (Report No. DOT HS 812 075). Washington, DC: National Highway Traffic Safety Administration, October, 2014. 28.

45) Susan Crawford, The Tesla Dividend: Better Internet Access, March 25, 2016 (discussing the bandwidth and connectivity needed to support Telsa's updates and AI) https://backchannel.com/the-tesla-dividend-better-internet-access-db175e1835f6#.lgibeu4i8.

46) Kumar Saha, "More OTA updates coming to a car near you," Toronto Star, February 5, 2016 (stating that GM has said it will never use OTA for updates related to safety systems) https://beta.thestar.com/autos/2016/02/05/more-ota-software-updates-coming-to-a-car-near-you.html.

47) Bellissimo, A., Burgess, J. and Fu, K. Secure software updates: Disappointments and new challenges. In *Proceedings of USENIX Hot Topics in Security*, (July 2006).

48) Bellissimo, Anthony, John Burgess, and Kevin Fu. "Secure Software Updates: Disappointments and New Challenges." *HotSec*. 2006.

49) Denning, Tamara, Tadayoshi Kohno, and Henry M. Levy. "Computer security and the modern home." *Communications of the ACM* 56.1 (2013): 94-103.

date channel of the TCU itself.[50]

This problem is even more acute in the broader Internet of Things context. Unlike automobiles, the design of many IoT devices presents technological challenges for established methods of providing secure updates. As one analyst describes, "Embedded devices are designed for low power consumption, with a small silicon form factor, and often have limited connectivity."[51] Such device constraints may be sufficient for achieving intended tasks, but sporadic network connectivity can thwart the downloading of security updates,[52] and limited computing capacity may not support the cryptography that plays an essential role in secure updates. While cryptography is essential to authenticate messages, ensure the integrity of updates, and sign code, modern cryptographic algorithms were designed for the standard computing environment – PCs and servers – and require more energy and computational power than many highly resource-constrained IoT devices offer.[53] Existing cryptographic implementations, therefore, may overwhelm the power of the device or at least greatly diminish its performance.[54]

The potential security risks posed by non-updatable, aging IoT devices, has led to warnings about the "Internet of Treacherous Things,"[55] and the "zombie apocalypse of smart devices"[56] created by unreasonable demands on individuals' time and attention bodes poorly for security. While it may be reasonable to expect that including secure update capacity may be cost-effective in certain functionalities involved in the operations of automobile, it may not be in others. The problem is only compounded in the context of other, lower-end products; security will require addressing the vulnerability challenge in software upgrades for anything from garage door openers to routers, refrigerators and all the other devices that software makes "smart" and *vulnerable*.

The challenge in the automotive and broader IoT context is further exacerbated at the moment in a product's life-cycle when the manufacturer stops providing product support. The risk posed by these devices may be great: how to manage it is an open question. Perhaps updates could be provided by independent entities, or perhaps devices could be disabled when they are no longer capable of being actively managed. These are critical questions for IoT security, that may not be addressed through the logic of a single firm's economic analysis.

50) Foster, I., Prudhomme, A., Koscher, K., & Savage, S. (2015). Fast and vulnerable: a story of telematic failures. In *9th USENIX Workshop on Offensive Technologies (WOOT 15)*.

51) WIND, Security In The Internet Of Things: Lessons from the Past for the Connected Future, at 3, available at http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf.

52) Bellissimo, Anthony, John Burgess, and Kevin Fu. "Secure Software Updates: Disappointments and New Challenges." *HotSec*. 2006.

53) See generally NIST Lightweight Cryptography project description, http://www.nist.gov/itl/csd/ct/lwc-project.cfm.

54) Cirani, Simone, et al. "IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios." *Sensors Journal, IEEE* 15.2 (2015): 1224-1234, 1225. New, lighter weight crypto primitives such as SIMON and SPECK, may address this issue, but they are not yet deployed. Beaulieu, Ray, et al. "The SIMON and SPECK Families of Lightweight Block Ciphers." *IACR Cryptology ePrint Archive* 2013 (2013): 404. And data protection regulators have called on standard setting bodies to "develop lightweight encryption and communication protocols adapted to the specificities of IoT, guaranteeing confidentiality, integrity, authentication and access control," Article 29 Working Group IoT Opinion.

55) http://www.technologyreview.com/news/534196/an-internet-of-treacherous-things/.

56) http://www.wired.co.uk/magazine/archive/2012/12/ideas-bank/the-zombie-apocalypse-of-smart-devices-is-coming.

C. Additional Public Concerns Raised by Relying on Private Incentives for OTA Development

One factor that will increase private incentives for, and speed the development of, OTA update capacity is the use of update channels for non-safety and security related upgrades. As car-makers realize the "powerful and lucrative after-market ... one that can deliver revenues long after the original sale,"[57] software update mechanisms will become more attractive. Yet expanding OTA capacity in this way raises legal, technical and behavioral issues that could reduce the effectiveness of OTA updates as a means for mitigating security and safety risks.

Indeed, some manufacturers are already approaching their products with a Silicon Valley mindset, envisioning OTA updates as a means to deploy new features.[58] Tesla routinely uses its OTA update functionality to add new features, including self-driving technology.[59] CEO Elon Musk emphasizes the software, tech-centric nature of Tesla, contrasting it with the industrial engineering focus of the automotive industry as a whole. As one commentator wrote, "[t]he mindset of software-dependent industries that earn their profits through an ongoing march of products with new features and functions doesn't yet exist among automotive corporations, it inevitably will."[60]

Some expansion in this direction might be desirable. IBM, for example, has estimated that electronics and embedded software comprise 50% of the car warranty costs.[61] OTA updates used to repair software under warranty would seem to be a non-problematic additional use of the OTA channel.[62] While using it for non-safety and security (and non-recall) repairs could limit competition in the software repair portion of the automotive marketplace, it could offer substantial utility to consumers if the cost of such repairs went down and the convenience went up.

Yet even as incentives for private actors to develop OTA update capacity increases, assigning the design of update channels development primarily to the judgment of those focused on new-feature deployment raises the likelihood that a number of public values will be undervalued in that design. In particular, it raises three distinct risks: compromising security, limiting competition, and undermining consumer protections and privacy.

1) Compromising Security

First, the use of OTA capacity for non-security and safety updates may undermine security. Post-purchase software updates always pose some risk, as they update systems that the manufacturer no longer exclusively controls. Consumers may have modified the product in ways that matter for the update. Each use of the OTA update channel creates a possibility for introducing vulnerabilities.

57) http://www.redbend.com/data/upl/whitepapers/red_bend_update_car_ecu.pdf pp.2-3.

58) http://www.reuters.com/article/2015/06/24/us-autos-gm-technology-idUSKBN0P42UY20150624#XOX87kMK8YXvkl2y.97 (For example, Tesla CEO Elon Musk stated that it could be used to add "new features such as automated parking or limited hands-free driving.").

59) "Your Autopilot has arrived" Teslamotors, October 14, 2015, (discussing the incremental introduction of self-driving technology through 7.0 software update in combination with an earlier hardware upgrade). https://www.teslamotors.com/blog/your-autopilot-has-arrived.

60) http://embedded-computing.com/articles/preparing-for-the-convergence-of-iot-and-automotive/#.

61) http://www.redbend.com/data/upl/whitepapers/red_bend_update_car_ecu.pdf pp.2-3.

62) http://www.redbend.com/data/upl/whitepapers/red_bend_update_car_ecu.pdf pp.2-3.

Use of the OTA update channel for non-security critical functions can fuel consumer distrust,[63] to the detriment of security. Given the critical function OTA updating is likely to play in the automotive software environment, and the possibility that updating will be mandatory, responsible use is critically important. Using the update channel to push non-safety and security focused updates may depress trust and foment push back. Resistance to automatic updating for security and safety recalls (and potentially warranty related fixes) risks sacrificing security and safety to protect the potential profits from ancillary car services.

In the desktop environment the use of update channels to perform non-security critical updates has been criticized.[64] A recent study found that unexpected new features in a security update as well as difficulty assessing the need and benefit of updates reduced users' willingness to install updates.[65] A prime example of the potential backlash from misuse of an update channel comes from Microsoft. In 2006, Microsoft pushed a non-security related update out to customers. The update, called Windows Genuine Advantage, opened an Internet connection and sent information about the computer and software versions to Microsoft without consumer permission. The update was aimed at rooting out unlicensed versions of Microsoft products. The software was dubbed "Windows Genuine Spyware" and Microsoft found itself facing a class action lawsuit.[66] Microsoft backpedaled downgrading the update from "critical" to "high priority" and dropping the "phone home" feature.[67] Whether the incident reduced updating of Microsoft products is uncertain, however it is the sort of unexpected "feature" that researchers found to depress updating generally.

The worst-case scenario occurred recently in the automotive context: a forced OTA update created a risk to human safety. The Tesla's Model S car received the Summons self-parking feature that allowed the owner (or other user) to park the car while standing 10 feet away through an OTA update.[68] Using Tesla's smartphone app or the keyfob, the owner could with one touch put the car in motion. With a second touch the car would

63) See Fagan, Michael, Mohammad Maifi Hasan Khan, and Ross Buck. "A study of users' experiences and beliefs about software update messages." *Computers in Human Behavior* 51 (2015): 504-519. See also Williams, Kristy L., Updates are Not Available: FDA Regulations Deter Manufacturers from Quickly and Effectively Responding to Software Problems Rendering Medical Devices Vulnerable to Malware and Cybersecurity Threats (August 6, 2013). Wake Forest Intellectual Property Law Journal, Forthcoming. Available at SSRN: http://ssrn.com/abstract=2350906 (reviewing regulatory obligations and recommending changes)advocating that "automatic systems should be employed strictly fosecurity-related purposes. Any other changes that vendors may wish to make should be presented to users separately from security updates, and in a forthright manner that does not make them appear to be security updates. Vendors should not require users to consent to modifications in the license in order to access a necessary security update." Id. p.36 ("frustration related to misunderstandings can result, at least in part to the large portion of our samples not trusting updates").

64) For a discussion of update channel misuse see Jennifer A. Chandler, "Contracting Insecurity: Software License Terms that Undermine Cybersecurity," in Harboring Data: Information Security, Law and the Corporation, Stanford University Press (2009) Andrea M. Matwyshyn, editor.

65) Vaniea, Kami E., Emilee Rader, and Rick Wash. "Betrayed by updates: how negative experiences affect future security." *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM, 2014.

66) The plaintiff's claims that the use of the update channel to distribute WGA violated the EULA was ultimately rejected, *Johnson v. Microsoft Corporation*, No. C06-0900RAJ (W.D. Wash. June 23, 2009).

67) http://www.informationweek.com/microsofts-wga-sued-as-spyware-/d/d-id/1044797?.

68) Glenn Derene, Tesla Model S Update Improves Safety of Its Summon Feature: In response to Consumer Reports' concerns, Tesla updates software on its self-parking function, Consumer Reports March 09, 2016 http://www.consumerreports.org/hybrids-evs/video-tesla-model-s-update-improves-safety-of-its-summon-feature/.

come to a stop. But, if that second touch didn't occur – for example as Consumer Reports discovered during testing if the keyfob was dropped or the app disabled – the car would continue moving. Consumer Reports complained to Tesla, advocating for a so-called "dead-man's switch" that would ensure the car stopped if the owner's finger was no longer in contact with the screen or keyfob.[69] Tesla issued a second OTA update to address the problem; however, because of limits in the connectivity between the keyfob and the car, only the smartphone app was retrofitted with a dead-man's switch.[70]

This non-security and safety update, then, offered consumers an attractive new feature, but at a potentially significant human-safety cost. Such missteps, in turn, could induce fear in Tesla owners and lead them to avoid updates – especially if users are not able to assess the contents of an update prior to installation. As one Tesla enthusiast wrote, "I have no idea what Tesla did to my car since the release notes were identical between what I had and what I just got. I can't say that I've noticed anything different since the update but I assume something was fixed or improved."[71]

2) Limiting Competition

Second, other uses of an OTA update mechanism could reduce competition in the marketplace.

Software has emerged as an anti-competitive tool in a host of contexts thanks to the anticircumvention provisions of the Digital Millenium Copyright Act. Misusing the prohibitions on trafficking in tools that circumvent access or use controls on copyrighted works enacted to protect movies and music against wholesale copying, companies have attempted to block competitors from offering aftermarket parts through the use of authentication systems and other lock-out codes.[72] Companies have attempted to use software to inhibit competition in various after-market parts markets including toner cartridges[73], garage door openers[74], and computer maintenance services[75], as well as thwart competition in the cellular market.[76]

69) Id.

70) Id.

71) Rob M., How Does a Tesla Over-the-Air Software Update Work?, Teslarati, June 21, 2014 http://www.teslarati.com/tesla-air-software-update-work/#4sQvOFh8midyulct.99.

72) For a thorough overview of the misuse of §1201 of the DMCA to thwart competition see Electronic Frontier Foundation, Unintended Consequences: 16 Years Under the DMCA, https://www.eff.org/files/2014/09/16/unintendedconsequences2014.pdf pp.17-27.

73) Lexmark v. Static Control Components, 387 F.3d 522 (6th Cir. 2004).

74) Chamberlain Group v. Skylink Technologies, 381 F.3d 1178 (Fed. Cir. 2004).

75) Storage Technology v. Custom Hardware Engineering, 421 F.3d 1307 (Fed. Cir. 2005).

76) Exemptions were awarded to allow cell-phone unlocking in §1201 Rulemakings in 2006 and 2009. None was granted in 2012 leading consumer to petition the White House, activity at the FCC to get carriers to agree to unlocking post term policies, and ultimately the enactment of the Unlocking Consumer Choice and Wireless Competition Act which made unlocking Public Law 113-144, 128 Stat. 1751 (2014). The Librarian of Congress adopted amendments to reflect the law. See Exemption to Prohibition on Circumvention of Copyright Protection Systems for Wireless Telephone Handsets, 79 FR 50552 (Aug. 25, 2014) (codified at 37 CFR 201.40(b)(3), (c)). In the just completed 2015 §1201 Rulemaking a broader exemption permitting unlocking of cellphones; all-purpose tablet computers; portable mobile connectivity devices; and wearable wireless devices (i.e., smartwatches, fitbits) that have "previously been lawfully acquired and activated on the wireless telecommunications network of a wireless carrier" was adopted. Library of Congress, Copyright Office 37 CFR Part 201 [Docket No. 2014-07] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Final Rule, 65944 Federal Register / Vol. 80, No. 208 / Wednesday, October 28, 2015. For a thorough overview of the cellphone unlocking exemptions, White House, FCC and legislative activity proceeding the 2015 Rulemaking see, Jonathan Band, "The End of the Cell Phone Unlocking Saga?" August 7, 2014. http://ssrn.com/abstract=2483291.

In the automotive context, OTA could be used to alter vehicle performance more quickly and easily than an after-market part or service provider can offer. The ease and convenience of manufacturer-provided updates could easily undercut the market for similar add-ons or modifications provided by third parties. For example, the OTA update channel could be used to easily upgrade a stereo system, limiting consumer interest in after market options.[77] In addition, similar to the concerns at the heart of the network-neutrality debate, providing some third-party service providers with preferential access to the OTA update channel could undermine competition and consumer autonomy.[78] The ease and convenience offered by the OTA delivery, might offset the often higher price.

The recently concluded Triennial 1201 Exemption Rulemaking under the Digital Millennium Copyright Act provides a sense of the competition issues arising as automakers embed cars with code. The Register of Copyrights received multiple petitions related to automobiles.[79] As in other markets, software-based lock-out codes, authentication sequences, and encryption constrain consumers' and third-party service providers' interactions with lawfully-purchased automobiles.

Specifically, petitioners reported that technical protection measures interfered with the ability of owners and independent repair shops to modify and repair vehicles.[80] Farmers, complained that Trusted Platform Modules (TPM) technology constrains who can work on agricultural vehicles, both directly and indirectly. Direct constraints enabled by TPM-protected software include denying independent repair shops the full-featured versions of their software. Indirect constraints are imposed by the sheer cost of licensing the separate software required to access various cars systems. These practices force owners to bring their vehicles to dealers for repairs, as neither owners nor their independent mechanics have access to the tools and information necessary to get the vehicle back on the road, which raises the costs of owning, modifying, and repairing the vehicle.

The Consumer Electronic Association explained further that its members needed access to vehicle software to develop and use aftermarket vehicular technology to repair, replace, enhance and improve the safety of vehicles. Similarly, the AAA raised concerns about the ability of manufacturers to "lock consumers into closed systems where options and competition are limited or eliminated."

The filings provide a window into the manner in, and length to which, manufacturers today use software as a means of limiting competition, and securing revenue from add on services. While not specifically about OTA updates, it too will involve software, and provide a privileged means for altering vehicles post-purchase. Given the potential leverage software offers to car manufacturers today, it makes sense to ask whether the

77) http://embedded-computing.com/articles/preparing-for-the-convergence-of-iot-and-automotive/#.

78) Id.

79) Petitions for exemption can be viewed here: http://copyright.gov/1201/2014/petitions/ # 12, 14, 23, 24 are specifically about automotive vehicles.

80) See, Comment of Electronic Frontier Foundation In the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. 1201 Docket No. 2014-07 U.S. Copyright Office, Library of Congress, February 6, 2015; Comment of the Intellectual Property & Technology Law Clinic, University of Southern California In the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. 1201 Docket No. 2014-07 U.S. Copyright Office, Library of Congress February 6, 2015.

development of an OTA update function will have anti-competitive effects.

Similar concerns about access to proprietary technical information, and the means to make sense of it, have fueled the battle to pass "right-to repair" laws. In January 2014 trade associations reached an agreement with independent garages and retailers under which auto companies will make diagnostic codes and repair data available in a common format by the 2018 model year.[81] The European Commission requires car manufacturers to provide equal access to technical information to authorized dealers and independent repair shops.[82] But even with equal access, the cost of diagnostic tools, software licenses, and training on multiple software products can squeeze independent repair shops out of the market, leaving consumers with fewer options to service their vehicles.[83]

3) Undermining Consumer Protections and Consumer Privacy

Software updates have demonstrated the capacity to reduce the functionality of lawfully-purchased products, reducing their value to consumers. Companies such as Amazon have raised consumer ire by monkeying with consumer purchases. In 2009 Kindle users had their own "1984" moment when Amazon removed two of George Orwell's classic tomes, "1984" and, "Animal Farm," because the versions were made available for purchase illegitimately. No doubt expressing many consumers' sentiments, one consumer told the New York Times, "I never imagined that Amazon actually had the right, the authority or even the ability to delete something that I had already purchased."[84]

While the use of software updates or post-purchase connectivity for wholesale removal of digital goods is generally infrequent, software updates routinely downgrade and modify consumer products post-purchase. Often this occurs with little user understanding, although perhaps – if not automatically applied – with some limited indication of assent through the omnipresent click-through-screen. For example, a digital TV Tuner was downgraded to allow broadcasters enhanced ability to constrain consumers' ability to record shows off the air in their format of choic e.[85] Similarly, firmware updates were used to remove the ability of portable media players to record FM radio.[86] Apple was derided by one digital rights organization as among the worst offenders – using software "upgrades" to break the Internet streaming feature, restrict the number of streaming users per day, limit the number of times a song purchased on iTunes could be burned, and removing the capacity to rip purchased songs into DRM-free formats.[87] Given that a Tesla enthusi-

81) The agreement mirrors a recently adopted Massachusetts law.

82) Antitrust: Commission adopts revised competition rules for motor vehicle distribution and repair, EUROPEAN COMMISSION (May 2010), http://europa.eu/rapid/press-release_IP-10-619_en.htm. "This regulation is partially based on a decision by the European Commission against DaimlerChrysler, Toyota, General Motors and Fiat, which concerned these manufacturers' restricting independent mechanics' access to technical information." Id.

83) See Hawker, Norman W., Under Threat: Competition in the Automotive Service Aftermarket (November 13, 2008). Available at SSRN: http://ssrn.com/abstract=1337103 or http://dx.doi.org/10.2139/ssrn.1337103 Pp11-14 ("OEM can effectively deny independents access to the tools, codes and training needed to diagnose and repair problems by charging cost prohibitive rates").

84) http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html?_r=0.

85) https://www.eff.org/deeplinks/2007/06/ati-downgrades-its-tuners-and-its-customers.

86) https://www.eff.org/deeplinks/2006/10/creative-labs-upgrade-removes-fm-radio-recording.

87) https://www.eff.org/deeplinks/2007/05/convert-mp3-upgrading-itunes-7-2.

ast – a relatively tech savvy demographic – admitted to knowing little about the software updates he received, it seems likely that the weak consumer understanding of updates found in other sectors will persist in the automotive context.

Software update functionality, and connectivity generally, has also been used to undermine user privacy. Software update channels have been used to collect data about customers without notice or meaningful consent. The WGA incident discussed above is a prime example of this problem. More generally, digital goods and services combined with ongoing connectivity have led to increased collection of data about individuals.[88] Location based services generate detailed data about individuals' daily lives.[89] The ease with which data about location can be collected on mobile platforms has been a source of ongoing public and policy maker concern. Media services of all sorts collect listening, viewing and reading habits to personalize offerings.

Car telematic and media services generate and collect similar data, providing car companies potentially vast amounts of information about drivers location[90] and media preferences. But cars today are instrumented to collect a vast amount of other data. A recently released report by Senator Edward J. Markey (D-MA) compiling information received from thirteen major automobile manufacturers[91] that responded to a request about information being collected included: geographic location (7 manufacturers); system settings for event

88) For a discussion of how interactivity and connectivity create opportunities for post-purchase data collection on uses of information goods see, Deirdre K. Mulligan and Aaron J. Burstein, "Implementing Copyright Limitations in Rights Expression Languages", in Digital Rights Management: ACM CCS-9 Workshop, DRM 2002, Washington, DC, November 18, 2002, Revised Papers (Lecture Notes In Computer Science), Joan Feigenbaum, ed., Volume 2696, Springer-Verlag Publishing, pp.137-154 (2003), and Deirdre K. Mulligan, John Han, and Aaron J. Burstein "How DRM-based Content Delivery Systems Disrupt Expectations of 'Personal Use'", presented at the 2003 ACM Workshop on Digital Rights Management, also in Proceedings of the 3rd ACM Workshop On Digital Rights Management, Washington, DC (2003); for a similar analysis of how the introduction of IoT in home energy delivery creates privacy challenges see Mulligan, Deirdre K., Wang, Longhao, and Burstein, Aaron J., "Privacy in the Smart Grid: An Information Flow Analysis," Final Report prepared for CIEE and California Energy Commission (March 1, 2011), and P.S. Subrahamanyam, D. Mulligan, D. Wagner, E. Jones, U. Shankar and J. Lerner Network Security Architecture for Demand Response/Sensor Networks, for the California Energy Commission, Public Interest Energy Research Group, June 2006; and, for a detailed case study of a particular product offering see, Deirdre K. Mulligan and Aaron K. Perzanowski, The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident, Berkeley Technology Law Journal, Vol. 22, p.1157, (2007).

89) See e.g., Nick Doty, Deirdre K. Mulligan, Eric Wilde, "*Privacy Issues of the W3C Geolocation API*," UC Berkeley: School of Information. Report 2010-038.

90) The lack of regulatory privacy protections for location data outside the telecommunications sector creates an uneven playing field. Many years ago the Cellular Telecommunications and Internet Association petitioned the Federal Communications Commission to rectify the imbalance and create technology neutral protections for location information that would cover its use in automotive systems among others. In the Matter of Petition of the Cellular Telecommunications Industry Association for a Rulemaking to Establish Fair Location Information Practices WT Docket No. 01-72 DA-01-696 . Advocacy organizations supported this petition predicting the growth of location based services in other sectors and the risks to privacy. Comments of the Center for Democracy and Technology Before the Federal Communications Commission In the Matter of Petition of the Cellular Telecommunications Industry Association for a Rulemaking to Establish Fair Location Information Practices WT Docket No. 01-72 DA-01-696. The FCC never acted upon the petition. WT Docket No. 01-72 DA-01-696 Petition of the Cellular Telecommunications and Internet Association.

91) Nineteen companies were queried in total. Only sixteen responded to the request: BMW, Chrysler, Ford, General Motors, Honda, Hyundai, Jaguar Land Rover, Mazda, Mercedes-Benz, Mitsubishi, Nissan, Porsche, Subaru, Toyota, Volkswagen (with Audi), and Volvo. Aston Martin, Lamborghini, and Tesla failed to respond to similar letters. Of the sixteen responding, three – Honda, Porsche, and Mercedes-Benz did not provide information about data collection. The robustness of the responses from the remaining thirteen varied. Office of Senator Edward J. Markey, Tracking and Hacking: Security & Privacy Gaps put American Drivers at Risk, February 2015. (Markey Report)

data recorder (EDR) devices (5 manufacturers), which can include data such as sudden changes in speed, steering angle, brake application, seat belt use, air bag deployment, and fault/error codes; operational data (7 manufacturers), including speed, direction or heading of travel, distances and times traveled, fuel level and consumption, status of power windows, doors, and locks, tire pressure, tachometer and odometer readings, mileage since last oil change, battery health, coolant temperature, engine status, exterior temperature and pressure.[92] Through the embedded sensors cars generate detailed profiles of driving activity. Sometimes collections, such as EDRs, may be episodic and narrowly event driven – prompted by a crash for example – while other data collections are routine. After market parts, such as insurance provided dongles for personalized mileage based insurance premiums, similarly generate detailed profiles of driving patterns. Collected data often leaves the vehicle. For example, eight of the twelve companies that responded to Senator Markey's inquiry reported that transmitting and storing driving history data in a server off-board the vehicle.[93]

Ⅳ. A Public Framework for Cyber Security Design

The government must play a role in advancing cybersecurity objectives in the IoT. Leaving the question of cybersecurity in the hands of private actors poses risks. The public good nature of cyber security, the difficulty of establishing ROI, and the lack of deep cybersecurity expertise in relevant sectors nearly ensure underinvestment. The ambiguity of cybersecurity objectives, coupled with the tensions between potential cybersecurity approaches and other public values, such as privacy and competition, establish a need for broader stakeholder participation in settling cybersecurity's meaning in the specific context and prioritizing among competing public values.[94]

Three principles must guide the development of public frameworks for cybersecurity in the IoT, including the creation of the OTA update mechanisms in the automotive sector.

- Cybersecurity is a public good that requires strategies to overcome barriers to its production stemming from positive and negative externalities;
- Cybersecurity is a political construct that requires public input and agreement on its goals and means; and
- Cybersecurity and other public values – such as privacy and competition – must be considered in consort as design objectives, and injected into design from the beginning.

Below we explain the crucial role these principles play in producing secure, trustworthy systems to support appropriate public cybersecurity objectives consistent with other value commitments. Then we assess government efforts in the automotive sector to date in light of these principles highlighting both promising directions and needed course corrections.

92) Markey Report at 8.
93) Id. at 10.
94) *See* Deirdre K. Mulligan and Fred B. Schneider, *Doctrine for cybersecurity*, DAEDALUS 140.4, 70–92 (2011) (arguing that cybersecurity is a public good and suggesting that public health [itself a public good] might provide inspiration for approaches to cybersecurity).

1. Principles for a Public Cyber Security Design Framework

a. Protecting public values requires that cyber security be understood as a public good; not a private interest.

As the automobile example so far demonstrates, treating cybersecurity as a private good to be produced by the market is likely to result in less than optimal investment in cybersecurity as well as a misalignment between private actions to advance cybersecurity and public cybersecurity needs.

Rather, cybersecurity demonstrates characteristics of a public good. Cybersecurity will be underproduced by the market. It is non-rivalrous because one user benefiting from the security of a networked system does not diminish the ability of any other user to benefit from the security of that system. And it is non-excludable because users of a secure system cannot be easily excluded from benefits security brings.

Moreover, given the risks posed by security vulnerabilities in cyberphysical systems, such as automobiles, there is a heightened need to generate activities that improve the level of cybersecurity across the automotive sector, including after-market parts. As in the public health context, in which legal requirements and regulatory incentives seek to bolster the health and resistance to disease at the population level through a range of actions that both reduce vulnerabilities to disease in the population (such as vaccines) and respond to emerging risks (such as reporting of specific infectious diseases), cybersecurity in the automotive industry requires the production of more secure systems as well as secure and robust OTA update mechanisms to address emerging risks and a changing threat landscape.

As a public good, cybersecurity in the automotive market, and all others, depends not only on technical progress, but on reaching political agreement about its relative value in comparison to other societal values, and the institutions and methods used to resolve conflicts between values and stakeholders, and the individual and societal level interests. Ensuring that the automotive sector develops adequately secure systems – those that respond to the threats and risks, while protecting other values – requires interventions to overcome positive and negative externalities that lead rational entities to underinvest. It also requires activities that support the development of appropriate cyber security expertise in the automotive sector, and harness the vast cyber security expertise of other sectors and in academia.

b. Protecting public values requires clarifying cyber security objectives in the automotive sector within a participatory framework that enlists the range of public and private stakeholders

An emerging body of research demonstrates that framing an issue as a security concern raises an issue above politics as usual, both demanding and affording decision makers the capacity to respond in escalated and expedited ways. In particular, "securitization" legitimates deviations from standard processes, substantive rules and norms, and typically affords disproportionate access to resources.[95] Where, as in cyber security, the objects in need of protection may often be owned and managed by private actors, securitization poses complicated issues for public values.

The risks of allowing security objectives to be

95) Buzan et. al. 1998.

defined by individual actors increases where, as in the context of cyber security, consistent, shared definitions do not yet exist.[96] Researchers have documented deep divergence in understandings about the meaning of cyber security, and related concepts, in policy documents including legislative texts, government strategy, standard setting bodies, international organizations, and research.[97] The lack of common definitions has served as a barrier to international communication and cooperation at the nation state level[98], and to interdisciplinary research.[99] Technology scholar Helen Nissenbaum has documented the significant implications for technical design and public policy of competing conceptions of security, one rooted in computer security (confidentiality, integrity, availability) and the other in national security.[100] By contrast still, subsequent authors have identified a further shift within the discipline of computer science, so that "the majority of today's computer scientists are no longer merely aiming for bug-free, unhackable systems ... [but rather] ... now regard security as a process, including aspects of social engineering, organisational behaviour, and training."[101]

Cyber security, then, remains an ambiguous concept, requiring both contextual refinement as well as political consensus. There currently exists no clear metric to guide decisions about its pursuit — or even to identify what type of "cyber security" should be pursued — nor parameters to guide its contextual application in the automotive sector in light of perceptions about the risks to human health and safety that can result from cyber security failures.

For this reason, articulating context-specific goals is "a prerequisite for achieving enhanced cybersecurity."[102] Goals define agreed-upon kinds and levels of cyber security, characterizing who is to be secured, at what costs (monetary, technical, convenience, and societal values), and against what kinds of threats. The goals might be absolute or they might — as they typically do — specify a range of permissible trade-offs. Trade-offs speak to the political nature of cyber security, its interaction with other values, and the need for broad involvement in establishing goals.

Research and experience from other contexts in which goals and outcomes are difficult to define, risks manifest in heterogeneous ways arising from complex interactions of events or behaviors, and trade-offs are contested, suggest possible contours of such a goal-setting process.[103]

96) New America. Global Cyber Definitions Database. www.newamerica.org/cyber-global/cyber-definitions/; Nissenbaum, Helen. "Where Computer Security Meets National Security1." *Ethics and Information Technology* 7.2 (2005): 61-73; Hansen, Lene, and Helen Nissenbaum. "Digital disaster, cyber security, and the Copenhagen School." *International Studies Quarterly* 53.4 (2009): 1155-1175; Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. "Defining Cybersecurity." *Technology Innovation Management Review* 4.10 (2014); Giles, Keir, and William Hagestad. "Divided by a common language: Cyber definitions in Chinese, Russian and English." *Cyber Conflict (CyCon), 2013 5th International Conference on*. IEEE, 2013.

97) Id.

98) Giles, Keir, and William Hagestad. "Divided by a common language: Cyber definitions in Chinese, Russian and English." *Cyber Conflict (CyCon), 2013 5th International Conference on*. IEEE, 2013.

99) Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. "Defining Cybersecurity." *Technology Innovation Management Review* 4.10 (2014).

100) Nissenbaum, Helen. "Where Computer Security Meets National Security1." *Ethics and Information Technology* 7.2 (2005).

101) Silomon, Jantje AM, and Richard E. Overill. "Cybersecurity's Can of Worms." *Journal of Information Warfare* 11.1 (2012): 1 at 14.

102) Mulligan & Schneider, "Doctrine for Cybersecurity," 70.

103) *See* Kenneth A. Bamberger, *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L. J. 377, 387 (2006); David Thaw, *The Efficacy of Cybersecurity Regulation* 30 Georgia State University Law Review 1 (2014).

In such contexts, risk remediation lends itself neither to specific top-down behavioral regulation, nor to *ad hoc* bottom-up measures. Rather, where risks are difficult to assess, require granular expertise and knowledge, and involve competing values, they are best addressed through processes that include multi-stakeholder input mechanisms.[104]

On the one hand, such mechanisms bring to bear both the range of expertise and views necessary to frame cyber security goals. They permit the enlistment of regulated parties who possess information about market demands, private incentives, and proprietary firm technologies and processes; technologists from a range of sectors who can bring important expertise to bear; and representatives of consumers, citizens, and advocacy groups.

On the other, these mechanisms facilitate coordination around cyber security efforts by sharpening shared objectives and means, and imbue the resulting policy measures with enhanced legitimacy. Reflecting the public-good nature of security, they permit a public, participatory dialogue around the cyber security goals.

c. Protecting public values requires recognizing that values are embedded in design, so cybersecurity *and other values* should be integrated at the design stage, not treated as a later "add on"

Building cyber security into technical systems implicates other values. Ensuring that particular values are given appropriate weight in technical systems requires that they be considered as a source of potential design requirements, and not an afterthought.

In the privacy context, regulators – and the broader privacy community – have fully embraced the understanding that values are best protected when they are considered from the inception product design. Efforts by regulators, advocates, academics, and corporations all seek to move privacy deeper into the design process. There is an evolving set of engineering, decisional, and review processes and tools to advance this goal. The goal is to ensure that technical systems, not just policy, are part of privacy solutions and privacy defenses.

More broadly, there is a growing recognition that a values-in-design approach is essential if a wide range of values – fairness, non-discrimination, competition, accessibility and privacy – is to survive the shift to the fully interconnected and computationally driven society. The real tensions between values, and the constituencies that champion them, are emerging most starkly in battles over encryption; values are as embedded in computer artifacts and computational systems as they are in other social fabric. Attending to them fully requires engineering and computational attention and resources, as well as inputs from relevant stakeholders.

Thus, to achieve the optimal mix of cybersecurity, privacy, and competition, all values must be in view when objectives are being determined and strategies chosen. This is particularly important if strategies are built into technical systems, as those can be far more costly and difficult to retrofit, and can unnecessarily skew the mix of competing values. The introduction of an OTA

104) Kenneth A. Bamberger and Deirdre K. Mulligan, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE, 189-192 (2015) (discussing the FTC's use of "nonenforcement regulatory tools, public visibility, and transparency" to enlist a range of public and private actors in governing privacy).

update channel creates an opportunity to intentionally or unintentionally upend the existing balance among the values of safety, competition, and privacy – while adding cyber security to the calculus. Cybersecurity surely need not destabilize the current alignment, but if the other values are not considered in the setting of cybersecurity policy or more specifically in the design choices of the OTA update channel they surely will be.

d. Learning from previous cases

Decision making around technology and risk in other contexts demonstrates the ways in which failure either to permit effective multi-stakeholder participation or to include value goal-setting before or during the technical design phase, thwarts the possible effectiveness and legitimacy of these governance processes. Indeed, the policy landscape is riddled with instructive failures – as well as some successes.

During the development of electronic voting systems, for example, privacy, security, and usability issues were unaccounted for during the design of the first generation of direct-to-record systems. This resulted in election scandals, limits on election officials' ability to conduct meaningful oversight, state investigations and commissions, law suits and equipment recalls. While technical experts repeatedly and consistently warned of the risks posed by the systems and offered alternative designs to mitigate them, the regulatory and procurement processes left little opportunity for their input to affect design choices until after systems were deployed. The result was costly to states and private actors alike, and placed a key democratic function at unnecessary risk. Similarly, in the roll-out of the smart grid privacy and security were only partly addressed during the development of technical standards, leaving states to fill policy gaps, and constrain technology after the fact. In both instances, the processes were focused on the relevant firms and failed to provide opportunities for timely engagement by relevant stakeholders.

Another context, the DMCA anti-circumvention provision and triennial rulemaking proceeding to establish exemptions, provides concrete evidence of the risks of enforcing one value through technical design without considering the ripple effect this will have on other values. The parade of anti-competitive and anti-consumer uses to which corporations have attempted to enlist anti-circumvention technology is legendary. The perceived failure to build competing values into anti-circumvention technology law has thus resulted in a situation in which it has fallen to: judges, ruling in specific court cases, to protect competing public values by revisiting design decisions; and private parties arguing for exemptions every three years before the Copyright Office – all after the fact. The tenuous connection between the goals of the DMCA – to protect against the copying or distribution of protected works – and its use to lock-out competition was viewed as so brash and attenuated by one judge that he wrote, the "proposed construction would allow any manufacturer of any product to add a single copyrighted sentence or software fragment to its product, wrap the copyrighted material in a trivial "encryption" scheme, and thereby gain the right to restrict consumers' rights to use its products in conjunction with competing products. In other words…. allow virtually any company to attempt to leverage its sales into after-market monopolies – a practice that both the antitrust laws, and the doctrine of copyright misuse, normally

prohibit."[105]

The build-out of the OTA update functionality, too, will destabilize values unless those other values are brought fully into the fold. This requires that other values be considered *a source of design requirements* for the OTA technology itself, not left for the lawyers or a separate agency to address. The OTA update functionality can be designed in ways that are more or less intrusive on individual privacy. The functionality can be designed in ways that leave more room open for competition – perhaps by maintaining a narrow rule about what can be pushed down it – and personal repair. Expanding the viable design space to include privacy protective and pro-competitive solutions requires that these values be a source of design inputs.

One instructive model from our prior work – the development of the "smart grid" – provides an affirmative model of the way that design can respond to multiple values if presented at an appropriate time, and considered as a legitimate source of input. In that context we found that privacy was potentially at risk due to the flow of energy usage information from the Home Area Network (HAN) to the utilities. The devices in a home area network – smart appliances, thermostats, computers etc. – may store and transmit sensitive and detailed information about the home and its occupants. We noted that local routing and storage of energy usage and home device information could keep sensitive information within the skin of the home, while supporting essential utility activities. Local storage and routing provides a structural constraint[106] limiting other uses of the information by the utility and limiting third-party access. For example, because the HAN devices are located in a customer's home law enforcement and other third parties will need to overcome greater hurdles to gain access.[107] A similar approach could inform the design of the OTA update channel. It might suggest different storage locations, different security protections for data, different protocols for transmitting data etc. Yet only if values like privacy are considered up front will this matter.

2. Assessing policymaking effort to date

a. Beginning steps to address safety

Policymakers have begun to recognize and take action regarding the critical health and safety risks posed by cybersecurity vulnerabilities in the automotive sector.

These responses have ranged in both source and extent. The Department of Homeland Security has provided research funding to support the development of a comprehensive industry standard for OTA updates, including technical design specifications, reference source code and best practice guidance for integration, testing, and deployment underscores the potential serious risks to the public posed by unpatched automobile software.[108] NHTSA and the FBI recently released a public

105) Id. at 1201.

106) *See* Harry Surden, *Structural Rights in Privacy*, SMU LAW REVIEW, vol. 60, p.1605 (2007).

107) If any of this information is transmitted to and stored by a utility or third party, however, law enforcement agents would probably be able to obtain it with a lower burden process, such as subpoena or court order.

108) Department of Homeland Security (DHS) Science and Technology Directorate (S&T), Press Release announcing 1.2 million dollar award to University of Michigan project, Secure Software Update Over-the-Air for Ground Vehicles Specification and Prototype, October 29, 2015 https://www.dhs.gov/science-and-technology/news/2015/10/29/st-awards-univ-michigan-12m-automotive-cyber-security.

service announcement alerting carmakers and owners to the potential cyber security threats posed by remote exploits.[109)]

More significantly, NHTSA (the National Highway Traffic Safety Administration), the agency (within the Department of Transportation) charged with writing and enforcing Federal Motor Vehicle Safety Standards, has effected shifts in its organizational structure, and pursued new research directions, in response to these emerging risks. In 2012, the agency established a new division, Electronic Systems Safety Research, to conduct research on the safety, security, and reliability of complex, interconnected, electronic vehicle systems. The research program is focused on three areas: electronics reliability (including functional safety); automotive cyber security; and, automated vehicles. Agency researchers evaluate, test, and monitor automotive cyber vulnerabilities, and conduct their own research on automated vehicles.

NHTSA also established an internal agency working group, the Electronics Council, responsible for cross agency coordination on vehicle electronics, including cybersecurity, and is consulting with other government agencies, vehicle manufacturers, suppliers, and the public. The agency's multilayered approach to cyber security has adopted a set of goals related to research, knowledge-building, and development of best cyber security practices, including: establishing comprehensive research plans for automotive cybersecurity and developing enabling tools for applied research; facilitating the implementation of effective, industry-based best practices and voluntary standards for cybersecurity and information-sharing fora; fostering the development of new system solutions for automotive cybersecurity;, researching the feasibility of developing minimum performance requirements for automotive cybersecurity; and gathering foundational research data and facts to inform potential future Federal policy and regulatory activities.

NHTSA recognizes explicitly that the vulnerability of all vehicle entry points, including Wi-Fi, infotainment, and the OBD-II port. And its approach focuses on solutions to harden the vehicle's electrical architecture against potential attacks *and* to ensure vehicle systems take appropriate safe steps after a successful attack — addressing the need for structures to allow for the management of cyber insecurity. In particular, its approach focuses on the development of four main technical areas: preventive measures and techniques implemented in hardware and software; real-time intrusion (hacking) detection measures; real-time response methods; and after the fact assessment with the goal of development of a fix and dissemination of the fix to all relevant stakeholders. It thus also emphasizes the importance of supporting the auto industry's information sharing and analysis center (Auto-ISAC) through voluntary sharing of cybersecurity threat and vulnerability information, information about countermeasures, and expansion of the Auto-ISAC to include members of the automotive supplier community and other participants in the connected vehicle ecosystem. These activities are essential given the successful hacks know today.

NHTSA's approach, then, focuses on technological remedies to cyber security and hacking threats, and recognizes the essential importance of engaging private automobile manufacturers in the project of technological design. NHTSA's actions,

109) Federal Bureau of Investigation, Motor Vehicles Increasingly Vulnerable to Remote Exploits, Alert Number I-031716-PSA, March 17, 2016.

moreover, have begun to influence private behavior – the agency's's ire was a powerful incentive for GM to find a way to hack around the lack of OTA upgrade functionality in Generation 8 OnStar to make good on its recall obligations.

b. Haphazard consideration of competing values

What NHTSA's approach specifically does not do, however, is integrate broadly into these design discussions consideration of many of the other public values identified as relevant to automobile cybersecurity decisionmaking.

To be sure, in a small way, NHTSA has shown a recognition of the privacy implications of cyber security risks and solutions, adopting a privacy rule to address their own access and use of vehicle Event Data Recorder (EDR) data.[110]

But the agency has been unwilling to address the full range of privacy and other concerns entwined with increased computation and connectivity, claiming, for example, that it has limited statutory authority to address the broader privacy concerns and consumer interests raised by policy makers, commentators, and participants in rulemaking proceedings. Tellingly, the professional association that generated the EDR standard chastised NHTSA for its failure to "consider the relevant societal concerns expressed by the general public,"[111] That group cautioned that, to "fully achieve the goals of the regulation while fully protecting the privacy rights of owners and drivers."[112] Explaining the importance of public acceptance, the association argued "that widespread use of EDRs without adequate consumer protection presents serious privacy issues and creates a certain consumer backlash … (while) adequate consumer protection assures consumer acceptance."

Thus, while NHTSA has begun to take the lead in promoting issues around cybersecurity design, it has explicitly excluded consideration of the multiple public values implicated by that design. Those discussions, instead, have fallen to others willing to step into the gap. Accordingly, although these discussions and the measures that have produced underscore the multiple values implicated by automobile technology, they are happening in a piecemeal fashion, often themselves far removed from the core discussion about cybersecurity design.

The State of California was one of the first to address the dynamic cycle of technological innovation, increased data collection, privacy concern, and policy response. In 2003, the legislature enacted the first law requiring automobile manufacturers that install "event data recorders" (EDR) in vehicles to disclose that fact in the owner's manual; limited the retrieval and use of EDR data to vehicle service and repair, and to public safety; and set limits on data disclosed for safety purposes including the removal of identifiers and prohibitions on disclosure for other purposes.[113] As surveillance technology became a standard feature in automobiles, moreover, California stepped in to limit what it considered abusive uses of data in the rental car market. In 2004, then-California

110) Federal Motor Vehicle Safety Standards; Event Data Recorders, 77 Fed. Reg. 74144, 74150-51 (proposed Dec. 13, 2012) (codified at 49 C.F.R. pt. 563).

111) Institute of Electrical and Electronics Engineers Vehicular Technology Society (IEEE/VTS), comments to the National Highway Traffic Safety Administration (NHTSA) regarding Automotive Electronic Control Systems Safety and Security in light vehicles.

112) Id.

113) Automobile "Black Boxes" – California Vehicle Code section 9951.

Attorney General Bill Lockyear brought an action under the Business and Professions Code[114] as well as the California Constitution[115] against a rental car franchise for failing to adequately notify renters of the presence of a GPS device in their rental vehicles.[116] The settlement included restitution, civil penalties, and most importantly an injunction prohibiting the use of information about rental car drivers for similar purposes in the future. The injunction provided the blueprint for a sweeping 2005 California law that prohibits the use of information gathered through onboard surveillance technology in rental vehicles to impose fines or surcharges on consumers. While information can be used for a limited set of purposes without consent, it generally requires rental companies to obtain consent prior to using or disclosing information about vehicle use.[117] Shortly after its passage, the state used it to recover $90,000 in travel-restriction surcharges for customers who were wrongly tracked and billed through onboard GPS devices.[118][119]

In the intellectual property and competition context, two exemptions granted in response to petitions in the recent DMCA rulemaking further recognized the need to accommodate multiple values in the design and embedding of code in vehicles. They clarify that vehicle owners may circumvent various technical protection measures used to limit access to vehicle software for the purpose of repairing and modifying it consistent with other laws, and researchers may similarly circumvent to engage in good faith research consistent with other laws.[120] One exception is aimed at maintaining competition and consumer autonomy in the marketplace, the other at ongoing improvements in security.

And Congress has begun to recognize the implications of automobile cyber security for multiple values. In the wake of the Markey Report discussed above, the auto industry has begun to address privacy issues. For example, in November 2014 two large trade associations released a set of privacy principles[121] to guide the collection and use of privacy sensitive information generated by onboard technology. The guidelines recognize the heightened privacy interests in certain kinds of information that can be collected through onboard systems, and requires signatories to obtain affirmative consent prior to using geolocation, biometric, or driver behavior information for marketing or sharing it with unaffiliated third parties for their own use. Subsequently, Senators Markey and Richard E. Blumenthal (D-CT) introduced legislation directing the Federal Trade Commission – the lead federal consumer protection regulator – in consultation with NHTSA, to develop privacy protections for "driving data" (any electronic information collected about a vehicle's status, or that of the owner, lessee, driver, or passenger of

114) section 17500.

115) Article I, Section 1 of the California Constitution secures to all Californians the right to privacy.

116) http://ag.ca.gov/newsalerts/cms04/04-129_complaint.pdf

117) Electronic Surveillance in Rental Cars - California Civil Code section 1936.

118) https://oag.ca.gov/system/files/attachments/press_releases/n1388_judgment.pdf?.

119) Id. (The AG leveled an additional $200,000 civil penalty against the company.).

120) See exemption 6 on automotive repair and modification, and exemption 7 for good-faith security research on a broad range of devices including automotives, Library of Congress, Copyright Office 37 CFR Part 201 [Docket No. 2014-07] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Final Rule, 65944 Federal Register / Vol. 80, No. 208 / Wednesday, October 28, 2015.

121) ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC., and ASSOCIATION OF GLOBAL AUTOMAKERS, CONSUMER PRIVACY PROTECTION PRINCIPLES: PRIVACY PRINCIPLES FOR VEHICLE TECHNOLOGIES AND SERVICES, November 12, 2014.

the vehicle).[122] The bill requires, among other things, that the privacy standards: require car-makers to inform consumers about the collection, transmission, retention, and use of driving data and them to opt out of data collection and retention without losing key navigation or other features (when technically feasible, and not for EDRs or other safety or regulatory systems); and, prohibits the use of personal driving information for advertising or marketing purposes unless a consumer has opted in to such use.

Ⅴ. A Path Forward

Existing fora for addressing cybersecurity issues in the automotive context are unlikely to provide the frame for a necessary wide-ranging discussion about the public values that must be considered in setting goals, and designing responses to emergent risks. While NHTSA has begun to articulate design goals, and seeks to support voluntary private consultation processes, it has explicitly eschewed – as the Department of Transportation has more generally, as in the setting of policy related to drone technology[123] – a role of convenor around the breadth of public values that cybersecurity design implicates. Discussions around those other values, in turn, have occurred in piecemeal fashion, removed from core discourse over cybersecurity policy-setting and design.

This fragmented approach offers little hope for crafting successful national policy in the face of increasing safety and security threats. On the one hand, it threatens the capacity to shape effective responses; indeed, our research demonstrates the ways in which regulators' failure to address multiple values at the design stage of technological policymaking can lead to serious failures in implementation, including unanticipated national security vulnerabilities and costly retrofits.[124] On the other, it undermines the legitimacy needed when setting public policy in complex technical areas by obscuring processes for both drawing on stakeholder expertise, and reaching consensus when values are contested.

The risk of such a fragmented approach is evident in the existing tussles around drones. As unmanned drones have become more popular and widely used, concerns about privacy and safety have escalated. Policy makers at the state and federal level have responded to these perceived risks through the adoption of new laws and regulations. Individuals have engaged in a range of self-help strategies as well. In February 2015, the Federal Aviation Administration ("FAA") announced proposed rules regarding the operation of small unmanned aircraft systems ("sUAS"). These are defined as a small unmanned aerial vehicle ("sUAV") under 55 pounds, and the equipment necessary for the safe and efficient operation of that aircraft. The proposal includes rules about the operation of drones, such as: operating only in daylight conditions and within a visual line-of-sight, and flying under 500 feet and under 100 miles per hour. It also includes rules about operator certification and drone registration. The rules went through a Notice of Proposed Rulemaking ("NPRM") process, soliciting public comments. While several commentators raised privacy concerns, privacy was considered out of

122) The Security and Privacy in Your Car (SPY Car) Act of 2015.

123) CITE.

124) Bamberger & Mulligan, PIAs.

scope.

In the meantime State legislatures have passed a range of laws regulating drones. Many of the laws address privacy concerns. Twenty-seven states have passed drone-related legislation since 2013, and 45 states have considered over 150 drone-related bills in 2015 (Karol, 2015; NCSL, 2016). Each state and each bill has taken a slightly different approach. Some define drones flying over private property under certain heights (such as 350 feet in California) as a form of trespass. Other laws and bills prohibit image and video recording by drones, tying drone surveillance to "peeping tom" and voyeurism laws, while others prohibit the use of drones for certain purposes (often hunting), or in certain places and events.

In part due to this fractured policy development, President Obama issued a Presidential Memorandum to address privacy, civil rights, and civil liberties in regards to domestic use of unmanned aircraft systems, or drones.[125] The Memo called for the Department of Commerce, through the National Telecommunications and Information Administration ("NTIA"), to create a multi-stakeholder engagement process to develop a framework for privacy, accountability, and transparency for commercial and private unmanned aircraft systems.[126] In March 2015, the NTIA began soliciting comments regarding privacy, accountability, and transparency issues. The multi-stakeholder group began meeting in August 2015 to begin drafting a framework. While it is important that privacy issues are being addressed, relegating them to an ancillary process limits the ability of privacy concerns to influence the design of drone technology.

Drones show us what happens if public processes fail to account for relevant social issues – rejection, loss of trust, public upheaval and self-help, and a patchwork of inconsistent state regulations. As we recommended in the smartgrid context, "(r)esolving privacy issues implicates grid cybersecurity, and innovation and competition in the devices and services that operate within the Smart Grid. Regulators at all levels therefore should not consider them in isolation but rather… take the interdependencies among these issues fully into account."

There is successful experience and competency in the federal government that suggest possible paths forward. In the privacy and consumer protection contexts, the Federal Trade Commission has successfully used its administrative capacity to both bring together and empower a wide range of stakeholders, and draw on dispersed technical and private expertise.[127] In particular, the FTC has advanced privacy by design through enforcement actions, guidance documents, workshops, and staff reports. Acquiring a growing number of technologists on staff, and creating connections with the technical research community,

125) White House. (2015, Feb. 15). *Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems*. Retrieved from https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

126) The Presidential Memo also created several guidelines for federal government use of unmanned aircraft systems (UAS), including limits on collection, use, retention, and sharing for data collected by UAS, calling on federal agencies to create non-discrimination policies for the data collected, and calling on federal agencies to create accountability and transparency policies and procedures to regarding what data are collected by federal UAS.

127) Kenneth A. Bamberger and Deirdre K. Mulligan, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE, 189-192 (2015) (discussing the FTC's use of "nonenforcement regulatory tools, public visibility, and transparency" in governing privacy).

has moreover allowed the FTC itself to grow its expertise and to participate meaningfully in conversations about design choices and privacy. The National Telecommunications and Information Administration (NTIA), part of the Department of Commerce, has further undertaken a series of multi-stakeholder processes to develop privacy codes of conduct in different domains. Indeed, one of these Multi-stakeholder processes attempted to fill the gap, left by the failure of the Federal Aviation Administration – like NHTSA, also an agency within the Department of Transportation – to address privacy issues with respect to drones.[128] Moreover, the National Institute of Standards and Technology (NIST), a research-only agency also within the Department of Commerce, has done significant work bringing together privacy engineering expertise to enhance executive branch technological competence around privacy's inclusion in technological discussions.[129]

The stakeholder expertise approach, and broad vantage points, of the FTC and Department of Commerce models, should be brought to bear to questions of automobile cybersecurity. This is not to say that consideration of privacy and other values should be administratively partitioned off from core design discussions; this would only exacerbate current regulatory failures. Rather these agencies should work with the Department of Transportation – with its authority to consider values implicated by transportation technology clarified, if needed, by Congress – to bring together the required expertise, relevant stakeholders, and policy focus necessary to address the rising cyber security threat.

Ⅵ. Conclusion

The automotive industry provides an excellent opportunity to establish processes for ensuring that cybersecurity is understood as a public good, that its objectives and means are publicly determined, and that their implementation is informed and coupled with technical as well as policy protections for other core public values. This requires inclusive multi-stakeholder processes, robust expertise to identify risks and mitigation strategies, and prioritizing and reconciling values that are expressed through design.

128) National Telecommunications and Information Administration (NTIA), Docket 150224183-5183-01 Privacy, Transparency and Accountability in Regards to the Commercial and Private use of Unmanned Aircraft Systems (UAS). Both NHTSA and the FAA are part of the Department of Transportation. The UAS multi-stakeholder process resulted from a February 15, 2015, Presidential Memorandum "Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems," establishing a "multi-stakeholder engagement process at NTIA to develop and communicate best practices for privacy, accountability, and transparency issues regarding commercial and private UAS use in the NAS.

129) http://www.nist.gov/itl/csd/privacy-engineering-workshop.cfm.

〈References〉

Alam, Mahbubul, Movimento Group, "Preparing for the convergence of IoT and automotive," Embedded Computing, http://embedded-computing.com/articles/preparing-for-the-convergence-of-iot-and-automotive/#

Alderson, David and Kevin Soo Hoo, "The Role of Economic Incentives in Securing Cyberspace," Stanford University Center for International Security and Cooperation, November 2004.

Alliance of Automobile Manufacturers, Inc., and Association of Global Automakers, Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services, November 12, 2014.

Auto Alliance and Global Automakers, Key Research Findings on Consumers and Auto Safety Recalls, October 7, 2015.

Automobile "Black Boxes" - California Vehicle Code section 9951 section 17500

Bamberger, Kenneth A., *Regulation as Delegation: Private Firms, Decisionmaking, and Accountability in the Administrative State*, 56 DUKE L. J. 377 (2006).

Bamberger, Kenneth A., *Global Terror, Private Infrastructure, and Domestic Governance* 211, in THE IMPACT OF GLOBALIZATION ON THE UNITED STATES: LAW AND GOVERNANCE, B. Crawford, ed., Vol. 2, 2008.

Bamberger, Kenneth A., and Deirdre K. Mulligan. "Privacy decisionmaking in administrative agencies." *University of Chicago Law Review* 75.1 (2008): 75.

Bamberger, Kenneth A., and Deirdre K. Mulligan, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE, MIT (2015).

Bamberger, Kenneth A., Technologies of Compliance: Risk and Regulation in a Digital Age, 88 Tex. L. Rev. 669 (2010).

Band, Jonathan, "The End of the Cell Phone Unlocking Saga?" August 7, 2014. http://ssrn.com/abstract=2483291.

Bellissimo, A., Burgess, J. and Fu, K. Secure software updates: Disappointments and new challenges. In *Proceedings of USENIX Hot Topics in Security*, (July 2006).

Bento, Luís Conde, Ricardo Parafita, and Urbano Nunes. "Intelligent traffic management at intersections supported by v2v and v2i communications." *Intelligent Transportation Systems (ITSC), 2012 15th International IEEE Conference on*. IEEE, 2012.

Blanchard, Keith, Why the Internet of Things will be worse than a zombie apocalypse, The Week, August 17, 2015 http://theweek.com/articles/571728/why-internet-things-worse-than-zombie-apocalypse

Brisbourne, Alex, KORE,Tesla's Over-the-Air Fix: Best Example Yet of the Internet of Things?, Wired, February, 2014, http://www.wired.com/insights/2014/02/teslasteslas-air-fix-best-example-yet-internet-things/.

Buzan, Barry, Ole Wæver, and Jaap De Wilde. *Security: a new framework for analysis*. Lynne Rienner Publishers, 1998.

California Constitution Article I, Section 1.

California v. Acceleron Corp. et.al., November 9, 2004, http://ag.ca.gov/newsalerts/cms04/04-129_complaint.pdf.

Center for Democracy and Technology Before the Federal Communications Commission In the Matter of Petition of the Cellular Telecommunications Industry Association for a Rulemaking to Establish Fair Location Information Practices WT Docket No. 01-72 DA-01-696. The FCC never acted upon the petition. WT Docket No. 01-72 DA-01-696 Petition of the Cellular Telecommunications and Internet Association.

Chamberlain Group v. Skylink Technologies, 381 F.3d 1178 (Fed. Cir. 2004).

Chandler, Jennifer A., "Contracting Insecurity: Software License Terms that Undermine

Cybersecurity," in Harboring Data: Information Security, Law and the Corporation, Stanford University Press (2009) Andrea M. Matwyshyn, editor.

CHARETTE, Robert N. "This car runs on code. 2009." *IEEE Spectrum* (2013); http://blogs.wsj.com/digits/2013/11/11/chart-a-car-has-more-lines-of-code-than-vista/.

Checkoway, D. McCoy, D. Anderson, B. Kantor, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. Comprehensive Experimental Analyses of Automotive Attack Surfaces, In Proceedings of the USENIX Security Symposium, San Francisco, CA, Aug. 2011.

Cirani, Simone, et al. "IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios." *Sensors Journal, IEEE* 15.2 (2015): 1224-1234, 1225.

Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. "Defining Cybersecurity." *Technology Innovation Management Review* 4.10 (2014).

Crawford, Susan, The Tesla Dividend: Better Internet Access, March 25, 2016 https://backchannel.com/the-tesla-dividend-better-internet-access-db175e1835f6#.lgibeu4i8.

Denning, Tamara, Tadayoshi Kohno, and Henry M. Levy. "Computer security and the modern home." *Communications of the ACM* 56.1 (2013): 94-103.

Derene, Glenn, "Tesla Model S Update Improves Safety of Its Summon Feature: In response to Consumer Reports' concerns, Tesla updates software on its self-parking function," Consumer Reports March 09, 2016 http://www.consumerreports.org/hybrids-evs/video-tesla-model-s-update-improves-safety-of-its-summon-feature/.

Department of Homeland Security (DHS) Science and Technology Directorate (S&T), Press Release announcing 1.2 million dollar award to University of Michigan project, Secure Software Update Over-the-Air for Ground Vehicles Specification and Prototype, October 29, 2015 https://www.dhs.gov/science-and-technology/news/2015/10/29/st-awards-univ-michigan-12m-automotive-cyber-security.

Doty, Nick, Deirdre K. Mulligan, and Erik Wilde. "Privacy issues of the W3C Geolocation API." *arXiv preprint arXiv:1003.1775* (2010).

Dreyfuss, Emily, "Big Android Makers Will Now Push Monthly Security Updates" Wired August 6, 2015, http://www.wired.com/2015/08/google-samsung-lg-roll-regular-android-security-updates/.

Durumeric, Zakir, et al. "The matter of Heartbleed." *Proceedings of the 2014 Conference on Internet Measurement Conference*. ACM, 2014.

Electronic Frontier Foundation, Unintended Consequences: 16 Years Under the DMCA, https://www.eff.org/files/2014/09/16/unintendedconsequences2014.pdf.

Electronic Frontier Foundation In the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. 1201 Docket No. 2014-07 U.S. Copyright Office, Library of Congress, February 6, 2015

Electronic Surveillance in Rental Cars - California Civil Code section 1936 https://oag.ca.gov/system/files/attachments/press_releases/n1388_judgment.pdf?.

European Commission, Article 29 Data Protection Working Party Opinion 8/2014 on the Recent Developments on the Internet of Things," 2014.

EUROPEAN COMMISSION, "Commission adopts revised competition rules for motor vehicle distribution and repair," (May 2010), http://europa.eu/rapid/press-release_IP-10-619_en.htm.

Exemption to Prohibition on Circumvention of Copyright Protection Systems for Wireless Telephone Handsets, 79 FR 50552 (Aug. 25, 2014) (codified at 37 CFR 201.40(b)(3), (c)).

Fagan, Michael, Mohammad Maifi Hasan Khan, and Ross Buck. "A study of users' experiences and beliefs about software update messages." *Computers in Human Behavior* 51 (2015): 504-519.

Federal Bureau of Investigation, Motor Vehicles Increasingly Vulnerable to Remote Exploits, Alert Number I-031716-PSA, March 17, 2016.

Federal Motor Vehicle Safety Standards; Event Data Recorders, 77 Fed. Reg. 74144, 74150-51 (proposed Dec. 13, 2012) (codified at 49 C.F.R. pt. 563).

Federal Trade Commission Staff Report, Internet of Things: Privacy & Security in a Connected World, 2015 ("FTC IoT Report"). Available online: http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

Fleishman, Glenn, An Internet of Treacherous Things, MIT Technology Review, January 13, 2015 http://www.technologyreview.com/news/534196/an-internet-of-treacherous-things/.

Foster, I., Prudhomme, A., Koscher, K., & Savage, S. (2015). Fast and vulnerable: a story of telematic failures. In *9th USENIX Workshop on Offensive Technologies (WOOT 15)*.

Giles, Keir, and William Hagestad. "Divided by a common language: Cyber definitions in Chinese, Russian and English." *Cyber Conflict (CyCon), 2013 5th International Conference on*. IEEE, 2013.

Greenberg, Andy, Hackers Remotely Kill a Jeep on the Highway－With Me in It, Wired (July 21, 2015), available at http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

Greenberg, Andy, GM Took 5 Years to Fix a Full-Takeover Hack in Millions of OnStar Cars, September 10, 2015 http://www.wired.com/2015/09/gm-took-5-years-fix-full-takeover-hack-millions-onstar-cars/.

Gustafsson, Fredrik. "Automotive safety systems." *Signal Processing Magazine, IEEE* 26.4 (2009): 32-47.

Hansen, Lene, and Helen Nissenbaum. "Digital disaster, cyber security, and the Copenhagen School." *International Studies Quarterly* 53.4 (2009): 1155-1175.

Hawker, Norman W., Under Threat: Competition in the Automotive Service Aftermarket (November 13, 2008). Available at SSRN: http://ssrn.com/abstract=1337103 or http://dx.doi.org/10.2139/ssrn.1337103.

Howard, Bill, GM fixes, refixes OnStar RemoteLink hack, ExtremeTech (August 3, 2015), at http://www.extremetech.com/extreme/211483-gm-fixes-refixes-onstar-remotelink-hack.

Institute of Electrical and Electronics Engineers

Vehicular Technology Society (IEEE/VTS), comments to the National Highway Traffic Safety Administration (NHTSA) regarding Automotive Electronic Control Systems Safety and Security in light vehicles.

Intellectual Property & Technology Law Clinic, University of Southern California In the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. 1201 Docket No. 2014-07 U.S. Copyright Office, Library of Congress February 6, 2015.

Internet Engineering Taskforce, RFC 7452 Architectural Considerations in Smart Object Networking March 2015.

In the Matter of Petition of the Cellular Telecommunications Industry Association for a Rulemaking to Establish Fair Location Information Practices, WT Docket No. 01-72 DA-01-696.

Jenson, Scott, "The zombie apocalypse of smart devices is coming" Wired, December 6, 2012 http://www.wired.co.uk/magazine/archive/2012/12/ideas-bank/the-zombie-apocalypse-of-smart-devices-is-coming.

Johnson v. Microsoft Corporation, No. C06-0900RAJ (W.D. Wash. June 23, 2009).

Keizer, Gregg, Microsoft's WGA Sued As 'Spyware', Information Week, June 30, 2006 http://www.informationweek.com/microsofts-wga-sued-as-spyware-/d/d-id/1044797?.

Keizer, Gregg. (2008) Microsoft: We Took Out Storm Botnet. eWeek, April 22. http://www.computerworld.com/s/article/9079653/Microsoft_We_took_out_Storm_botnet.

Korosec, Kirsten, "Obama administration to fast-track "talking" car mandate," May 14, 2015, http://fortune.com/2015/05/14/v2v-communication-cars/.

Koscher, A. Czeskis, F. Roesner, S. Patel,T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental security analysis of a modern automobile, In Proceedings of the IEEE Symposium and Security and Privacy, Oakland, CA, May 2010.

Library of Congress, Copyright Office 37 CFR Part 201 [Docket No. 2014-07] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Final Rule, 65944 Federal Register / Vol. 80, No. 208 / Wednesday, October 28, 2015.

Lexmark v. Static Control Components, 387 F.3d 522 (6th Cir. 2004).

Library of Congress, Copyright Office 37 CFR Part 201 [Docket No. 2014-07] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Final Rule, 65944 Federal Register / Vol. 80, No. 208 / Wednesday, October 28, 2015.

McCarthy, C., Harnett, K., & Carter, A., *A summary of cybersecurity best practices.* (Report No. DOT HS 812 075). Washington, DC: National Highway Traffic Safety Administration, October, 2014.

Merritt, Rick, "IBM tells story behind Chevy Volt design," EE Times, May 4, 2011, www.eetimes.com/document.asp?doc_id=1259444.

Morris, David Z., How Will Talking Cars Change Our Roads?, Fortune (January 8, 2016), available at http://fortune.com/2016/01/08/

connected-vehicles-impact-cities/.

Mulligan, Deirdre K. and Fred B. Schneider. "Doctrine for Cybersecurity." *Daedalus* 140.4 (2011): 70-92.

Mulligan, Deirdre K. , & Kenneth A. Bamberger, *The Coming Design Wars* (forthcoming)

Mulligan, Deirdre K., & Kenneth A. Bamberger, *Apple v. FBI: Just One Battle in the 'Design Wars'* THE RECORDER (Monday, March 21, 2016) (available at http://www.law.com/sites/lawcomcontrib/2016/03/18/apple-v-fbi-just-one-battle-in-the-design-wars/?slreturn=20160303212714).

Mulligan, Deirdre K. and Aaron J. Burstein, "Implementing Copyright Limitations in Rights Expression Languages", in Digital Rights Management: ACM CCS-9 Workshop, DRM 2002, Washington, DC, November 18, 2002, Revised Papers (Lecture Notes In Computer Science), Joan Feigenbaum, ed., Volume 2696, Springer-Verlag Publishing, pp.137-154 (2003).

Mulligan, Deirdre K., John Han, and Aaron J. Burstein. "How DRM-based content delivery systems disrupt expectations of personal use." *Proceedings of the 3rd ACM workshop on Digital rights management*. ACM, 2003.

Mulligan, Deirdre K., Longhao Wang, and Aaron J. Burstein. "Privacy in the smart grid: an information flow analysis." *Available at SSRN 1815605* (2011).

Mulligan, Deirdre K., and Aaron K. Perzanowski. "The magnificence of the disaster: Reconstructing the Sony BMG rootkit incident." *Berkeley Technology Law Journal* 22.3 (2007): 1157-1232.

National Science Foundation, "Interdisciplinary Pathways towards a More Secure Internet", A report on the NSF-sponsored Cybersecurity Ideas Lab held in Arlington, Virginia, February 2014, http://www.nsf.gov/cise/news/CybersecurityIdeasLab_July2014.pdf.

National Telecommunications and Information Administration (NTIA), Docket 150224183-5183-01 Privacy, Transparency and Accountability in Regards to the Commercial and Private use of Unmanned Aircraft Systems (UAS).

National Traffic and Motor Vehicle Safety Act, 49 U.S.C. Chapter 301.

New America. Global Cyber Definitions Database. www.newamerica.org/cyber-global/cyber-definitions/;.

Nissenbaum, Helen. "Where Computer Security Meets National Security1." *Ethics and Information Technology* 7.2 (2005): 61-73.

NIST Lightweight Cryptography project description, http://www.nist.gov/itl/csd/ct/lwc-project.cfm.

O'Brien, Danny, "ATI Downgrades Its Tuners and its Customers," Electronic Frontier Foundation, June 5, 2007, https://www.eff.org/deeplinks/2007/06/ati-downgrades-its-tuners-and-its-customers.

Office of Senator Edward J. Markey, Tracking and Hacking: Security & Privacy Gaps put American Drivers at Risk, February 2015. (Markey Report).

Online Trust Alliance, IoT Trust Framework－Security, Privacy & Sustainability Release 11-6 https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework_11-6c.pdf.

Red Bend Software, "Updating Car ECUs

Over-The-Air (FOTA)", 2011. http://www.redbend.com/data/upl/whitepapers/red_bend_update_car_ecu.pdf.

Saha, Kumar, "More OTA updates coming to a car near you," Toronto Star, February 5, 2016 https://beta.thestar.com/autos/2016/02/05/more-ota-software-updates-coming-to-a-car-near-you.html.

Scheibel, Michael, Christian Stüble, and Marko Wolf. "Design and implementation of an architecture for vehicular software protection." *Embedded Security in Cars Workshop (ESCAR'06)*. 2006.

Silomon, Jantje AM, and Richard E. Overill. "Cybersecurity's Can of Worms." *Journal of Information Warfare* 11.1 (2012): 1 at 14.

Slater, Derek, "Creative Labs "Upgrade" Removes FM Radio Recording" Electronic Frontier Foundation, October 17, 2006, https://www.eff.org/deeplinks/2006/10/creative-labs-upgrade-removes-fm-radio-recording.

Stone, Brad, "Amazon Erases Orwell Books From Kindle," New York Times, July 17, 2009, http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html?_r=0.

Storage Technology v. Custom Hardware Engineering, 421 F.3d 1307 (Fed. Cir. 2005).

Subrahmanyam, P.A. et al., "Network Security Architecture for Demand Response/Sensor Networks," Tech. Report, Calif. Energy Commission, Public Interest Research Group, Jan. 2008.

Surden, Harry, *Structural Rights in Privacy*, SMU Law Review, vol. 60, p.1605 (2007).

Teslamotors, "Your Autopilot has arrived" October 14, 2015. https://www.teslamotors.com/blog/your-autopilot-has-arrived.

Teslarati, Rob M., How Does a Tesla Over-the-Air Software Update Work?, June 21, 2014 http://www.teslarati.com/tesla-air-software-update-work/#4sQvOFh8midyulct.99.

Thaw, David, *The Efficacy of Cybersecurity Regulation* 30 Georgia State University Law Review 1 (2014).

The Security and Privacy in Your Car (SPY Car) Act of 2015.

Thomson, J. R. *High Integrity Systems and Safety Management in Hazardous Industries*. Butterworth-Heinemann, 2015.

Unlocking Consumer Choice and Wireless Competition Act Public Law 113-144, 128 Stat. 1751 (2014).

Vaniea, Kami E., Emilee Rader, and Rick Wash. "Betrayed by updates: how negative experiences affect future security." *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM, 2014.

von Eitzen, Christopher, "Google Uses Remote Delete to Remove Android Apps from Smartphones." The H Security, June 25, 2010. Available at http://www.h-online.com/security/news/item/Google-uses-remote-delete-to-remove-Android-apps-from-smartphones-Update-1029188.html.

von Lohmann, Fred, "Convert to MP3 BEFORE Upgrading to iTunes 7.2!" Electronic Frontier Foundation, May 31, 2007 https://www.eff.org/deeplinks/2007/05/convert-mp3-upgrading-itunes-7-2.

Wash, Rick, et al. "Out of the Loop: How Automated Software Updates Cause Unintended Security Consequences." *Symposium on Usable Privacy and Security (SOUPS)*. 2014(discussing why humans must remain

"in-the-loop").

White House. (2015, Feb. 15). *Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems.* Retrieved from https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

White, Joseph, "General Motors developing wireless download of new features Detroit," June 24, 2015, http://www.reuters.com/article/2015/06/24/us-autos-gm-technology-idUSKBN0P42UY20150624#XOX87kMK8YXvkl2y.97.

Williams, Kristy L., Updates are Not Available: FDA Regulations Deter Manufacturers from Quickly and Effectively Responding to Software Problems Rendering Medical Devices Vulnerable to Malware and Cybersecurity Threats (August 6, 2013).

WIND, Security In The Internet Of Things: Lessons from the Past for the Connected Future, available at http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf.

Wright, Robert, and Andy Sharman, Cyber hack triggers mass Fiat Chrysler car recall, Financial Times (July 24, 2015), available at http://www.ft.com/cms/s/0/2bafe3e0-321f-11e5-8873-775ba7c2ea3d.html.