

Recommended by Christopher Koopman, Caleb Watney, and 1 other



Adam Thierer

research fellow at @Mercatus Center [<http://t.co/UwBwKd05Yh>] at George Mason Univ where I cover digita...  
Jun 26 · 8 min read



## 10 Takeaways about Connected Car Privacy & Security

This Wednesday, June 28th, the Federal Trade Commission (FTC) and the National Highway Traffic Safety Administration (NHTSA) are hosting a joint workshop “to examine the consumer privacy and security issues posed by automated and connected motor vehicles.”<sup>[1]</sup>  
The agenda for the event includes remarks from officials from both

agencies as well as keynote speeches and panel discussions from various experts and stakeholders in the field.[2]

I have been invited to participate in the third panel of the workshop, which is focused on the privacy issues surrounding connected vehicle technology. The panels are meant to be free-flowing discussions, so no one will be delivering prepared remarks. But in preparation for the general discussion, I have made an attempt to boil down my own research on these matters into 10 key takeaways about connected car privacy and security issues.

1. **Avoid “silver-bullet” thinking:** The most important thing to remember in discussions about connected car security and privacy is that no silver-bullet solutions exist to these concerns. Policymakers should avoid top-down technological mandates and instead focus on encouraging collaborative, multifaceted, multi-stakeholder initiatives and approaches to enhance connected car security and privacy.[3]

2. **Security and privacy are relative terms with evolving benchmarks:** While we may be able to achieve some rough consensus about baseline security and privacy protections, the reality is that these issues are in a constant state of flux and that many other values are also in play. Compared with static systems, security within dynamic, interconnected systems is far more complicated because adversaries and the nature of threats are constantly evolving.[4]

3. **Security and privacy objectives can sometimes come into conflict:** Information-sharing and ongoing feedback between various parties will be a crucial way to assess and correct security vulnerabilities. But that may open the door to the sharing of more information about drivers/owners. In turn, government-mandated security requirements would be problematic because they could create backdoors and give an advantage to adversaries (including hostile governments).[5]

4. **Consider the full range of values and trade-offs in play:** Those trade-offs include not only cost and convenience factors, but the potential for more sophisticated and tailored features in our vehicles. While privacy and security are important values, if they come at the expense of improved products and services, it could undermine consumer welfare in various ways (i.e., diminished competition, fewer

choices, higher prices, etc). It would be even more problematic if regulation undermined the potential for new technologies to help reduce vehicle accidents and fatalities.<sup>[6]</sup> For example, a 2015 Boston Consulting Group study found that more widespread adoption of advanced driver assist system technologies could help avoid approximately 28 percent of all motor vehicle crashes in the US and prevent about 9,900 fatalities per year, resulting in savings of more than \$250 billion in societal costs each year.<sup>[7]</sup> Policymakers should conduct a thorough benefit-cost analysis of any proposed regulations to determine how these various issues are valued by the public or could be diminished by inefficient interventions.<sup>[8]</sup>

**5. Think more broadly about potential “solutions”:** Solutions to privacy and security matters must be layered, multifaceted, collaborative, flexible, and responsive to changing circumstances. In this sense, the search for “solutions” has no final destination; we will have to constantly devise new methods to deal with new threats.

**6. Preemptive, top-down privacy and security mandates would be unwise:** Regulation of this dynamic sector is likely to back-fire. Regulation won’t likely be able to keep up with either new threats or public demands for new and better features. Regulation could also curtail new forms of innovation and competition.<sup>[9]</sup> Blanket, one-size-fits-all policy prescriptions tend not to work well in fast-moving technology sectors.

**7. “Soft law” governance should prevail over “hard law” approaches:** What this means in terms of the role of policy is that all roads lead back to “soft law” approaches and ongoing multistakeholder collaboration in particular. Various informal governance mechanisms are evolving that are supplanting traditional regulatory approaches to new technological innovations.

**8. Industry-established best practices are already in place and set a very high bar:** The automotive sector has already established an impressive set of privacy and security best practices. Created in August 2015, the Auto Information Sharing and Analysis Center (ISAC), whose membership covers 99% of all light-duty vehicles, allows real-time information-sharing and cross-industry coordination in response to new vulnerabilities.<sup>[10]</sup> The industry also developed a comprehensive set of “Privacy Principles for Vehicle Technologies and

Services,” formulated by the Association of Global Automakers and the Auto Alliance in November 2014.<sup>[11]</sup> Private standards and certification bodies, such as the Society of Automotive Engineers (SAE) and the Institute of Electrical and Electronics Engineers (IEEE), also play an important role. The IEEE, for example, “has developed information security standards that address specific areas such as encryption, storage, and hard copy devices.”<sup>[12]</sup>

9. **“Regulation” can mean more than preemptive administrative mandates.** Related to the previous point, third party validators can also be effective “regulators” and serve as a check on compliance with industry best practices and standards. Litigation and the threat of industry liability will also help regulate of corporate behavior when things go wrong.<sup>[13]</sup> The automotive sector already attracts significant litigation activity when compared to other sectors, and that trend is certain to continue. <sup>[14]</sup> Meanwhile, the Federal Trade Commission already possesses broad “unfair and deceptive practices” authority to investigate problematic corporate behavior and to hold companies to the promises they make to consumers.<sup>[15]</sup> And the National Highway Traffic Safety Administration has sweeping recall authority to pull dangerous products off the market once problems are discovered.<sup>[16]</sup> When combined with the fact that “manufacturers have powerful reputational incentives at stake here, which will encourage them to continuously improve the security of their systems,” the potential for effective self-regulation is high.<sup>[17]</sup> No automaker wants the bad publicity that accompanies car “hacks” or deficient code that leads to problematic outcomes. Innovators in this arena have a great incentive to understand and quickly deal with these issues because the future of their brands is at stake. Finally, insurance companies already help encourage better safety and security practices over time and will continued to do so for connected cars.<sup>[18]</sup>

10. **Consumer education can help:** One of the most constructive roles that government officials can play is to—along with industry and various stakeholders—help educate the public about privacy and security risks associated with new connected car technologies. The FTC already partners with several other federal agencies to provide OnGuardOnline, a website that offers wide-ranging security, safety, and privacy tips for both consumers and businesses.<sup>[19]</sup> The FTC also has created a YouTube page featuring informational videos on these

issues.<sup>[20]</sup> As part of its 2015 staff report on Internet of Things issues, the FTC said it “will develop new consumer and business education materials in this area” in coming months and years.<sup>[21]</sup> NHTSA also educates car owners on about a number of risk factors, including distracted and drowsy driving, seat belt safety, speeding concerns, tire safety, and more.<sup>[22]</sup> These same education approaches could be repurposed to address connected vehicle concerns. Such consumer awareness efforts can bolster those already being crafted by industry and nonprofit groups focused on improving connected car security and privacy.

---

### ***Additional Reading:***

- ***Filing:*** Adam Thierer & Caleb Watney, “Comment on the Federal Automated Vehicles Policy,” Comment on Federal Automated Vehicles Policy before the National Highway Traffic Safety Administration, December 5, 2016, <https://www.mercatus.org/publications/comment-federal-automated-vehicles-policy>.
- ***Law Review Article:*** Adam Thierer & Ryan Hagemann, Removing Roadblocks to Intelligent Vehicles and Driverless Cars,” Mercatus Center *Working Paper*, September 2014, <https://www.mercatus.org/system/files/Thierer-Intelligent-Vehicles.pdf>.
- ***Law Review Article:*** Adam Thierer, “The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation,” *Richmond Journal of Law and Technology*, Vol. 21, No. 6 (2015), [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2494382](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2494382).
- ***Podcast:*** “A Conversation with Adam Thierer,” *Smarter Cars*, April 1, 2017, <https://www.mercatus.org/podcasts/04012017/smarter-cars-conversation-adam-thierer>.
- ***Oped:*** Andrea O’Sullivan, “Let Driverless Car Innovators—Not Bureaucrats—Work Out Security, Privacy Issues,” *Reason*, June 14, 2017, <https://reason.com/archives/2017/06/14/let-driverless-car-innovatorsnot-bureauc>.

- **Oped:** Adam Thierer, “When the Trial Lawyers Come for the Robot Cars,” *Slate*, June 10, 2016, [http://www.slate.com/articles/technology/future\\_tense/2016/06/if\\_a\\_driverless\\_car\\_crashes\\_who\\_is\\_liable.html](http://www.slate.com/articles/technology/future_tense/2016/06/if_a_driverless_car_crashes_who_is_liable.html).
- **Oped:** Adam Thierer & Caleb Watney, “Every Day Matters with Driverless Cars,” *The Hill*, October 20, 2016, <http://thehill.com/blogs/congress-blog/technology/301938-every-day-matters-with-driverless-cars>.
- **Oped:** Adam Thierer & Andrea O’Sullivan, “Leave the Internet of Things Alone,” *US News*, June 12, 2017, <https://www.usnews.com/opinion/economic-intelligence/articles/2017-06-12/dont-stifle-the-internet-of-things-with-regulation>.
- **Blog post:** Adam Thierer, “Don’t Hit the (Techno-)Panic Button on Connected Car Hacking & IoT Security,” *Technology Liberation Front*, February 10, 2015, <https://techliberation.com/2015/02/10/dont-hit-the-techno-panic-button-on-connected-car-hacking-iot-security>.

---

**Endnotes:**

[1] Federal Trade Commission, “FTC, NHTSA to Conduct Workshop on June 28 on Privacy, Security Issues Related to Connected, Automated Vehicles,” March 20, 2017, <https://www.ftc.gov/news-events/press-releases/2017/03/ftc-nhtsa-conduct-workshop-june-28-privacy-security-issues>.

[2] <https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected>.

[3] Andrea O’Sullivan, “Let Driverless Car Innovators—Not Bureaucrats—Work Out Security, Privacy Issues,” *Reason*, June 14, 2017, <https://reason.com/archives/2017/06/14/let-driverless-car-innovatorsnot-bureauc>.

[4] Kevin Beaver, “Information Security Is Not Stagnant, but Dynamic,” *Security Intelligence*, August 5, 2015,

<https://securityintelligence.com/information-security-is-not-stagnant-but-dynamic>.

[5] Andrea O’Sullivan, “Giving Government ‘Backdoor’ Access to Encrypted Data Threatens Personal Privacy and National Security,” *Reason*, June 16, 2015, <https://reason.com/archives/2015/06/16/crypto-wars-weaken-encryption-security>.

[6] Adam Thierer & Caleb Watney, “Every Day Matters with Driverless Cars,” *The Hill*, October 20, 2016, <http://thehill.com/blogs/congress-blog/technology/301938-every-day-matters-with-driverless-cars>; Adrienne Roberts, “Can Auto Fatalities Go to Zero?” *Wall Street Journal*, June 23, 2017, <https://www.wsj.com/articles/can-auto-fatalities-go-to-zero-1498239201>.

[7] Boston Consulting Group, *A Roadmap to Safer Driving Through Advanced Driver Assistance Systems*, September 29, 2015, <https://www.mema.org/resource/roadmap-safer-driving-through-advanced-driver-assistance-systems>.

[8] Adam Thierer, “A Framework for Benefit-Cost Analysis in Digital Privacy Debates,” *George Mason University Law Review* 20, no. 4 (Summer 2013): 1066–69.

[9] Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*, (Arlington, VA: Mercatus Center at George Mason University, 2nd Edition, 2016): 2, <http://mercatus.org/permissionless/permissionlessinnovation.html>.

[10] <https://www.automotiveisac.com/faq.php>

[11] <https://autoalliance.org/connected-cars/automotive-privacy-2/principles>.

[12] United States Government Accountability Office, “Internet of Things: Status and Implications of an Increasingly Connected World,” GAO-17-75, May 2017, at 27. <http://www.gao.gov/assets/690/684590.pdf>.

[13] John Villasenor, “Who Is at Fault When a Driverless Car Gets in an Accident?” *Atlantic*, April 25, 2014. (“When confronted with new,

often complex, questions involving products liability, courts have generally gotten things right.”)

[14] Bryant Walker Smith, “Automated Driving and Product Liability,” *Michigan State Law Review*, Vol. 1, (2017), *forthcoming*, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2923240](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2923240).

[15] Federal Trade Commission, “A Brief Overview of the Federal Trade Commission’s Investigative and Law Enforcement Authority,” Revised July 2008, <https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority>.

[16] National Highway Traffic Safety, “Motor Vehicle Defects and Safety Recalls: What Every Vehicle Owner Should Know,” <https://www-odi.nhtsa.dot.gov/recalls/recallprocess.cfm>.

[17] Adam Thierer and Ryan Hagemann, “Removing Roadblocks to Intelligent Vehicles and Driverless Cars,” *Wake Forest Journal of Law & Policy*, Vol. 5, No2 (2015), 40.

[18] Sasha Kucharczyk, “How AI and Autonomy Will Usher in a New Age for Car Insurance,” *ReadWrite*, June 12, 2017, <https://readwrite.com/2017/06/12/ai-autonomy-auto-insurance-tl1>.

[19] Federal Trade Commission, “OnGuardOnline,” <https://www.consumer.ftc.gov/features/feature-0038-onguardonline>. (The agency also contributes to the Department of Homeland Security’s “Stop. Think. Connect.” Educational effort. See, U.S. Department of Homeland Security, “Stop.Think.Connect.” <https://www.dhs.gov/stopthinkconnect>.)

[20] Federal Trade Commission, “FTCvideos,” *YouTube*, <https://www.youtube.com/user/FTCvideos>, *archived at* <https://perma.cc/N35M-9L5Y> (last visited June 26, 2017).

[21] Federal Trade Commission, *The Internet of Things: Privacy and Security in a Connected World*, (January 2015): 53.

[22] National Highway Traffic Safety Administration, “Risky Driving,” <https://www.nhtsa.gov/risky-driving>; National Highway Traffic Safety Administration, “Road Safety,” <https://www.nhtsa.gov/road-safety>, (last visited June 26, 2017).

