epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

☎ +1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

June 20, 2017

Michael Kratsios
U.S. Deputy Chief Technology Officer
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, DC 20504

Dear Deputy Chief Technology Officer Kratsios:

We write to you in advance of this week's meeting about emerging technologies. American consumers face unprecedented privacy and security threats. The unregulated collection of personal data and the growth of the Internet of Things has led to staggering increases in identity theft, security breaches, and financial fraud in the United States. And drones pose a unique threat to privacy. These issues have a significant impact on the future of privacy and cybersecurity for the United States.

EPIC is a public-interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC is a leading advocate for consumer privacy and has appeared before the Congress on several occasions, and has actively participated in the proceedings of the Federal Trade Commission ("FTC") and the Federal Communications Commission ("FCC").[1] EPIC has taken a particular interest in the unique privacy problems of Internet of Things, drones, and connected cars.[2]

[1] *See, e.g,* Statement of Khaliah Barnes, hearing on *The Internet of Cars* before the House Committee on Oversight and Government Reform, November 18, 2015, https://epic.org/privacy/edrs/EPIC-Connected-Cars-Testimony-Nov-18-2015.pdf; Marc Rotenberg, EPIC Executive Director, Testimony before the House Comm. on Energy & Commerce, Subcomm. on Communications and Technology, *Communications Networks and Consumer Privacy: Recent Developments* (April 23, 2009), https://epic.org/privacy/dpi/rotenberg_HouseCom_4-09.pdf; Letter from EPIC to the House Comm. on Energy and Commerce on FCC Privacy Rules (June 13, 2016), https://epic.org/privacy/consumer/EPIC-FCC-Privacy-Rules.pdf; Letter from EPIC to the Senate Comm. on Commerce, Science, and Transportation on FTC Oversight (Sept. 26, 2016), https://epic.org/privacy/consumer/EPIC-Letter-Sen-Comm-CST-FTC-Oversight.pdf.

[2] Comments of EPIC to NTIA, *On the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things* (June 2, 2016), https://epic.org/apa/comments/EPIC-NTIA-on-IOT.pdf; *EPIC v. FAA*, No. 15-1075 (D.C. Cir. Filed Mar. 31, 2015); *See also Domestic Unmanned Aerial Vehicles (UAVs) and Drones*, EPIC, https://epic.org/privacy/drones/; *See also* EPIC, *EPIC v. FAA, Challenging the FAA's Failure to Establish Drone Privacy Rules,* https://epic.org/privacy/litigation/apa/faa/drones/; Statement of EPIC, *Paving the Way for Self-Driving*

The Internet of Things Poses Numerous Privacy and Security Risks

The Internet of Things ("IoT") poses significant privacy and security risks to American consumers.[3] The Internet of Things expands the ubiquitous collection of consumer data. This vast quantity of data could be used for purposes that are adverse to consumers, including remote surveillance. Smart devices also reveal a wealth of personal information about consumers, which companies may attempt to exploit by using it to target advertising or selling it directly. Because the IoT generates data from all aspects of consumers' daily existence, these types of secondary uses could lead to the commercialization of intimate segments of consumers' lives.

Many IoT devices feature "always on" tracking technology that surreptitiously records consumers' private conversations in their homes.[4] These "devices raise numerous privacy concerns. Even if the owner of device is aware of the tracking, a visitor to their home may not. Companies say that the devices rely on key words, but to detect those words, the devices must always be listening. And the key words are easily triggered. For example, several Amazon Echo devices treated a radio broadcast about the device as commands.[5] A San Diego television report about a girl using an Echo to order a $170 dollhouse and four pounds of sugar cookies triggered Echo devices across the city to make the same purchase.[6] A recent law enforcement request for Amazon Echo recordings[7] shows that "always on" devices will be much sought-after sources of information by law enforcement, foreign and domestic intelligence agencies, and, inevitably, cybercriminals. In 2015, EPIC filed an FTC complaint about the Samsung SmartTVs and recommended new consumer safeguards.[8] While the FTC has failed to act on the complaint, many computer criminals have exploited these vulnerabilities.

Another significant risk to consumers in the IoT is security, of both the users' data and their physical person. Many of the same security risks that currently threaten our data will only expand in the Internet of Things. The damage caused by malware, phishing, spam, and viruses

Vehicles, 115th Cong. (2017), S. Comm. on Commerce, Science, and Transportation (June 14, 2017), https://epic.org/testimony/congress/EPIC-SCST-Paving-Self-Driving-Vehicles-Jun2017.pdf.

[3] *See* Comments of EPIC to NTIA, *On the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things* (June 2, 2016), https://epic.org/apa/comments/EPIC-NTIA-on-IOT.pdf; *Internet of Things,* EPIC, https://epic.org/privacy/internet/iot/.

[4] EPIC Letter to DOJ Attorney General Loretta Lynch, FTC Chairwoman Edith Ramirez on "Always On" Devices (July 10, 2015), https://epic.org/privacy/internet/ftc/EPIC-Letter-FTC- AG-Always-On.pdf.

[5] Rachel Martin, *Listen Up: Your AI Assistant Goes Crazy For NPR Too*, NPR (Mar. 6, 2016), http://www.npr.org/2016/03/06/469383361/listen-up-your-ai-assistant-goes-crazy-for-npr-too.

[6] Carlos Correa, *News Anchor Sets off Alexa Devices Around San Diego Ordering Unwanted Dollhouses*, CW6 (Jan. 5, 2017), http://www.cw6sandiego.com/news-anchor-sets-off-alexa- devices-around-san-diego-ordering-unwanted-dollhouses/.

[7] *See* Christopher Mele, *Bid for Access to Amazon Echo Audio in Murder Case Raises Privacy Concerns*, N.Y. Times (Dec. 28, 2016), https://www.nytimes.com/2016/12/28/business/amazon- echo-murder-case-arkansas.html.

[8] *Samsung "SmartTV" Complaint*, EPIC, https://epic.org/privacy/internet/ftc/samsung/.

will have an increasingly large array of networks in which to spread.[9] Additionally, not all wireless connections in the IoT are encrypted.[10]

It is not only the owners of IoT devices who suffer from the devices' poor security. The IoT has become a "botnet of things"—a massive network of compromised web cameras, digital video recorders, home routers, and other "smart devices" controlled by cybercriminals who use the botnet to take down web sites by overwhelming the sites with traffic from compromised devices.[11] The IoT was largely to blame for attacks in 2016 that knocked Twitter, Paypal, Reddit, Pinterest, and other popular websites off of the web for most of a day.[12] They were also behind the attack on security blogger Brian Krebs' web site, one of the largest attacks ever seen.[13]

These problems will not be solved by the market. Because poor IoT security is something that primarily affects other people, neither the manufacturers nor the owners of those devices have any incentive to fix weak security. Compromised devices still work fine, so most owners of devices had no idea that their IP cameras, DVRs, and home routers are no longer under their own control. As Bruce Schneier said in recent congressional testimony, a manufacturer who puts a sticker on the box that says "This device costs $20 more and is 30 percent less likely to annoy people you don't know" probably will not get many sales.[14]

EPIC urges the Administration to address the numerous privacy and security risks related to the "Internet of Broken Things."

Recommendations for Addressing the Privacy and Security Risks of the Internet of Things

EPIC recommends that legal requirements ensure that companies providing "Internet of Things" services adopt Privacy Enhancing Technologies; do not track, profile, or monitor users; minimize data collection; and ensure security in both design and operation of Internet-connected devices.[15]

EPIC urges that the government should require companies that collect data from smart devices to implement Privacy Enhancing Technologies. EPIC has long advocated for Privacy

[9] *See* EUROPEAN COMM'N, A DIGITAL AGENDA FOR EUROPE, 16-18 (2010), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF.

[10] Federal Motor Vehicle Safety Standards; Event Data Recorders, Docket No. NHTSA-2012-0177 (Comments of Privacy Coalition), 10 https://epic.org/privacy/edrs/EPIC-Coal-NHTSA-EDR-Cmts.pdf; Nick Feamster, *Who Will Secure the Internet of Things?*, FREEDOM TO TINKER (Jan. 19, 2016) https://freedom-to-tinker.com/blog/feamster/who-will-secure-the-internet-of-things/.

[11] *See* Bruce Schneier, *We Need to Save the Internet from the Internet of Things*, Schneier on Security (Oct. 6, 2016), https://www.schneier.com/essays/archives/2016/10/we_need_to_save_the_.html.

[12] *See* Scott Hilton, *Dyn Analysis Summary of Friday October 21 Attack*, Dyn.com (Oct. 26, 2016), http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.

[13] *See* Brian Krebs, *KrebsOnSecurity Hit With Record DDoS*, KrebsOnSecurity (Sept. 21, 2016), https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.

[14] Testimony of Bruce Schneier before the House Committee on Energy & Commerce, Understanding the Role of Connected Devices in Recent Cyber Attacks, 114th Cong. (2016).

[15] *See* Comments of EPIC to NTIA, *On the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things* (June 2, 2016), https://epic.org/apa/comments/EPIC-NTIA-on-IOT.pdf.

Enhancing Technologies ("PETs") to protect privacy.[16] PETs limit data collection and embed privacy protection.[17] Rather than building a connected car that can store potentially limitless travel records, for instance, a PET would automatically delete old data after a certain amount of time, or prevent individual data from being automatically synced with a central database.

The government must also protect consumers' rights to limit data collection and use. Individuals should retain control over their personal data, including the right to limit the collection and use of data beyond that necessary to the provision of the service. A "notice and choice" or consent-based approach to privacy protections simply does not work in the Internet of Things. Instead, Fair Information Practices must be fully applied to the Internet of Things.[18] This approach would grant consumers affirmative rights and place privacy responsibilities on companies who collect consumer data from connected devices.

Companies that collect data from smart devices must be required to provide access to this data for consumers. Many of the consumer benefits[19] of the Internet of Things—reduced costs, time savings, increased convenience—require or would be greatly improved by providing consumers with access to their data. Furthermore, consumers should also be able to access the basic logic behind any algorithm used by a company or vendor to make a decision about a consumer. For instance, if a Smart Grid central database determines that, based on their energy consumption, certain energy consumers will have their power switched off at certain times of the day, those consumers must be informed that their data classification has changed. Transparency is therefore a vital component of informed user choice.[20]

Companies should also be required to adopt the principle of data minimization, so that only so much data is used and stored as is necessary to ensure the functionality of their products or services.[21] Minimization itself can be accomplished in several ways. Data could be collected periodically or randomly, rather than constantly; or companies could take data samples from a representative percentage of products, rather than collecting data from every product. Companies could collect only aggregated data to avoid obtaining granular information about particular consumers. For example, a Smart Grid could collect aggregate data from an entire apartment building, rather than collecting individual data from each apartment, or even from individual devices within each apartment. Aggregation combined with deletion – i.e., storing individual data only for as long as it takes to develop an aggregate computation – could allow for very accurate aggregation, while ensuring a degree of anonymity for the consumers. Data retention periods should be restricted as well.

[16] Herbert Burkert, *Privacy-Enhancing Technologies: Typology, Critique, Vision* in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 125 (Philip E. Agre and Marc Rotenberg eds. 1998).

[17] Alec Foege, *IBM's Jeff Jonas on Baking Data Privacy into Predictive Analytics*, DATA INFORMED (Nov. 20, 2013) http://data-informed.com/ibms-jeff-jonas-baking-data-privacypredictiveanalytics/#sthash.hBM0lg1N.dpuf.

[18] See EPIC, *The Code of Fair Information Practices*, http://epic.org/privacy/consumer/code_fair_info.html.

[19] *See, e.g., 4 ways the internet of things will radically change your life*, WHITEBOARD http://www.whiteboardmag.com/4-ways-the-internet-of-things-will-radically-change-your-life/.

[20] *Id*.

[21] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 23-24 (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

Aerial Drones: A Unique Privacy Threat

EPIC believes that strong drone privacy rules are vital for the safe integration of commercial drones in the National Air Space. The present course is simply not sustainable.

Drones pose a unique threat to privacy. The technical and economic limitations to aerial surveillance change dramatically with the advancement of drone technology. Small, unmanned drones are already inexpensive; the surveillance capabilities of drones are rapidly advancing; and cheap storage is readily available to maintain repositories of surveillance data. A Pew Research Center and Smithsonian Magazine survey found that 63% of Americans objected to allowing personal and commercial drones to fly through most U.S. airspace.[22] However, in recent years individual drone use has soared, and the FAA predicts that 7 million drones will be sold by 2020.[23] As drone use increases so do the risks to privacy and safety.

Drones are now regularly equipped with high definition cameras that increase the ability of a user to conduct domestic surveillance.[24] The DJI Inspire 2 is a high-end, commercially available hobbyist drone about the size of a small desktop printer and weighs less than eight pounds, yet it can transmit high definition video to an operator over four miles away and can live-stream that video.[25] Even lower-end hobbyist drones costing less than $100 can stream live video. The Hubsan X4 H502E DESIRE, a drone that can fit in the palm of your hand, utilizes a front facing high definition camera with 720P resolution that can stream live video up to 200 meters away.[26] Drones can be used to view individuals inside their homes and can facilitate the harassment and stalking of unsuspecting victims.[27] Drones can also be modified with tools that can enable them to gather personal information using infrared cameras, heat sensors, GPS, automated license plate readers, and facial recognition devices.[28]

[22] Aaron Smith, *U.S. Views of Technology and the Future,* Pew Research Center, Apr. 17, 2014, http://www.pewinternet.org/2014/04/17/us-views-of-technology-and-the-future/.

[23] Sally French, *Drone Sales in the U.S. More Than Doubled In The Past Year,* Market Watch, May 28, 2016, http://www.marketwatch.com/story/drone-sales-in-the-us-more-than-doubled-in-the-past-year-2016-05-27; *FAA Aerospace Forecast: Fiscal Years 2016-2036*, FAA, 2016, https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/FY2016-36_FAA_Aerospace_Forecast.pdf.

[24] Petition for Rulemaking Submitted by EPIC, Mar. 8, 2012, https://epic.org/apa/lawsuit/EPIC-FAA-Drone-Petition-March-8-2012.pdf; Univ. of Wash. Tech. and Pub. Policy Clinic, *Domestic Drones: Technical and Policy Issues* 12 (2013), https://www.law.washington.edu/clinics/technology/reports/droneslawan policy.pdf.

[25] DJI, *Inspire 2*, http://www.dji.com/inspire-2/info#specs.

[26] Hubsan, *X4 H502E DESIRE*, https://www.hubsanus.com/shop/h502e.html.

[27] Petition for Rulemaking Submitted by EPIC, *supra* note 6.

[28] *Id.*; Ciara Bracken-Roche et al., Surveillance Studies Centre, *Surveillance Drones: Privacy Implications of the Spread of Unmanned Aerial Vehicles (UAVs) in Canada* 46, Apr. 30, 2014, http://www.sscqueens.org/sites/default/files/Surveillance_Drones_Report.pdf; Mary Papenfuss, *Utah Couple Arrested Over 'Peeping Tom' Drone,* Huffington Post, Feb. 17, 2017, http://www.huffingtonpost.com/entry/peeping-tom-drone_us_58a6847fe4b045cd34c03e56.

Drones also pose risks to security and cybersecurity. Close calls between drones and traditional aircraft have risen significantly as their use becomes more widespread.[29] Furthermore, the very features that make drones easy to operate also make them susceptible to cyberattacks.[30] Hackers exploit weaknesses in drone software to take over operation of a drone and access the camera and microphones.[31]

The privacy risks of drones, as well as the safety and security vulnerabilities, underscore the need for the FAA to develop drone privacy regulations. *EPIC urges the Administration to issue regulations on drone privacy as mandated by Congress*.

The FAA Has Failed to Implement the Requirements of the FAA Modernization Act

The FAA has failed to take the action mandated by Congress. The FAA Modernization Act required the FAA to create a Comprehensive Plan to integrate drones into the National Airspace and subsequently conduct a notice and comment rulemaking. In the Plan, the FAA identified privacy as an important issue to address, acknowledging that "as demand for [drones] increases, concerns regarding how [drones] will impact existing aviation grow stronger, especially in terms of safety, privacy, frequency crowding, and airspace congestion."[32]

Under the FAA Modernization Act, Congress required the FAA to implement the recommendations of the Comprehensive Plan via a public rulemaking within 46 months of the enactment of the Act. The FAA identified privacy as an important issue directly related to domestic drones, yet the agency has failed to address privacy in the agency's only public rulemaking on drones in the National Airspace.[33] Indeed it has been over 60 months and the FAA has failed to implement the rulemaking that addresses the issues identified in the Comprehensive Plan, including privacy, as required by Congress.[34]

The FAA Has Failed to Conduct the Required Drone Privacy Report

Soon after the FAA's Comprehensive Plan identified privacy as an important drone integration issue, the agency was ordered by Congress to conduct a drone privacy report, which

[29] Alan Levin, *Drone-Plane Near misses, Other Incidents Surge 46% in U.S.,* Bloomberg, Feb. 23, 2017, https://www.bloomberg.com/news/articles/2017-02-23/drone-plane-near-misses-other-incidents-surged-46-in-u-s; Steve Miletich, *Pilot of Drone That Struck Woman at Pride Parade Gets 30 Days in Jail,* The Seattle Times, Feb. 24, 2017, http://www.seattletimes.com/seattle-news/crime/pilot-of-drone-that-struck-woman-at-pride-parade-sentenced-to-30-days-in-jail/.

[30] Kacey Deamer, *How Can Drones Be Hacked? Let Us Count the Ways,* Live Science, Jun. 10, 2016, http://www.livescience.com/55046-how-can-drones-be-hacked.html.

[31] Wang Wei, *You Can Hijack Nearly Any Drone Mid-Flight Using This Tiny Gadget,* The Hacker News, Oct. 27, 2016, http://thehackernews.com/2016/10/how-to-hack-drone.html.

[32] Joint Planning and Dev. Office, Fed. Aviation Admin., *Unmanned Aircraft Systems (UAS) Comprehensive Plan: A Report on the Nation's UAS Path Forward* 4 (2013), https://www.faa.gov/about/office_org/headquarters_offices/agi/reports/media/UAS_Comprehensive_Plan.pdf.

[33] Operation and Certification of Small Unmanned Aircraft Systems, 81 Fed. Reg. 42,063 (June 28, 2016) (codified at 14 C.F.R. pts. 21, 43, 61, 91, 101, 107, 119, 133, and 183).

[34] FAA Modernization and Reform Act of 2012, Pub. L. 112-95 § 332, 126 Stat. 73-75.

the agency failed to do. In the 2014 Consolidated Appropriations Act, Congress required the FAA to conduct a drone privacy study, stating:

> Without adequate safeguards, expanded use of UAS and their integration into the national airspace raise a host of concerns with respect to the privacy of individuals. For this reason, the FAA is directed to conduct a study on the implications of UAS integration into national airspace on individual privacy.[35]

The report specifically required the FAA to study "how the FAA can address the impact of widespread use of UAS on individual privacy as it prepares to facilitate the integration of UAS into the national airspace."[36] The report was to be submitted to Congress within 18 months of enactment of that appropriations bill and completed "well in advance of the FAA's schedule for developing final regulations on the integration of UAS into the national airspace."[37] Nearly 38 months since the bill was enacted, the FAA has failed to produce the report. Furthermore, EPIC obtained documents through a Freedom of Information Act request that suggested that the FAA has no intention of complying with Congress' directive to produce a report.[38]

EPIC's Lawsuit, EPIC v. FAA

Immediately after the passage of the FAA Modernization Act, EPIC and more than one hundred legal experts and organization petitioned the FAA to undertake a rulemaking to establish privacy regulations prior to the deployment of commercial drones in the National Airspace.[39] More than two years later, the FAA responded to the petition by refusing to conduct a separate drone privacy rulemaking but said privacy would be considered in an upcoming rulemaking on small drones.[40] However, the FAA later stated that privacy issues were "beyond the scope of the rulemaking"[41] and did not consider privacy in its final rule,[42] prompting EPIC to file suit.[43] EPIC is challenging the FAA's refusal to consider privacy and to conduct a comprehensive drone rulemaking as required by Congress.

<u>EPIC urges the Administration to protect the public from the privacy risks posed by drones</u>. Any privacy and security risks are no longer hypothetical and the longer the FAA waits to issue comprehensive privacy rules, the longer the public is at risk.

[35] 160 Cong. Rec. 1186 (2014), https://www.congress.gov/crec/2014/01/15/CREC-2014-01-15-bk2.pdf.

[36] *Id.*

[37] *Id.*

[38] https://epic.org/privacy/litigation/apa/faa/drones/EPIC-16-07-20-FAA-FOIA-20160921-Production.pdf.

[39] Petition for Rulemaking Submitted by EPIC, *supra* note 6.

[40] Letter from Fed. Aviation Admin. to EPIC (Nov. 26, 2014), https://epic.org/privacy/drones/FAA-Privacy-Rulemaking-Letter.pdf.

[41] Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9,544 (proposed Feb. 23, 2015).

[42] Operation and Certification of Small Unmanned Aircraft Systems, 81 Fed. Reg. 42,063 (June 28, 2016) (codified at 14 C.F.R. pts. 21, 43, 61, 91, 101, 107, 119, 133, and 183).

[43] EPIC v. FAA, No. 16-1297 (D.C. Cir.); https://epic.org/privacy/litigation/apa/faa/drones/.

Connected Cars

Connected vehicles pose substantial safety and privacy risks.[44] Wide-scale malicious automobile hacking is no longer theoretical.[45] Although a full-scale remote car hijacking is certainly a serious risk to car owners and others,[46] hijacking is not the only risk posed by connected car vulnerabilities.[47] Connected cars leave consumers open to car theft, data theft, and other forms of attack as well. These attacks are not speculative; many customers have already suffered due to vulnerable car systems. For example, criminals have exploited vulnerabilities in connected cars to perpetrate car "ransomware" scams, "where a car is disabled by malicious code until a ransom is paid."[48]

Car manufacturers must adopt data security measures. Early mitigation of threats to public safety may reduce auto fatalities, spur innovation, and result in safer vehicles.[49] There should be great concern that each of autonomous car maker wants to be the first to have their vehicle available to the public can poses substantial safety risks.[50] A functioning autonomous vehicle does not mean security and the race to be the first with a functioning, marketable autonomous vehicle jeopardizes the safety and security of consumers.

Recently, Charlie Miller, whose research led Chrysler to recall 1.4 million vehicles after he hacked into a Jeep,[51] stated the danger in self-driving ridesharing and taxi services stating that "Autonomous vehicles are at the apex of all the terrible things that can go wrong. . . Cars are already insecure, and you're adding a bunch of sensors and computers that are controlling them. .

[44] 8 U.S. Gov. Accountability Office, GAO-14-649T, Consumers' Location Data: Companies Take Steps to Protect Privacy, but Practices Are Inconsistent, and Risks May Not be Clear to Consumers (2014), http://gao.gov/products/GAO-14-649T; Jeff John Roberts, *Watch Out That Your Rental Car Doesn't Steal Your Phone Data,* Fortune, Sep. 1, 2016, http://fortune.com/2016/09/01/rental-cars-data-theft/.

[45] Brief of *Amicus Curiae* EPIC, *Cahen v. Toyota Motor Corporation*, No. 16-15496 (9th Cir. Aug. 5, 2016), *available at* https://epic.org/amicus/cahen/EPIC-Amicus-Cahen-Toyota.pdf.

[46] *See, e.g.*, Andy Greenberg, *Hackers Remotely Kill a Jeep On the Highway–With Me in It*, Wired (July 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[47] *See* Bruce Schneier, *The Internet of Things Will Turn Large-Scale Hacks Into Real World Disasters*, Motherboard (July 25, 2016), http://motherboard.vice.com/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster (explaining that information systems face three threats: theft (i.e. loss of confidentiality), modification (i.e. loss of integrity), and lack of access (i.e. loss of availability)).

[48] Nora Young, *Your Car Can be Held for Ransom*, CBCradio (May 22, 2016), http://www.cbc.ca/radio/spark/321-life-saving-fonts-ransomware-cars-and-more-1.3584113/your-car-can-be-held-for-ransom-1.3584114.

[49] *See generally*, Ralph Nader, *Unsafe at Any Speed* (1965).

[50] Mike Isaac, *Lyft and Waymo Reach Deal to Collaborate on Self-Driving Cars,* New York Times, May 14, 2017, https://www.nytimes.com/2017/05/14/technology/lyft-waymo-self-driving-cars.html; Alex Davies, *Detroit Is Stomping Silicon Valley in the Self-Driving Car Race,* Wired, Apr. 3, 2017, https://www.wired.com/2017/04/detroit-stomping-silicon-valley-self-driving-car-race/.

[51] Andy Greenberg, *After Jeep Hack, Chrysler Recalls 1.4 Million Vehicles for Bug Fix,* Wired, Jul 24, 2015, https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/; Andy Greenberg, *Hackers Remotely Kill A Jeep on the Highway—With Me In It,* Wired, Jul. 21, 2015, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/; Andy Greenberg, *The Jeep Hackers Are Back To Prove Car Hacking Can Get Much Worse,* Wired, Aug. 1, 2016, https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/.

. If a bad guy gets control of that, it's going to be even worse."[52] The potential risks that connected cars pose to the driver, as well as the potential risk to the public, cannot be understated.

EPIC urges the Administration to take these security flaws into account as it examines the future of transportation as it relates to these vehicles. *National minimum standards for safety and privacy are needed to ensure the safe deployment of connected vehicles.*

Conclusion

America provides unequaled opportunities for innovation. But to sustain innovation over time requires wise policies that safeguard fundamental rights. As Thomas Edison said, "What man creates with his hand, he must control with his head."[53]

The Internet of Things, drones, and connected cars all wide-ranging challenges for consumer privacy, cyber security, and public safety. The government should act now to ensure these technologies are implemented in a way that benefits consumers and respects important values. EPIC welcomes the opportunity to work with Administration on these issues.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

[52] Andy Greenberg, *Securing Driverless Cars From Hackers Is Hard. Ask The Ex-Uber Guy Who Protects Them*, Wired, Apr. 12, 2017, https://www.wired.com/2017/04/ubers-former-top-hacker-securing-autonomous-cars-really-hard-problem/.
[53] *See* MARC ROTENBERG, ET AL, PRIVACY IN THE MODERN AGE, THE SEARCH FOR SOLUTIONS (The New Press 2015).