The Internet of Things:

Implications for Copyright and Privacy

Seth Greenstein
David Golden
April 24, 2018

CONSTANTINE | CANNON
NEW YORK | WASHINGTON | SAN FRANCISCO | LONDON

"We shape our tools and, thereafter, our tools shape us."

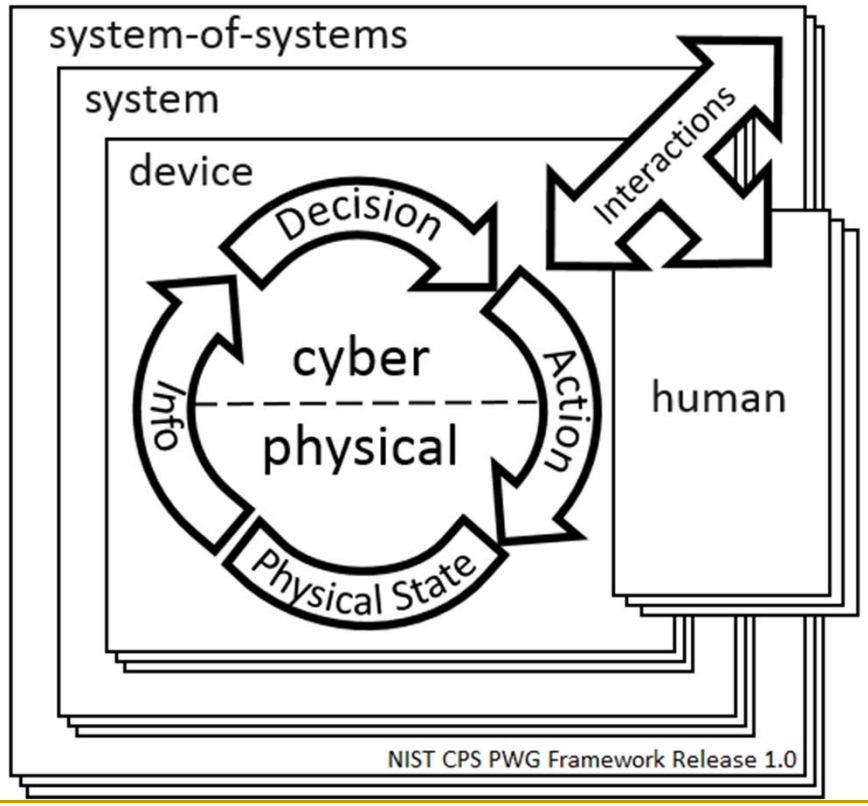
John Culkin (1967)

What is the "Internet of Things"?

"An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment."

Mohammad Sabzinejad Farasha, et.al. Ad Hoc Networks 36(1), January 2016. p. Abstract

What is the "Internet of Things"?



Cyber-Physical Systems Framework
https://pages.nist.gov/cpspwg/

What is the "Internet of Things"?

"We must first define what we mean by 'things.'"

Francois Jammes, "Internet of Things in Energy Efficiency," Ubiquity: An ACM Publication, February 2016, p. 2

What is the "Internet of Things"?

"There is no consensus amongst industry on how to define the Internet of Things … . Furthermore, there was no consensus on whether developing such a definition would be useful."

Internet of Things Cybersecurity Colloquium, NIST (December 2017)
https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8201.pdf

What is the "Internet of Things"?

"IoT involves *sensing*, *computing*, *communication*, and *actuation*."

Jeffrey Voas, "Networks of 'Things,'" NIST Special Publications 800-183 (July 2016), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf

What is the "Internet of Things"?

- Everyday devices sense and accumulate data about some aspect of their environment
- Communicate instructions or data to influence the action of other devices over the environment via IP or other network protocol

Examples

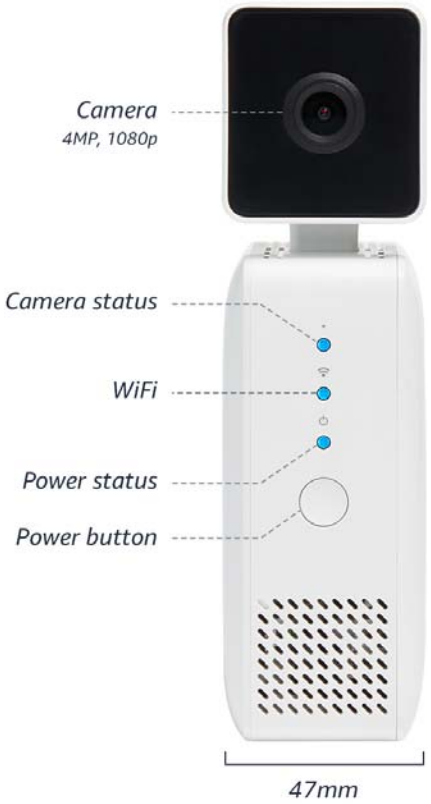
More Examples

Still More Examples

AIY

Google Vision

Google Voice



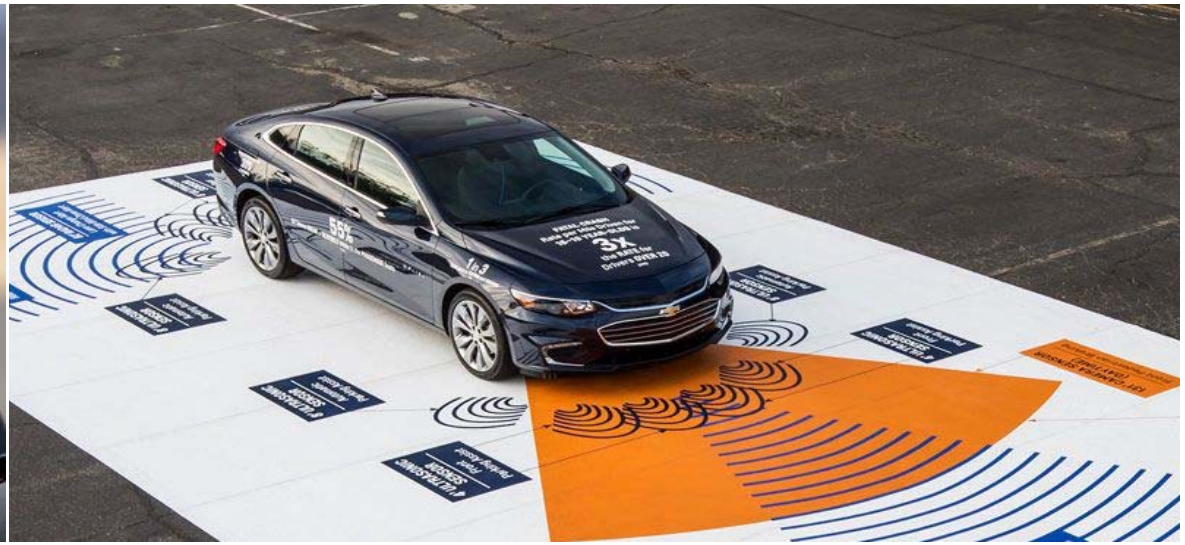
Amazon DeepLens

On Star

Imagine a vehicle that was never lost

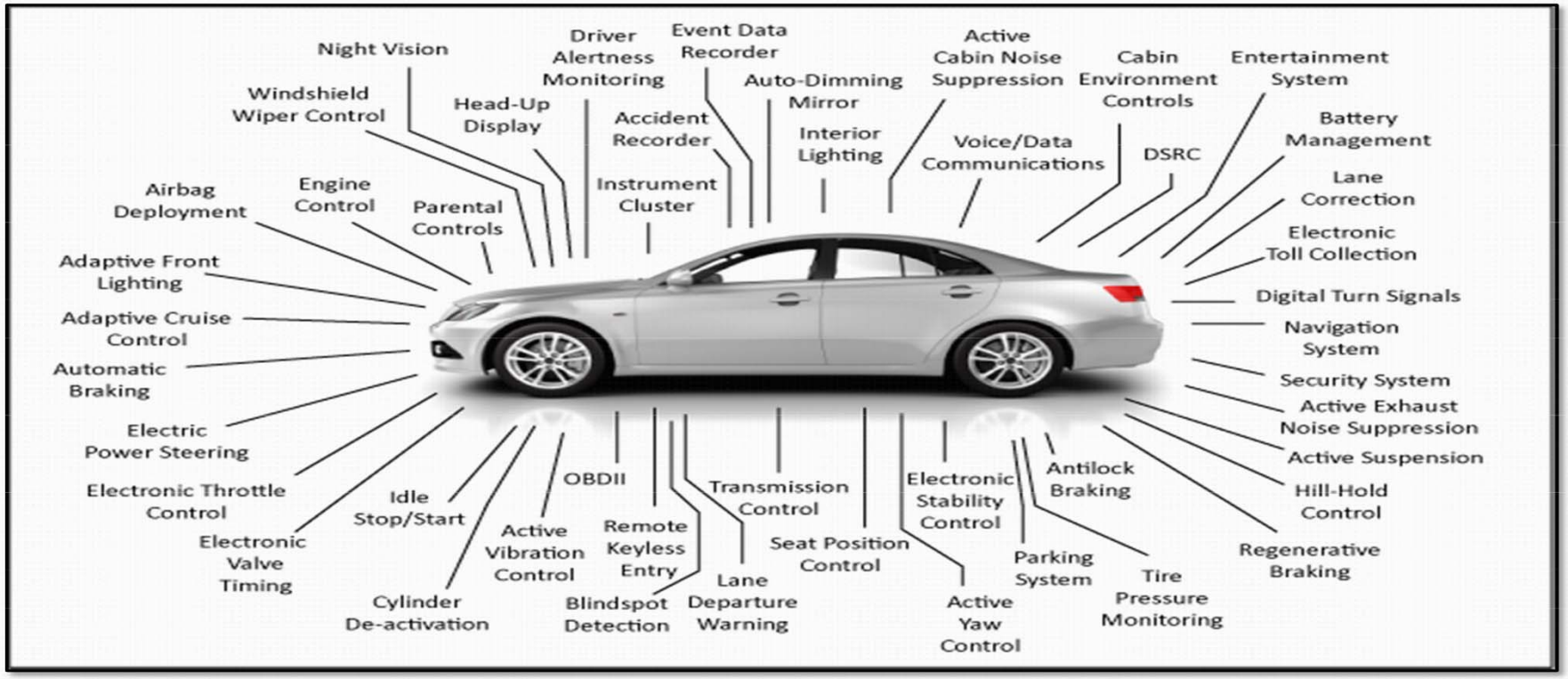
That was smart enough to identify when it had a potential issue,* and could even help make its own maintenance appointments.*
That could help Advisors predict how severe a crash was* and how likely it was to cause life-threatening injuries in order to better assist emergency responders.
That was capable of connecting to the internet — with an in-vehicle Wi-Fi® hotspot* that's fast enough for your passengers to stream movies and videos at high quality.
That could help you become a smarter driver.*
That could help authorities recover itself* if it were ever stolen.
That could save you money by finding you deals* at the places you love to eat and shop.

Car Sensors



Car or Computer?

Electronic Modules Controlled by Embedded Software



Copyright Issues for the IoT

- What is protectible?
- Ownership vs. Licensing?
  - Effects on consumer rights, research, interoperability
- DMCA Section 1201
- Copyright Office "Embedded Software" Study
- Librarian Triennial Exemptions Proceeding

What is Protectible?

- **Section 102(b) –** copyright does not extend to any "idea, procedure, system, method of operation, concept, principle, or discovery"
  - "Idea/expression dichotomy"
- ***Computer Associates Intern. Inc. v. Altai,*** 982 F. 2d 693 (2d Cir. 1992)
  - Abstraction of expression vs. ideas
  - Filtration of non-copyrightable data, merger, *scenes a faire*

What is Protectible? (cont'd)

- ***Feist Pubs. Inc. v. Rural Tel. Serv. Co.,*** 499 U.S. 340 (1991) (facts and data not copyrightable; structure, sequence, and organization of data could be protectible if original).
- ***Oracle America vs. Google,*** 750 F. 3d 1339 (Fed. Cir. 2014)
  - API declaring code and structure, sequence, and organization copyrightable

Ownership vs. Licensing

- Implications for Sections 107, 109, 117--
  - First sale (right to transfer ownership)
  - Maintenance/Repair/Customization
  - Interoperability
  - Reverse Engineering/Security Research
- Enforceability of shrink/click wrap licenses
  - ***ProCD Inc. v. Zeidenberg*,** 86 F.3d 1447 (7th Cir. 1996)

Ownership vs. Licensing (cont.)

- When is a License *Not* a License?
- Look primarily to duration and degree of retained control
  - ***Vernor v. Autodesk, Inc.***, 621 F.3d 1102 (9th Cir. 2010)
  - ***DSC Commc'ns Corp. v. Pulse Commc'ns, Inc.***, 170 F.3d 1354 (Fed.Cir.1999)
  - ***Krause v. Titleserv, Inc.***, 402 F.3d 119 (2nd Cir. 2005)

Ownership v. Licensing (cont'd)

- EULA – Amazon Echo
  - **Use of the Amazon Software.** You may use Amazon Software solely for purposes of enabling you to use the Amazon Services as provided by Amazon, and as permitted by these Conditions of Use and any Service Terms. You may not incorporate any portion of the Amazon Software into other programs or compile any portion of it in combination with other programs, or otherwise copy (except to exercise rights granted in this section), modify, create derivative works of, distribute, assign any rights to, or license the Amazon Software in whole or in part.
  - **No Reverse Engineering.** You may not reverse engineer, decompile or disassemble, tamper with, or bypass any security associated with the Amazon Software, whether in whole or in part.

Ownership v. Licensing (cont'd)

- EULA – Nest
  - You agree not to, and you will not permit others to, (a) license, sell, rent, lease, assign, distribute, transmit, host, outsource, disclose or otherwise commercially exploit the Product Software or make the Product Software available to any third party, (b) copy or use the Product Software for any purpose other than as permitted in Section 1, (c) use any portion of the Product Software on any device or computer other than the Product that you own or control, (d) remove or alter any trademark, logo, copyright or other proprietary notices, legends, symbols or labels in the Product Software, or (e) modify, make derivative works of, disassemble, reverse compile or reverse engineer any part of the Product Software (except to the extent applicable laws specifically prohibit such restriction for interoperability purposes, in which case you agree to first contact Nest Labs and provide Nest Labs an opportunity to create such changes as are needed for interoperability purposes). You may not release the results of any performance or functional evaluation of any of the Product Software to any third party without prior written approval of Nest Labs for each such release.

DMCA – Section 1201(a) and (b)

- (a)(1) Technological protection of Access controls
  - "No person shall circumvent a technological measure that effectively controls access to a work protected under this title."
- (a)(2) Prohibition on making or trafficking in tools that circumvent access controls.
- (b) Prohibition on making or trafficking in tools that circumvent controls that effectively protect the rights of a copyright owner (e.g., Copy controls) in a protected work.

DMCA – Section 1201(a) Case Law

- Does not preclude circumvention of measures that do not effectively control access to a protected work
  - ***Lexmark v. Static Control Components*****,** 387 F.3d 522 (6th Cir. 2004) (TPM between laser printers and replacement toner cartridges)
  - ***Chamberlain Group v. Skylink Techs.*****,** 381 F.3d 1178 (Fed. Cir. 2004) (TPM for universal garage door opener)
  - ***Ford Motor Co. v. Autel Intelligent Techs.*****,** (E.D. Mich. Jul. 1, 2016)(TPM for non-copyrightable data in automotive diagnostics)
  - Keurig K-cups, HP inkjet cartridges, etc.

Software-Enabled Consumer Products Study

- Report of the Register of Copyrights, December 2016
  - https://www.copyright.gov/policy/software/software-full-report.pdf
- Initiated by request of Senators Grassley and Leahy
  - Notice of Inquiry Dec. 15, 2015, https://copyright.gov/fedreg/2015/80fr77668.pdf
  - Public Comments Feb. 17, 2016
  - Public Roundtables May 18 (DC) and May 24 (SF), 2016

Software-Enabled Consumer Products (cont'd)

- "[S]oftware's ubiquity raises significant policy issues across a broad range of subjects, including privacy, cybersecurity, and intellectual property rights. These include questions about the impact of existing copyright law on innovation and consumer uses of everyday products and innovative services that rely on such products."
- "[M]any of these issues also arise with respect to the Internet of Things, a subset of software-enabled products that 'connect, communicate or transmit information with or between each other through the Internet.'"

Key Questions

- Whether and how existing copyright law doctrines address issues relating to products with embedded software
- How existing doctrines do/not allow for resale, repair, customization, security research, and interoperability
- What is the scope and reach of licensing practices, including the relationship of contract and copyright law.
- Whether reliance on flexible copyright doctrines, with potentially uncertain outcomes, is sufficient.
- Whether bright-line legislative fixes are necessary.

Summary of Responses

- No evidence that consumers have been prevented from transferring ownership of software-enabled products
- Limited evidence that state contract law has interfered with consumer rights.
- Properly applied, doctrines of fair use, idea/expression dichotomy and merger, *scenes a faire*, and maintenance limitation facilitate repair and improvement, security research, and interoperability.
- A new statutory framework "might help reduce some uncertainty," but is not necessary at this time.
- Report may be a "roadmap" for courts and businesses.
- Does *not* consider impact of DMCA Section 1201.

Copyright Office Section 1201 Study

- December 29, 2015 Notice of Inquiry
- Public Comment period March 3/April 1, 2016
- Roundtables May 19-20 (DC), May 25 (SF)
- Report issued June 2017
  - https://www.copyright.gov/policy/1201/section-1201-full-report.pdf

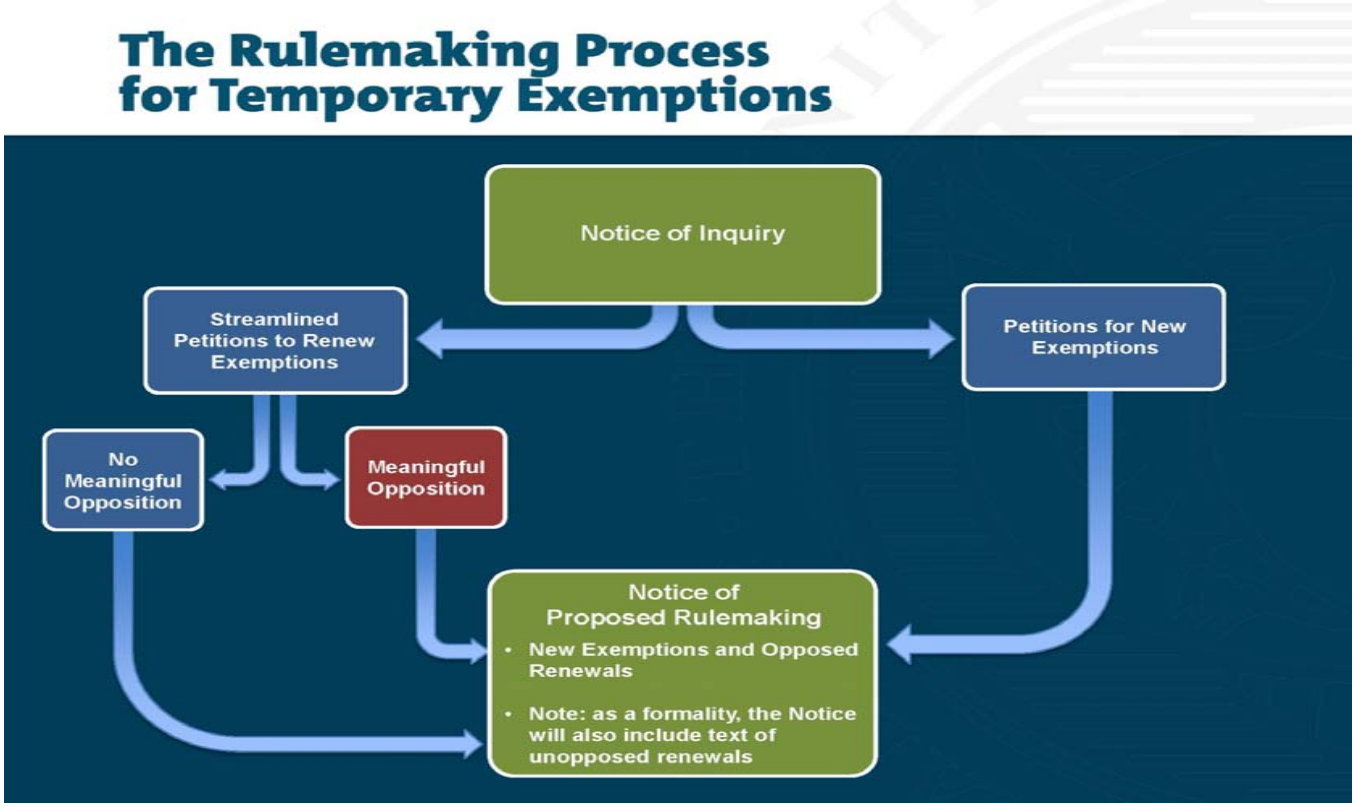
Copyright Office Section 1201 Study -- Summary

- Statutory structure and scope are sound
- Antitrafficking provisions "critical enforcement tools against piracy," but –
  - Beneficiaries of exemptions can develop circumvention tools for their own use
  - Librarian should have discretion to adopt exemptions allowing third-party assistance "at the direction of" a beneficiary
    - Such a third party is also a "user"
- Consider expanding exemptions for security and encryption research

Copyright Office Section 1201 Study -- Summary

- Consider permanent exemptions
- Streamline process for renewing exemptions where no substantial opposition

Copyright Office Section 1201 Process



DMCA – Section 1201(a) Triennial Review

- (1)"No person shall circumvent a technological measure that effectively controls access to a work protected under this title."
- The prohibition shall not apply to users of a copyrighted work in a particular class of works, if such persons are, or are likely to be in the succeeding 3-year period, adversely affected by virtue of such prohibition in their ability to make noninfringing uses of that particular class of works.

DMCA – Section 1201(a)

- John Deere tractor software EULA:

License Restrictions, Circumvention. Security measures ("SM") means any of the following: technological measures under the Digital Millennium Copyright Act, copyright protection measures, application enabling mechanisms, passwords, key codes, encryption or other security devices. You agree that you will not: (a) attempt to defeat a SM or defeat a SM that protects the [software] and that would constitute a violation under applicable law related to circumvention of technological measures that protect software, copyrighted works, or other intellectual property rights, and (b) traffic in, purchase, manufacture, design, import, offer, sell or distribute any circumvention or hacking device that is designed to circumvent or hack the [software] or [product] to the extent unlawful under applicable law.

DMCA – Section 1201(a) Rulemaking

- The Librarian conducts a triennial rulemaking review to determine whether to issue a three-year exemption for users who are likely to be adversely affected. https://www.copyright.gov/1201/2018/
- New Procedure
  - Petitions to renew prior exempt uses in specified classes
    - Granted where no meaningful opposition
  - Petitions for New Exemptions

DMCA – Section 1201(a) Rulemaking

- Notice of Inquiry and Requests for Petitions, https://www.gpo.gov/fdsys/pkg/FR-2017-06-30/pdf/2017-13815.pdf
- Seventh triennial process ongoing now
- Classes most relevant to IoT
  - Class 5: Computer Programs – Unlocking
  - Class 6: Computer Programs – Jailbreaking
  - Class 7: Computer Programs – Repair

DMCA – Section 1201(a) Exemption Renewal

- "The petitions demonstrated the continuing need and justification for the exemption to prevent owners of motorized land vehicles from being adversely impacted in their ability to diagnose, repair, and modify their vehicles as a result of TPMs that protect the copyrighted computer programs on the electronic control units ('ECUs') that control the functioning of the vehicles."
  - 82 Fed. Reg. at 49554.

Key Issues under DMCA for IoT

- Scope of protection under Section 1201
  - Protection against unauthorized access, copying, trafficking in tools
- But -- Technological measures also can be used to protect business models, unprotectable programs or data
- Complexity of software limits ability of individuals to circumvent for exempt purposes
- Assistance from third-party users
- Ability of third parties to create and acquire tools

DMCA Section 1201 Rulemaking – What's Next

- Hearings April 10-13 in DC, April 23-25 in LA
- Rulemaking decision expected October 2018
- Appeal?
- Legislation?

Privacy and Security Issues

- Do IoT devices pose privacy and security risks?
  - The short answer: Yes.
- The Current Legal Landscape
- The Future Legal Landscape
- Federal Enforcement and Guidance

Do IoT Devices Pose Privacy and Security Risks?

- Federal Trade Commission, ***Internet of Things, Privacy and Security in a Connected World*** (January 2015)
  - ". . . as consumers install more smart devices in their homes, they may increase the number of vulnerabilities an intruder could use to compromise personal information."
  - ". . . if a vulnerability were discovered after manufacture, it may be difficult or impossible to update the software or apply a patch . . . Many companies – particularly those developing low-end devices – may lack economic incentives to provide ongoing support or software security updates at all . . .."

Do IoT Devices Pose Privacy and Security Risks? (cont'd)

- Federal Trade Commission, ***Internet of Things, Privacy and Security in a Connected World*** (January 2015)
  - "one participant indicated that fewer than 10,000 households using the company's IoT home-automation product can 'generate 150 million discrete data points a day' or approximately one data point every six seconds for each household."
  - ". . . the trend towards abundant collection of data creates a 'non-targeted dragnet collection from devices in the environment.'"

Do IoT Devices Pose Privacy and Security Risks? (cont'd)

- The short answer: Yes.
- Business Insider, ***Hackers once stole a casino's high-roller database through a thermometer in the lobby fish tank*** (April 15, 2018), http://www.businessinsider.de/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4
- The Verge, ***How an army of vulnerable gadgets took down the web today*** (October 21, 2016), https://www.theverge.com/2016/10/21/13362354/dyn-dns-ddos-attack-cause-outage-status-explained

The Current Legal Landscape

- Federal
  - Privacy Act of 1974
  - Computer Fraud Abuse Act of 1986
  - Electronic Communications Privacy Act
  - Health Insurance Portability and Accountability Act of 1996
  - Children's Online Privacy Act of 1998
- State laws

The Current Legal Landscape: Federal laws

- No federal laws specifically address IoT devices (yet).
- However, existing statutes – some of which are decades old – may be applicable.
- Privacy Act of 1974 (5 U.S.C. § 552a)
  - Regulates the collection, maintenance, use, and dissemination of personal information by federal agencies
  - DOJ overview: https://www.justice.gov/opcl/file/793026/download

The Current Legal Landscape: Federal laws (cont'd)

- Computer Fraud and Abuse Act (18 U.S.C. § 1030)
  - "Protected computer" is a computer "which is used in or affecting interstate or foreign commerce or communication . . ."
  - Provides for criminal penalties and civil actions related to unauthorized access of computers and theft of information
  - Controversial with privacy advocates and has been amended several times since its initial passage in 1986
  - DOJ manual: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

The Current Legal Landscape: Federal laws (cont'd)

- Electronic Communications Privacy Act (18 U.S.C. § 2510)
  - Protects electronic communications and applies various degrees of protection based on perceived privacy interests
  - DOJ manual: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf
- Health Insurance Portability and Accountability Act (Pub. L. No. 104-191)
  - Together with the HITECH Act, HIPAA governs the collection, use, and disclosure of protected health information
- Children's Online Privacy Act (15 U.S.C. § 6501)
  - Imposes certain requirements on collection of data from children under 13

The Current Legal Landscape: State Laws

- States are increasingly passing laws that impose disclosure and design requirements on electronic devices that collect personal data, including IoT devices.
- For example, according to NCSL, at least 32 states have enacted laws that require governments and businesses to dispose of personal information data.
  - http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx

The Future Legal Landscape: Proposed Legislation

- S.1691: Internet of Things Cybersecurity Improvement Act of 2017
  - "To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies."
  - Requires devices to:
    - Be patchable
    - Not contain known vulnerabilities
    - Rely on industry-standard protocols
    - Not contain hard-coded passwords
- California SB-327: Requires IoT devices to be equipped with "reasonable security features"

Federal Enforcement and Guidance

- Enforcement is still nascent.
  - For example, the FTC has brought enforcement actions against ASUS and D-Link under (15 U.S.C. § 45(a)) for inadequate security of IoT devices and online services.
    - In the Matter of ASUSTeK Computer, Inc.
      - Violations of Section 4 of the FTC Act
      - Consent order
    - FTC v. D-Link Corporation and D-Link Systems, Inc.
      - Violations of Section 5 of the FTC Act
      - Dismissed on D-Link motion

Federal Enforcement and Guidance (cont'd)

- Federal agency guidance is increasing but not coordinated.
  - FTC
    - Staff Report, Internet of Things, Privacy and Security in a Connected World (January 2015)
    - Public Comment on NIST "Communicating IoT Security Update Capability to Improve Transparency for Consumers" Working Group (2017)
    - IoT Home Inspector Challenge (82 FR 840, 2017)
  - FDA
    - Design Considerations and Premarket Submission Recommendations for Interoperable Medical Devices (2017, 82 FR 42101)

QUESTIONS?

Thank you!

Seth Greenstein

sgreenstein@constantinecannon.com

David Golden

dgolden@constantinecannon.com