Drinker Biddle

Law, Policy, and the Internet of Things -- What You Need To Know

Jason R. Baron
Of Counsel
Bennett B. Borden
Partner & Chief Data Scientist
Laura H. Phillips
Partner
Drinker Biddle & Reath LLP
Washington, D.C.

Overview

- An overview of the IoT world, 2017 & beyond
- The IoT's infrastructure and networks that have to be in place to support the IoT
- IoT and E-discovery
- Government oversight of the IoT: a patchwork of laws and regs
- Emerging IoT case law & regulatory actions
- Providing advice to clients on the use of analytics collected from the IoT, including ethical questions that arise

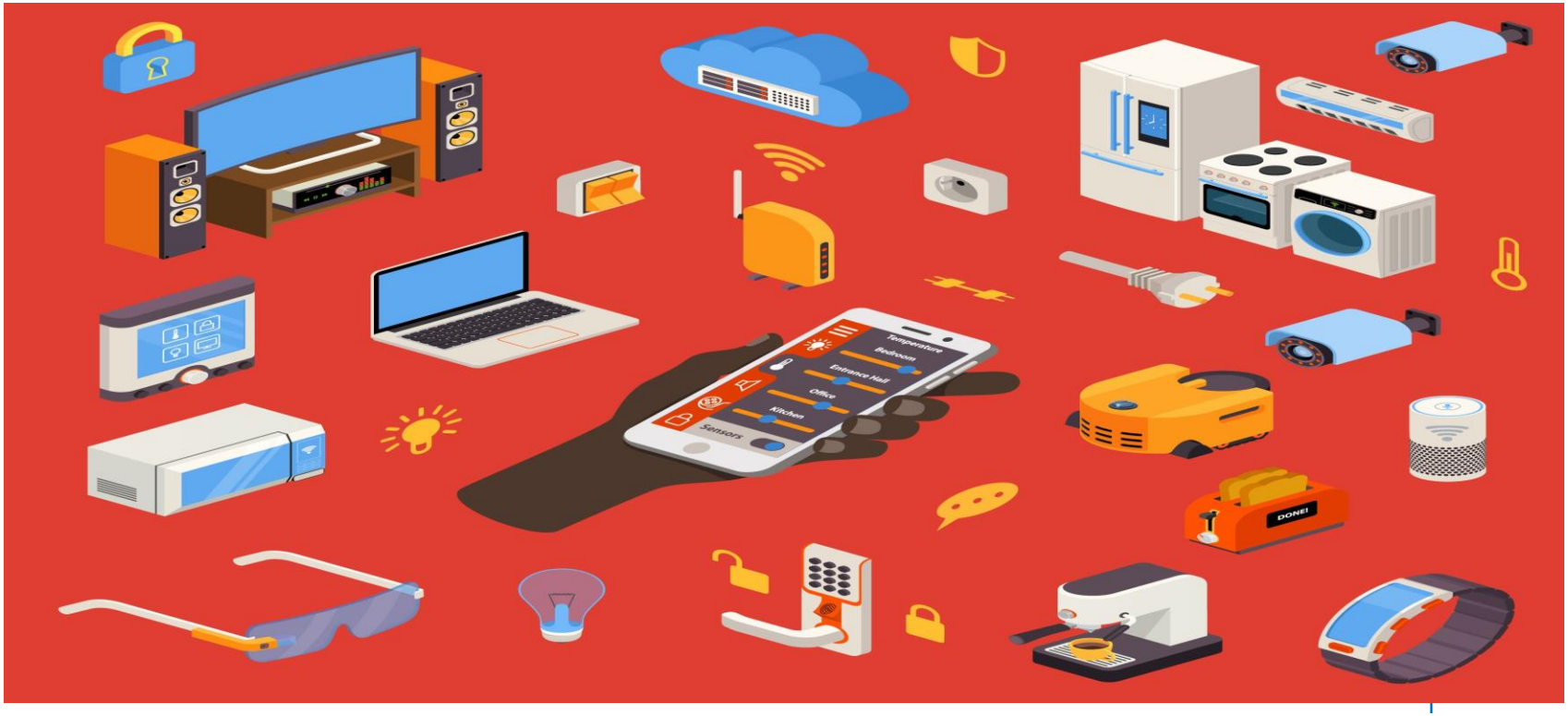
Internet of Things: Definition

- “The term Internet of Things generally refers to scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention. There is, however, no single, universal definition.”

Source: Internet Society, http://www.internetsociety.org/doc/iot-overview?gclid=EAIaIQobChMIp4XHtNG-1QIVAglpCh3j7AjDEAAYAyAAEgLin_D_BwE

First Use of Term IoT

- The term "the Internet of Things" was coined by Kevin Ashton of Procter & Gamble, later at MIT's Auto-ID Center, in 1999.



Scope of IoT

IoT scope

- Smart parking
- On-board diagnostic systems
- Sharing information on the road
- ...

- Smart farming
- Preparing the soil
- Monitoring optimal conditions for planting
- ...

- Smart bulbs
- Smart domotic systems
- ...

- Payment & ticketing
- Information exchange
- Location services
- ...

- Smart clothes (Wearables)
- Smart appliances
- Relaxing time
- ...

- Environmental monitoring
- Energy management
- Security services
- ...

- Activity trackers
- Biomedical sensors
- Diseases monitoring
- ...

Source: https://image.slidesharecdn.com/presentacininglesmayo2015nngeneric-150629150942-lva1-app6892/95/internet-of-things-definition-of-a-concept-11-638.jpg?cb=1435590651

3 Waves of IoT

Origin & Definition: Internet Of Things

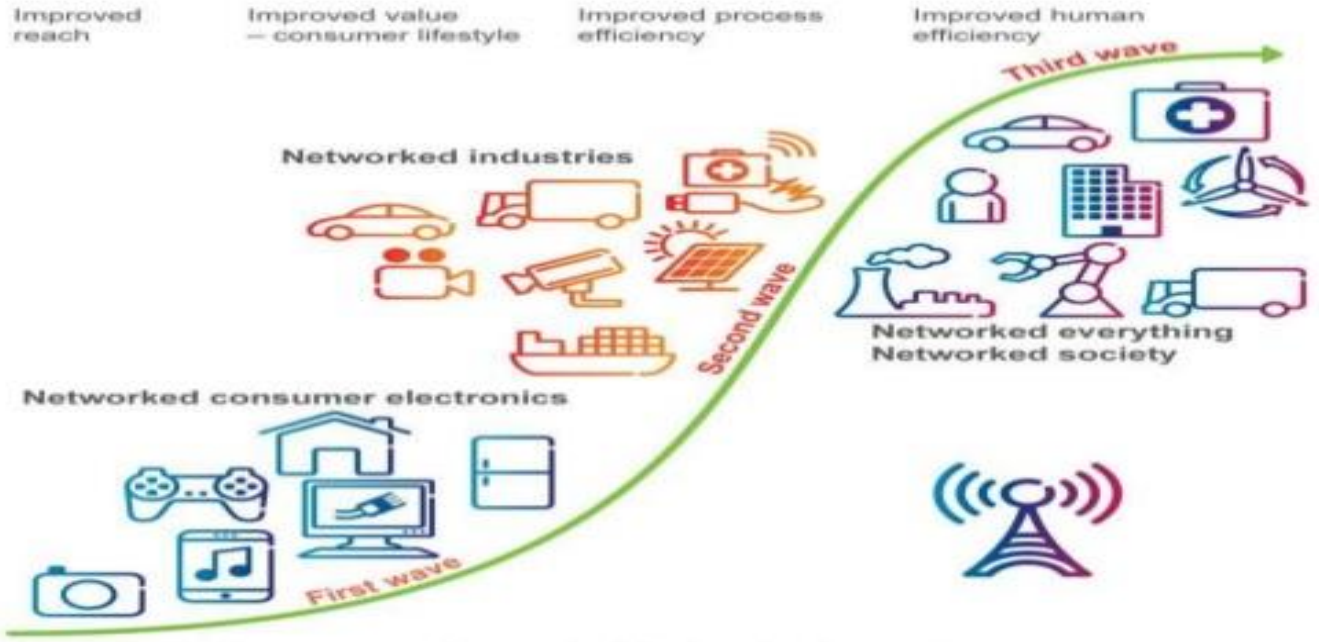
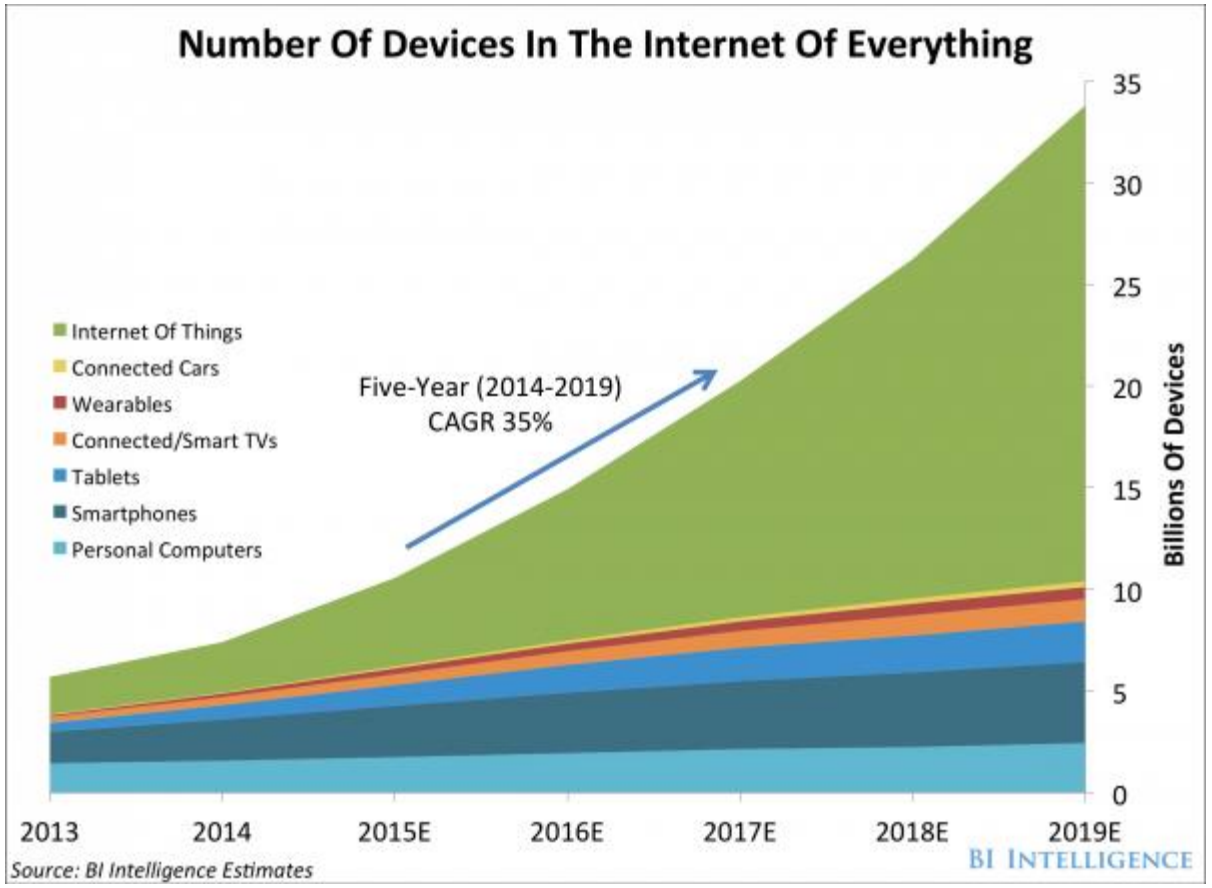


Figure 2. The three waves of connected device development.

Growth of IoT



Quotes on IoT device growth

- Gartner: 21 billion IoT devices to invade by 2020

  Source: http://www.gartner.com/newsroom/id/3165317

- "According to a new update to the International Data Corporation (IDC) *Worldwide Semiannual Internet of Things Spending Guide*, global IoT spending will experience a compound annual growth rate (CAGR) of 15.6% over the 2015-2020 forecast period, reaching $1.29 trillion in 2020."

  - Source: http://www.businesswire.com/news/home/20170104005270/en/Internet-Spending-Forecast-Grow-17.9-2016-Led

The IoT's infrastructure: networks and devices

Facilities and Networks That Have to be in Place to Support the IoT

- **Internet of Things:** A network of internet-connected objects able to collect and exchange data using embedded sensors.
- **Internet of Things device:** Any stand-alone internet-connected device that can be monitored and/or controlled from a remote location.
- **Internet of Things ecosystem:** All the components that enable businesses, governments, and consumers to connect to their IoT devices, including remotes, dashboards, networks, gateways, analytics, data storage, and security.
- **Entity:** Includes businesses, governments, and consumers.
- **Physical layer:** The hardware that makes an IoT device, including sensors and networking gear.
- **Network layer:** Responsible for transmitting the data collected by the physical layer to different devices.
- **Application layer:** This includes the protocols and interfaces that devices use to identify and communicate with each other.
- **Remotes:** Enable entities that utilize IoT devices to connect with and control them using a dashboard, such as a mobile application. They include smartphones, tablets, PCs, smartwatches, connected TVs, and nontraditional remotes.
- **Dashboard:** Displays information about the IoT ecosystem to users and enables them to control their IoT ecosystem. It is generally housed on a remote.
- **Analytics:** Software systems that analyze the data generated by IoT devices. The analysis can be used for a variety of scenarios, such as predictive maintenance.
- **Data storage:** Where data from IoT devices is stored.
- **Networks:** The internet communication layer that enables the entity to communicate with their device, and sometimes enables devices to communicate with each other.

Source: From “Business Insider” (Dec 19, 2016): http://www.businessinsider.com/what-is-the-internet-of-things-definition-2016-8?IR=T

Much of IoT's Value Derives from Massive Connection of Devices

- In the US, private companies build and maintain wired and wireless infrastructure. Physical infrastructure is a precondition of connection.
- Private investment depends upon commercialization use cases.
- The business case for massive, ubiquitous IoT is not fully developed. Carriers need to maintain integrity of their networks.
- Devices range from smartphones to small, passive RFID devices. Other devices that may operate in highly decentralized manners, or in industrial settings.
- The FCC has RF equipment certification requirements that can be implicated by importing or marketing of these devices.

U.S. Communications Networks and IoT

- Wired Infrastructure for IoT
  - Commercial co-axial cable and fiber (Traditionally cable companies)
  - Telephone company twisted pair (Telephone companies pushing fiber closer to landline consumers for other purposes – Verizon Fios)
  - Evolving to IP, broadband infrastructure (where available) would allow IoT connectivity at minimal, incremental cost
  - However, wired infrastructure is not everywhere; there have to be simple, inexpensive means of providing “last inch” or “last meter” connectivity.

US Communications Networks and IoT

- Wireless Infrastructure – It's all about the Spectrum
  - Licensed Cellular – in U.S., data on cellular networks is typically 4G LTE; carriers are working on standardizing and rolling out 5G. The FCC is looking at millimeter wave and mid-band spectrum for 5G.
  - Unlicensed spectrum – no expectation of protection from interference; spectrum commons model.
  - Shared spectrum – many proposed models for co-existence; each community somewhat wary of the other.
  - Satellite
    - Cost of transport and latency, power of IoT device suggest that high earth orbit satellites may not be the way to support IoT.
    - FCC considering proposals to license low earth orbit very small non-geostationary satellites that could be better suited for some applications.

Communications Networks and IoT

- Vulnerabilities can arise from a lack of coordination or stated policy.
- The FCC's Notice of Inquiry on the security of 5G networks was withdrawn by the Republican FCC Chairman.
  - *FCC's main role is with equipment certification and as the agency allocating non-government spectrum; policing interference issues*
- NTIA stakeholder process on updating security of IoT devices and other software updates has made some recommendations.
- Senate just passed the DIGIT Act which would require cross agency coordination on security threats.

IoT and e-Discovery

What Does IoT Mean for e-Discovery?

- Today's reality: constant creation of new data sources
  - Cybersecurity implications
  - IoT data as evidence
  - Future proofing your e-discovery process

Preservation of IoT Data

This is particularly tricky:

- IoT Data can be ephemeral
- IoT Data can be voluminous
- Separating IoT data into that which is relevant to a particular claim or defense can be difficult if you don't build advanced search capabilities into the system.

Producing IoT Data

- IoT Data is often stored in structured databases
- Design search and export capabilities into the system (or not…)
- This is where the concept of "proportionality" in the Federal Rules of Civil Procedure can come into play.

> - Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense **and proportional** to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.

See FRCP 26(b)(1) (as amended in 2015) (emphasis added)

Discovery of IoT Software

- As with any software, discovery of IoT software is challenging and usually requires a great deal of negotiation.
- Discovery of predictive algorithms and algorithmic outcomes is especially difficult.
- Experts are usually required.

Government Oversight of the IoT

Examples of the IoT Statutory Patchwork in the U.S.

- The current legal framework covers a wide variety of information that can be connected to the IoT:
  - the Health Insurance Portability and Accountability Act of 1996 (HIPAA),
  - the Fair Credit Reporting Act of 1970 (FCRA),
  - the Family Educational Rights and Privacy Act of 1974 (FERAA),
  - the Right to Financial Privacy Act of 1978 (RFPA),
  - the Children's Online Privacy Protection Act of 1998 (COPPA)
  - the Freedom of Information Act (FOIA) both protects sensitive private information and guarantees public access to government data.

An IoT Regulatory Patchwork

- No current regulations (at least in the U.S.) specifically address the IoT holistically
  - The FTC protects consumers
  - The FDA regulates medical devices
  - The FCC regulates radio, wire, satellite and cable communications.
  - The FAA regulates flight safety
  - Etc.

Dep't of Energy Smart Grid Reporting

- Section 1302 of the Energy Independence and Security Act of 2007, 42 USC 17382, directs the Secretary of Energy, through the Assistant Secretary of the Office of Electricity Delivery and Energy Reliability, to

> "…report to Congress concerning the status of smart grid deployments nationwide and any regulatory or government barriers to continued deployment. The report shall provide the current status and prospects of smart grid development, including information on technology penetration, communications network capabilities, costs, and obstacles. It may include recommendations for State and Federal policies or actions helpful to facilitate the transition to a smart grid."

Emerging Case Law & Regulatory Actions

Fitbit Caselaw

- Personal injury case in Calgary relying on FitBit data to establish that a person's mobility and quality of life has been impacted. Counsel stated he would use his client's FitBit data and compare it to data of the general population for her age and profession to show that she deserves compensation. The plaintiff's attorney did not subpoena FitBit directly, but rather, Vivametrica, an open source data analytics platform that collects data from smartphones and wearable fitness devices (with user consent) to analyze and identify health trends.
- Sources: https://www.theatlantic.com/technology/archive/2014/11/when-fitbit-is-the-expert-witness/382936/

  http://www.canadianlawyermag.com/5450/Data-fit-for-the-courtroom.html
- Connecticut murder case where IoT devices in the home and on the murder victim led police to arrest the victim's husband
- Source: https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-silent-witness.html
- Criminal case where prosecutors used Fitbit data as evidence disproving rape allegations.

Source*: See* Jacob Gershman, *Prosecutors Say Fitbit Device Exposed Fibbing in Rape Case*, Wall St. J. Blog (Apr. 21, 2016, 1:53 PM), http://blogs.wsj.com/law/2016/04/21/prosecutors-say-fitbit-device-exposed-fibbing-in-rape-case/ https://perma.cc/6DNV-NTL4]

See generally K. Saphner, "You Should Be Free to Talk the Talk and Walk the Walk: Applying *Riley v. California* To Smart Activity Trackers," 100 Minn. L. Rev. 1689 (2016)

Examples of Other IoT-Related Caselaw (Present and Future)…

- Murder case where detectives were seeking recordings from Amazon Echo device
- https://www.nytimes.com/2016/12/28/business/amazon-echo-murder-case-arkansas.html?action=click&contentCollection=N.Y.%20%2F%20Region&module=RelatedCoverage&region=Marginalia&pgtype=article
- Ingenious lightbulb hack can cause seizures, spy on “air-gapped” networks
- https://www.forbes.com/sites/thomasbrewster/2016/04/01/philips-lightbulb-hack-epileptic-seizures-data-theft/#5bd622f078de
- St. Jude Medical brings false advertising & conspiracy case against MedSec holdings, alleged to have disseminated misleading information about security weaknesses of pacemakers
- http://media.sjm.com/newsroom/news-releases/news-releases-details/2016/St-Jude-Medical-Brings-Legal-Action-Against-Muddy-Waters-and-MedSec/default.aspx
- Maker of smart vibrators settles data collection lawsuit for $3.75 million
- https://www.nytimes.com/2017/03/14/technology/we-vibe-vibrator-lawsuit-spying.html
- “Flood of lawsuits may define IoT cybersecurity standards”
- https://www.cyberscoop.com/lawsuits-iot-cybersecurity-standards/

FTC v D-LINK Corporation et al., No. 3:17-CV-00039-JD (N.D. Cal.)

In January 2017, the Federal Trade Commission filed a complaint in federal court against D Link Corporation, a global manufacturer of computer networking equipment and other connected devices such as IP cameras and baby monitors, alleging that the company made deceptive claims about the security of its products and engaged in unfair practices that put consumers' privacy at risk.

Examples identified by the FTC where D-Link allegedly failed to take reasonable steps to address well-known and easily preventable security flaws include:

- Hard-coding login credentials into D-Link camera software that could allow unauthorized access to cameras' live feed;
- Leaving users' login credentials for its mobile app unsecured in clear, readable text on consumers' devices;
- Mishandling its own private key code used to sign into D-Link software and as a result, it was publicly available online for six months; and
- Failing to take reasonable steps to prevent command injection, a known vulnerability that lets attackers take control of people's routers and send them unauthorized commands.

See press release from the FTC: https://www.ftc.gov/news-events/blogs/business-blog/2017/01/d-link-case-alleges-inadequate-internet-things-security

See Complaint : https://ftc.gov/enforcement/cases-proceedings/132-3157/d-link

Although the FTC ultimately dismissed the claims against D Link as part of a settlement, D Link is still required to respond to discovery requests from the FTC as though it is a party.

A copy of the dismissal is available here:
https://www.ftc.gov/system/files/documents/cases/2017.05.15_d.e._75_order_dismissing_dlc_wo_prej._and_req_disc.pdf

In re TRENDnet, Inc., Docket No. C-4426 (FTC)

- FTC applied Section 5 of the Federal Trade Commission Act to smart devices.
- TRENDnet: a networking hardware company, incorporated in California.
- The company's surveillance gadgets, like cloud cameras, were sold for home use.
- The FTC alleged that TRENDnet's 20 IP camera products failed to provide reasonable and appropriate measures to secure the live feeds from the IP cameras from hackers' unauthorized access to sensitive information at home; and that the camera software was also flawed, with malfunctioning login credentials and privacy settings. As a result, a hacker posted approximately 700 cameras' IP addresses obtained from the company's website. Those cameras were broadcasting daily activities from the home user's IP cameras. Nonetheless, without proper notice to consumers, TRENDnet falsely represented their products as reasonably secure.

Ashley Archer-Hayes et al. v. Toytalk Inc. et al. ("Hello Barbie" case), Case No. BC603467 (Sup. Ct. Cal.)

- In December 2015, a group of plaintiffs brought a class action against Mattel and the other makers of "Hello Barbie," an interactive product that makes recordings of a child's conversation when it plays with the doll. Among other claims, plaintiffs allege that because the doll cannot distinguish between children whose parents have registered and consented to recordings and children whose parents have not consented, it is making, storing and using recordings of unregistered children's conversations in violation of the Children's Online Privacy Protection Act ("COPPA").

Some Observations About the IoT, Analytics, and Ethics

Issues Specific to the IoT

- Granular information about human conduct
- What is considered societally advantageous
  - Right good/service; right person; right time; right price
- But…a misfit with current legal and regulatory regimes
  - What does ‘ownership’ mean in an IoT world?
  - The failure of notice and consent regimes, especially in IoT

How Do We Decide Who Gets What in an IoT World

- Street Repair
- Snow and Trash Removal
- Electricity Distribution
- Health Care Resources
- And many many more….

Electronic Home Assistants

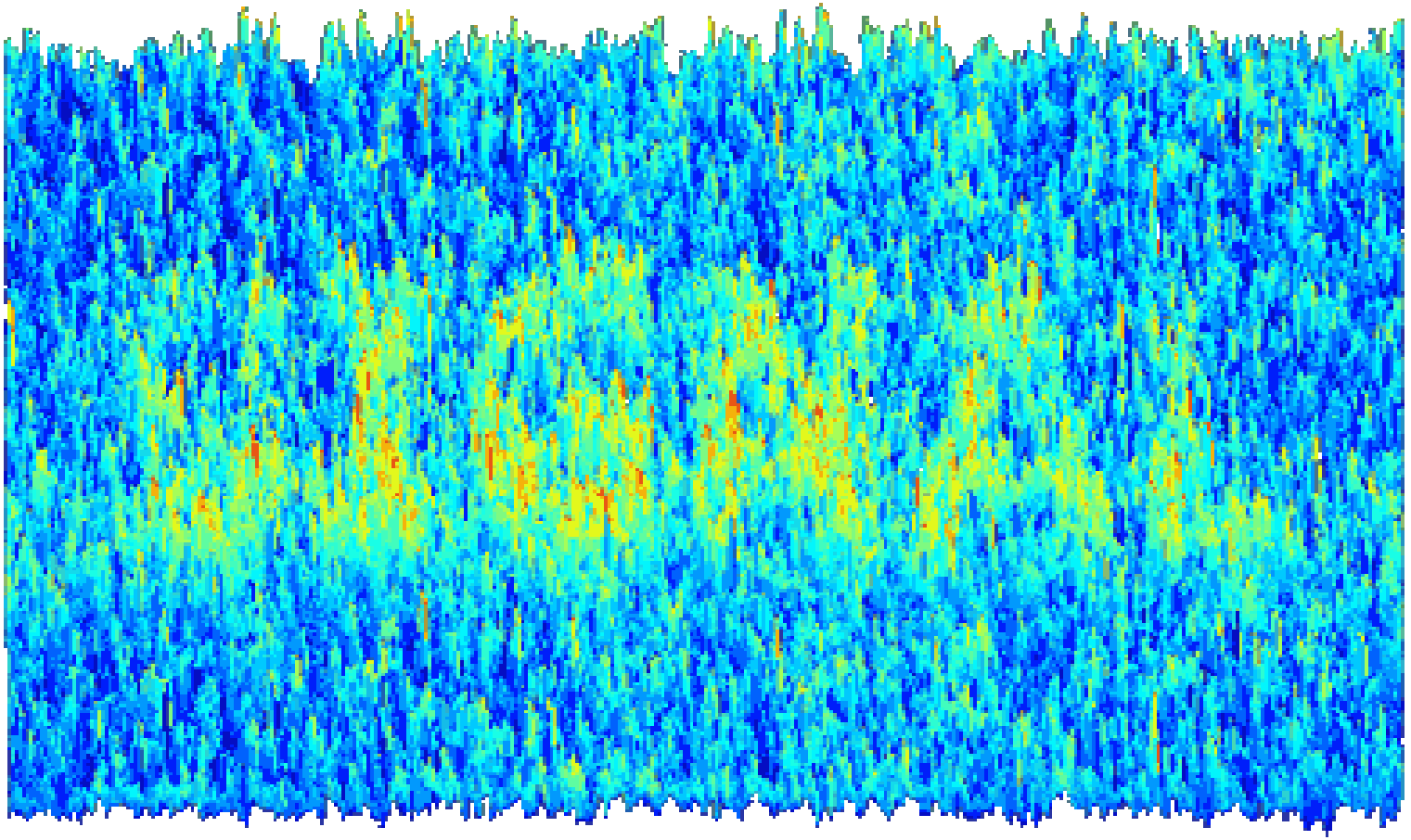
Toys or … Something Else

- Corporate understanding of the risks being created and acting reasonably to mitigate them

The Path Forward for IoT & the Law

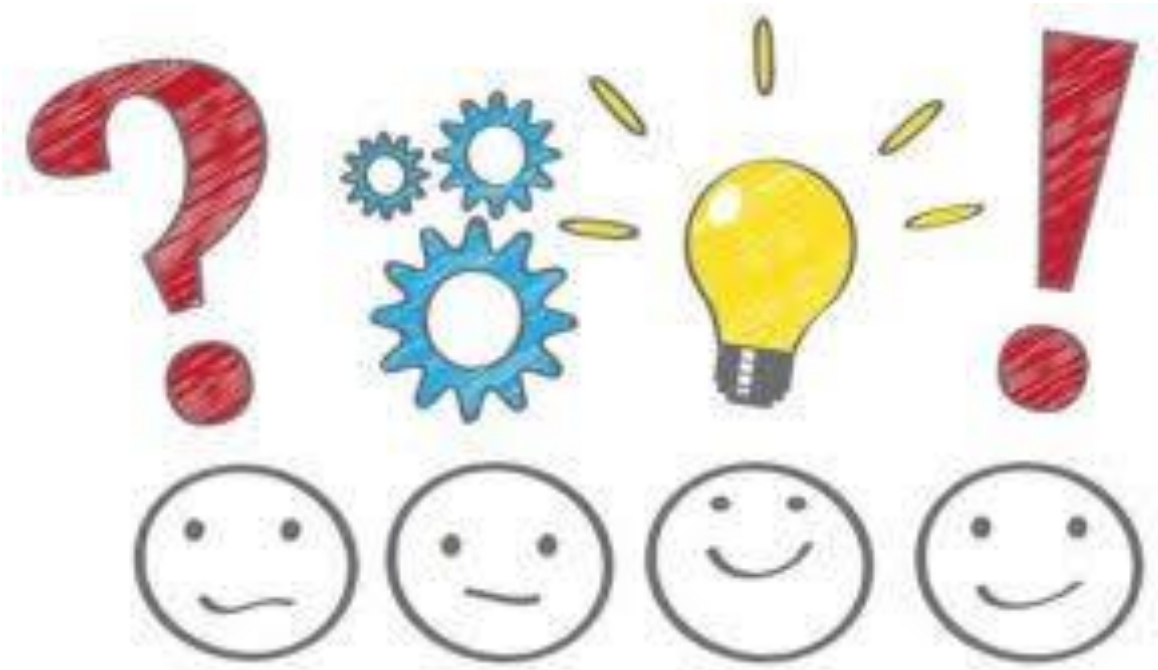
- The law is based upon reasonable conduct
- Identify and quantify risks in analytics projects
- Identify and implement migration strategies
- Include a diversity of opinion

Signal & Noise



Don’t Become Extinct

Final Thoughts and Questions



Contact Information

- Jason R. Baron, Of Counsel, Drinker Biddle
  - jason.baron@dbr.com
- Bennett B. Borden, Partner & Chief Data Scientist, Drinker Biddle
  - Bennett.Borden@dbr.com
- Laura H. Phillips, Partner, Drinker Biddle
  - laura.phillips@dbr.com