Discussion papers

• Elaine Mcardlle, The New Age of Surveillance, Harvard Law Today
  http://today.law.harvard.edu/feature/new-age-surveillance/

• Berkman Klein Center, Don’t Panic: Making progress on the `going dark’ debate,
  https://cyber.harvard.edu/pubrelease/dont-panic/


• Seymour Hersch, The Online Threat”, The New Yorker, 2010
Big Picture: trade-offs

Security

Privacy

Surveillance
The Apple-F.B.I. Case

Apple's New Challenge: Learning How the U.S. Cracked Its iPhone
The company lacks information on the method used to break into the iPhone of a gunman in San Bernardino, Calif.

March 29, 2016 • By KATIE BENNER, JOHN MARKOFF and NICOLE PERLROTH

U.S. Says It Has Unlocked iPhone Without Apple
The Justice Department announcement, in a court filing, ends an immediate legal battle over the San Bernardino shooting case but raises questions about Apple’s security.

March 28, 2016 • By KATIE BENNER and ERIC LICHTBLAUV

American Tech Giants Face Fight in Europe Over Encrypted Data
As Apple battles the F.B.I. over “unlocking” an iPhone, European governments are pushing for greater access to people’s digital lives.

March 27, 2016 • By MARK SCOTT

In Apple Debate on Digital Privacy and the iPhone, Questions Still Remain
It is unclear what will happen the next time the government tries to force Apple to break into one of its own phones.

March 28, 2016 • By ERIC LICHTBLAUV
Tension between privacy and security (ii)

British Prime Minister Suggests Banning Some Online Messaging Apps

By MARK SCOTT  JANUARY 12, 2015 1:27 PM  97

LONDON — Popular messaging services like Snapchat and WhatsApp are in the

Encrypted Messaging Apps Face New Scrutiny Over Possible Role in Paris Attacks

By DAVID E. SANGER and NICOLE PERLROTH  NOV. 16, 2015

WASHINGTON — American and French officials say there is still no definitive evidence to back up their presumption that the terrorists who massacred 129 people in Paris used new, difficult-to-crack encryption technologies to organize the plot.
The move thrusts WhatsApp further into a standoff between tech companies and law enforcement officials over access to digital data, one that pits Silicon Valley’s civil libertarian ideals against the federal government’s concerns over national security. Increased encryption will make it more difficult, if not impossible, for the authorities to intercept WhatsApp communications for investigations.

TECHNOLOGY

**WhatsApp Is Briefly Shut Down in Brazil for a Third Time**

By VINOD SREEHARSHA   JULY 19, 2016

A driver checking WhatsApp in São Paulo, Brazil. A state criminal court sought to punish WhatsApp for not handing over data requested by authorities as part of a criminal investigation. Andre Penner/Associated Press
The Internet of Things and Networked Sensors Open Uncharted Paths to Surveillance

A plethora of networked sensors are now embedded in everyday objects. These are prime mechanisms for surveillance: alternative vectors for information-gathering that could more than fill many of the gaps left behind by sources that have gone dark – so much so that they raise troubling questions about how exposed to eavesdropping the general public is poised to become. To paint an overall picture of going dark
Governance Challenges for the Internet of Things

• By 2025, the estimated number of connected devices should reach 100 billion;
• Privacy, security, and safety fears grow as the IoT creates conditions for increasing surveillance by governments and corporations.
• Fundamental question is: will the IoT be good for the many, or the mighty few?
• Very few articles on IoT governance;
• Two studies have shed light on challenges for the future with the IoT.
  – In 2013, the European Commission (EC) published a study focusing on relevant aspects for possible IoT governance regimes.
IoT: risks for citizens and customers

- Historically, innovation has caused the privacy and data protection regulatory framework to reinvent itself each time there was a major change in the quantity of personal data possible to be processed.
- In the IoT, where objects interact between themselves without requiring human commands, people are also affected.
- The availability of devices and sensors in an environment can drastically increase the amount of personal data being gathered.
- IoT contributes to blurring the boundaries between a “physical world” and cyberspace, in the sense that many actions we perform will be monitored, recorded, and used.
- The negative impact of IoT on society may be aggravated as data from sensors are used together with personal data already available, and foster a number of correlations and data crossings that can performed without any kind of control (e.g., techniques of re-identification of anonymized data).
Four principles that we can use to construct rules and norms for deploying IoT applications:

- notice and choice(*);
- data minimization;
- access to personal data;
- accountability.

Widespread agreement on the need for companies manufacturing IoT devices to incorporate reasonable security into these devices.

Rigorous security validity checks, authentication procedures, and data verification will be part of the foundation of IoT applications.

The inclusion of the manufacturers in the IoT regulation process depends on a global view that includes not only IoT norms and rules but also the privacy governance process in cyberspace.

(*) the Federal Trade Commission (FTC), advocates the fundamental privacy principle of "notice and choice." That is, companies must inform consumers how they plan to use and share their data, and give consumers choices about the use and sharing.

Cyberspace Governance, Harvard 2016
Role of Governance in IoT (i)

• A classical definition for Internet governance is the development and application by governments, the private sector, and civil society (in their respective roles) of shared principles, norms, rules, decision-making procedures, and programs that shape the Internet’s evolution and use.

• Does IoT need new governance mechanisms?

• Several IoT problems (such as security, interoperability standards, and protocols) might have solutions through the implementation of governance mechanisms, as occurs with the general Internet.

• A path to the future is to broaden the discussion around IOT governance, involving multistakeholder groups, in order to represent multiple views on IoT problems and issues.
Role of Governance in IoT (ii)

- The nature of privacy and security problems frequently associated with the IoT indicates that further research, analysis, and discussion are needed to identify possible solutions.
- The introduction of security and privacy elements in the very design of sensors, implementing Privacy by Design, must be taken into account for outcomes such as the homologation process of sensors by competent authorities.
- Concrete means to set limits on the amount or nature of the personal data collected should be developed.
- Citizens must have means to take measures to protect their rights whenever necessary.
- As with other technologies that aim to change human life, the IoT must be in all respects designed with people as its central focus. Privacy and ethics should be part of the technology’s agenda.

- **IoT governance & surveillance: opportunity for a research work (paper)**

Cyberspace Governance, Harvard 2016
References


• YA De Montjoye, L Radaelli, VK Singh, Unique in the shopping mall: On the re-identifiability of credit card metadata, Science Vol. 347, Issue 6221,


• Virgilio Almeida, Doneda, Danilo and Marilia Monteiro, Governance Challenges for the Internet of Things, IEEE Internet Computing, vol. 19, no. 4, 2015
THANKS!

Valmeida@cyber.law.harvard.edu