Data Governance Challenges: Earning Trust with Users, Customers and Governments Around the World
Fujitsu Laboratories Advanced Technology Symposium 2019

Daniel J. Weitzner weitzner@mit.edu, MIT IPRI Founding Director
$3T+/3B Person-enabling Internet Policy success

- ACLU v Reno
- $813B
- $470B
- $934B
- $1051B
- $230
- $?B
- No Back Doors

<table>
<thead>
<tr>
<th>Company</th>
<th>Market Cap</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>$813B</td>
</tr>
<tr>
<td>Facebook</td>
<td>$470B</td>
</tr>
<tr>
<td>Amazon</td>
<td>$934B</td>
</tr>
<tr>
<td>Apple</td>
<td>$1051B</td>
</tr>
<tr>
<td>YouTube</td>
<td>$230</td>
</tr>
<tr>
<td>iOS</td>
<td>$?B</td>
</tr>
</tbody>
</table>
Major challenges lie ahead

- Autonomous Vehicles
- AI, Automated Decision-making & Fairness
- Global Privacy Norms & Regulatory Models
- IOT Security
- HomeKit

- $763B
- $522B
- $744B
- $896B
- $X \times 211M$ units
- $230$
Future of Privacy and Data Governance

A.I. and Privacy Concerns Get White House to Embrace Global Cooperation

By Steve Lohr

April 3, 2019

Two hallmarks of American economic policy under President Trump are a reflexive aversion for regulation and go-it-alone nationalism.

But in technology policy, that stance is changing.

In September, the Trump administration abandoned its hands-off approach and began working closely with the 36-nation Organization for Economic Cooperation and Development to create international guidelines for the design and use of artificial intelligence.
Modern Data Governance Challenges & The Risk of Regulatory Failure

*Cybersecurity*: Measuring, managing and insuring against risk

*Privacy*: Unlocking value in personal data while being accountable to legal and ethical guidelines

*Trustworthy AI*: Building public and market trust in new AI technologies
Case Study: Managing Cybersecurity Risk
“The threat of cyber security may very well be the biggest threat to the U.S. financial system...[W]e spend nearly $600 million a year on these efforts and have more than 3,000 employees deployed to this mission... But the financial system is interconnected, and adversaries are smart and relentless–so we must continue to be vigilant.”

Jamie Dimon, Annual Letter to Shareholders (April 2019)
Core economic infrastructure may not be sufficiently protected against cyber attacks

MIT study reveals inconsistent protection and inability to measure risk in critical sectors: Electricity, Finance, Communications and Oil/Gas.

New research agenda - cross-sector risk measurement
Measuring cybersecurity risk using MPC

- **Problem:** Companies are unwilling to share sensitive information about cyber attacks that could lead to market/legal/regulatory repercussions against their firm.

- **Result:** We have a limited understanding of true cybersecurity risk and how to defend.

- **Solution:** Tools that can perform calculations over encrypted data - evaluating risk with data from firms to compute market trends without disclosing their sensitive data. [Lo, Vaikuntanathan, Reynolds, Weitzner]

Firms are using the platform and are willing to share sensitive information about how they defend their networks for the first time.
Encryption and surveillance

Apple encryption debate after San Bernardino terrorist attack - IPRI contribution to policy conversation:

Impact: Consensus shifts away from mandatory back doors

UK GCHQ Director Robert Hannigan:
The solution is not, of course, that encryption should be weakened, let alone banned. But neither is it true that nothing can be done without weakening encryption. *I am not in favour of banning encryption just to avoid doubt. Nor am I asking for mandatory backdoors.*

US Secretary of Defense Ash Carter: There will not be some simple, overall technical solution—a so-called 'back door' that does it all…. *I’m not a believer in backdoors or a single technical approach. I don’t think that’s realistic.*

European Commission Vice-President Anders Ansip: “*How will people trust the results of the election if they know that the government has a back door into the technology used to collect citizen’s votes?*”

US House of Representatives Encryption Working Group: Cryptography experts and information security professionals believe that it is *exceedingly difficult and impractical, if not impossible, to devise and implement a system that gives law enforcement exceptional access to encrypted data without also compromising security against hackers, industrial spies, and other malicious actors.*
Future of Cybersecurity

Australia’s encryption-busting law is ‘flawed,’ says tech industry

The Assistance and Access Bill 2018 has huge implications for cybersecurity, but tech companies and experts say it’s not worth the risk.

By Juniper | Dec 7, 2018, 1:10pm EST

Barr Revives Encryption Debate, Calling on Tech Firms to Allow for Law Enforcement

The attorney general, reopening the conversation on security vs. privacy, said that encryption and other measures effectively turned devices into “law-free zones.”

Attorney General William P. Barr’s address at a cybersecurity conference in New York on Tuesday was his first significant speech on “going dark.” Richard Drew/Associated Press

Australia just passed tough new legislation that requires tech companies to hand over user data when requested by law enforcement, even if that means building a backdoor into their encryption. The decision has huge implications for communications companies, not just in Australia but also across the rest of the world.

Technology giant Microsoft has warned that the Morrison government’s harming Australia’s international reputation as a trusted destination.

As chief legal officer, said foreign companies and governments wereng their data to Australia after the Assistance and Access Bill, whichsed powers to access the encrypted data of suspects, was rushedined into law late last year.

By Katie Benner

July 23, 2019
Case Study: Unlocking Value in Personal Data
Privacy Today: Stuck with a Brittle Option Set

TRUST US

GIFTS ‘N THINGS, INC. is committed to protecting your privacy. We will not collect any personal information about you when you visit our Internet site (other than the standard information automatically collected and stored in the Web server’s logs) unless you choose to provide it to us.
Does privacy mean being alone?

“The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness….They conferred, as against the government, the right to be let alone - the most comprehensive of rights and the right most valued by civilized men.”

Or, working together?

This Court has recognized the vital relationship between freedom to associate and privacy in one's associations. Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.

NAACP v. Patterson - 357 U.S. 449 (1958)
Privacy Challenge: The Facebook Explosion
Governance failure Mode: out-of-context use of data

Cambridge Analytica
MyDigitalSelf (research)
270k users
(commercial/political advertising)
87M users

No tools to manage purposes associated with personal data
## Implementing Privacy: policy and tech challenges - unsolved problems

<table>
<thead>
<tr>
<th>GDPR</th>
<th>Cal. Consumer Privacy Act</th>
<th>Apple proposal</th>
<th>Consumer Privacy Bill of Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lawful basis - Consent, etc.</td>
<td>Right to opt out of sale</td>
<td>Right to know</td>
<td>Purpose limitation enforcement</td>
</tr>
<tr>
<td>legitimate interest, etc</td>
<td>Right to know</td>
<td>Right to know</td>
<td>Right to respect for context</td>
</tr>
<tr>
<td>Right to be informed</td>
<td>Right to know</td>
<td>Right to know</td>
<td>Right to transparency</td>
</tr>
<tr>
<td>Right of access</td>
<td>Right to access</td>
<td>Right to access</td>
<td>Right to access</td>
</tr>
<tr>
<td>Right to rectification</td>
<td></td>
<td></td>
<td>Right to accuracy</td>
</tr>
<tr>
<td>Right to erasure (to be forgotten)</td>
<td>Right to have data deleted</td>
<td>Right to have data deleted</td>
<td>Right to accuracy</td>
</tr>
<tr>
<td>Right to restrict processing</td>
<td>No discrimination for exercise</td>
<td>Right to minimization</td>
<td></td>
</tr>
<tr>
<td>Right to portability</td>
<td></td>
<td>Right to minimization</td>
<td>Machine-readable formats</td>
</tr>
<tr>
<td>Right to object</td>
<td></td>
<td></td>
<td>Right to correction</td>
</tr>
<tr>
<td>Right to avoid automated decisionmaking &amp; explanation</td>
<td></td>
<td></td>
<td>Right to correction</td>
</tr>
<tr>
<td>Data Breach Notification</td>
<td>Right to security</td>
<td>Security &amp; Breach Notification</td>
<td></td>
</tr>
<tr>
<td>Fines &lt; 4% annual revenue</td>
<td>$7500/incident, 30 day cure</td>
<td>Fines</td>
<td></td>
</tr>
</tbody>
</table>

---

**Internet Policy Research Initiative**
Massachusetts Institute of Technology

---

**Graph privacy**

**Hard Delete**

**Effective Notice - HCI/UX**

**ML explanation**

---

**Purpose limitation enforcement**
Data governance challenge: realize value of data while respecting privacy (ie. purpose limits)
Traditional approach: access control

- Fitness intensity
- Driving Style
- Location
- Daily Fitness

Data Integration API

Service Developers &
Data Scientists

Targeted Advertising

Wellness Service
Modern governance: manage use and purpose

Stonebraker, M., Brodie, M., Kraska, T., Servan-Schreiber, S., Weitzner, D. J., Schengen: A Data Protection Database., VLBD Workshop Poly’19 (forthcoming)
Case Study: Toward Trusted Artificial Intelligence
Face Recognition
Early services fail to perform consistently

<table>
<thead>
<tr>
<th>Company</th>
<th>Darker Male</th>
<th>Darker Female</th>
<th>Lighter Male</th>
<th>Lighter Female</th>
<th>Gap</th>
</tr>
</thead>
<tbody>
<tr>
<td>“A”</td>
<td>94%</td>
<td>79%</td>
<td>100%</td>
<td>98%</td>
<td>20%</td>
</tr>
<tr>
<td>“B”</td>
<td>99%</td>
<td>65%</td>
<td>99%</td>
<td>94%</td>
<td>33%</td>
</tr>
<tr>
<td>“C”</td>
<td>88%</td>
<td>65%</td>
<td>99%</td>
<td>92%</td>
<td>34%</td>
</tr>
</tbody>
</table>

End Technological Injustice! Make The Safe Face Pledge Today.

Noel Sharkey  Contributor

AI & Big Data
I write about benefits, wrongs and hype of robots, AI, ML and new tech.

Joy Buolamwini is an enemy of the technologies of injustice. Her Algorithmic Justice League leads the resistance against the tyranny of big data and the ill-conceived uses of face recognition. Everywhere new
This is a “Shirley Card”

Named after a Kodak studio model named Shirley Page, they were the primary method for calibrating color when processing film.
Until about 1990, virtually all Shirley Cards featured Caucasian women.
As a result, photos featuring people with light skin looked fairly accurate.
Photos featuring people with darker skin, not so much...
Microsoft calls for laws to control facial-recognition technology and protect public

Originally published December 6, 2018 at 12:30 pm | Updated December 7, 2018 at 4:57 pm
Research Areas: 36 papers in 2018
- Cybersecurity (4 papers)
- Privacy (1 paper)
- AI Policy (5 papers)
- Networks (16 papers)
- Decentralized Web (3 papers)
- App Inventor (7 papers)

Students
- PhD: 14 current / 4 graduated
- Masters: 19 current / 22 graduated
- Undergrad: 11 current / 30 graduated
Policy at the MIT Schwarzman College of Computing

“The MIT Schwarzman College of Computing will seek to be not only a center of advances in computing, but also a place for teaching and research on relevant policy and ethics to better ensure that the groundbreaking technologies of the future are responsibly implemented in support of the greater good.”
Questions