Internet Policy Research Initiative

Daniel J. Weitzner <weitzner@mit.edu>
Founding Director

Goal: Building Internet of the Future on Strong Technical & Policy Foundations

Create a new field to help governments, other responsible institutions, and individuals to create public policy frameworks that will increase the trustworthiness of the interconnected digital systems. We accomplish this through:

- Engineering & public policy research
- Education
- Engagement

WILLIAM + FLORA Hewlett Foundation

Internet Policy Research Initiative
Massachusetts Institute of Technology

Internet Policy Research Initiative
Massachusetts Institute of Technology

Cybersecurity & Critical Infrastructure	Privacy Policy Group	Advanced Network Architecture (ANA)	Machine Understanding	Global Cybersecurity Policy Group	App Inventor

Leadership & PI’s

Founding Director
Daniel J. Weitzner, CSAIL

Hal Abelson - EECS
David Clark - CSAIL
Ken Oye - Political Science
Michael Fischer - Anthropology
Catherine Tucker - Sloan
Marc Zissman - Lincoln Lab
Tim Berners-Lee - CSAIL

Gerald Sussman - EECS
Lalana Kagal - CSAIL
Andrew Lo - Sloan
Simon Johnson - Sloan
Larry Susskind - DUSP
Vinod Vaikuntanathan - EECS
Stuart Madnick - Sloan
Chintan Vaishnav - Sloan
Karen Sollins - CSAIL
Howie Shrobe - CSAIL

Partners

GEORGETOWN LAW

Funding

WILLIAM + FLORA Hewlett Foundation

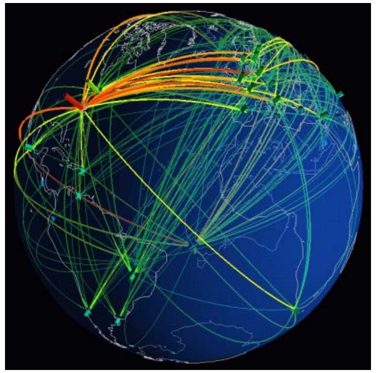
FORD FOUNDATION

NSF

$1B+/1B Person-enabling policy insights

$?B

230



$715B

$516B

ACLU
v
Reno

$542B

No
Back
Doors

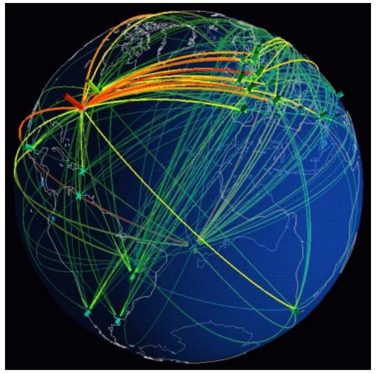
$X x 211M units

$872B

$1B+/1B Person-enabling policy insights

$?B

230



$715B

$516B

ACLU
v
Reno

$542B

No
Back
Doors

$X x 211M units

$872B

Autonomous Vehicles

HomeKit
IOT Security

Machine Learning Fairness

Global Privacy Norms

Research

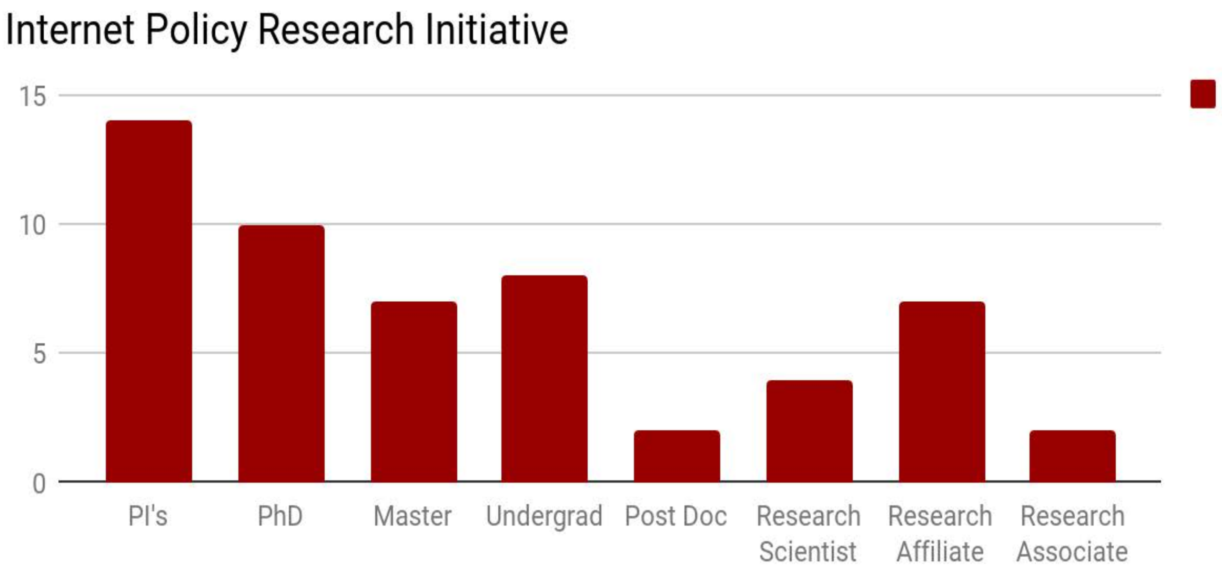
Research in 2017

- 38 Publications in 2017
- 15 Public speeches in 2017

Research highlights

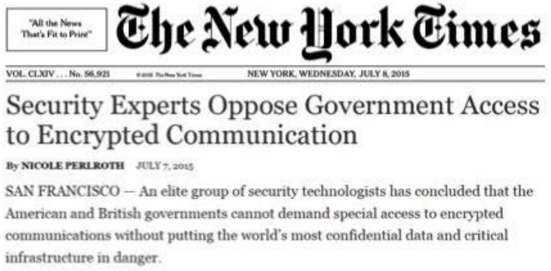
- **Security:** Critical Infrastructure Workshops and Paper
- **Privacy:** Better the devil you know: Personalized Data Controller Indicators that Expose Data Sharing in Smartphone Apps
- **Networks:** Detecting peering infrastructure outages in the wild
- **Machine understanding:** Getting up to speed on vehicle intelligence
- **DIG**: Share - A differentially-private wrapper for enterprise big data
- **TENS:** What Makes an Occupation Resilient to Automation? A Conceptual Framework

Principal Investigators (PI)	17
PhD Students	10
Master Students	7
Undergraduate Students	8
Post Doc & Research Scientist	6
Research Affiliate and Associate	7



Apple vs FBI

Apple encryption debate after San Bernardino terrorist attack - IPRI was able to sway the conversation with the Keys Under Doormat paper + Congressional testimony



"All the News That's Fit to Print"

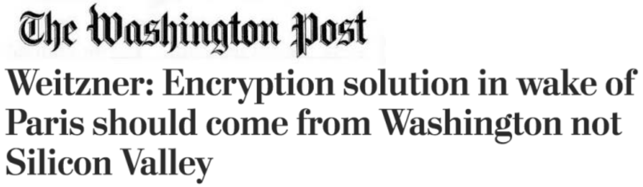
The New York Times

VOL. CLXIV . . . No. 56,921 ©2015 The New York Times NEW YORK, WEDNESDAY, JULY 8, 2015

Security Experts Oppose Government Access to Encrypted Communication

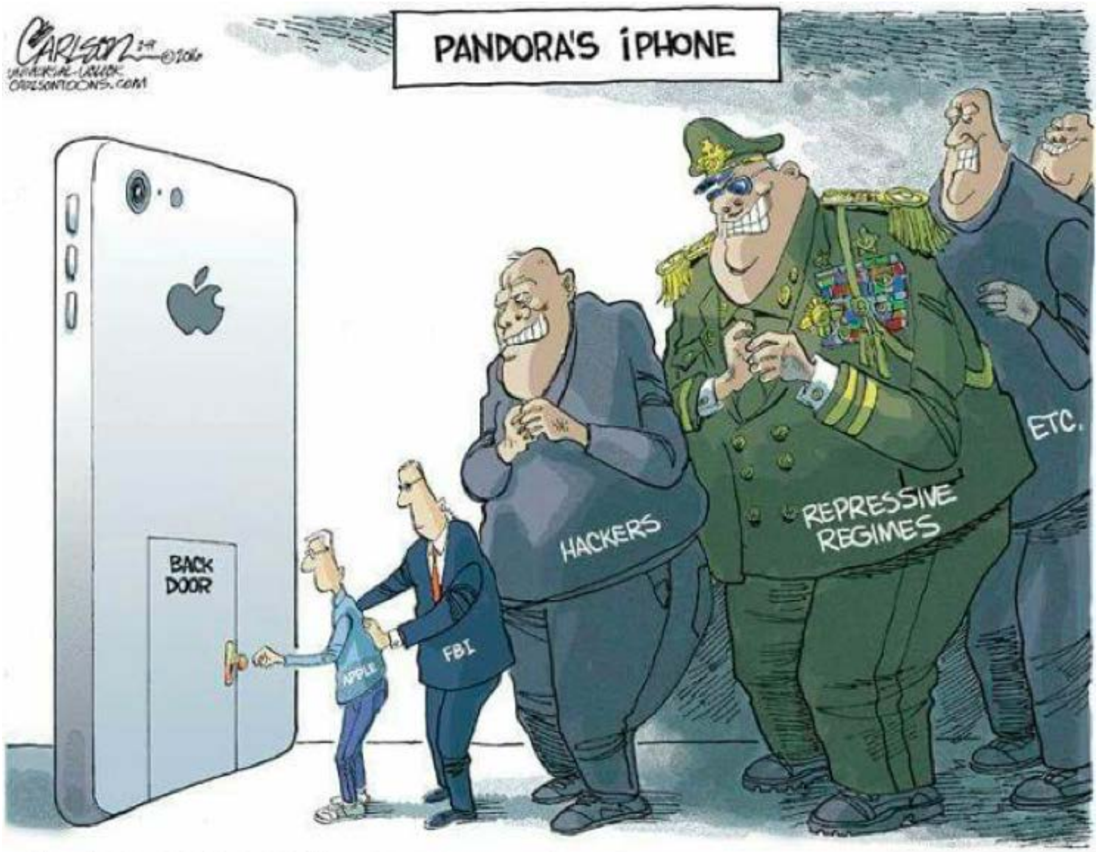
By NICOLE PERLROTH JULY 7, 2015

SAN FRANCISCO — An elite group of security technologists has concluded that the American and British governments cannot demand special access to encrypted communications without putting the world's most confidential data and critical infrastructure in danger.



The Washington Post

Weitzner: Encryption solution in wake of Paris should come from Washington not Silicon Valley



Research: "Keys Under Doormat"
Daniel Weitzner (IPRI)
Hal Abelson (IPRI)
Ron Rivest (EECS)
Mike Specter (IPRI)

MIT Internet Policy Research Initiative
Massachusetts Institute of Technology

Impact Case Study: “Keys Under Doormats” research

The New York Times

Security Experts Oppose Government Access to Encrypted Communication

The Washington Post

Weitzner: Encryption solution in wake of Paris should come from Washington not Silicon Valley

COMMITTEE ON ENERGY & COMMERCE · U.S. HOUSE OF REPRESENTATIVES

European Parliament

European Commission

Extensively cited in key government reports by the US Congress, European Parliament and the European Commission

2 Awards

[EFF Pioneer Award to KUD authors](#)
[M3AAWG J.D. Falk Award](#)

4 Congressional testimonies in 2015-2016

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.

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.

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?"

Debate on Encryption is Far From Over...

"Our society has never had a system where evidence of criminal wrongdoing was totally impervious to detection, especially when officers obtain a court-authorized warrant. But that is the world that technology companies are creating....

Responsible encryption is achievable. Responsible encryption can involve effective, secure encryption that allows access only with judicial authorization. Such encryption already exists. Examples include the central management of security keys and operating system updates; the scanning of content, like your e-mails, for advertising purposes; the simulcast of messages to multiple destinations at once; and key recovery when a user forgets the password to decrypt a laptop."

-- United States Deputy Attorney General Rod Rosenstein, Speech, Oct. 10, 2017

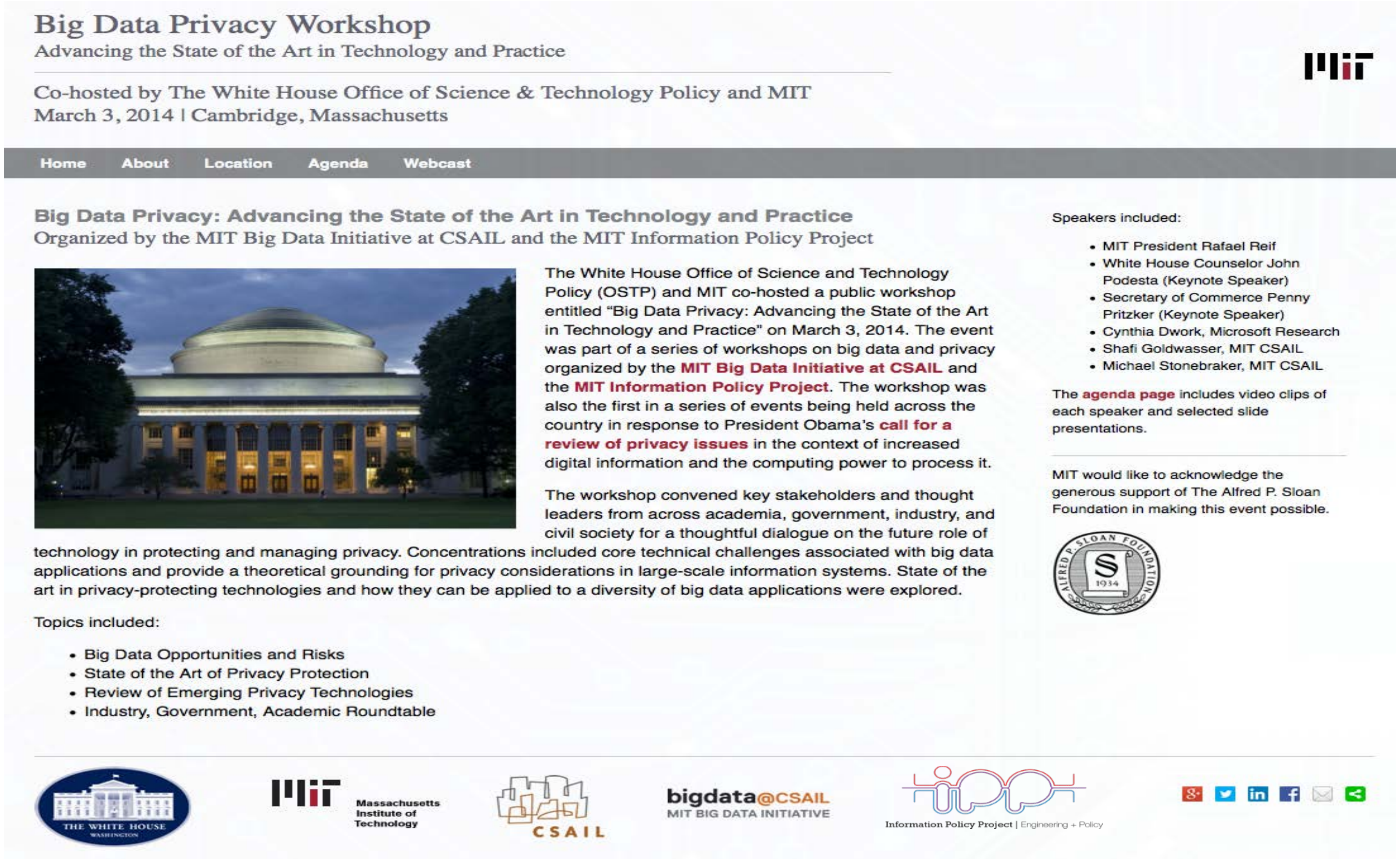
Keys under doormats - Next steps

Securing Critical Infrastructure

- Core economic infrastructure may not be sufficiently protected against cyber attacks
- MIT examining cybersecurity across four industries: Electricity, Finance, Communications and Oil/Gas. Taking a broad approach covering technical, political, and economic perspectives.
- New research agenda - cross-sector risk measurement

Research:
Joel Brenner (IPRI)

MIT/White House Privacy Workshop



Big Data Privacy Workshop

Advancing the State of the Art in Technology and Practice

Co-hosted by The White House Office of Science & Technology Policy and MIT
March 3, 2014 | Cambridge, Massachusetts

Big Data Privacy: Advancing the State of the Art in Technology and Practice

Organized by the MIT Big Data Initiative at CSAIL and the MIT Information Policy Project

The White House Office of Science and Technology Policy (OSTP) and MIT co-hosted a public workshop entitled "Big Data Privacy: Advancing the State of the Art in Technology and Practice" on March 3, 2014. The event was part of a series of workshops on big data and privacy organized by the **MIT Big Data Initiative at CSAIL** and the **MIT Information Policy Project**. The workshop was also the first in a series of events being held across the country in response to President Obama's **call for a review of privacy issues** in the context of increased digital information and the computing power to process it.

The workshop convened key stakeholders and thought leaders from across academia, government, industry, and civil society for a thoughtful dialogue on the future role of technology in protecting and managing privacy. Concentrations included core technical challenges associated with big data applications and provide a theoretical grounding for privacy considerations in large-scale information systems. State of the art in privacy-protecting technologies and how they can be applied to a diversity of big data applications were explored.

Topics included:

- Big Data Opportunities and Risks
- State of the Art of Privacy Protection
- Review of Emerging Privacy Technologies
- Industry, Government, Academic Roundtable

Speakers included:

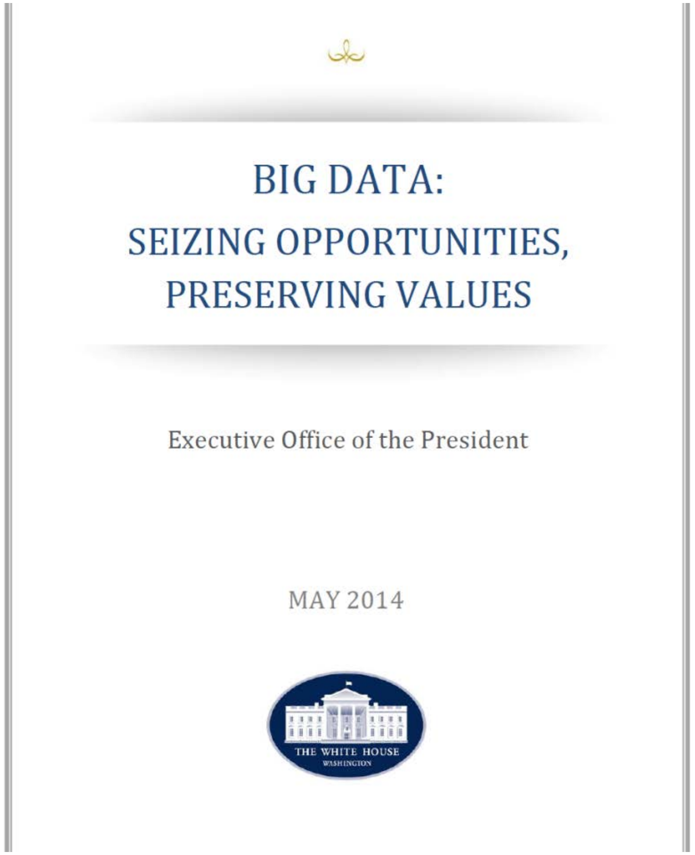
- MIT President Rafael Reif
- White House Counselor John Podesta (Keynote Speaker)
- Secretary of Commerce Penny Pritzker (Keynote Speaker)
- Cynthia Dwork, Microsoft Research
- Shafi Goldwasser, MIT CSAIL
- Michael Stonebraker, MIT CSAIL

The **agenda page** includes video clips of each speaker and selected slide presentations.

MIT would like to acknowledge the generous support of The Alfred P. Sloan Foundation in making this event possible.

ALFRED P. SLOAN FOUNDATION
1934
THE WHITE HOUSE
WASHINGTON
Massachusetts Institute of Technology
CSAIL
bigdata@CSAIL
MIT BIG DATA INITIATIVE
Information Policy Project | Engineering + Policy

New Privacy Priorities: Prevent Discrimination and Sustain Trust



BIG DATA:

SEIZING OPPORTUNITIES, PRESERVING VALUES

Executive Office of the President

MAY 2014

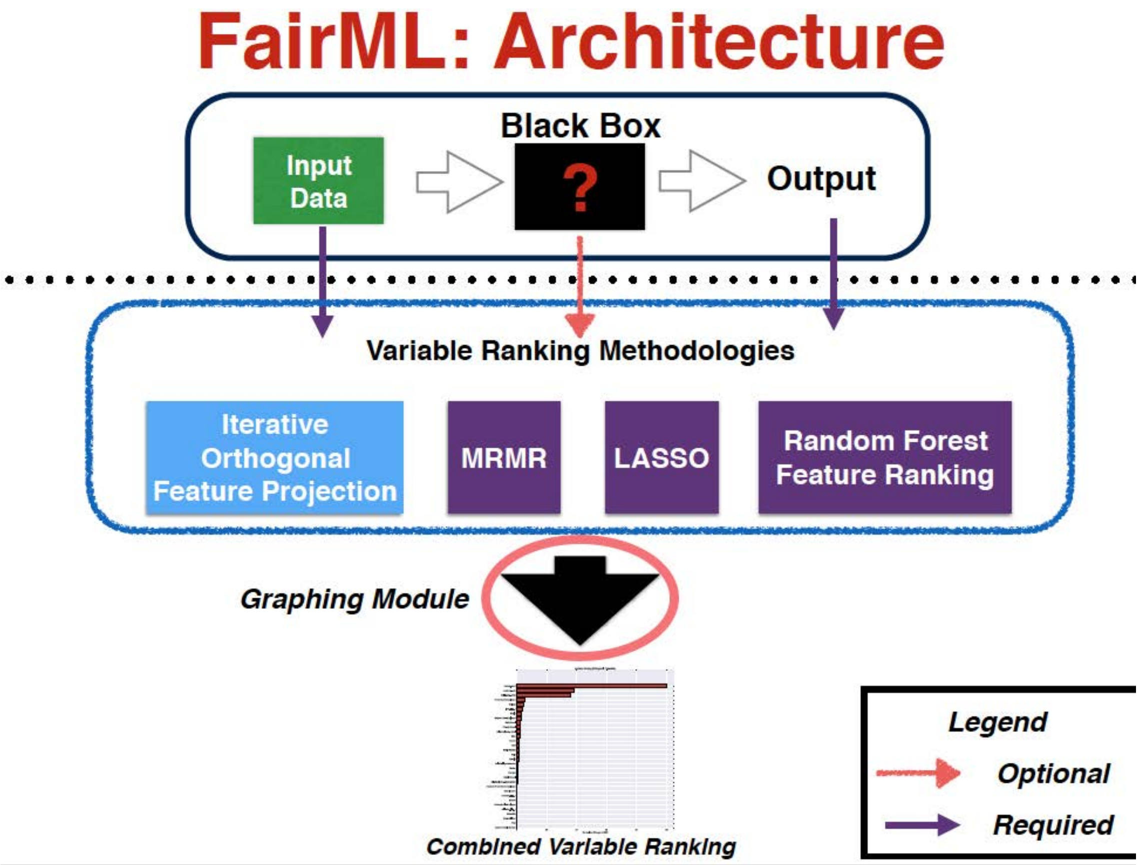
THE WHITE HOUSE
WASHINGTON

Discrimination: “The increasing use of algorithms to make eligibility decisions must be carefully monitored for potential discriminatory outcomes for disadvantaged groups, even absent discriminatory intent.“

Trust: “Public trust is required for the proper functioning of government….

As President Obama has unequivocally stated, “It is not enough for leaders to say: trust us, we won’t abuse the data we collect.”

Privacy and Big Data analysis



FairML: Architecture

Black Box

Input Data → ? → Output

Variable Ranking Methodologies

Iterative Orthogonal Feature Projection

MRMR

LASSO

Random Forest Feature Ranking

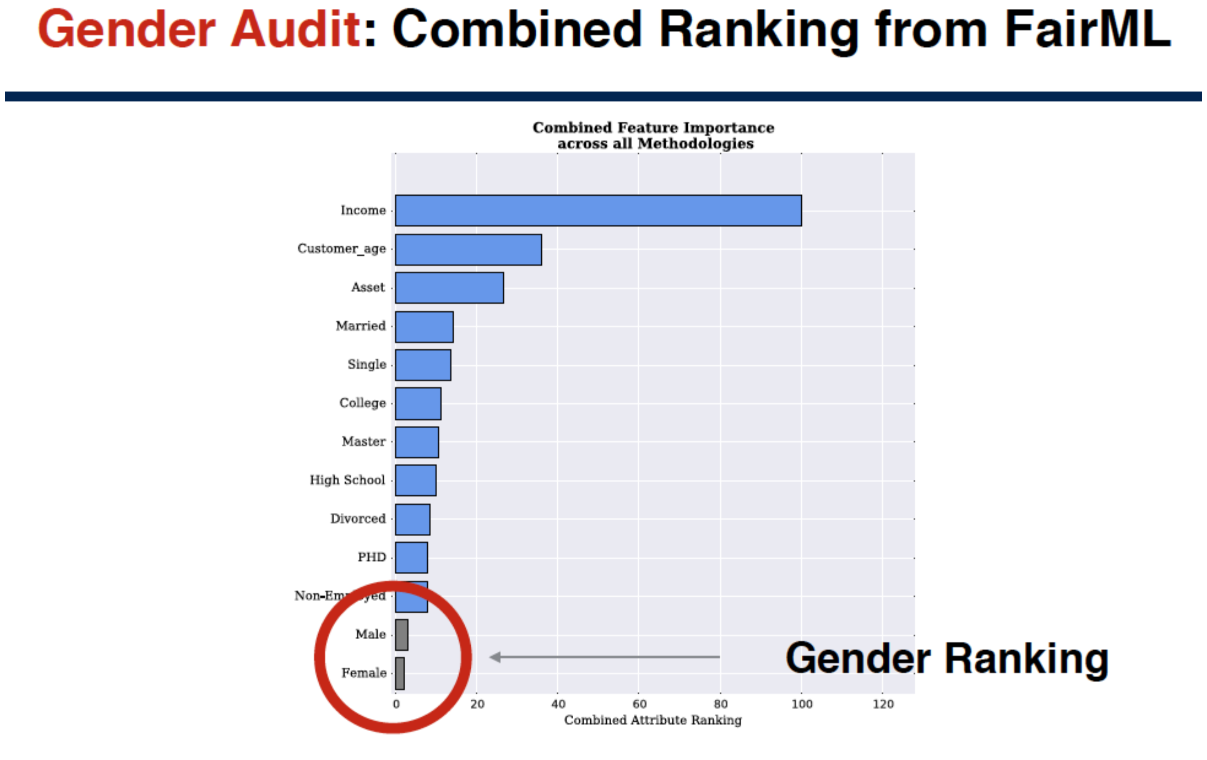
Graphing Module

Combined Variable Ranking

Legend

Optional

Required

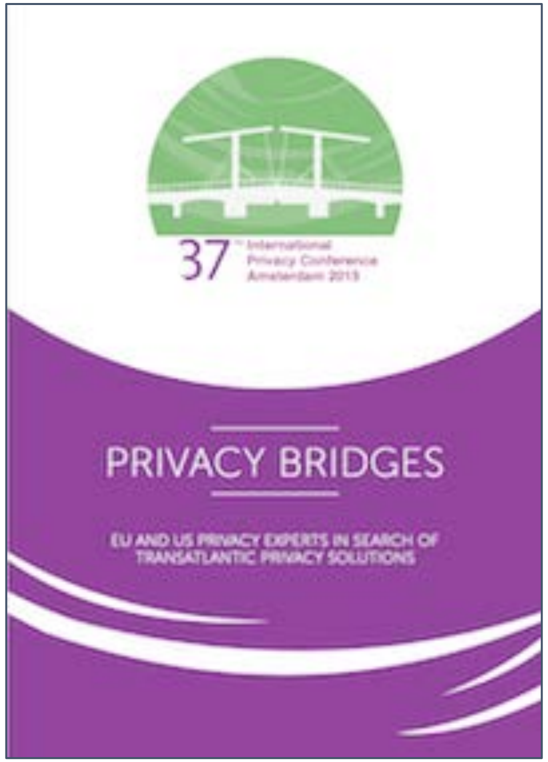


Gender Audit: Combined Ranking from FairML

Hurley, Mikella, and Julius Adebayo. "Credit Scoring in the Era of Big Data." *Yale JL & Tech.* 18 (2016): 148.

J. Adebayo
SM Thesis (2016)

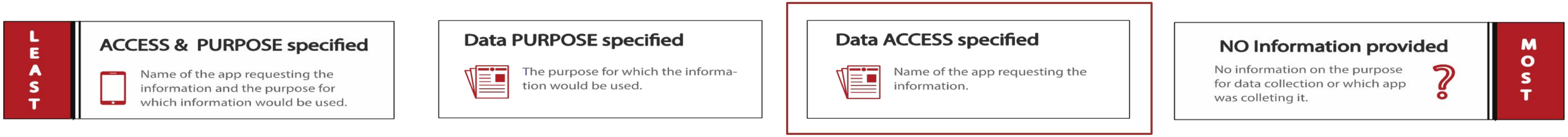
Privacy Bridges


37th International Privacy Conference Amsterdam 2015
PRIVACY BRIDGES
EU AND US PRIVACY EXPERTS IN SEARCH OF TRANSATLANTIC PRIVACY SOLUTIONS

Challenge: What steps that the European Union and the United States can take together to address the shared challenge to privacy protection posed by new technologies and new global businesses?

- 20 legal and computer science experts drawn half from the United States and half from Europe
- Recommendations were the centerpiece of the 37th International Conference of Privacy and Data Protection Regulators.
- https://privacybridges.mit.edu/

User Privacy Studies - HCI and mobile apps



LEAST

ACCESS & PURPOSE specified

Name of the app requesting the information and the purpose for which information would be used.

Data PURPOSE specified

The purpose for which the information would be used.

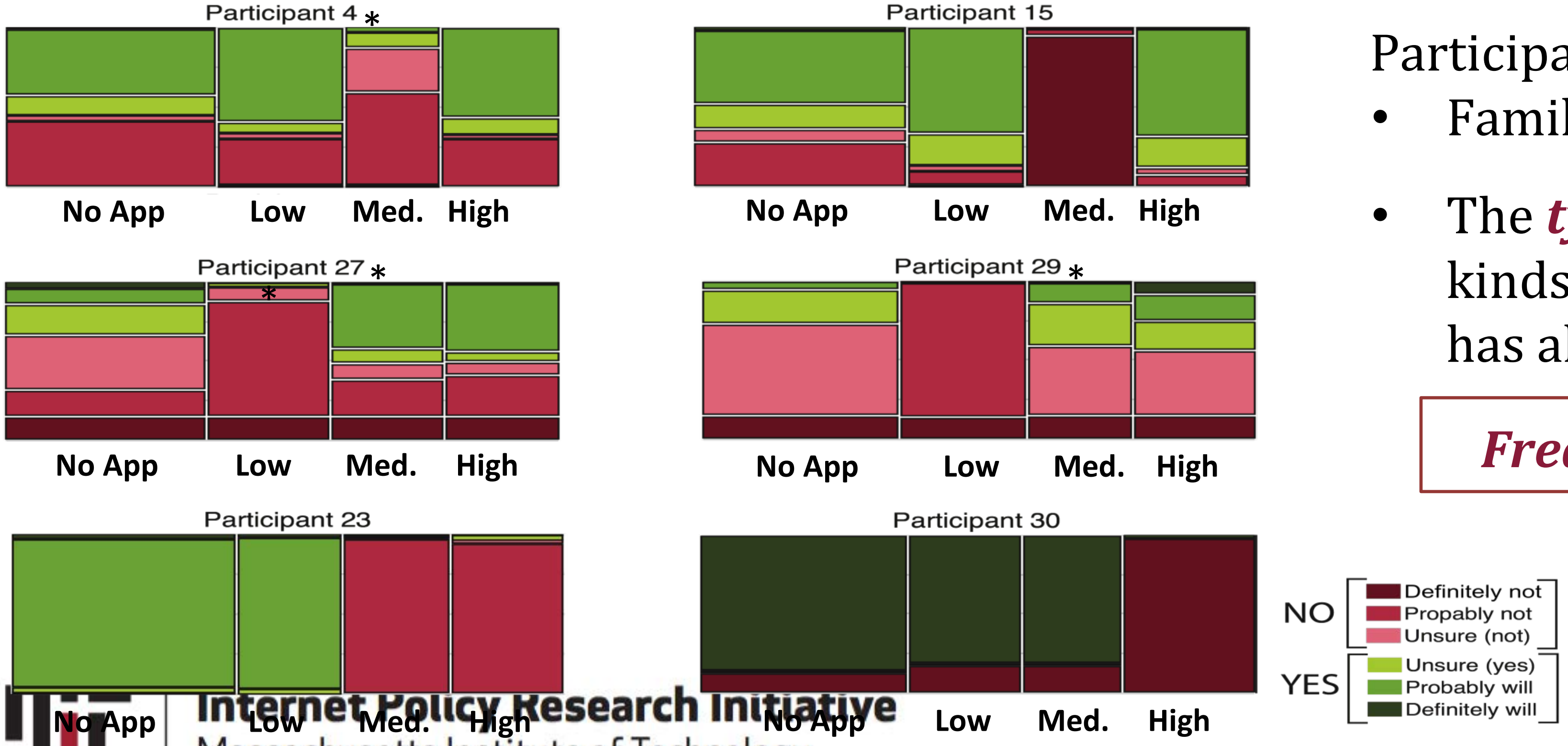
Data ACCESS specified

Name of the app requesting the information.

NO Information provided

No information on the purpose for data collection or which app was colleting it.

MOST



Participants based their decision on:

- Familiarity (i.e. ***trust***) with the app.
- The ***type*** of app, in particular what kinds of information the app already has already access to.

***Frequency** of use had **no** effect;*

Privacy Tipping Points in Smartphones Privacy Preferences
F Shih, I Liccardi, D Weitzner – Proceedings ACM CHI, 2015

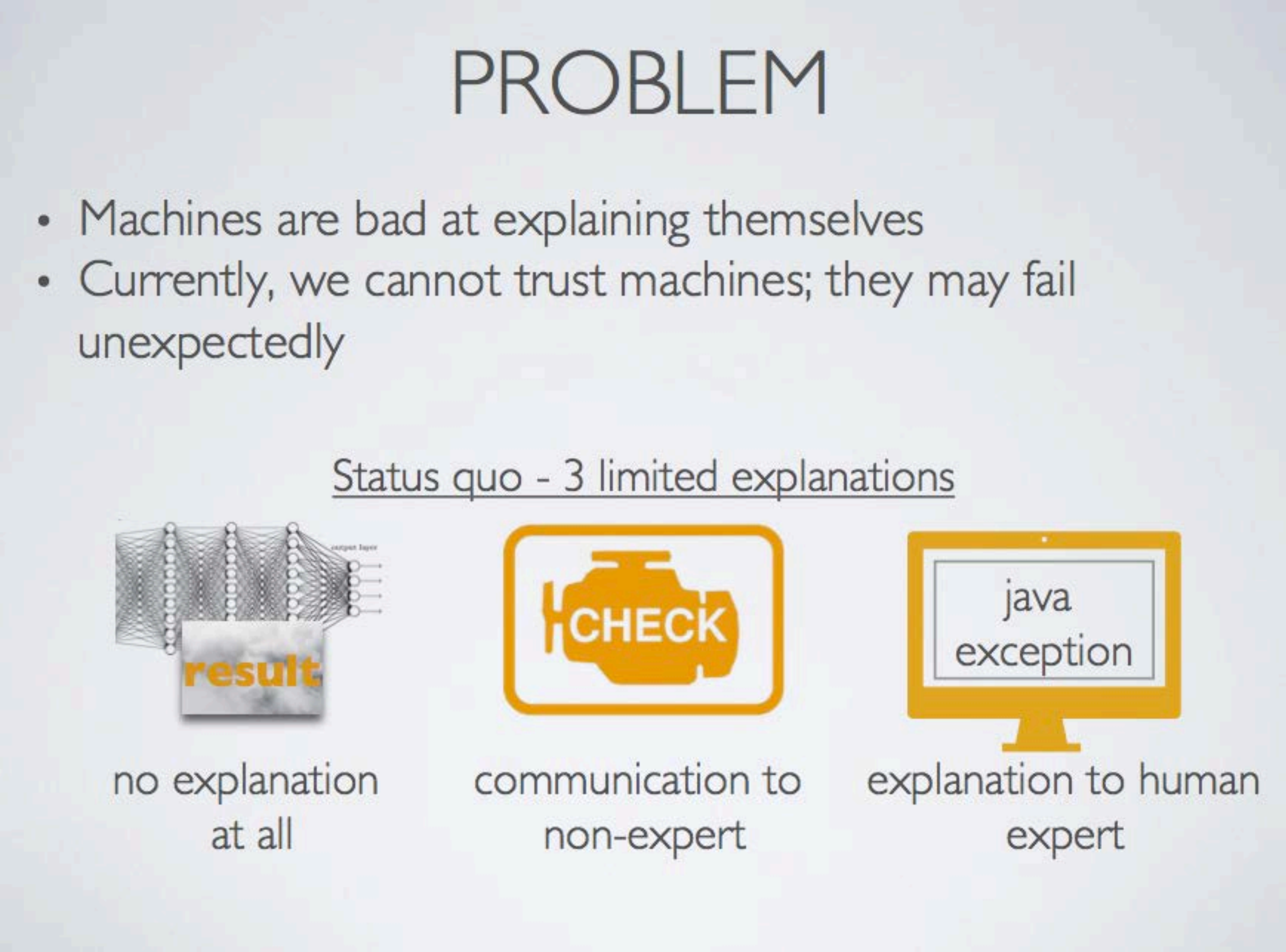
Autonomous Systems

Benefits:
-Safe
-Efficient
-Productive

Obstacles:
-Insurance
-Liability
-Regulation

"Does your car have any idea why my car pulled it over?"

Research Work: "The Car Can Explain"
Gerry Sussman (IPRI)
Leilani Gilpin (IPRI)



PROBLEM

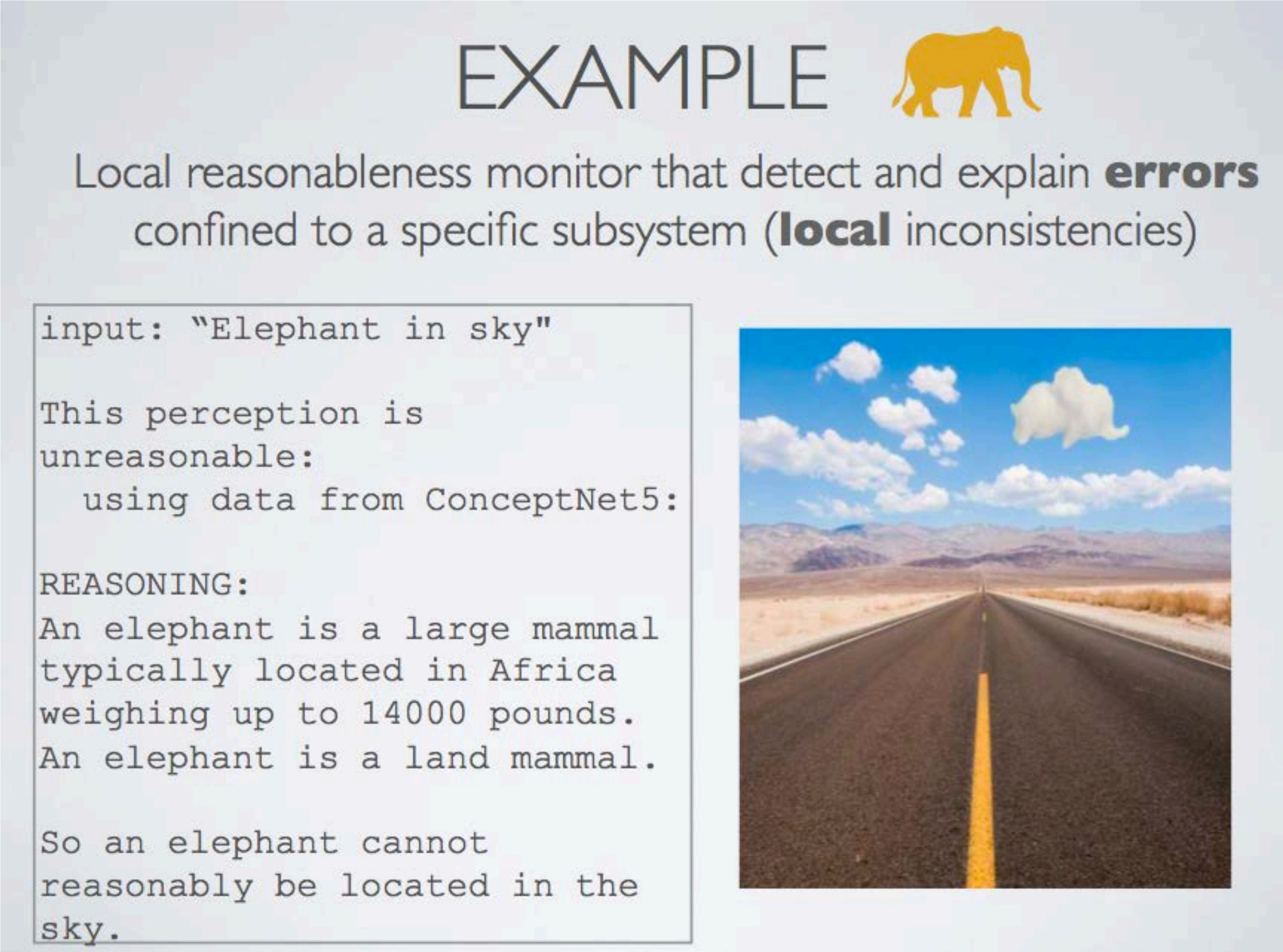
- Machines are bad at explaining themselves
- Currently, we cannot trust machines; they may fail unexpectedly

Status quo - 3 limited explanations

no explanation at all

communication to non-expert

explanation to human expert



EXAMPLE

Local reasonableness monitor that detect and explain **errors** confined to a specific subsystem (**local** inconsistencies)

```
input: “Elephant in sky"

This perception is
unreasonable:
  using data from ConceptNet5:

REASONING:
An elephant is a large mammal
typically located in Africa
weighing up to 14000 pounds.
An elephant is a land mammal.

So an elephant cannot
reasonably be located in the
sky.
```

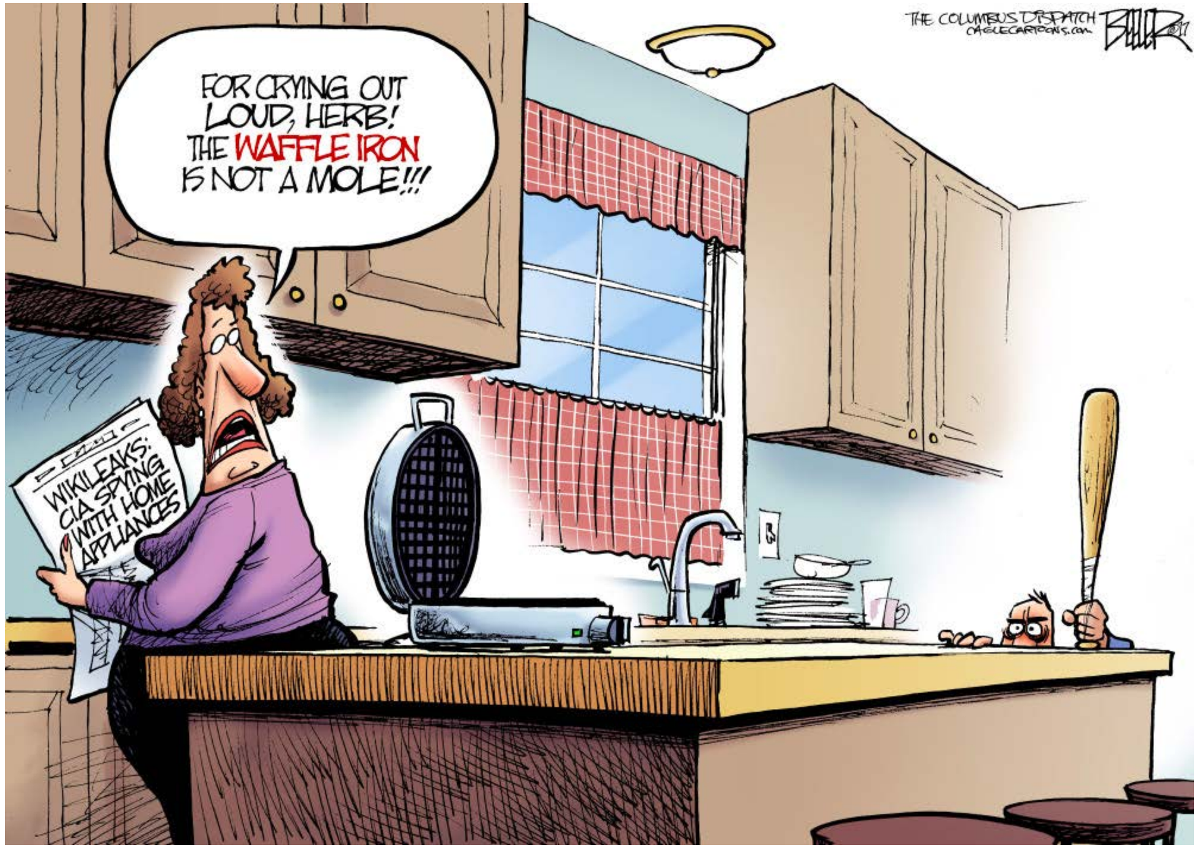
Advanced Network Architecture

- What does the internet of tomorrow look like?
- Fundamental Design Principles
- Governance
- Protocols
- Growth

Principal Research Scientist - David Clark

At Home Listening Devices

Really Cool.
But they also create privacy issues.


THE COLUMBUS DISPATCH
CAGLECARTOONS.com
BEELER ©17
FOR CRYING OUT LOUD, HERB! THE WAFFLE IRON IS NOT A MOLE!!!
WIKILEAKS: CIA SPYING WITH HOME APPLIANCES

Google Home
Voice-activated speaker

INTRODUCING
amazon echo

Always ready, connected, and fast. Just ask.

echo look

Cross-Disciplinary Research Around Campus

IPRI funding Internet policy work across MIT

Andrew Lo
(Sloan)

Vinod
Vaikuntanathan
(CSAIL)

Tools and methods for understanding systemic cybersecurity risk

Despite the increased awareness of cybersecurity risk, firms are reluctant to share the data necessary to understand and measure the prevalence of such risks, their magnitude, and the economic impact, leaving them unable to address these risks effectively. In this project, we aim to develop a secure multiparty computation platform that will give firms the ability to pool encrypted data while preserving confidentiality, and allow us to map the linkages across firms and compute summary statistics. By providing the markets with better information, firms will be equipped to make better decisions and manage cybersecurity risks more effectively and efficiently.

IPRI funding Internet policy work across MIT

Larry Susskind
(DUSP)

Cyber Negotiation Playbook for Critical Infrastructure Security

Cybersecurity is often portrayed as a ‘cat and mouse’ game testing the relative technical prowess of the attacker and the defender. However, it can equally be considered a battle of social wits. Negotiation in the cyber realm presents a significantly different dynamic from person-to-person negotiations typical of the boardroom, since there is no chance to read the face of the other side. You may have limited opportunity to negotiate in real time and, you probably will have no ability to ascertain the culture or values of the hacker. With critical infrastructure being under constant attack by hackers – both state sponsored and hobbyists, operators and managers must be prepared to negotiate with cyber terrorists. Our research involves work with managers of critical urban infrastructure to simulate attacks and help them develop a cyber negotiation playbook.

IPRI funding Internet policy work across MIT

Simon Johnson
(Sloan)

Stuart Madnick
(Sloan)

Cybersecurity Impacts on International Trade

Governments have reportedly arranged to incorporate various forms of spyware and malware in Internet-connected products. In response, some countries have denied entry or imposed restrictions on imported products with such potential risks. But this raises many policy issues, including (1) what is a questionable country (and is it OK if an “ally” spies on us?), (2) what products are of most concern, (3) assuming such restrictions quickly become worldwide policies with retaliations, what might be the long-term impact on international trade and the global economy as Internet-connected products proliferate, and (4) what voluntary standards could be put in place to lower the risk of trade wars? These issues need to be rigorously studied in advance of policy makers making quick decisions – in some crisis condition – without understanding the impacts and consequences.

Engagement

5

Residential MIT courses with new cybersecurity, privacy components

21

VIP political visitors to MIT to meet with IPRI

Hal Abelson teaching students in the MIT/Georgetown course on privacy legislation supported by IPRI: Privacy Legislation in Practice: Law and Technology, Spring 2016

GCHQ Hannigan
EU EDPS Buttarelli
Mass AG Healey
NSA Adm Rogers
US Secretary Pritzker
EU VP Ansip

Also:

ITU Sec Gen Zhao
FCC Commis. Clyburn
8 EU telecom regulators
European MEPs

Internet Policy Research Initiative
Massachusetts Institute of Technology

2016

The New York Times

FRONTLINE

LAWFARE

CNBC

Slate

MIT
Technology
Review

POPULAR
SCIENCE

THE INDEPENDENT

FORTUNE

The Washington Post

theguardian

npr

WIRED

Education

Education: How Engineering Students Learn Policy

Course offerings

- Foundations of Internet Policy
- Privacy Technology and Legislation (joint with Georgetown Law)
- Cybersecurity graduate seminar
- EECS systems & security courses
- Joint course with Shanghai Jiao Tong University in China

Degree Programs

- SB, now with IPRI SuperUROP
- M.Eng, now with IPRI research
- TPP, now with IPRI-focused courses and research opportunities
- PhD, now with IPRI research opportunities

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

MIT Technology & Policy Program

Internet Policy Research Initiative

GEORGETOWN LAW

MIT EECS
ELECTRICAL ENGINEERING AND COMPUTER SCIENCE

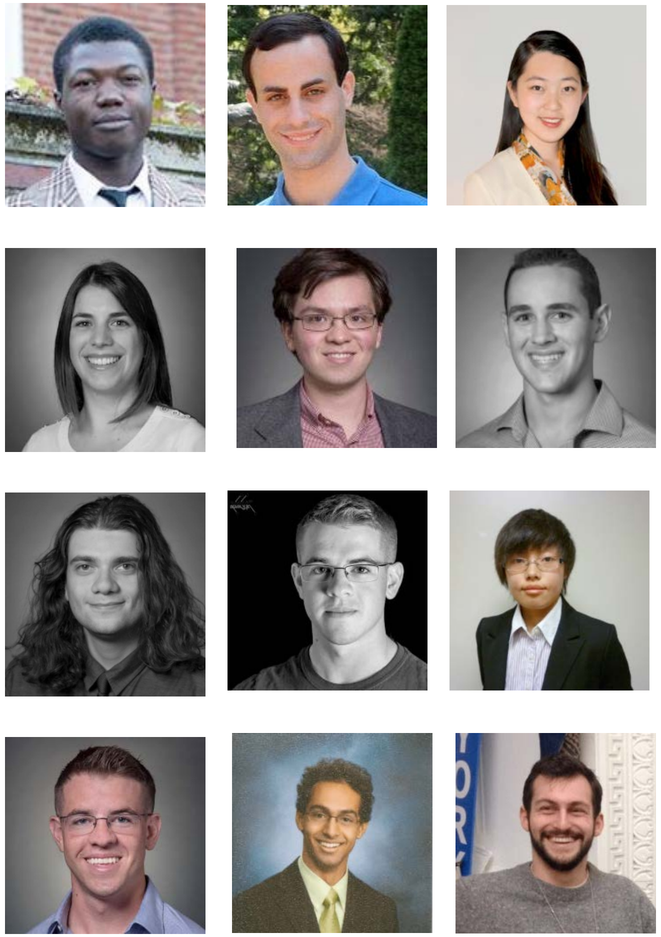
Internet Policy Research Initiative
Massachusetts Institute of Technology

Urgent need: Policy making with tech + policy skills

Example from the United States: Backgrounds of 535 voting members - US Congress

- 225 Law
- 201 Business
- 94 Education
- 24 Health care
- **5 Engineering**
- 3 Physics
- 1 Chemistry

Where Our Students Go



UNITED STATES NAVY

airbnb

OECD

THE WHITE HOUSE
WASHINGTON

Square

THE ASPEN INSTITUTE

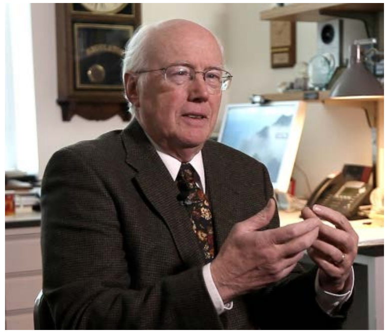
NTIA
U.S. DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS & INFORMATION ADMINISTRATION

Internet Policy Research Initiative Track Talks

Data Ownership Impact on Privacy and Security
Danny Weitzner

Blind Machine Learning
Vinod Vaikuntanathan

Internet Governance and Culture - David Clark



Cybersecurity Impacts on International Trade
Simon Johnson

Questions