BERKMAN
KLEIN CENTER
FOR INTERNET & SOCIETY
AT HARVARD UNIVERSITY

The Impact of Law and Regulation on Digital Technologies in Thailand

Bangkok, August 23, 2017

Dr. Urs Gasser
Professor of Practice, Harvard Law School
Executive Director, Berkman Klein Center for Internet & Society, Harvard University

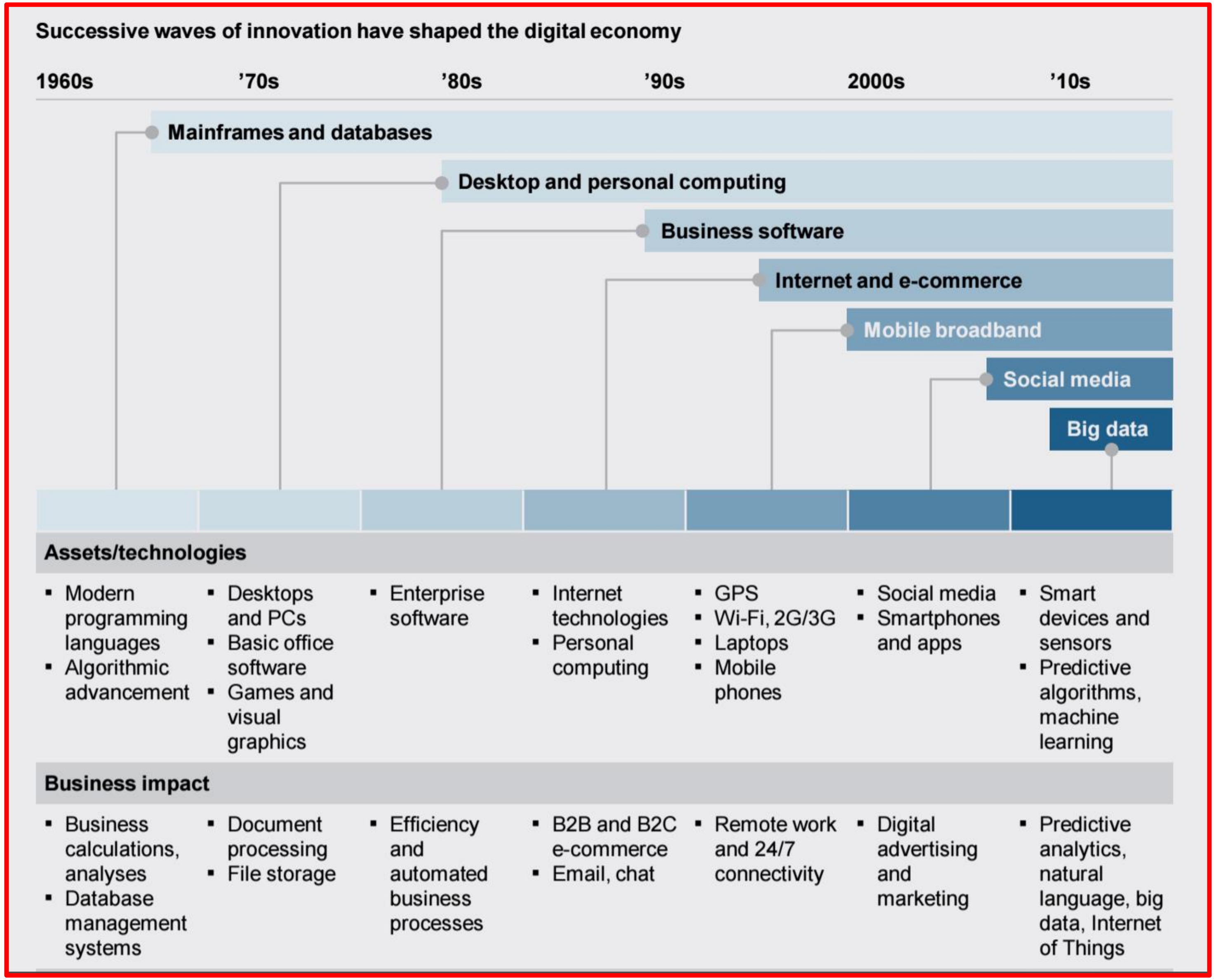
Overview

1. Segment 1: Internet Law and Regulation: Challenges and Possible Approaches
2. Segment 2: Substantive Issues – Comparative Perspectives
3. Segment 3: Approaches to National Digital Governance – Examples from other Countries
4. Segment 4: Closing Exercise

SEGMENT 1

1 Regulating the Digital Economy: Trends and Challenges

Accelerating Waves of Innovation



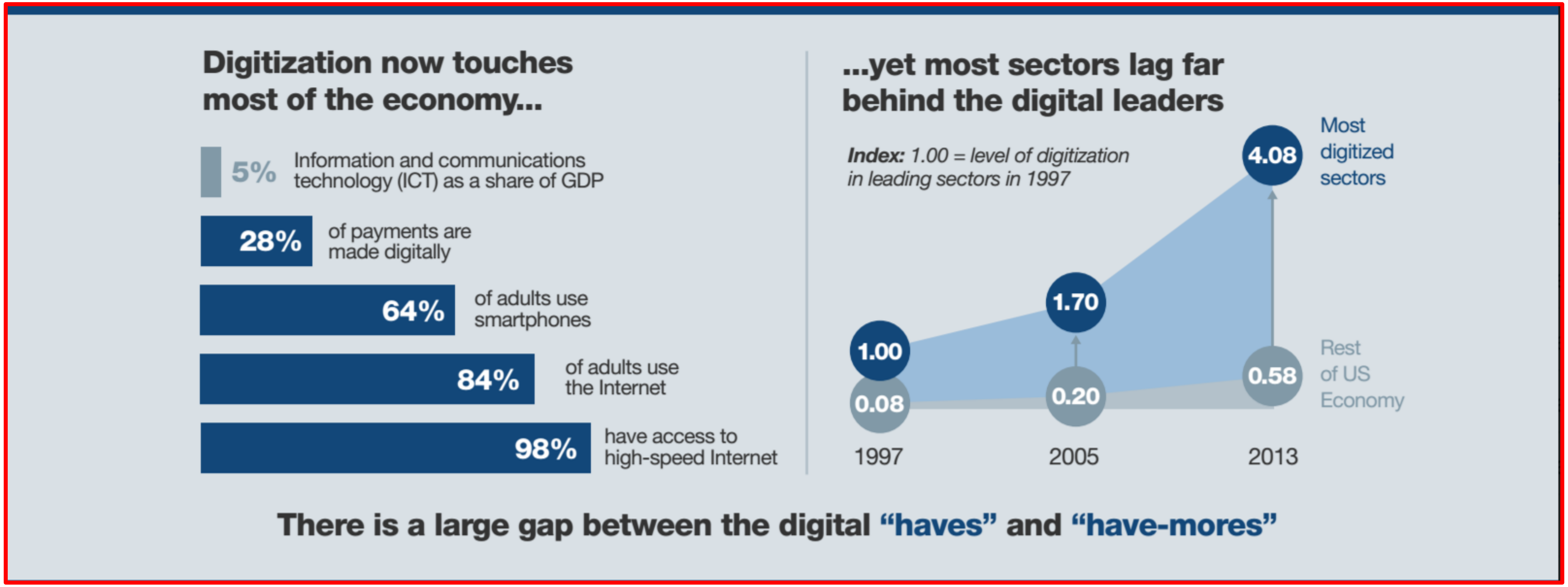
Successive waves of innovation have shaped the digital economy

1960s ’70s ’80s ’90s 2000s ’10s

- Mainframes and databases
- Desktop and personal computing
- Business software
- Internet and e-commerce
- Mobile broadband
- Social media
- Big data

Assets/technologies	▪ Modern programming languages ▪ Algorithmic advancement	▪ Desktops and PCs ▪ Basic office software ▪ Games and visual graphics	▪ Enterprise software	▪ Internet technologies ▪ Personal computing	▪ GPS ▪ Wi-Fi, 2G/3G ▪ Laptops ▪ Mobile phones	▪ Social media ▪ Smartphones and apps	▪ Smart devices and sensors ▪ Predictive algorithms, machine learning
Business impact	▪ Business calculations, analyses ▪ Database management systems	▪ Document processing ▪ File storage	▪ Efficiency and automated business processes	▪ B2B and B2C e-commerce ▪ Email, chat	▪ Remote work and 24/7 connectivity	▪ Digital advertising and marketing	▪ Predictive analytics, natural language, big data, Internet of Things

Impact on the Economy



Digitization now touches most of the economy...

5% Information and communications technology (ICT) as a share of GDP

28% of payments are made digitally

64% of adults use smartphones

84% of adults use the Internet

98% have access to high-speed Internet

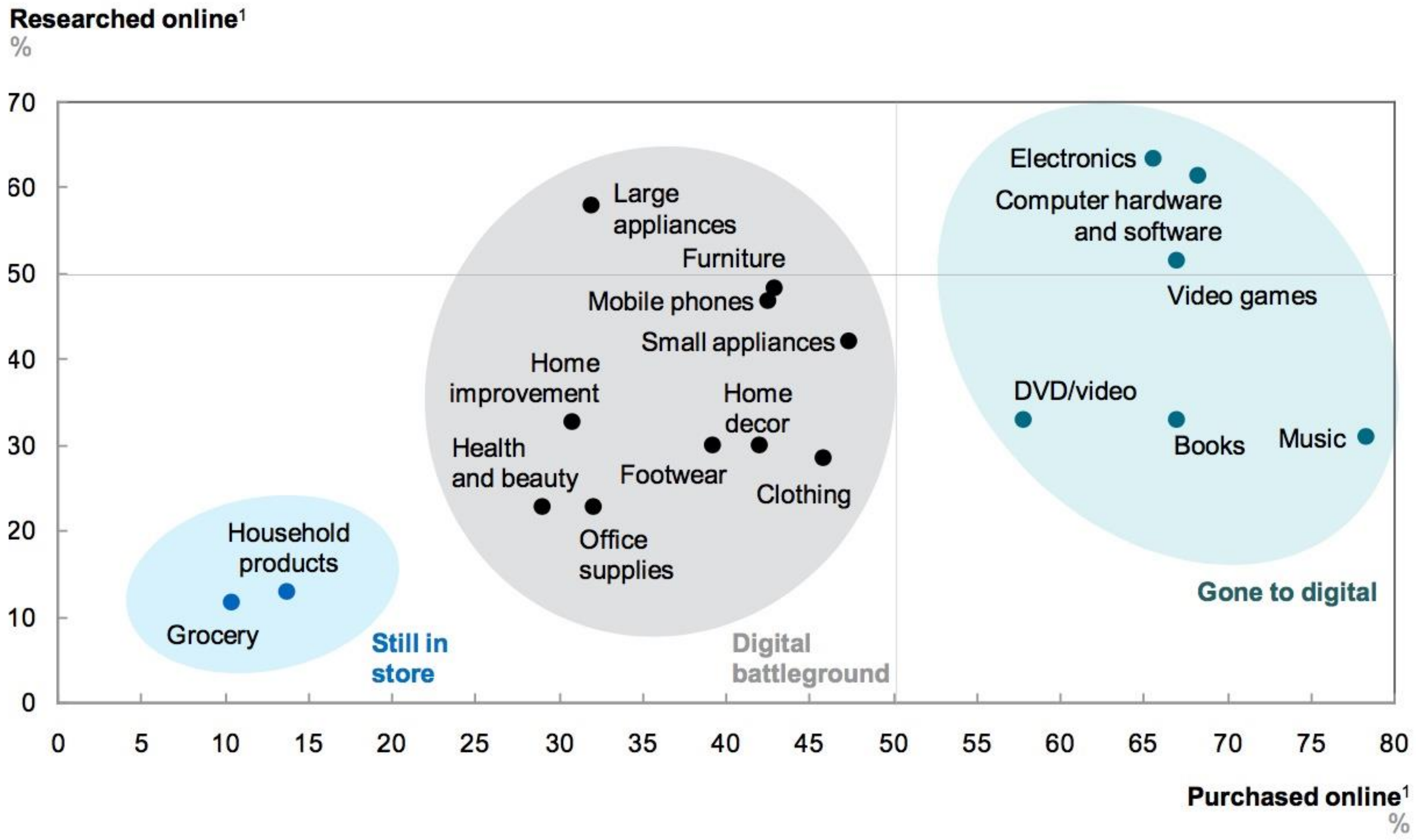
...yet most sectors lag far behind the digital leaders

Index: *1.00 = level of digitization in leading sectors in 1997*

There is a large gap between the digital “haves” and “have-mores”

Example: Online Purchases

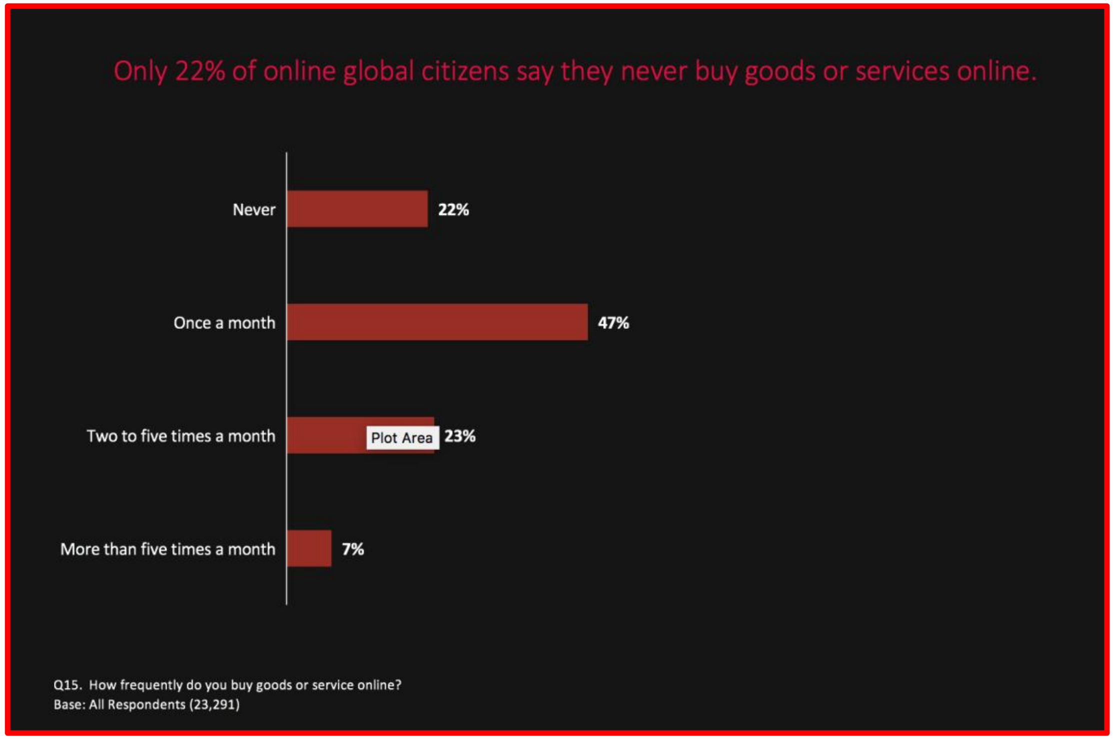
Customers are going online to make purchases in a broad range of product categories



[1] As a percentage of those who bought a product in the respective category in the last 6 months.

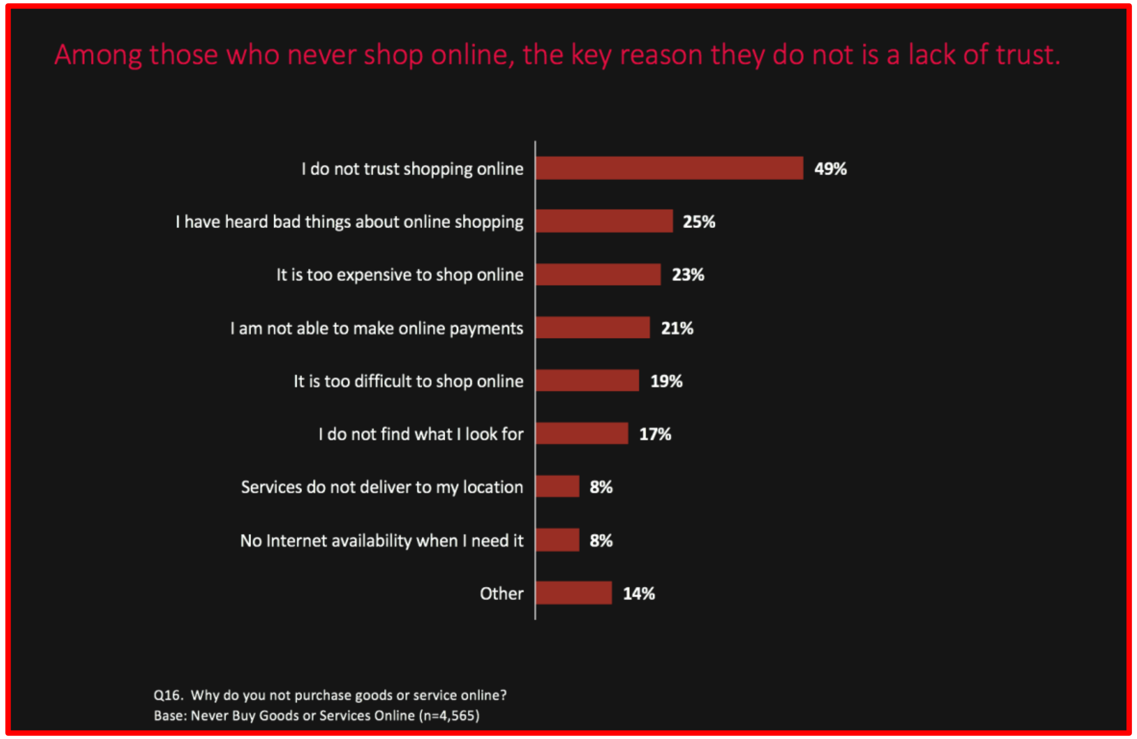
SOURCE: McKinsey TMT Digital Insights 2014 US yearly survey

Expanding Frontier – and Challenges



Only 22% of online global citizens say they never buy goods or services online.

Q15. How frequently do you buy goods or service online?
Base: All Respondents (23,291)

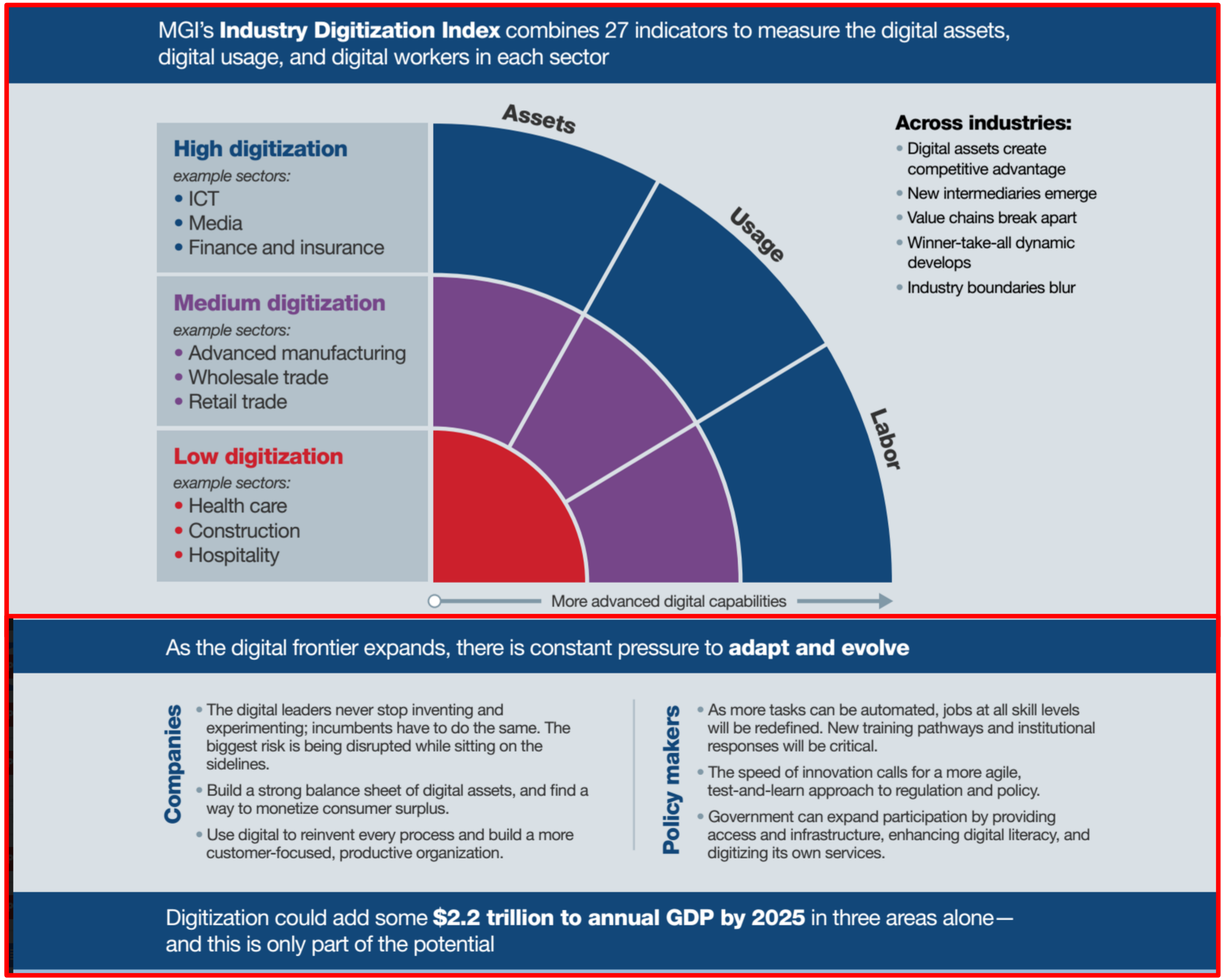


Among those who never shop online, the key reason they do not is a lack of trust.

Q16. Why do you not purchase goods or service online?
Base: Never Buy Goods or Services Online (n=4,565)

https://www.cigionline.org/internet-survey

Expanding Frontier – and Challenges



MGI's **Industry Digitization Index** combines 27 indicators to measure the digital assets, digital usage, and digital workers in each sector

High digitization

example sectors:

- ICT
- Media
- Finance and insurance

Medium digitization

example sectors:

- Advanced manufacturing
- Wholesale trade
- Retail trade

Low digitization

example sectors:

- Health care
- Construction
- Hospitality

Across industries:

- Digital assets create competitive advantage
- New intermediaries emerge
- Value chains break apart
- Winner-take-all dynamic develops
- Industry boundaries blur

As the digital frontier expands, there is constant pressure to **adapt and evolve**

Companies

- The digital leaders never stop inventing and experimenting; incumbents have to do the same. The biggest risk is being disrupted while sitting on the sidelines.
- Build a strong balance sheet of digital assets, and find a way to monetize consumer surplus.
- Use digital to reinvent every process and build a more customer-focused, productive organization.

Policy makers

- As more tasks can be automated, jobs at all skill levels will be redefined. New training pathways and institutional responses will be critical.
- The speed of innovation calls for a more agile, test-and-learn approach to regulation and policy.
- Government can expand participation by providing access and infrastructure, enhancing digital literacy, and digitizing its own services.

Digitization could add some **$2.2 trillion to annual GDP by 2025** in three areas alone—and this is only part of the potential

At the Core: Disruptive Technologies

- Technologies that create a new market and value network, by disrupting existing business, economics, culture, and the way we live.
- McKinsey identifies four factors of disruptive technologies:
    1. Rapidly advancing technology (“breakthrough”)
    2. Large scope of potential impact (e.g. IoT – billions of objects)
    3. Massive economic impact (e.g. advanced robotics and 6.3 trillion in labor costs globally)
    4. Economic impact that upends status quo (AI’s impact on jobs, lives)
- Technology is an important driver of disruptive innovation (but only one factor).
- Examples: Advanced robotics, AV, IoT, Cloud, 3D printing, AI

Disruptive Technologies: Two Examples

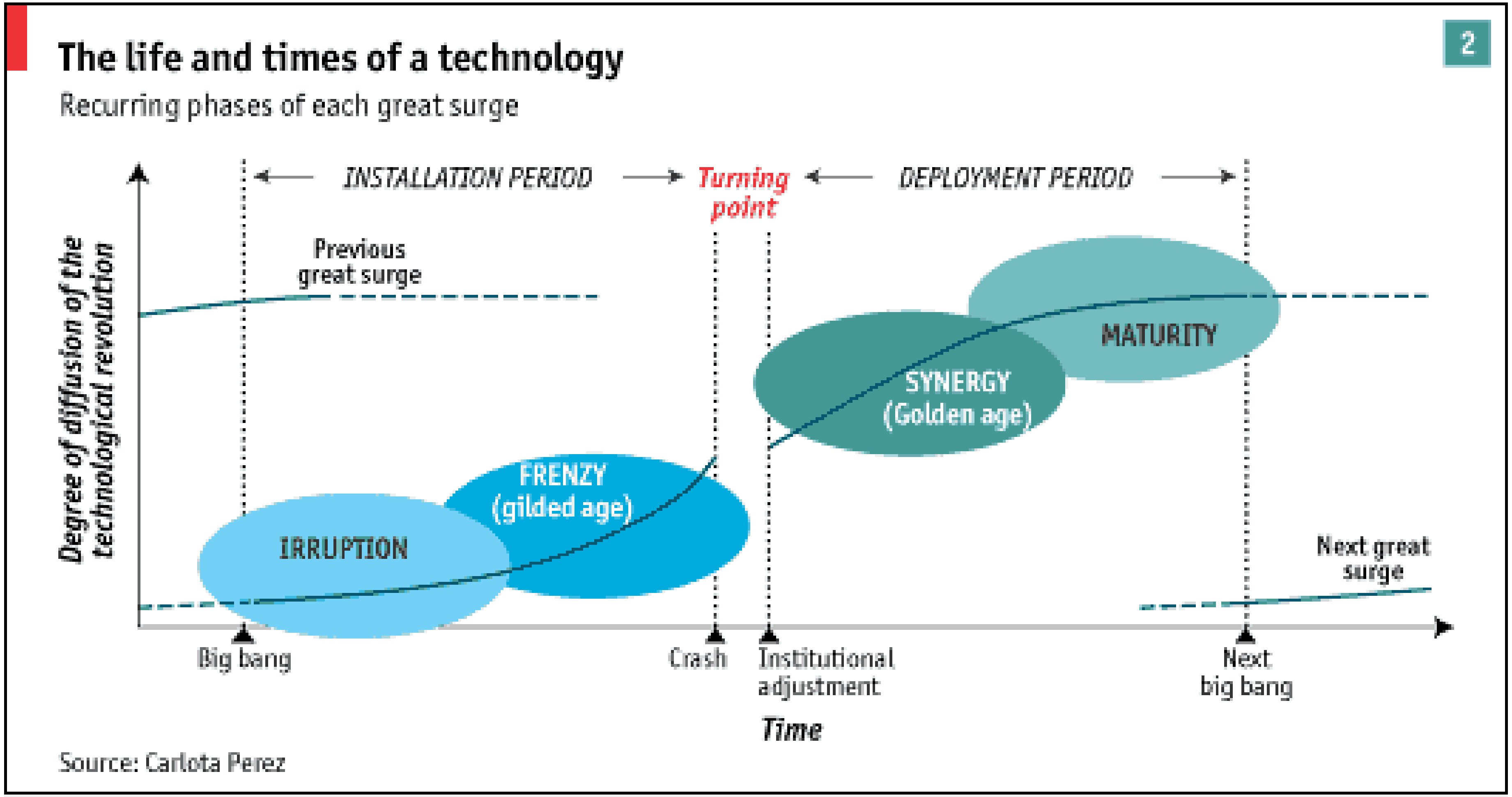
For each example, briefly identify some key challenges associated with it. The following questions might be helpful:

- What, where, and how are these technologies disrupting?
- What are the effects of the disruption?
- What are key legal and regulatory issues/concerns?
- What is different about the new disruptive technology, innovative business model, etc.?
- Who are the key actors involved?

airbnb

2 Law and Regulation: Traditional Response Patterns and New Challenges

Cycles of Disruption 1 (Carlota Perez)



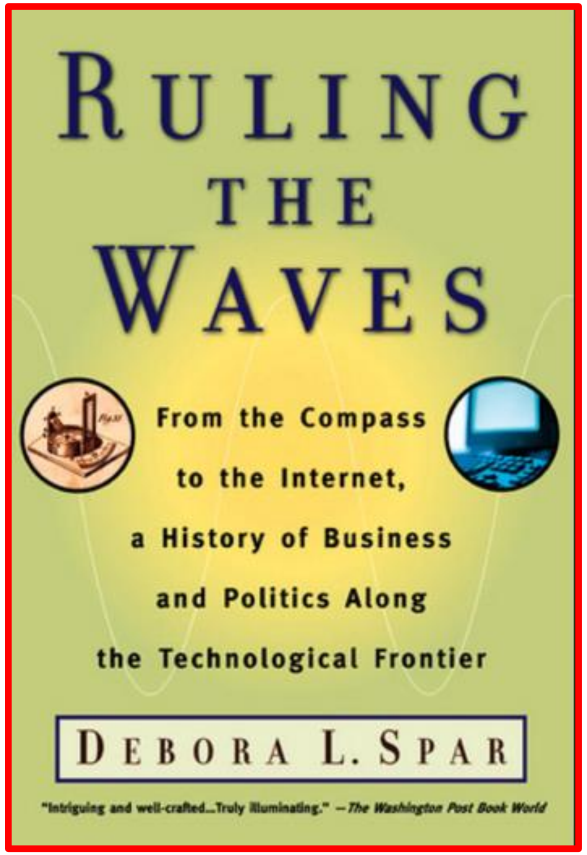
The life and times of a technology

Recurring phases of each great surge

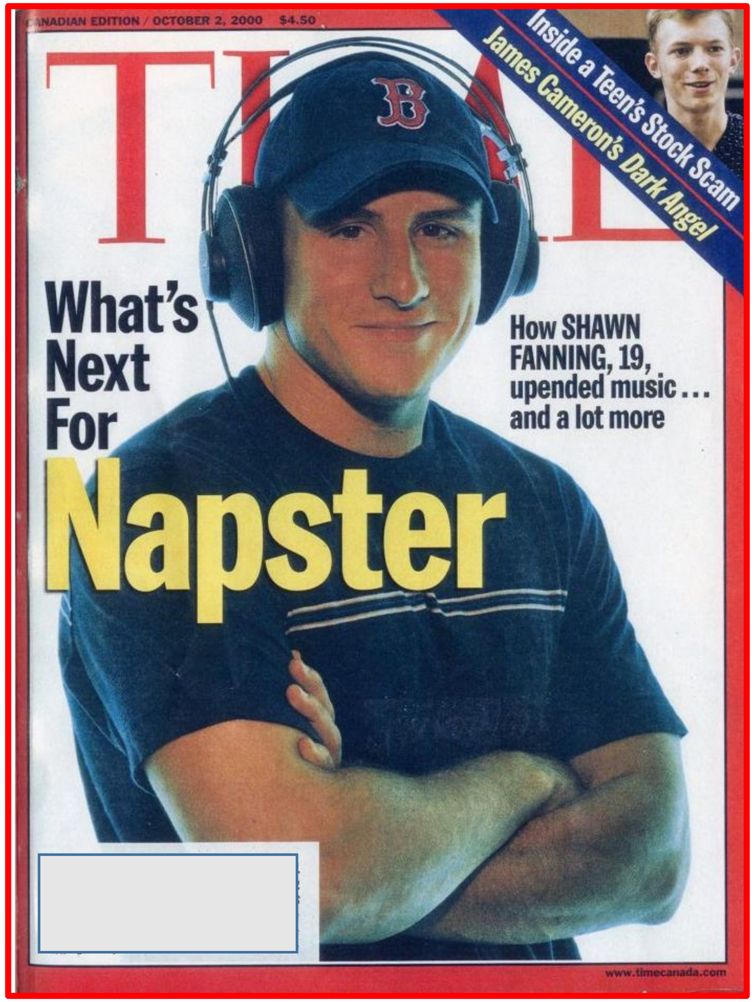
Source: Carlota Perez

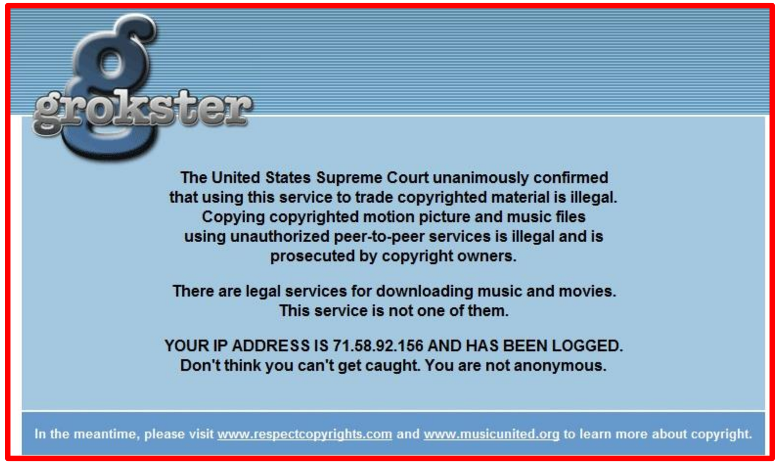
Cycles of Disruption 2 (Debora Spar)

- Cycle with four phases of innovation in information and communication technologies
  1. Innovation
  2. Commercialization
  3. Creative Anarchy
  4. Rules and Regulation
- Legal uncertainty at very early stages of innovation cycle
  - Legal system provides an early warning mechanism (e.g. IP law)


RULING THE WAVES
From the Compass to the Internet, a History of Business and Politics Along the Technological Frontier
DEBORA L. SPAR
"Intriguing and well-crafted...Truly illuminating." —The Washington Post Book World

Example: Digital Media Crisis


CANADIAN EDITION / OCTOBER 2, 2000 $4.50
TIME
Inside a Teen's Stock Scam
James Cameron's Dark Angel
What's Next For Napster
How SHAWN FANNING, 19, upended music... and a lot more
www.timecanada.com

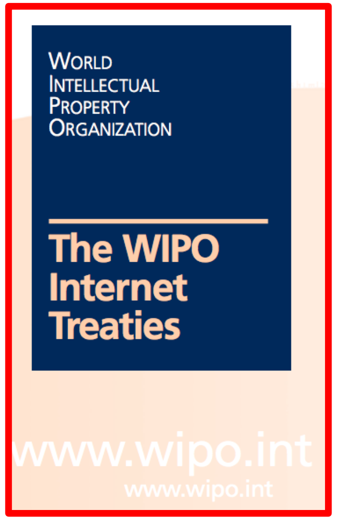


The United States Supreme Court unanimously confirmed that using this service to trade copyrighted material is illegal. Copying copyrighted motion picture and music files using unauthorized peer-to-peer services is illegal and is prosecuted by copyright owners.

There are legal services for downloading music and movies. This service is not one of them.

YOUR IP ADDRESS IS 71.58.92.156 AND HAS BEEN LOGGED. Don't think you can't get caught. You are not anonymous.

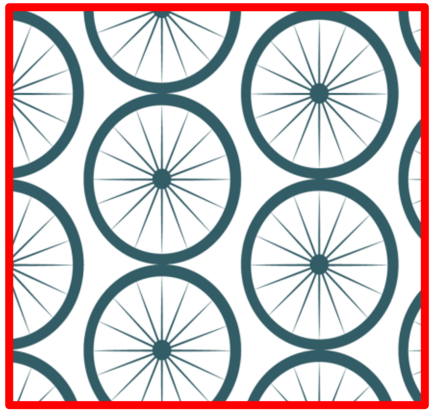
In the meantime, please visit www.respectcopyrights.com and www.musicunited.org to learn more about copyright.


World Intellectual Property Organization
The WIPO Internet Treaties
www.wipo.int
www.wipo.int

Legal Response Patterns

- The legal system has developed different approaches to interact with technological changes ("response patterns"):
  - *Subsumption*, i.e. application of old rules to new phenomenon (default approach)
  - *Innovation*, i.e. enactment of new law (legislator) or introduction of new doctrines (courts)
  - *Gradual responses* over time
- Discussion: How are these patterns challenged by today's developments in the digital economy and ecosystem?

www.shutterstock.com · 129835667

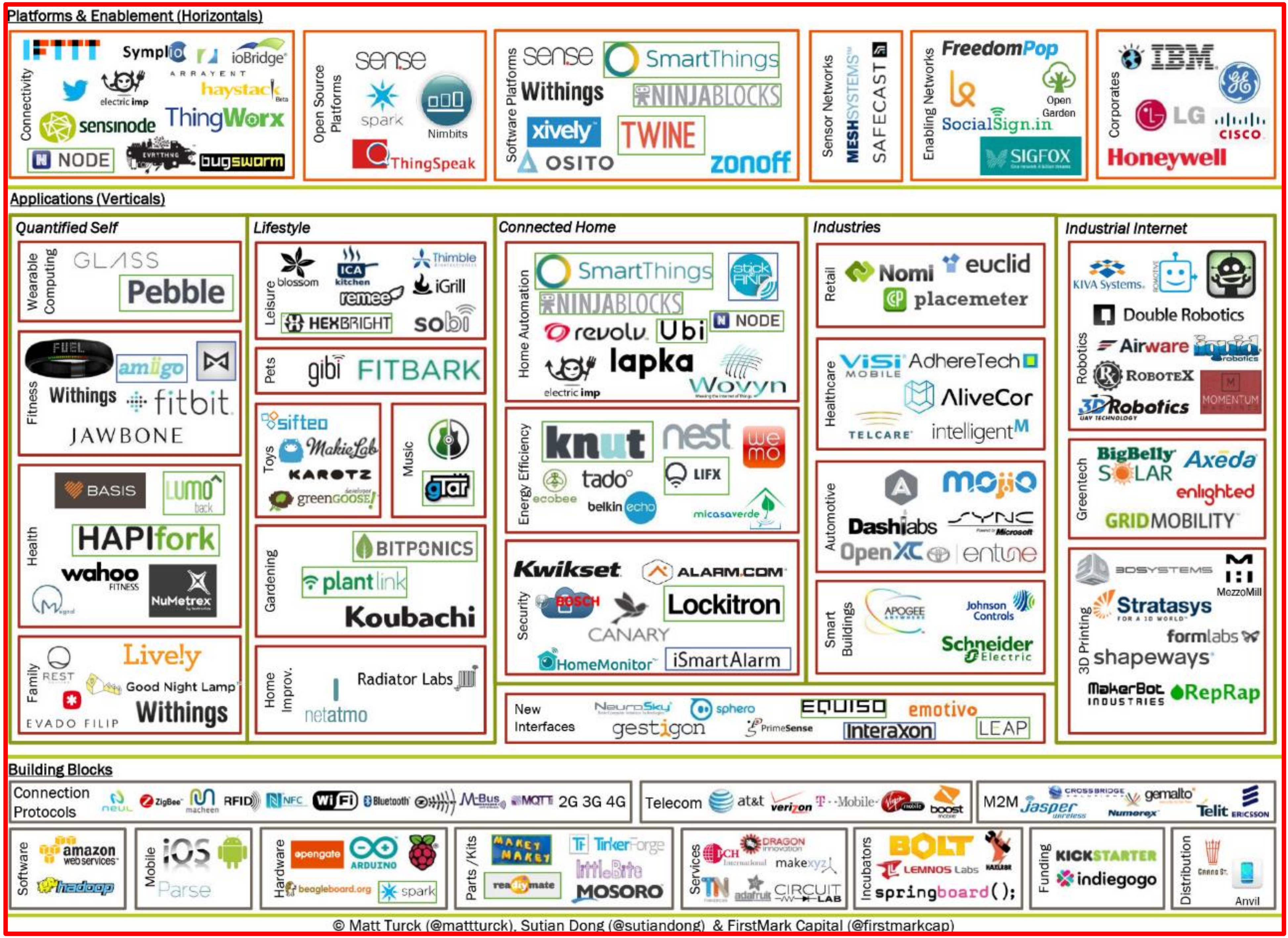


Regulating Disruptive Technologies in the Post-Regulatory State

Four broader attributes of the digital ecosystem make regulation of disruptive innovation even more complex:

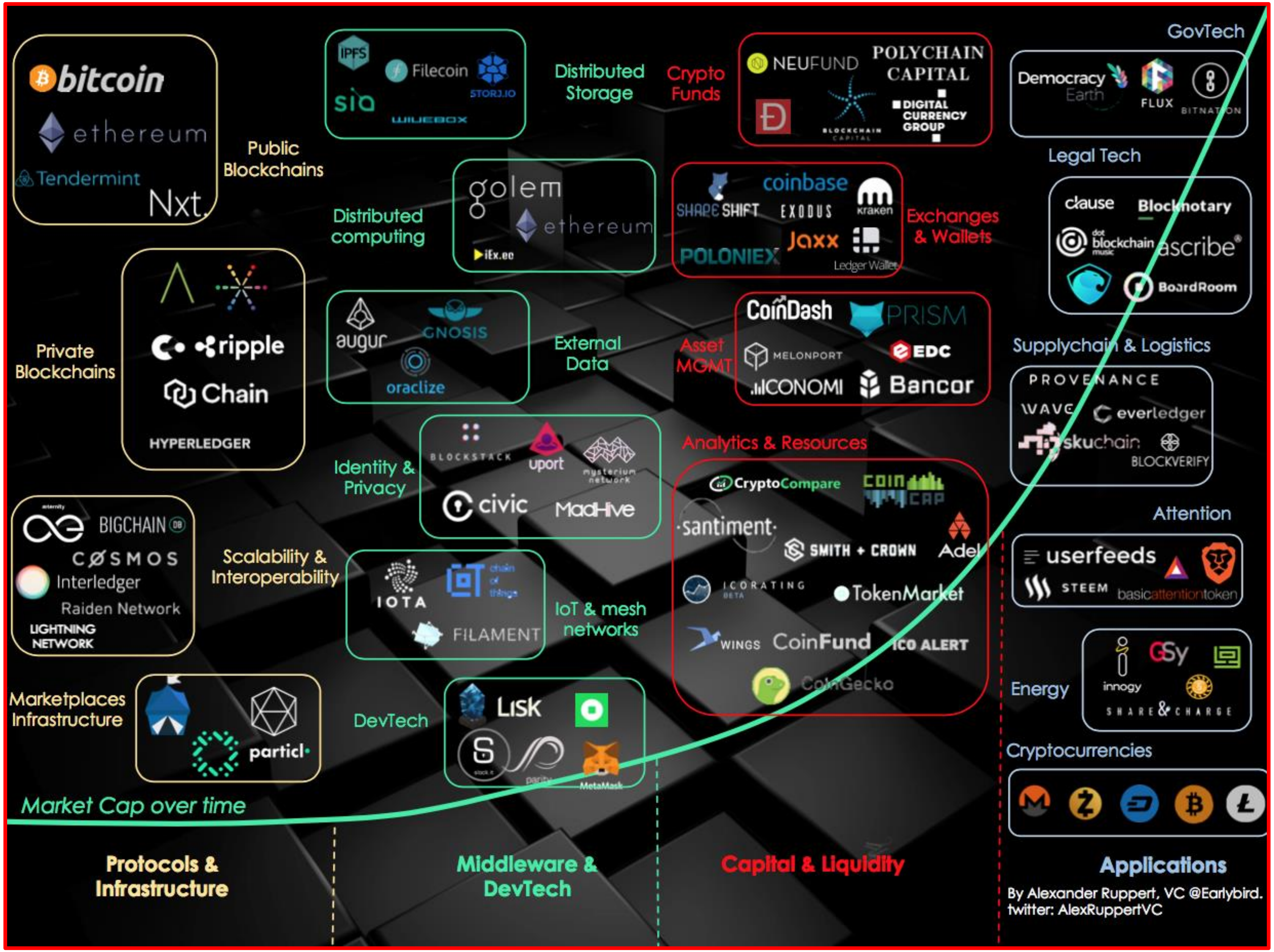
1. Variety in controllees
2. Variety in controllers
3. Variety in (and evolving) norms
4. Variety in control mechanisms

Example 1: IoT Ecosystem



© Matt Turck (@mattturck), Sutian Dong (@sutiandong) & FirstMark Capital (@firstmarkcap)

Example 2: Crypto Sector

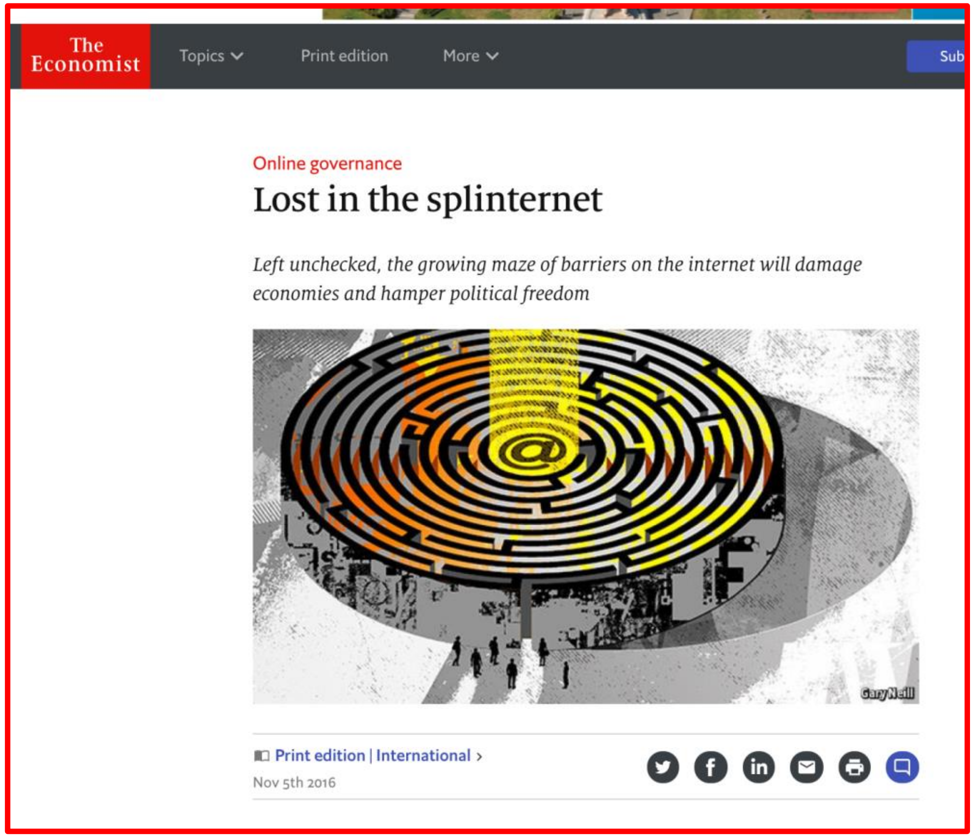


Regulating Digital Economy: Challenges for Lawmakers and Regulators

- Decision-makers face a variety of inherent challenges in “regulating” the digital economy, including:
  - *Justification*: Justifications for intervention, including market power, often shift faster than regulation can adapt.
  - *Prioritization*: Good regulation is a scarce resource.
  - *Reconciliation*: Managing competing policy goals and value trade-offs.
  - *Timing and Change*: Technology evolves faster than regulatory processes.
  - *Design*: Match legal designs with unique challenges of different technologies.
  - *Internationalization*: Regulatory challenges are increasing regional and global.
  - *Enforcement*: Law on the books versus law in action in decentralized environments.
  - *Unintended consequences*: Good intentions but undesirable outcomes are possible.

Biggest Ecosystem Challenge

How to avoid the fragmentation of the Internet and destroy the generative power of digital technologies?



Online governance

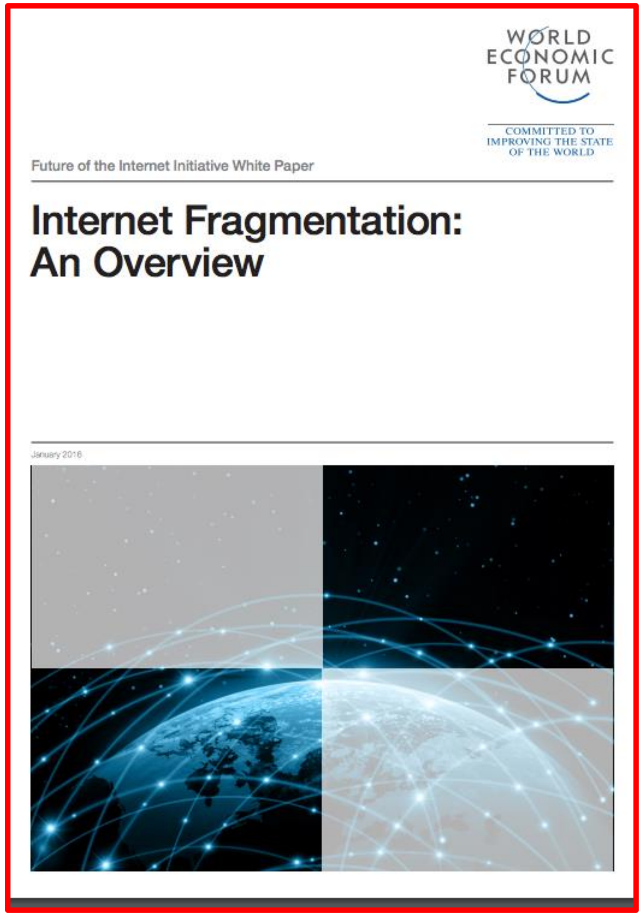
Lost in the splinternet

Left unchecked, the growing maze of barriers on the internet will damage economies and hamper political freedom

Print edition | International ›

Nov 5th 2016

https://www.economist.com/news/international/21709531-left-unchecked-growing-maze-barriers-internet-will-damage-economies-and



Future of the Internet Initiative White Paper

Internet Fragmentation: An Overview

January 2016

http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

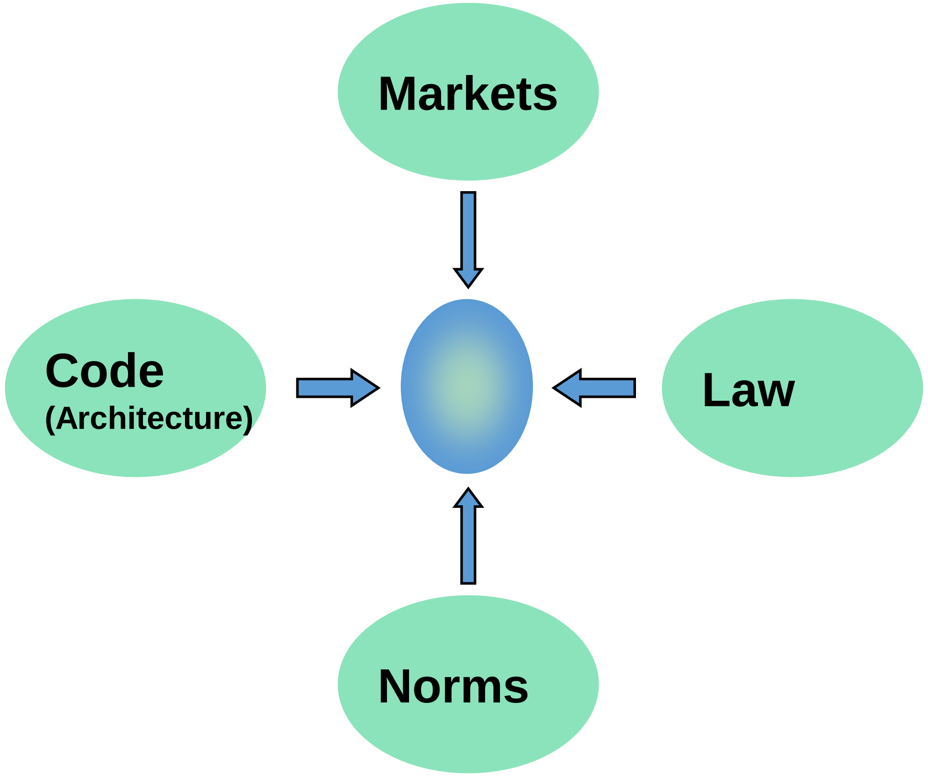
2 Regulatory Models in Cyberspace

Overview: Moving Beyond Law

- Addressing the fast-paced evolution and unique challenges of disruptive technologies requires a shift from law and government towards a more holistic *governance* approach.
- Effective governance in the digital age is based on three concepts:
  - Multimodal: Consider and combine different “modes of regulation”.
  - Multilayer: local, national, regional, and global engagement.
  - Multistakeholder: government, companies, civil society & academia, co-creating policy solutions.
- However, law continues to play a key role.

Governance: Multimodal

- Consider all "modes of regulation" and work towards blended regimes
  - Law
  - Standard setting
  - Transparency
  - Information sharing
  - Self-regulation
- Over the past decade, increased importance of "code" as a "regulator" in digital environments
- Requires interdisciplinary expertise, education, mind-set



Source: Lessig, Code and Other Laws of Cyberspace (1999)

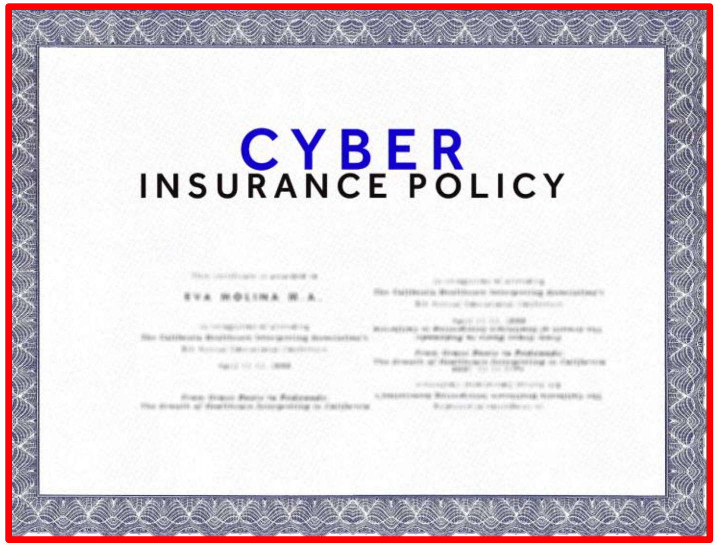
Example: Cybersecurity

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

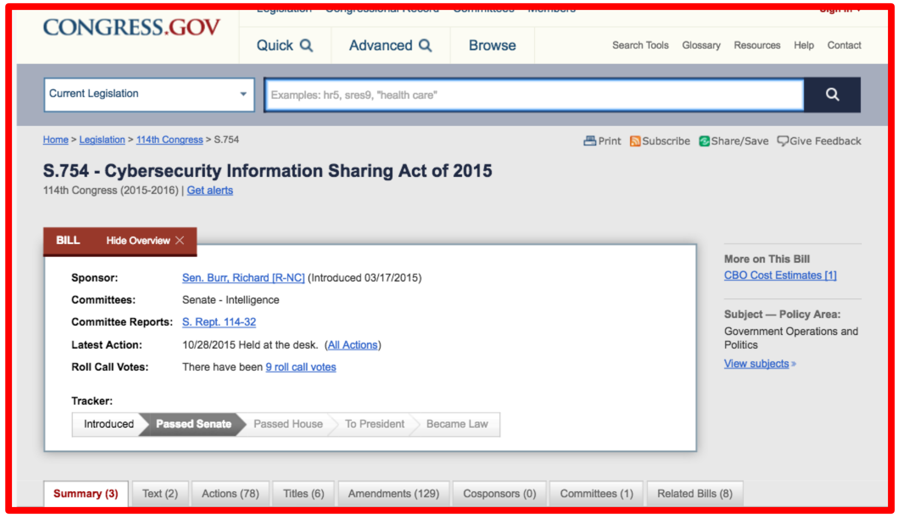
White Paper

Global Agenda Council on Cybersecurity

April 2016


CYBER INSURANCE POLICY

CH
National Campaign for Cyber Hygiene
Count, Configure, Control, Patch, Repeat
Items & Resources
Download Cyber Hygiene Toolkits Here



Home > Legislation > 114th Congress > S.754

S.754 - Cybersecurity Information Sharing Act of 2015

114th Congress (2015-2016) | Get alerts

Sponsor: Sen. Burr, Richard [R-NC] (Introduced 03/17/2015)

Committees: Senate - Intelligence

Committee Reports: S. Rept. 114-32

Latest Action: 10/28/2015 Held at the desk. (All Actions)

Roll Call Votes: There have been 9 roll call votes

Tracker: Introduced > Passed Senate > Passed House > To President > Became Law

More on This Bill

CBO Cost Estimates [1]

Subject — Policy Area:

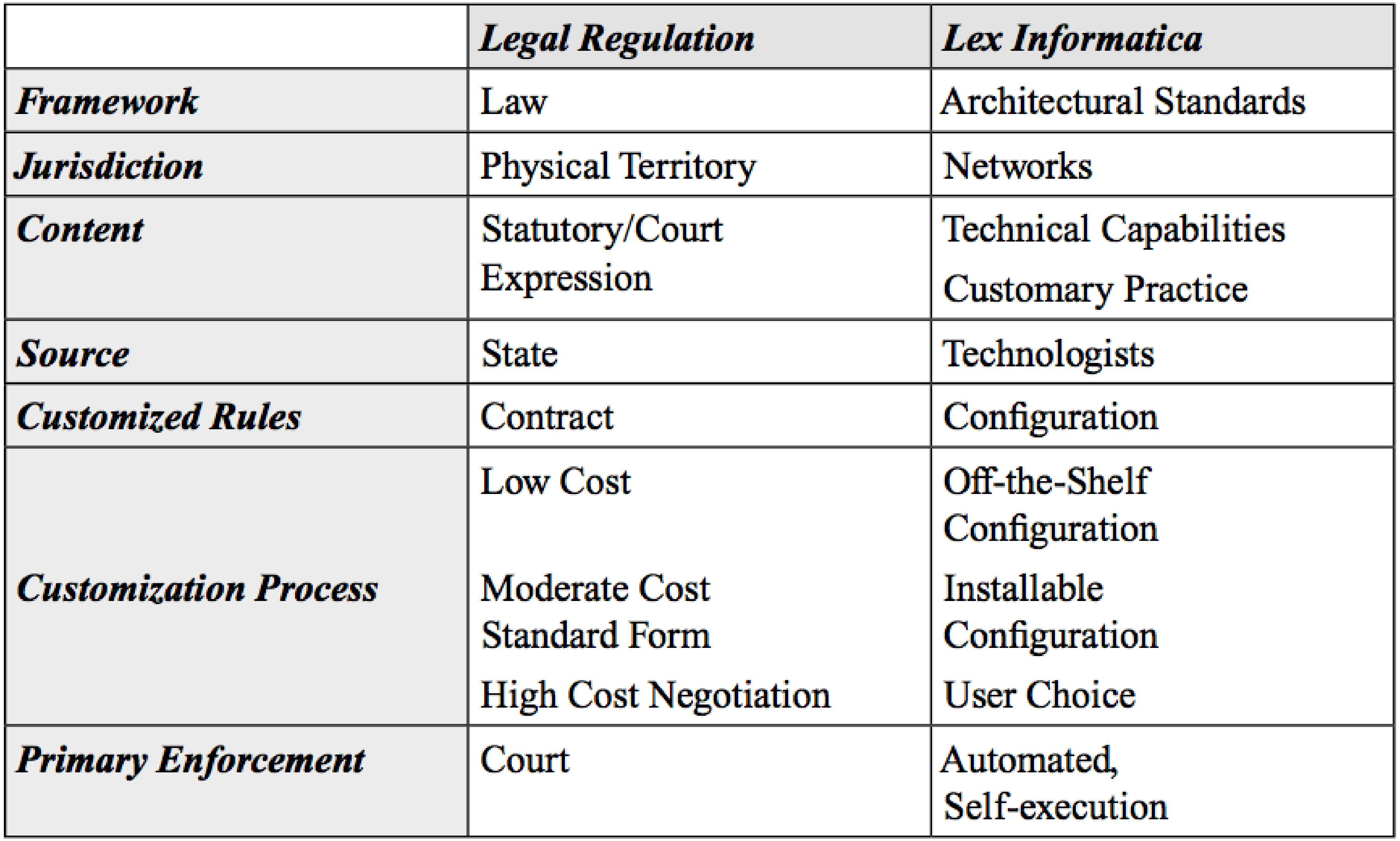
Government Operations and Politics

View subjects »

Deep Dive 1: Lex Informatica/Code-Based Regulation

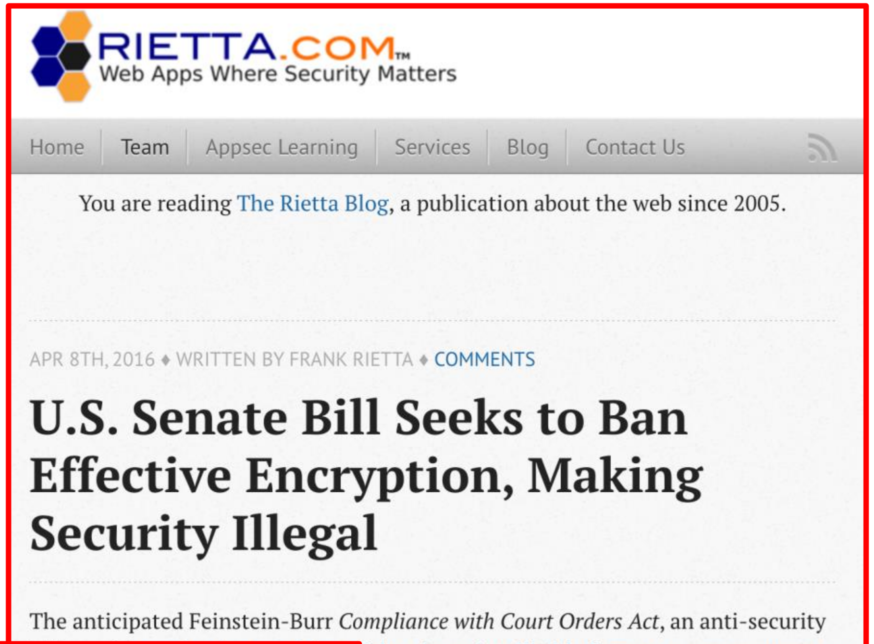
- New Chicago School: “Architecture” as a mode of regulation
  - In Cyberspace, architecture is code, and “code is Law” (Lawrence Lessig).
  - Design of code shapes/constrains human behavior in the digitally connected environment
  - Technologists set the rules through hardware and software choices
  - Governments can shape “code” and use it as indirect mode of regulation (example: content filters, DRM systems)
- Similarly, concept of *lex informatica* (Joel Reidenberg): Forming information policy rules through technology
  - In analogy to *lex mercatoria*
  - Parallel rule system, both regulatory tools (design and legal tools) are available to a hierarchical regulator

Legal Regulation v. Lex Informatica



	Legal Regulation	***Lex Informatica***
Framework	Law	Architectural Standards
Jurisdiction	Physical Territory	Networks
Content	Statutory/Court Expression	Technical Capabilities Customary Practice
Source	State	Technologists
Customized Rules	Contract	Configuration
Customization Process	Low Cost Moderate Cost Standard Form High Cost Negotiation	Off-the-Shelf Configuration Installable Configuration User Choice
Primary Enforcement	Court	Automated, Self-execution

Example: Encryption



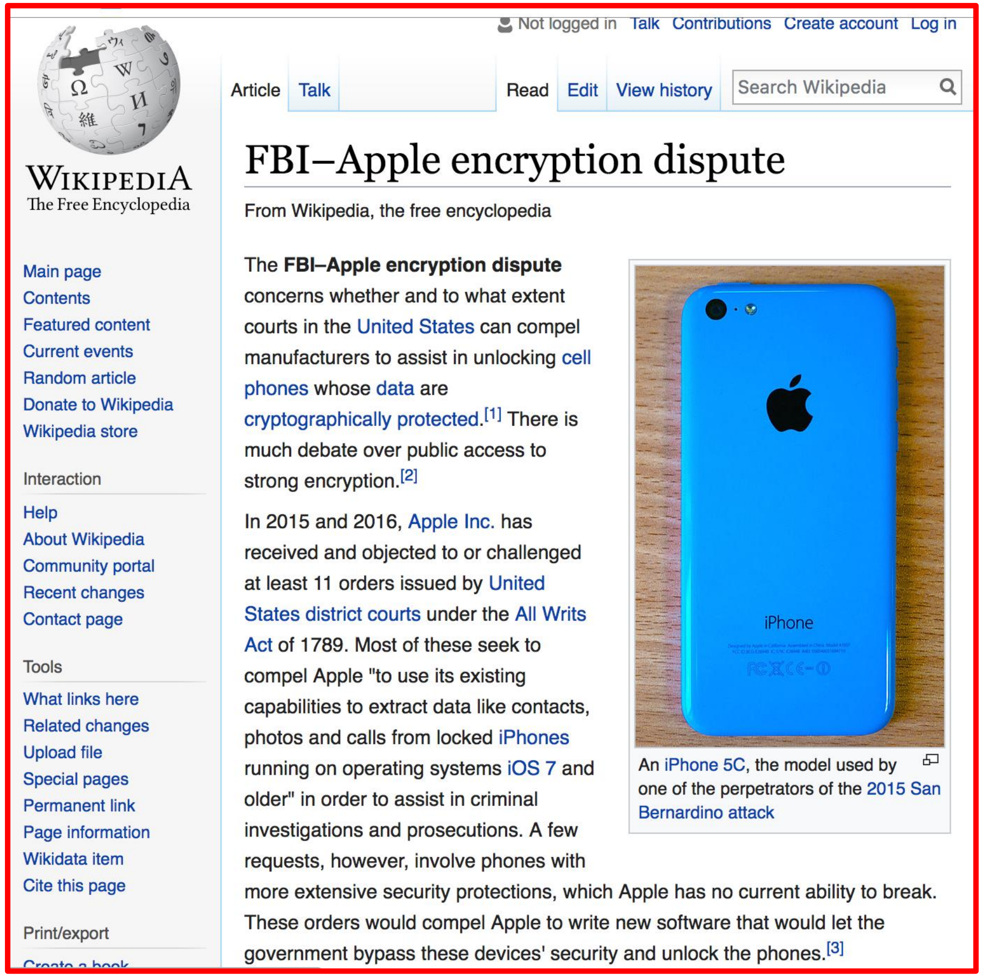
RIETTA.COM™
Web Apps Where Security Matters

You are reading The Rietta Blog, a publication about the web since 2005.

APR 8TH, 2016 ♦ WRITTEN BY FRANK RIETTA ♦ COMMENTS

U.S. Senate Bill Seeks to Ban Effective Encryption, Making Security Illegal

The anticipated Feinstein-Burr *Compliance with Court Orders Act*, an anti-security
f data in an intelligible format to a government
om). A draft copy was uploaded by The Hill
ether it has been submitted officially within the



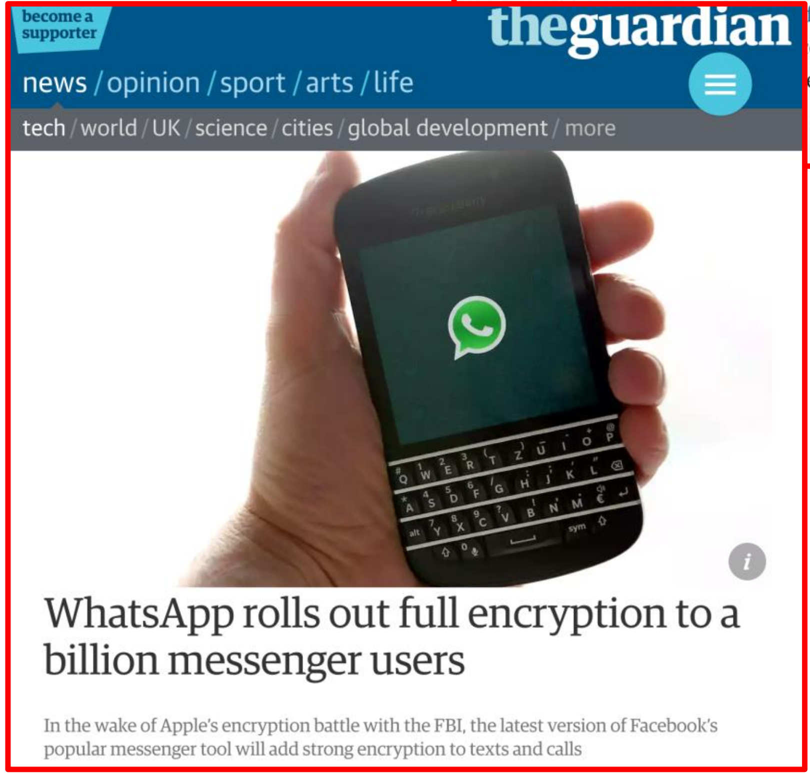
FBI–Apple encryption dispute

From Wikipedia, the free encyclopedia

The **FBI–Apple encryption dispute** concerns whether and to what extent courts in the United States can compel manufacturers to assist in unlocking cell phones whose data are cryptographically protected.[1] There is much debate over public access to strong encryption.[2]

An iPhone 5C, the model used by one of the perpetrators of the 2015 San Bernardino attack

In 2015 and 2016, Apple Inc. has received and objected to or challenged at least 11 orders issued by United States district courts under the All Writs Act of 1789. Most of these seek to compel Apple "to use its existing capabilities to extract data like contacts, photos and calls from locked iPhones running on operating systems iOS 7 and older" in order to assist in criminal investigations and prosecutions. A few requests, however, involve phones with more extensive security protections, which Apple has no current ability to break. These orders would compel Apple to write new software that would let the government bypass these devices' security and unlock the phones.[3]



become a supporter
theguardian
news / opinion / sport / arts / life
tech / world / UK / science / cities / global development / more

WhatsApp rolls out full encryption to a billion messenger users

In the wake of Apple's encryption battle with the FBI, the latest version of Facebook's popular messenger tool will add strong encryption to texts and calls

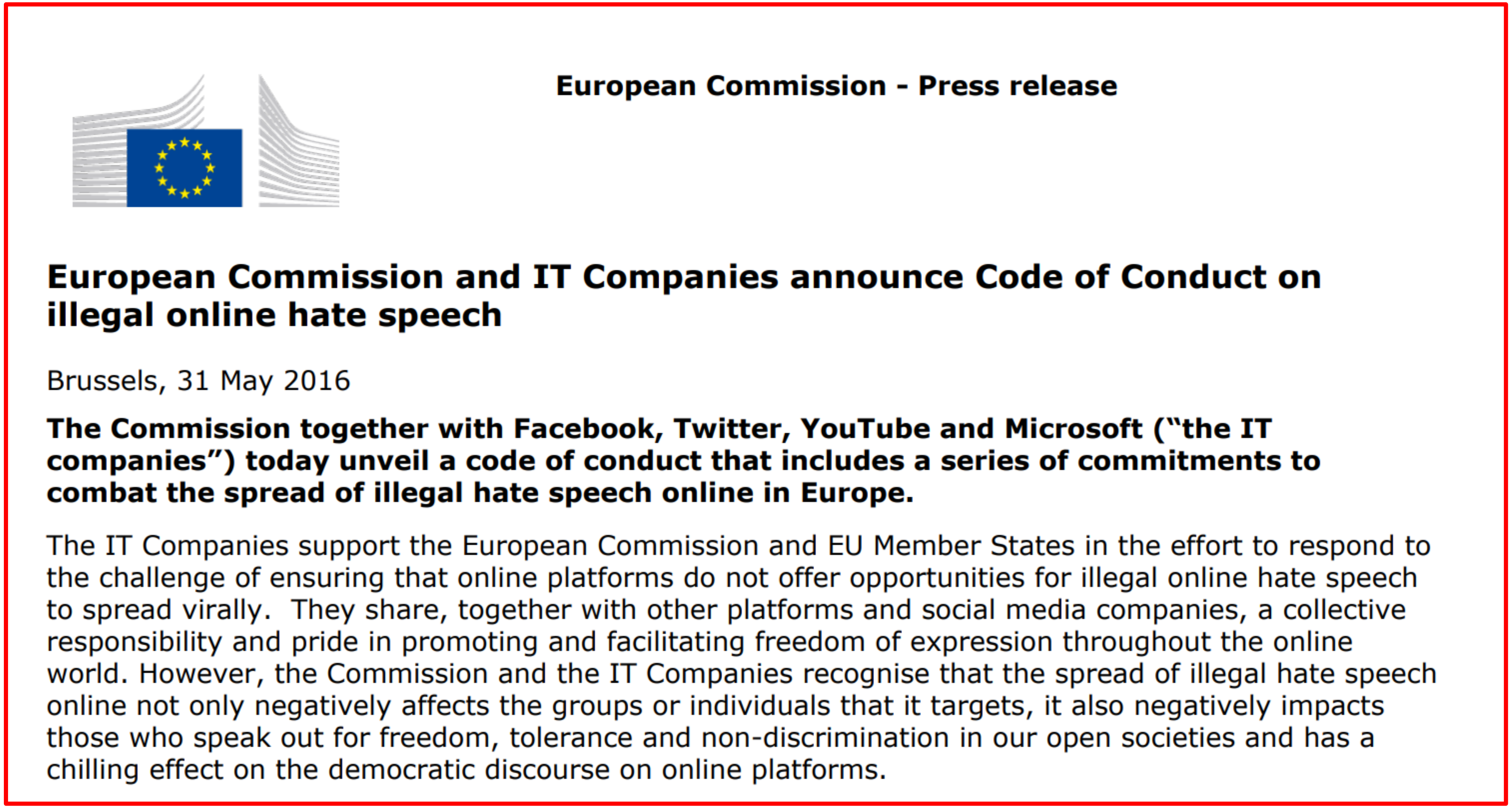
Discussion

- What are the strengths and weaknesses of code-based regulation?
- How does code-based regulation address the challenges of lawmaking and regulation in the digital economy? Which challenges remain unresolved?
- Where do you see the main areas of application?

Deep Dive 2: Self- and Co-Regulation

- Self-regulation based on the principle of subsidiarity, i.e. governmental intervention should only take place if actors in a relevant context are unable to find suitable solutions themselves.
- Two types of self-regulation:
  - Concept of private groups, who make autonomous decisions that limit behavior, bound by laws of general application.
  - Concept within a framework set by the government (directed self-regulation, co-regulation, etc.)
- Self-regulation to be considered where its application leads to higher efficiency than traditional legal mechanisms, and if compliance with private rules is higher than with alternative arrangements.

Example: Code of Conduct on Illegal Hate Speech (EU)



European Commission - Press release

European Commission and IT Companies announce Code of Conduct on illegal online hate speech

Brussels, 31 May 2016

The Commission together with Facebook, Twitter, YouTube and Microsoft ("the IT companies") today unveil a code of conduct that includes a series of commitments to combat the spread of illegal hate speech online in Europe.

The IT Companies support the European Commission and EU Member States in the effort to respond to the challenge of ensuring that online platforms do not offer opportunities for illegal online hate speech to spread virally. They share, together with other platforms and social media companies, a collective responsibility and pride in promoting and facilitating freedom of expression throughout the online world. However, the Commission and the IT Companies recognise that the spread of illegal hate speech online not only negatively affects the groups or individuals that it targets, it also negatively impacts those who speak out for freedom, tolerance and non-discrimination in our open societies and has a chilling effect on the democratic discourse on online platforms.

Discussion

- What are the strengths and weaknesses of self- and co-regulation?

- How does self-regulation address the challenges of lawmaking and regulation in the digital economy? Which challenges remain unresolved?

- Where do you see the main areas of application?

Deep Dive 3: A Role for Law & Regulation

- The tools of governance are critical for addressing disruptive technologies and innovation, but that does not mean law is irrelevant
- In the age of governance, law remains important in at least four ways:
    1. Law as embodiment of fundamental values
    2. Law as coordinating mechanism
    3. Law as indirect force
    4. Law as foundation
- Pro memoria: Digital technologies can also *strengthen* the rule of law, access to justice, and human rights

Law: Fundamental Values

- Law provides the formal space to engage in a public dialogue about the fundamental values that may be in conflict with the impacts of disruptive technologies
- Disruptive technologies create numerous tensions:
  - Privacy vs customization
  - Personal data security vs national security
  - Incumbent industries vs start-up platforms
  - Traditional forms of labor vs automation
  - …
- Law is space to stabilize the upheaval and discuss these fundamental values

Law: Coordinating Mechanism

- Law serves as a coordinating force that can bridge various stakeholders in ways that would be impossible otherwise, both in process and in result
  - *Procedural* coordination: the legislative and regulatory processes can create pathways for coordination and dialogue
    - Example: Apple v. FBI case resulted in congressional hearings, numerous legal briefs, all leading to coordination both within and across stakeholder groups
  - *Resultant* coordination: law and regulation can itself direct coordination
    - Example: reforms to government agency structure in order to improve both inter-agency coordination on cybersecurity risks, as well as information sharing systems between the public and private sectors

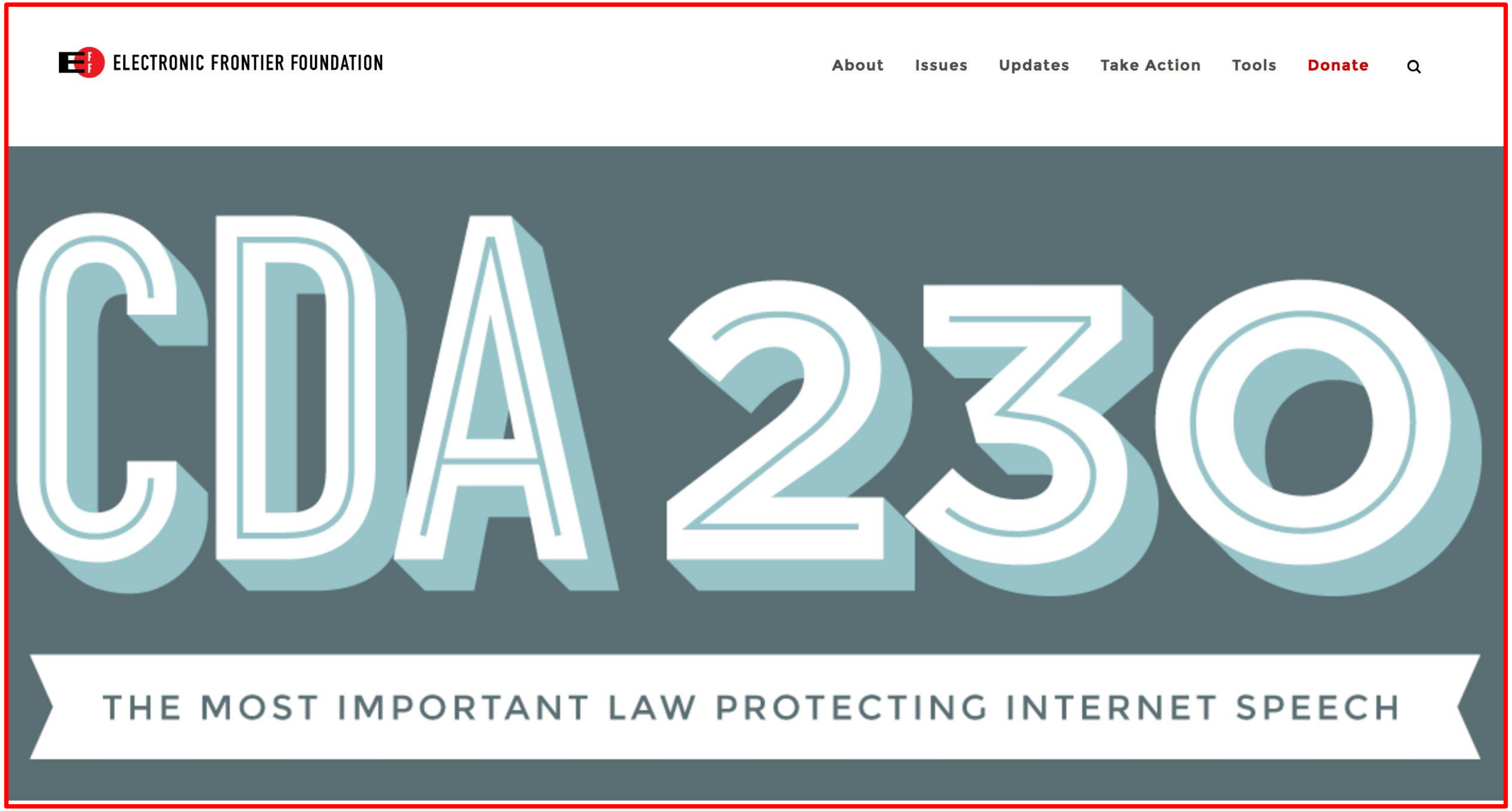
Law: Indirect Force

- Although there are many circumstances where application of law and regulation is ill-suited to directly addressing fast-paced disruptive technologies, it can be used effectively to *indirectly* affect these technologies
- Examples:
    - Directly regulating the privacy protections in products and services vs. enabling consumer protection agencies to monitor product and service privacy commitment and compliance
    - Direct imposing cybersecurity standards vs. supporting testing laboratories to increase transparency around cybersecurity practices

Law: Foundation and Enabler

- Digital technologies did not emerge in a legal vacuum – they reflect a legal foundation that already exists
- Relationship between sound and robust legal framework and innovation broadly acknowledged
- The interplay between law and technology is not static; just as disruptive technologies might trigger adjustments in law and regulation, changes to law and regulation will shape the next generation of disruptive technologies
    - Example: the complex and limiting regulatory system of taxicab licensing, insurance, and medallions was a primary factor in the structure of ride-sharing platforms

Example: CDA 230



ELECTRONIC FRONTIER FOUNDATION

CDA 230

THE MOST IMPORTANT LAW PROTECTING INTERNET SPEECH

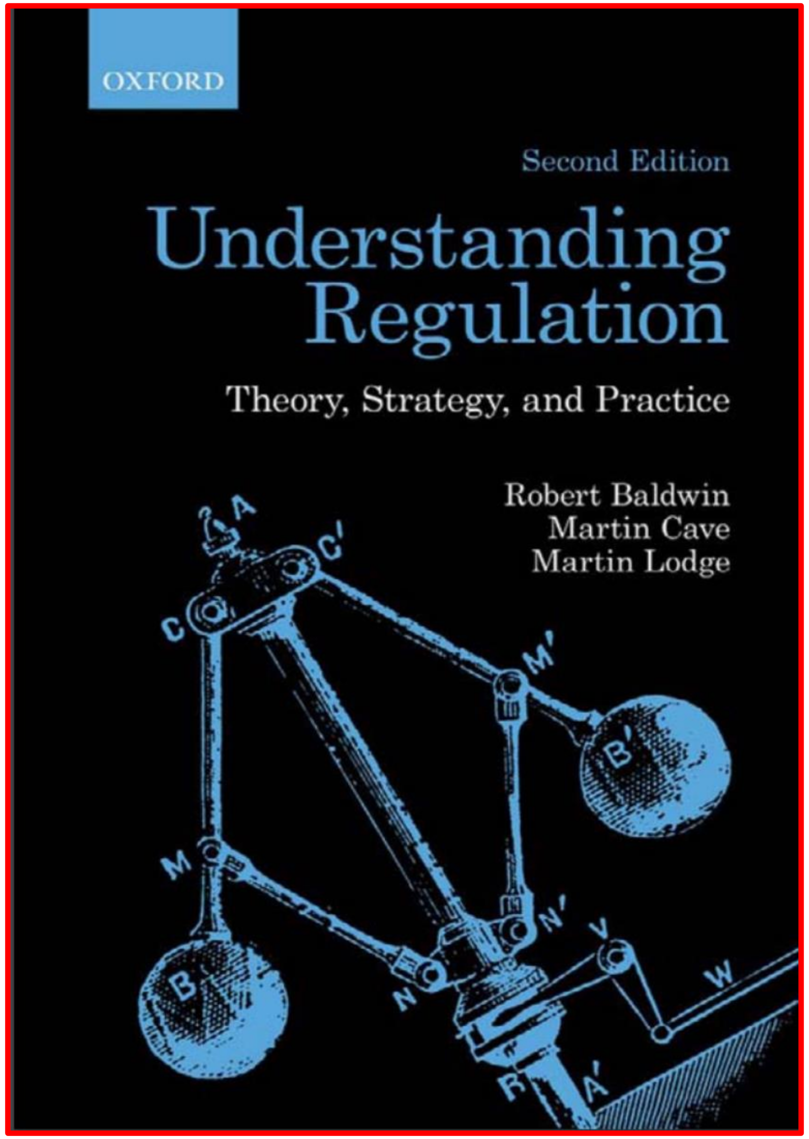
https://www.eff.org/issues/cda230

Regulatory (Legal) Strategies

Consider full spectrum of regulatory (legal) strategies (see Baldwin/Cave, Understanding Regulation):

- *Command & control*—where legal authority and the command of law is used to pursue policy objectives.
- *Incentive-based regimes*—where contracts, grants, loans, subsidies, or other incentives are used to influence conduct.
- *Market-harnessing controls*—where governments channel competitive forces to particular ends (for example, by using franchise auctions to achieve benefits for consumers).
- *Disclosure regulation*—where information is deployed strategically (e.g. so as to empower consumers).
- *Direct action*—where the state takes physical action itself (e.g. to contain a hazard or nuisance).
- *Rights and liability*—where rights and liability rules are structured and allocated so as to create desired incentives and constraints (e.g. rights to clean water are created in order to deter polluters).

Further Reading



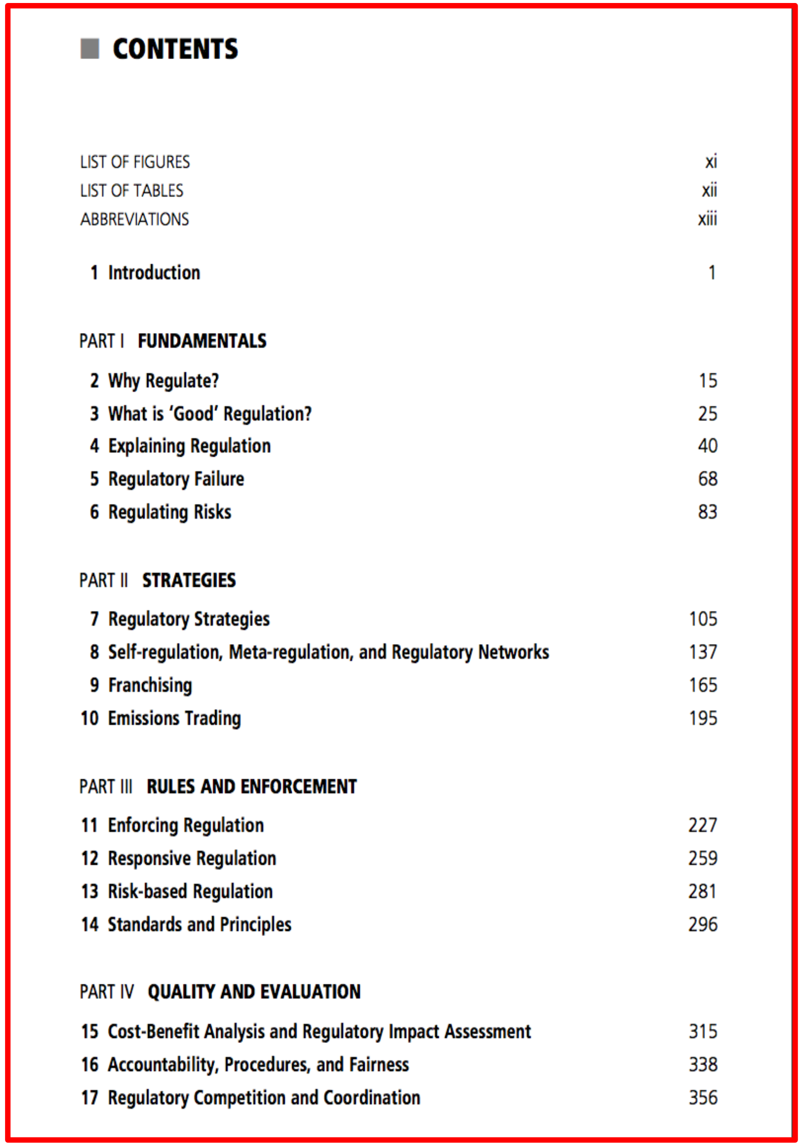
OXFORD

Second Edition

Understanding Regulation

Theory, Strategy, and Practice

Robert Baldwin
Martin Cave
Martin Lodge



CONTENTS

LIST OF FIGURES xi
LIST OF TABLES xii
ABBREVIATIONS xiii

1 Introduction 1

PART I FUNDAMENTALS

2 Why Regulate? 15
3 What is 'Good' Regulation? 25
4 Explaining Regulation 40
5 Regulatory Failure 68
6 Regulating Risks 83

PART II STRATEGIES

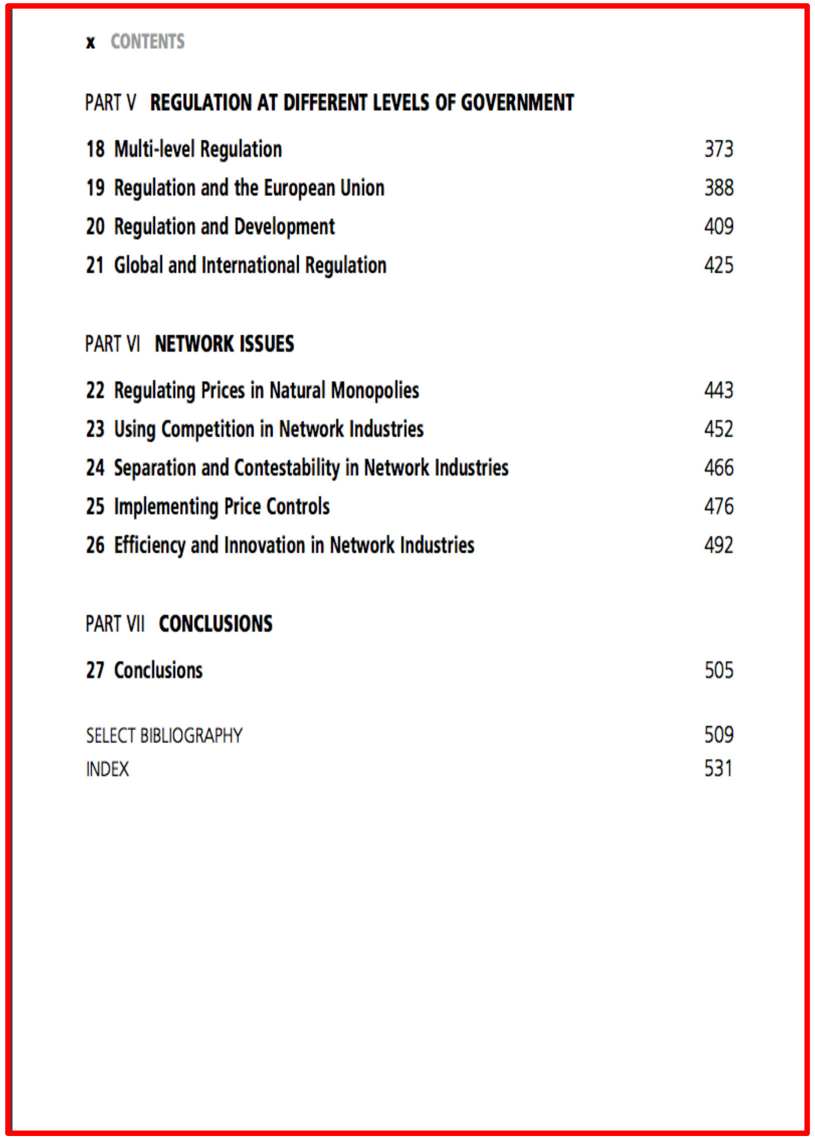
7 Regulatory Strategies 105
8 Self-regulation, Meta-regulation, and Regulatory Networks 137
9 Franchising 165
10 Emissions Trading 195

PART III RULES AND ENFORCEMENT

11 Enforcing Regulation 227
12 Responsive Regulation 259
13 Risk-based Regulation 281
14 Standards and Principles 296

PART IV QUALITY AND EVALUATION

15 Cost-Benefit Analysis and Regulatory Impact Assessment 315
16 Accountability, Procedures, and Fairness 338
17 Regulatory Competition and Coordination 356



PART V REGULATION AT DIFFERENT LEVELS OF GOVERNMENT

18 Multi-level Regulation 373
19 Regulation and the European Union 388
20 Regulation and Development 409
21 Global and International Regulation 425

PART VI NETWORK ISSUES

22 Regulating Prices in Natural Monopolies 443
23 Using Competition in Network Industries 452
24 Separation and Contestability in Network Industries 466
25 Implementing Price Controls 476
26 Efficiency and Innovation in Network Industries 492

PART VII CONCLUSIONS

27 Conclusions 505

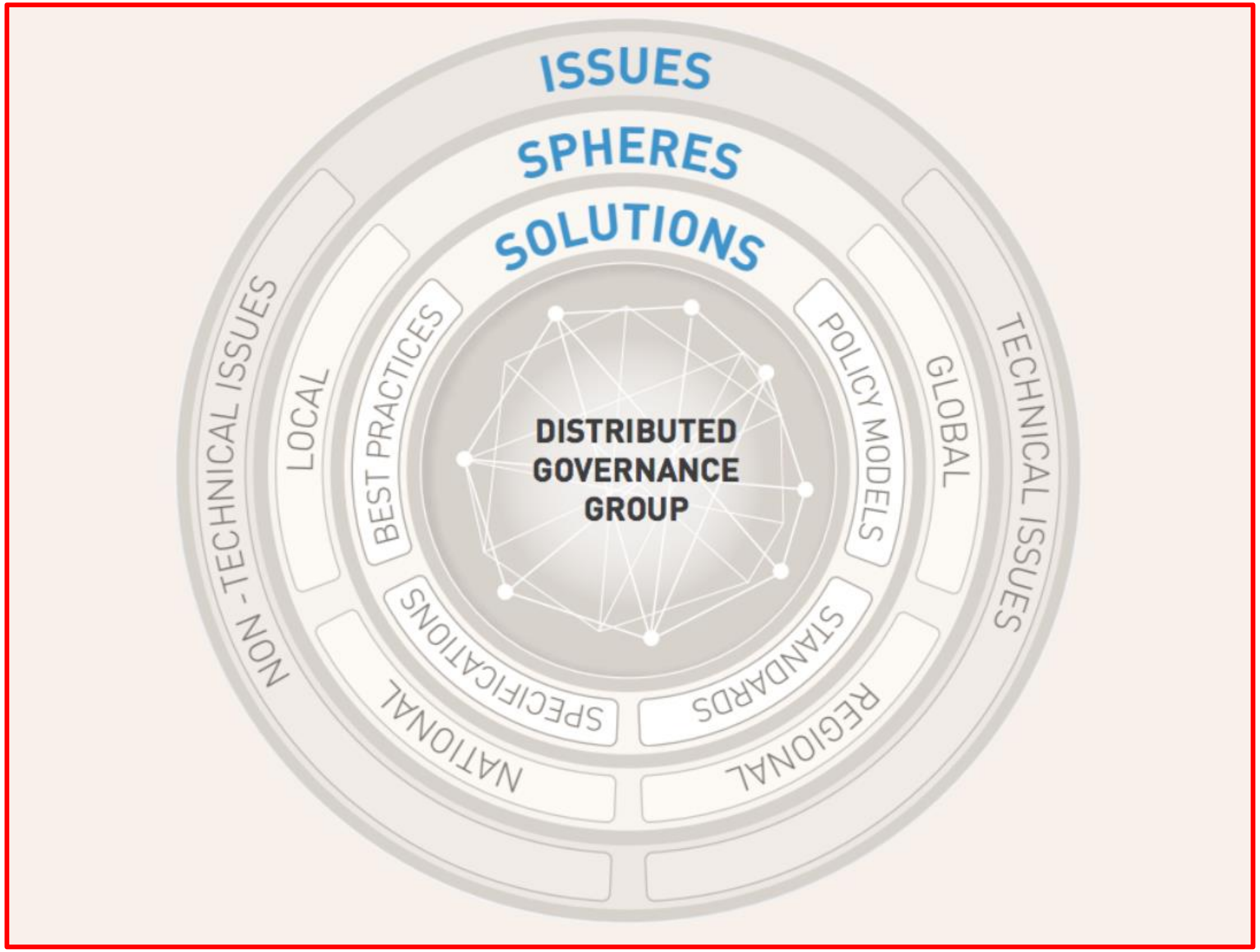
SELECT BIBLIOGRAPHY 509
INDEX 531

3 Multi-Stakeholder Governance

Governance: Multistakeholder

- Addressing the complex challenges and embracing the full potential of digital technologies requires a range of skills, knowledge, and perspectives that are often unavailable in a single place
- Robust solutions benefit from input from a variety of stakeholders, including:
    - Private sector
    - Governments
    - Academia
    - Civil society
- Important approach across all governance functions, incl. issues identification, development and selection of approaches, implementation, and evaluation

Collaborative, Decentralized IG Model

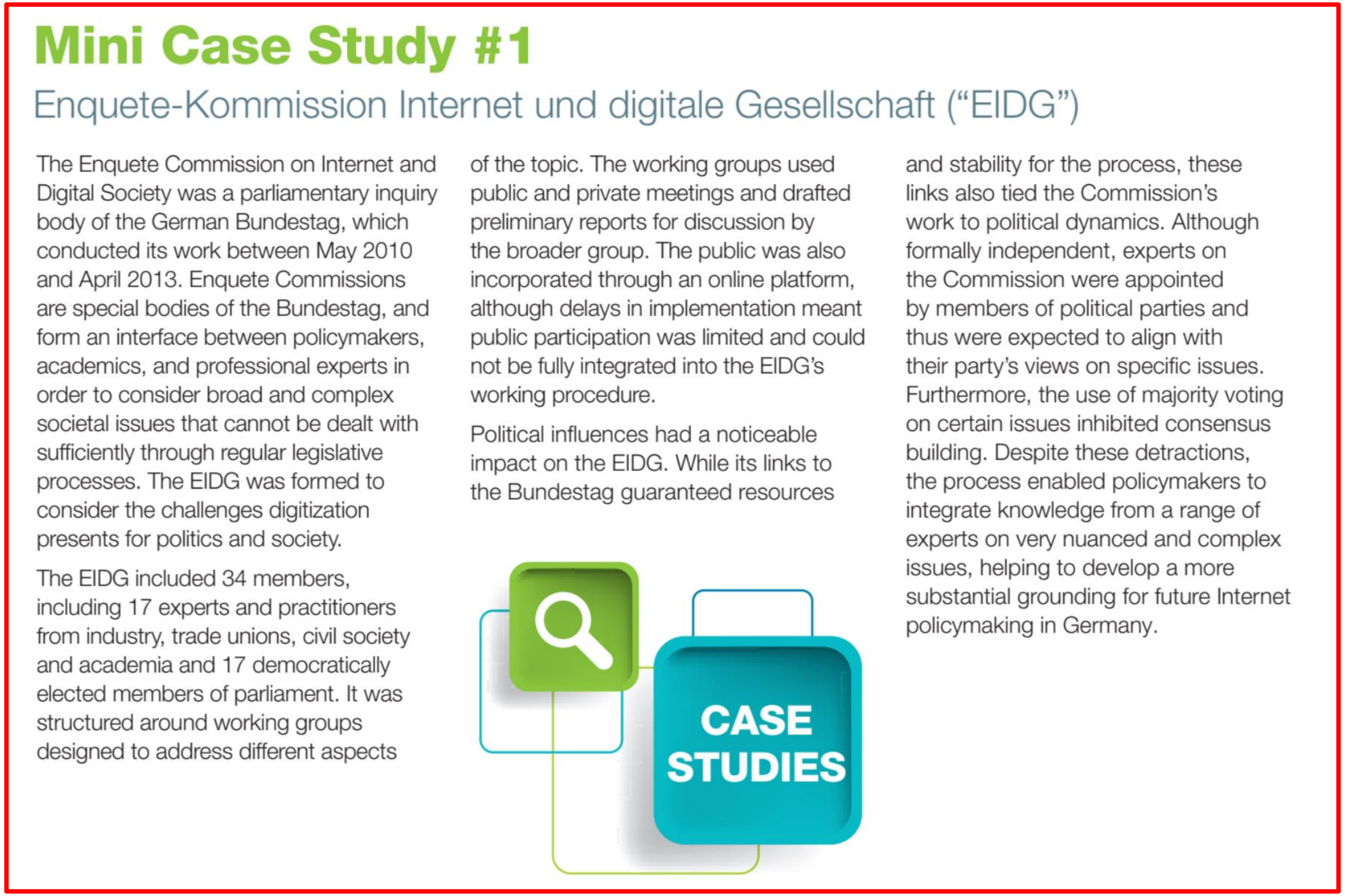


Towards a Collaborative, Decentralized Internet Governance Ecosystem

Report by the Panel on Global Internet Cooperation and Governance Mechanisms

Available at: https://www.internetsociety.org/sites/default/files/Internet%20Governance%20Report%20iPDF.pdf

Example: EIDG (Germany)



Mini Case Study #1

Enquete-Kommission Internet und digitale Gesellschaft ("EIDG")

The Enquete Commission on Internet and Digital Society was a parliamentary inquiry body of the German Bundestag, which conducted its work between May 2010 and April 2013. Enquete Commissions are special bodies of the Bundestag, and form an interface between policymakers, academics, and professional experts in order to consider broad and complex societal issues that cannot be dealt with sufficiently through regular legislative processes. The EIDG was formed to consider the challenges digitization presents for politics and society.

The EIDG included 34 members, including 17 experts and practitioners from industry, trade unions, civil society and academia and 17 democratically elected members of parliament. It was structured around working groups designed to address different aspects of the topic. The working groups used public and private meetings and drafted preliminary reports for discussion by the broader group. The public was also incorporated through an online platform, although delays in implementation meant public participation was limited and could not be fully integrated into the EIDG's working procedure.

Political influences had a noticeable impact on the EIDG. While its links to the Bundestag guaranteed resources and stability for the process, these links also tied the Commission's work to political dynamics. Although formally independent, experts on the Commission were appointed by members of political parties and thus were expected to align with their party's views on specific issues. Furthermore, the use of majority voting on certain issues inhibited consensus building. Despite these detractions, the process enabled policymakers to integrate knowledge from a range of experts on very nuanced and complex issues, helping to develop a more substantial grounding for future Internet policymaking in Germany.

https://cyber.harvard.edu/node/99052

Further Reading

https://cyber.harvard.edu/node/99052

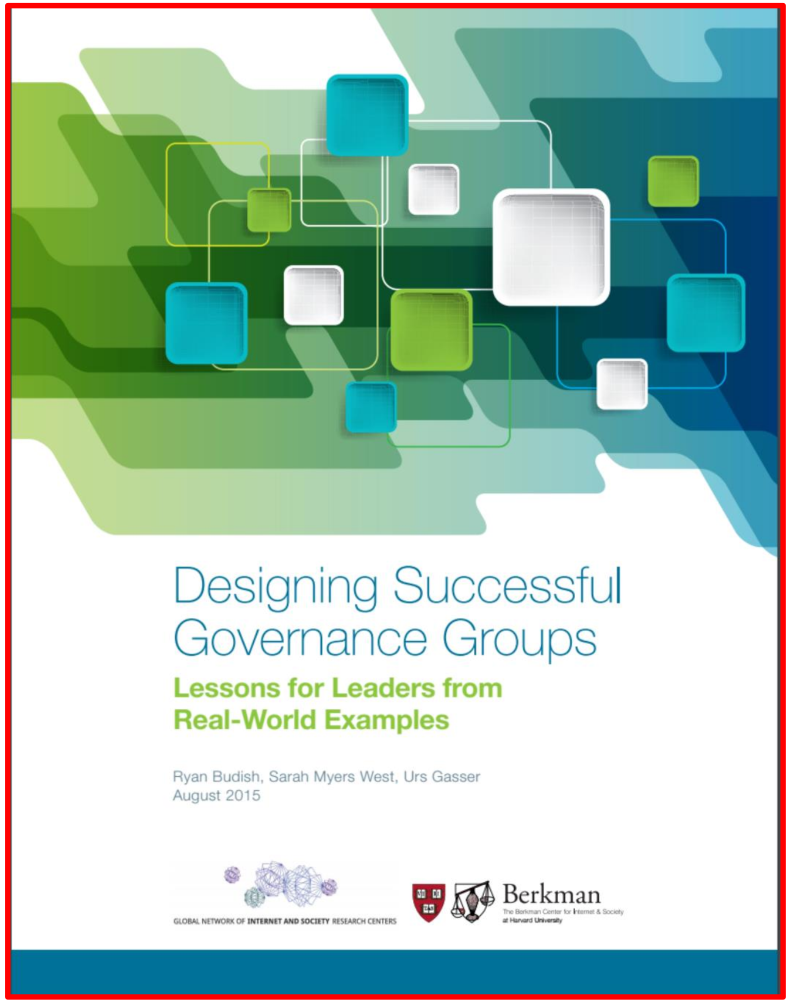
Urs Gasser, Ryan Budish, and Sarah Myers West

MULTISTAKEHOLDER AS GOVERNANCE GROUPS: OBSERVATIONS FROM CASE STUDIES

January 15, 2015
Berkman Center for Internet & Society Research Publication Series

WITHIN THE

GLOBAL NETWORK OF **INTERNET AND SOCIETY** RESEARCH CENTERS



Designing Successful Governance Groups

Lessons for Leaders from Real-World Examples

Ryan Budish, Sarah Myers West, Urs Gasser
August 2015

GLOBAL NETWORK OF **INTERNET AND SOCIETY** RESEARCH CENTERS

Berkman
The Berkman Center for Internet & Society at Harvard University

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2549270

Governance: Multilayered

- Many of the challenges of disruptive technologies occur at the local, national, regional, and global levels; effective solutions require working at and across each layer of governance
- Multilayered governance is not only necessary to “tame” disruptive technology, but also:

  “For governments and national policy making, facilitating increased international collaboration and complementing inward with more outward-looking approaches is now key to sustained success in innovation”

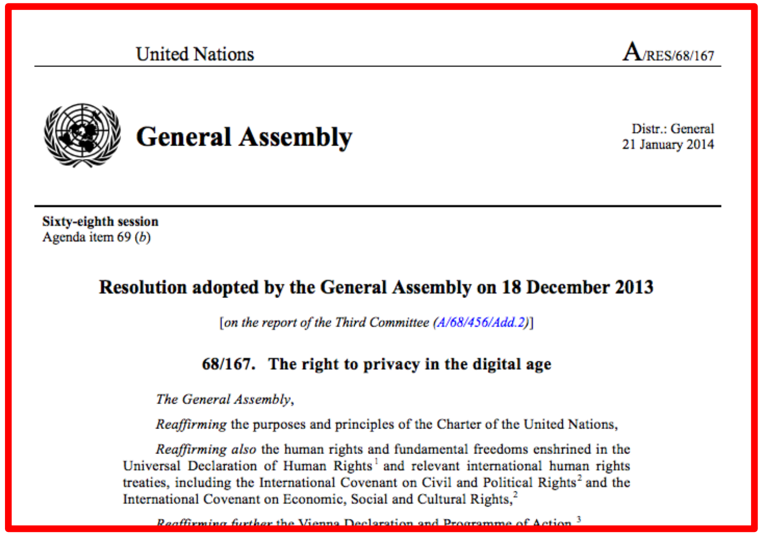
  The Global Innovation Index 2016: Winning with Global Innovation, p. 12
- Removing barriers to global cooperation and flow of ideas, knowledge, and people are new priorities in innovation policy

Example: Digital Privacy and Big Data

THE OECD
PRIVACY FRAMEWORK

OECD

2013



United Nations A/RES/68/167

General Assembly

Distr.: General
21 January 2014

Sixty-eighth session
Agenda item 69 (*b*)

Resolution adopted by the General Assembly on 18 December 2013

[*on the report of the Third Committee (A/68/456/Add.2)*]

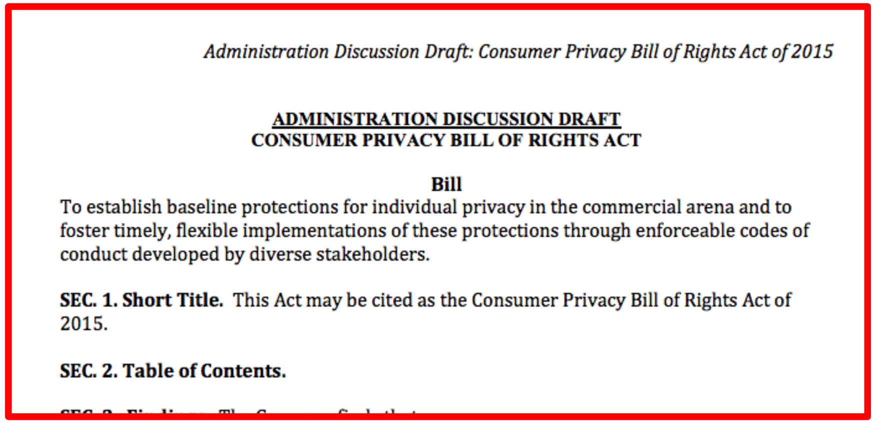
68/167. The right to privacy in the digital age

The General Assembly,

Reaffirming the purposes and principles of the Charter of the United Nations,

Reaffirming also the human rights and fundamental freedoms enshrined in the Universal Declaration of Human Rights[1] and relevant international human rights treaties, including the International Covenant on Civil and Political Rights[2] and the International Covenant on Economic, Social and Cultural Rights,[2]

Reaffirming further the Vienna Declaration and Programme of Action,[3]



Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015

ADMINISTRATION DISCUSSION DRAFT
CONSUMER PRIVACY BILL OF RIGHTS ACT

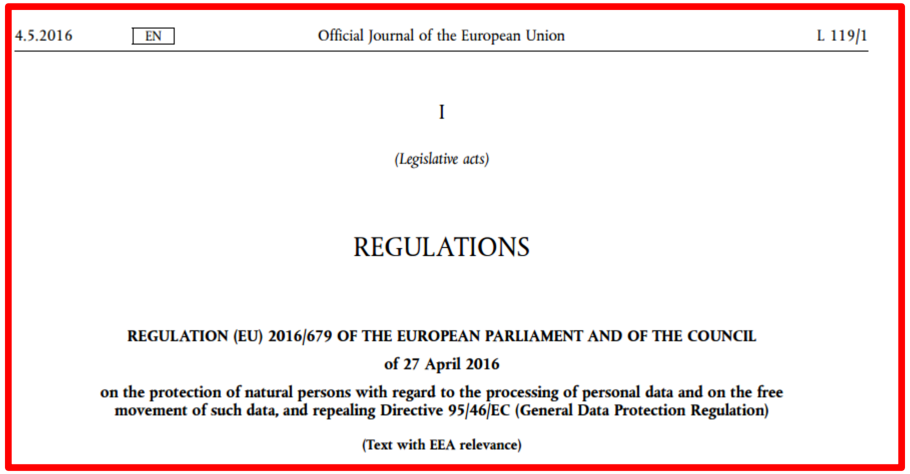
Bill

To establish baseline protections for individual privacy in the commercial arena and to foster timely, flexible implementations of these protections through enforceable codes of conduct developed by diverse stakeholders.

SEC. 1. Short Title. This Act may be cited as the Consumer Privacy Bill of Rights Act of 2015.

SEC. 2. Table of Contents.

SEC. 3. Findings. The Congress finds that



4.5.2016 EN Official Journal of the European Union L 119/1

I

(Legislative acts)

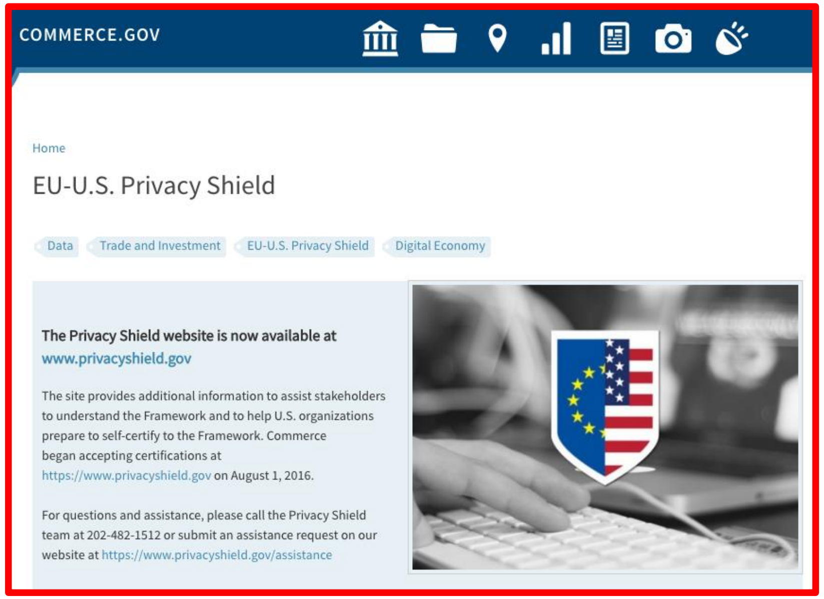
REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)



EU-U.S. Privacy Shield

The Privacy Shield website is now available at www.privacyshield.gov

The site provides additional information to assist stakeholders to understand the Framework and to help U.S. organizations prepare to self-certify to the Framework. Commerce began accepting certifications at https://www.privacyshield.gov on August 1, 2016.

For questions and assistance, please call the Privacy Shield team at 202-482-1512 or submit an assistance request on our website at https://www.privacyshield.gov/assistance

SEGMENT 2

1 Hate Speech on the Internet

Definitions and Perspectives

“*Hate speech*” as speech that demeans or attacks a person or people as members of a group with shared characteristics such as race, gender, religion, sexual orientation, or disability.

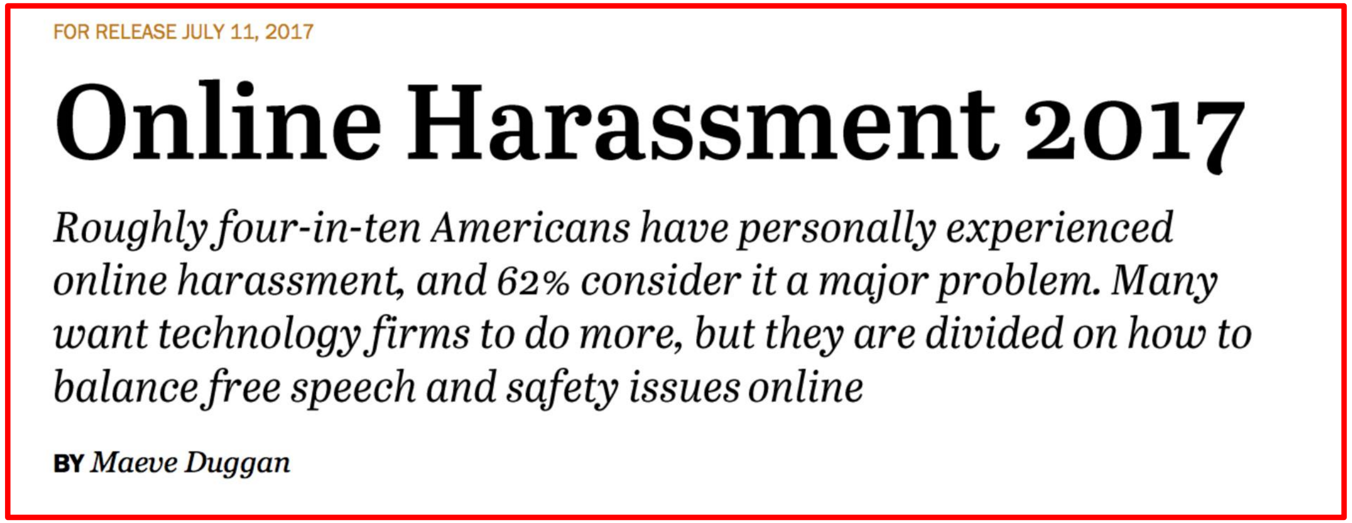
- Perspective 1: outcome-based with a focus on the harm to groups or individuals.
- Perspective 2: intent of the speaker.
- Perspective 3: content of the speech.

“*Online harrassment*” as “unwanted contact that is used to create an intimidating, annoying, frightening, or even hostile environment for the victim and that uses digital means to reach the victim” (A. Lenhart).

- Includes doxxing, revenge porn, gender-based harrassment, etc.

“*Dangerous speech*” as that which increases the risk of violence through a range of rethorical techniques and may contain explicit threats or incitement to violence (S. Benesch).

Phenomenon (US)



FOR RELEASE JULY 11, 2017

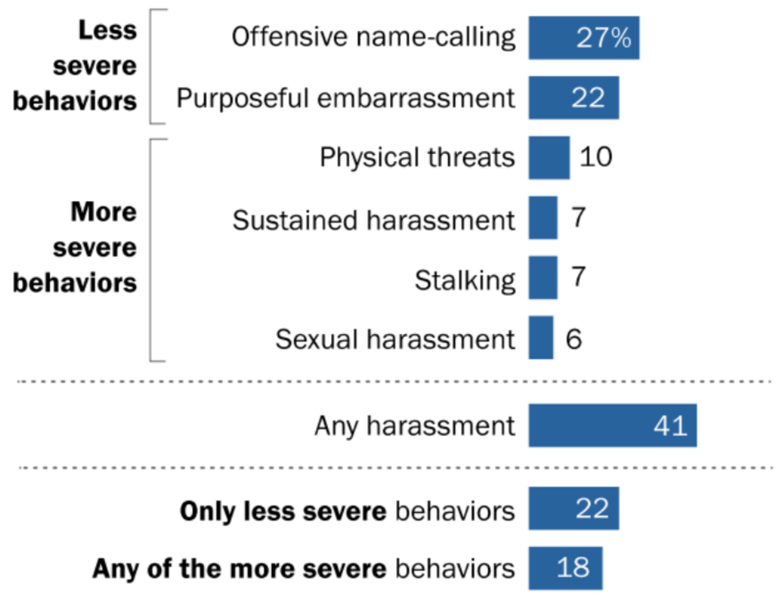
Online Harassment 2017

Roughly four-in-ten Americans have personally experienced online harassment, and 62% consider it a major problem. Many want technology firms to do more, but they are divided on how to balance free speech and safety issues online

BY *Maeve Duggan*

Roughly four-in-ten Americans have personally experienced online harassment

% of U.S. adults who have experienced ____ online



Source: Survey conducted Jan. 9 -23, 2017.
"Online Harassment 2017"

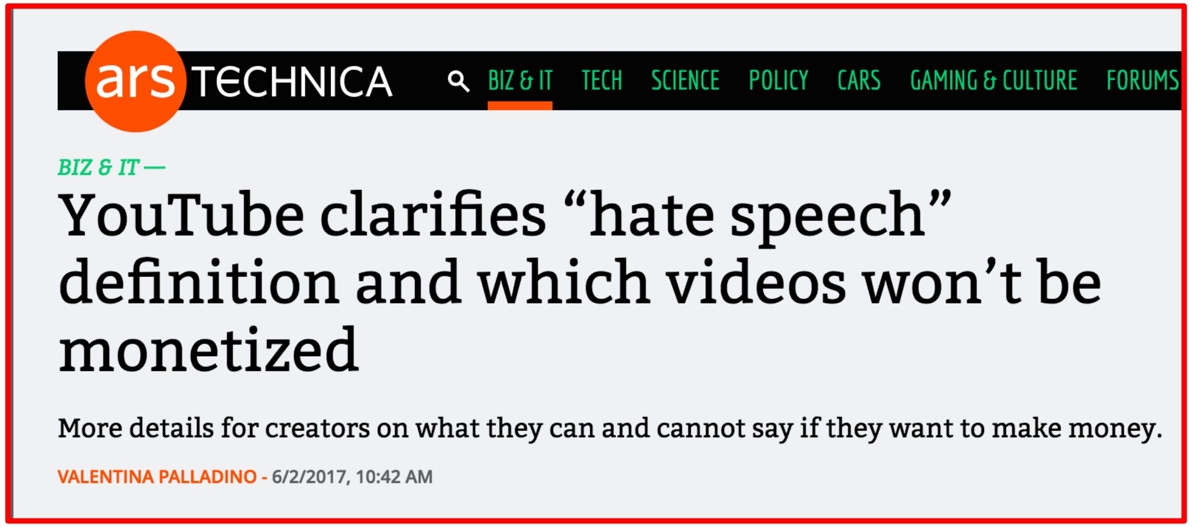
PEW RESEARCH CENTER

http://www.pewinternet.org/2017/07/11/online-harassment-2017/

Hate Speech Regulation: A Hard Problem

- *Definitional issues*: Hate or harmful speech consists a range of phenomenon that overlap and intersect, and include a variety of types of speech that cause different harms.
- *Normative issues*: Trade-offs and tensions between protecting the interests of vulnerable populations and victicms of harmful speech online and protecting freedom of expression; allocation of (shared?) responsibility among dynamic actors network.
- *Design issues*: Legal remedies often under- or overinclusive, plus enforcement problems; civil society responses important, but early-stage; role of intermediaries and commercial vs. public interests, etc.

Example: YouTube



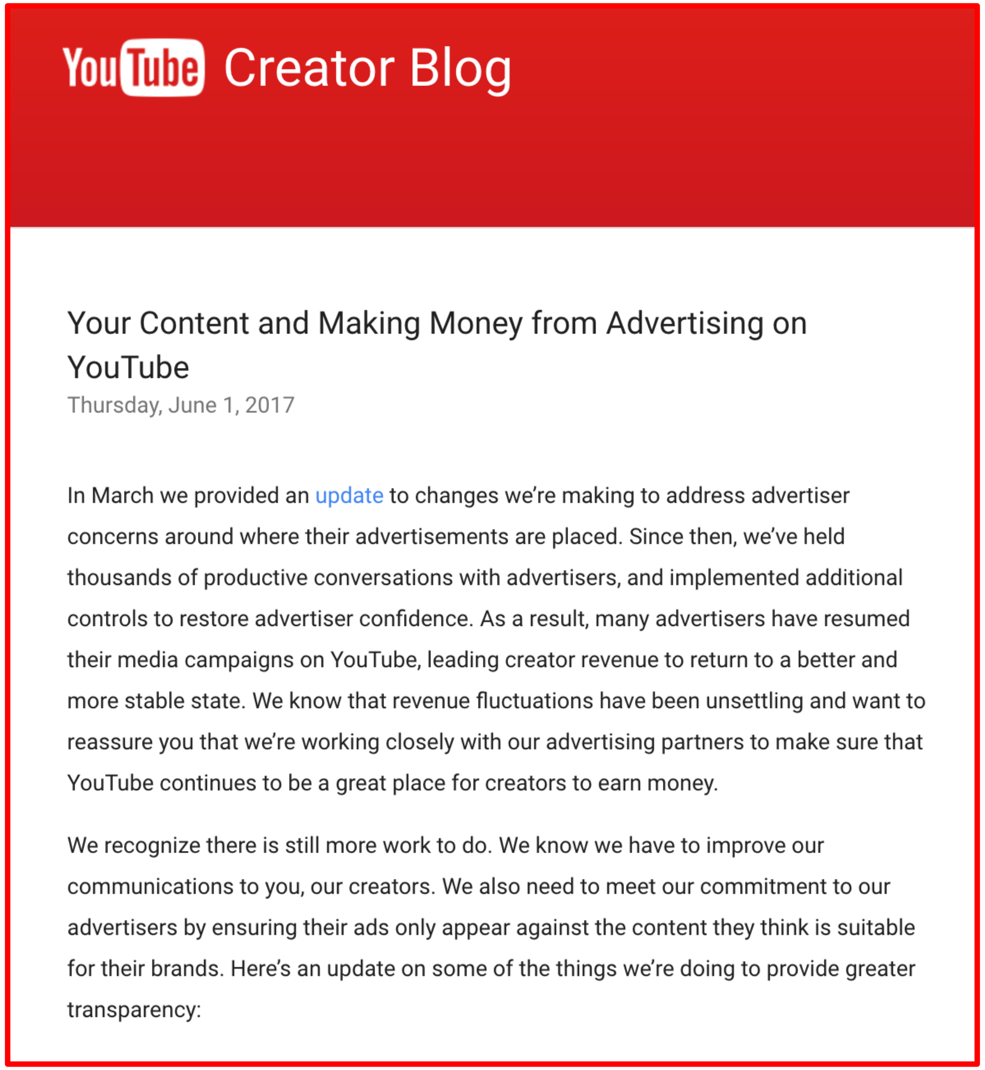
BIZ & IT —

YouTube clarifies “hate speech” definition and which videos won’t be monetized

More details for creators on what they can and cannot say if they want to make money.

VALENTINA PALLADINO - 6/2/2017, 10:42 AM

https://arstechnica.com/information-technology/2017/06/what-is-hate-speech-on-youtube-video-site-offers-clarity/



Your Content and Making Money from Advertising on YouTube

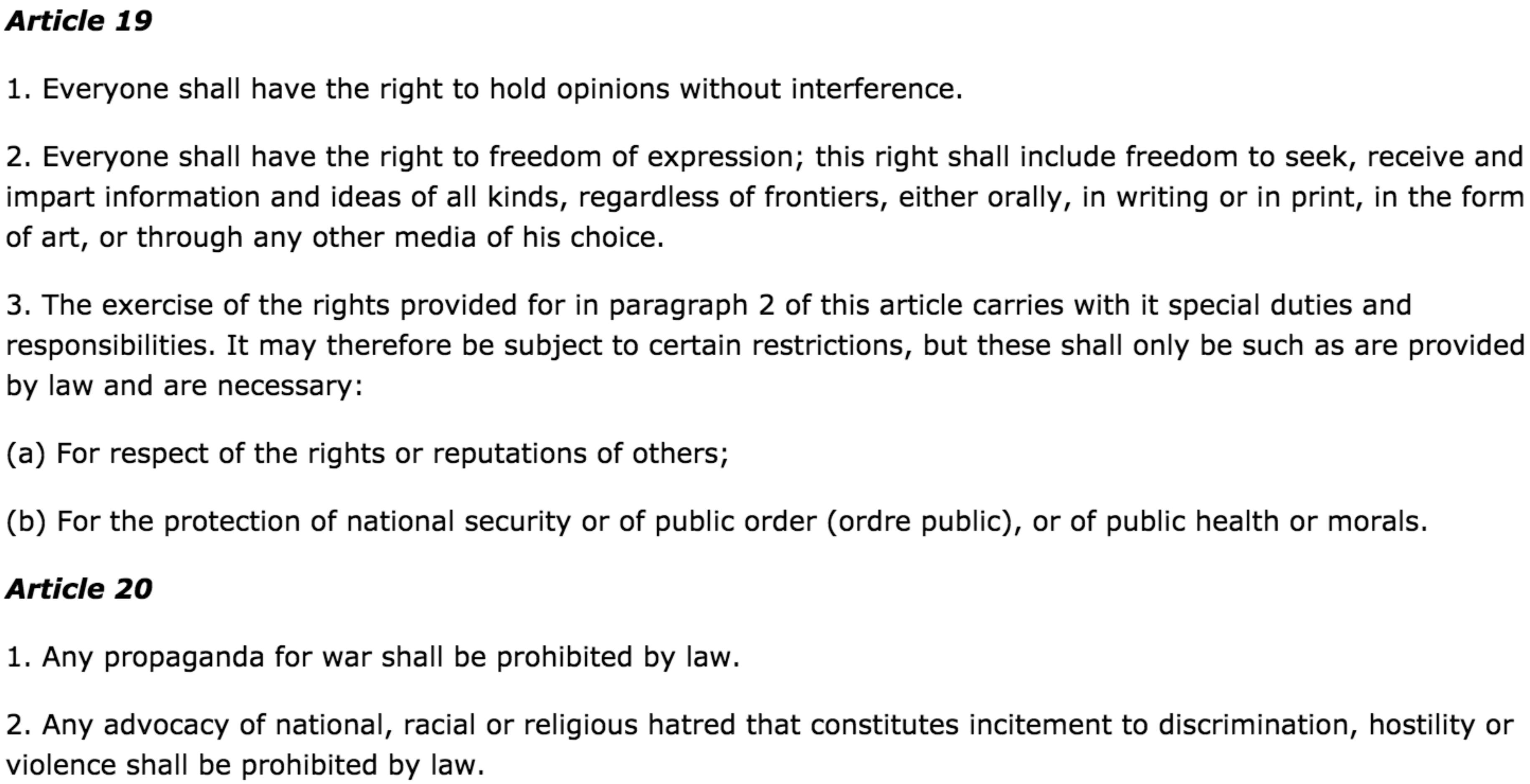
Thursday, June 1, 2017

In March we provided an update to changes we’re making to address advertiser concerns around where their advertisements are placed. Since then, we’ve held thousands of productive conversations with advertisers, and implemented additional controls to restore advertiser confidence. As a result, many advertisers have resumed their media campaigns on YouTube, leading creator revenue to return to a better and more stable state. We know that revenue fluctuations have been unsettling and want to reassure you that we’re working closely with our advertising partners to make sure that YouTube continues to be a great place for creators to earn money.

We recognize there is still more work to do. We know we have to improve our communications to you, our creators. We also need to meet our commitment to our advertisers by ensuring their ads only appear against the content they think is suitable for their brands. Here’s an update on some of the things we’re doing to provide greater transparency:

https://youtube-creators.googleblog.com/2017/06/your-content-and-making-money-from.html

Example: International Covenant on Civil and Political Rights (ICCPR)



Article 19

1. Everyone shall have the right to hold opinions without interference.

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) For respect of the rights or reputations of others;

(b) For the protection of national security or of public order (ordre public), or of public health or morals.

Article 20

1. Any propaganda for war shall be prohibited by law.

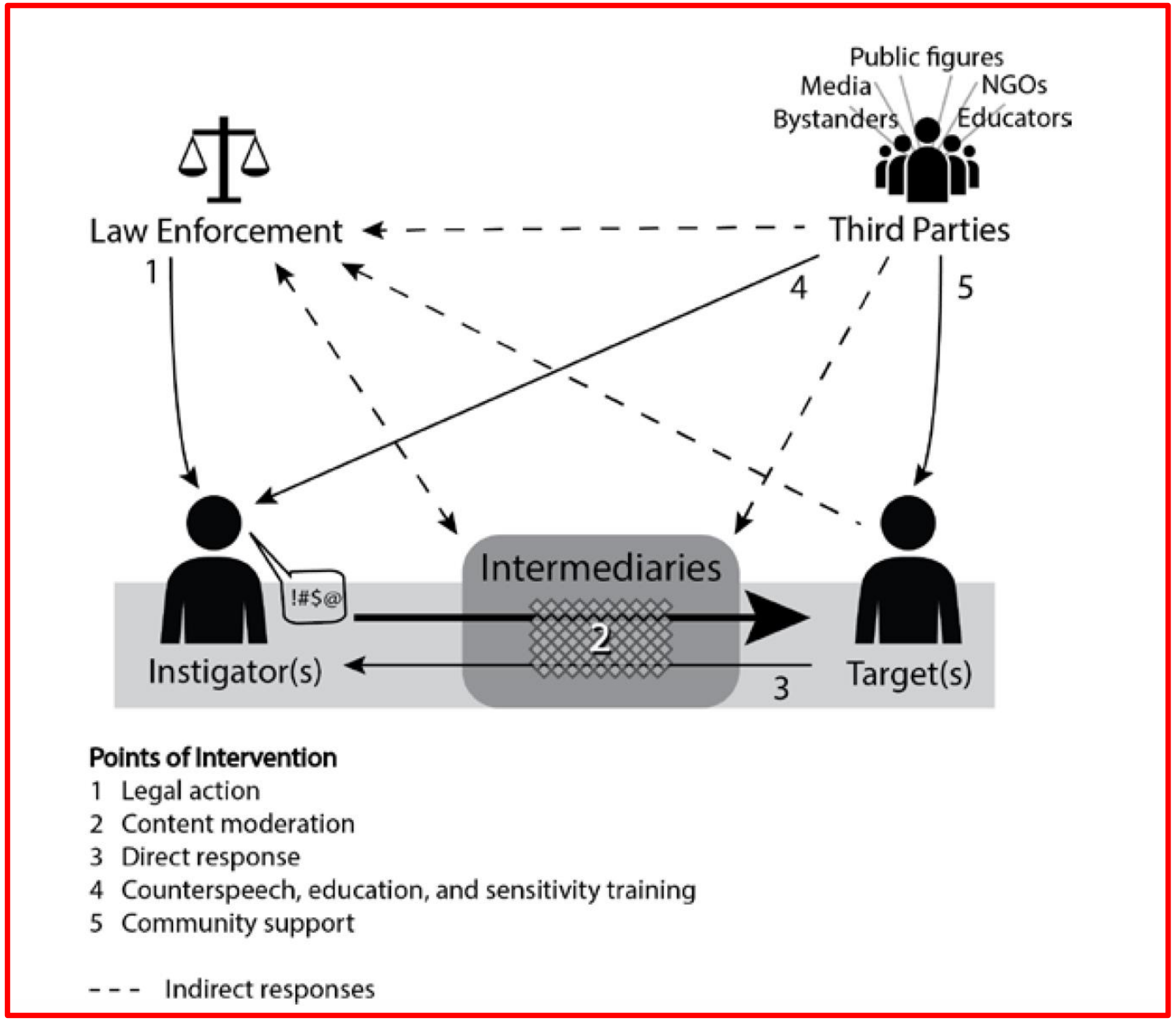
2. Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.

State of Research

Despite increasing attention to the topic, we still lack a full understanding of the reach and impact of harmful speech online and know relatively little about the efficacy of different interventions. Moreover, our understanding of the collateral costs of various interventions is rudimentary. Core questions include:

- How widespread is the phenomenon, who participates, who is harmed, and how?
- Is it increasing or decreasing, and how does it vary over time? Or is there evidence that the prevalence of harmful speech is steady and only receiving increased attention online?
- Are there signs of the normalization of harmful speech online? How are the actors that participate in harmful speech organized? How are they influenced by leaders, governments, public figures, and the media?
- What is the social network structure of groups that engage in harmful speech and what is the role of key influencers? How can we better understand the interplay between ingroup and out-group interactions?
- What contextual factors are associated with the incidence, intensity, and impact of harmful speech online?

Complex Dynamics: Actors, Interventions



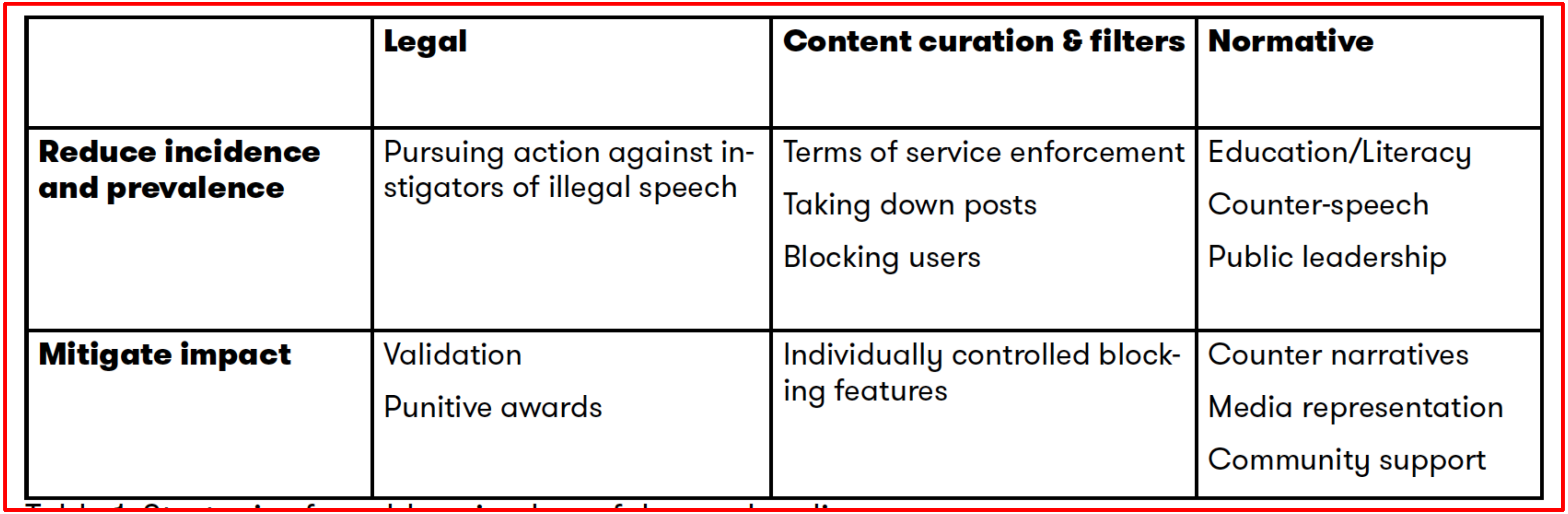
Points of Intervention

1 Legal action
2 Content moderation
3 Direct response
4 Counterspeech, education, and sensitivity training
5 Community support

- - - Indirect responses

https://cyber.harvard.edu/publications/2016/UnderstandingHarmfulSpeech

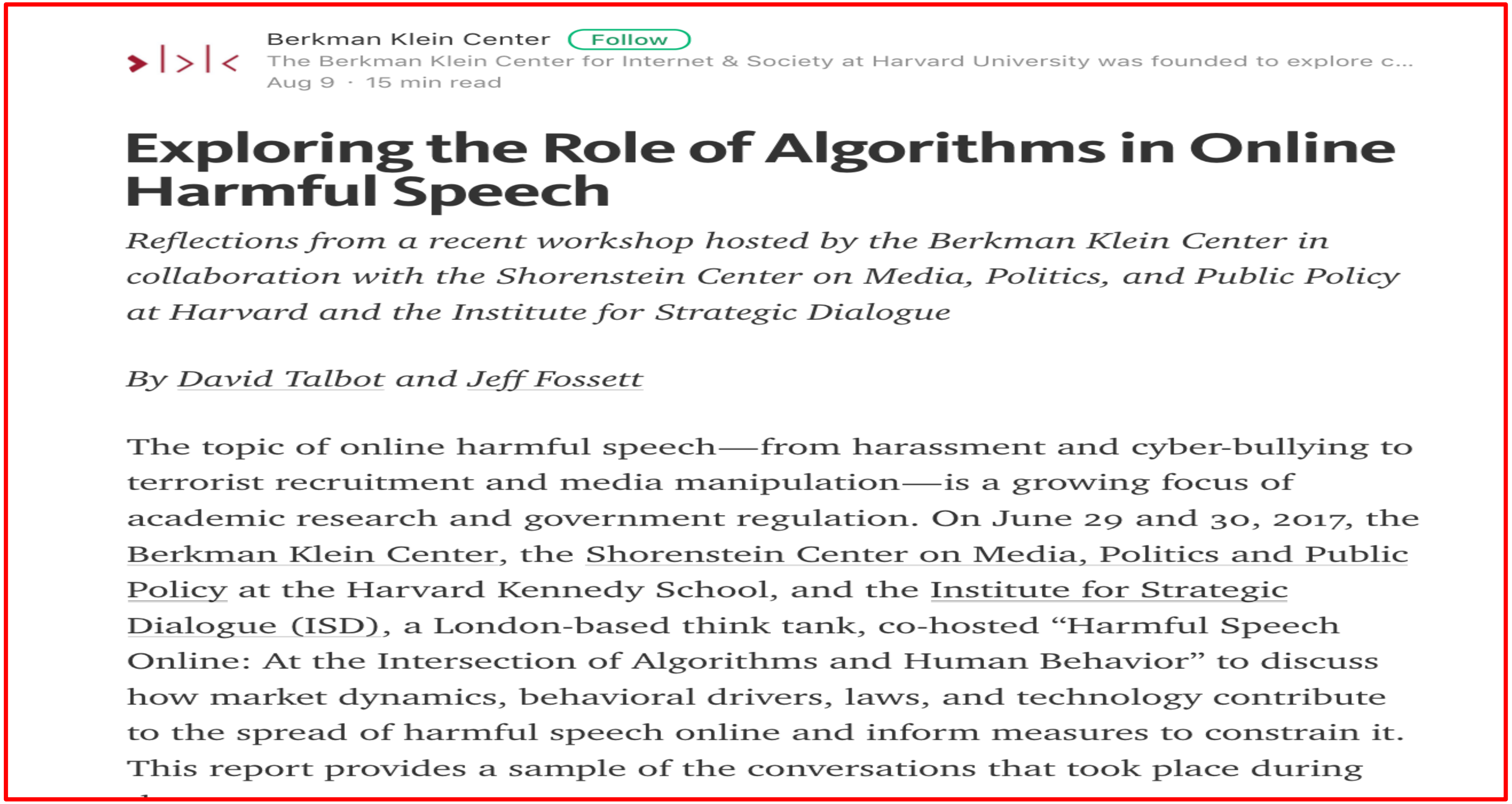
Possible Approaches and Strategies



	Legal	Content curation & filters	Normative
Reduce incidence and prevalence	Pursuing action against instigators of illegal speech	Terms of service enforcement Taking down posts Blocking users	Education/Literacy Counter-speech Public leadership
Mitigate impact	Validation Punitive awards	Individually controlled blocking features	Counter narratives Media representation Community support

https://cyber.harvard.edu/publications/2016/UnderstandingHarmfulSpeech

Complicating Factor: Rise of Algorithms



Berkman Klein Center Follow

The Berkman Klein Center for Internet & Society at Harvard University was founded to explore c...

Aug 9 · 15 min read

Exploring the Role of Algorithms in Online Harmful Speech

Reflections from a recent workshop hosted by the Berkman Klein Center in collaboration with the Shorenstein Center on Media, Politics, and Public Policy at Harvard and the Institute for Strategic Dialogue

By David Talbot and Jeff Fossett

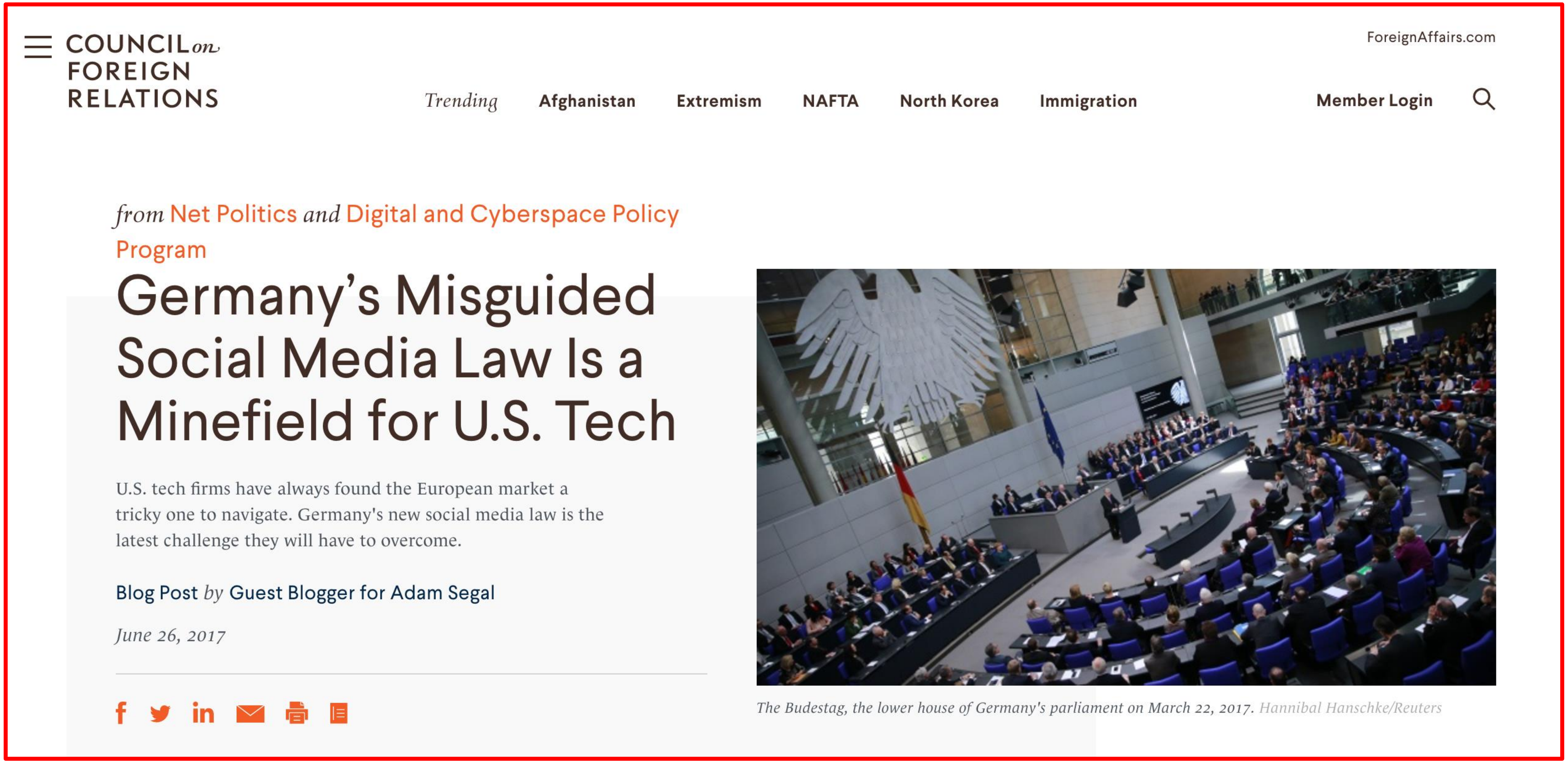
The topic of online harmful speech—from harassment and cyber-bullying to terrorist recruitment and media manipulation—is a growing focus of academic research and government regulation. On June 29 and 30, 2017, the Berkman Klein Center, the Shorenstein Center on Media, Politics and Public Policy at the Harvard Kennedy School, and the Institute for Strategic Dialogue (ISD), a London-based think tank, co-hosted "Harmful Speech Online: At the Intersection of Algorithms and Human Behavior" to discuss how market dynamics, behavioral drivers, laws, and technology contribute to the spread of harmful speech online and inform measures to constrain it. This report provides a sample of the conversations that took place during

https://medium.com/berkman-klein-center/exploring-the-role-of-algorithms-in-online-harmful-speech-1b804936f279

Case Study 1: NetzDG (Germany)

- Social media platforms with more than 2 million registered users are required to delete “evidently unlawful” content within 24 hours of being flagged.
- Where the decision is not “evident”, operators have up to 7 days to assess the content. They can take longer if users are asked to weigh in, or if they pass the decision onto a joint industry body (“regulated self-regulatory body”).
- Platforms that receive more than 100 complaints (incl. flagged content) must publish a bi-annual report in German on how they deal with such complaints.
- Platforms meeting the threshold criteria must establish a point of contact within Germany to facilitate contact with government authorities and illicit content has to be stored within EU territory for 10 weeks to allow for investigation.
- If platforms consistently fail to comply with these requirements, they face fines of up to €50 million.

Reactions & Discussion



from Net Politics *and* Digital and Cyberspace Policy Program

Germany's Misguided Social Media Law Is a Minefield for U.S. Tech

U.S. tech firms have always found the European market a tricky one to navigate. Germany's new social media law is the latest challenge they will have to overcome.

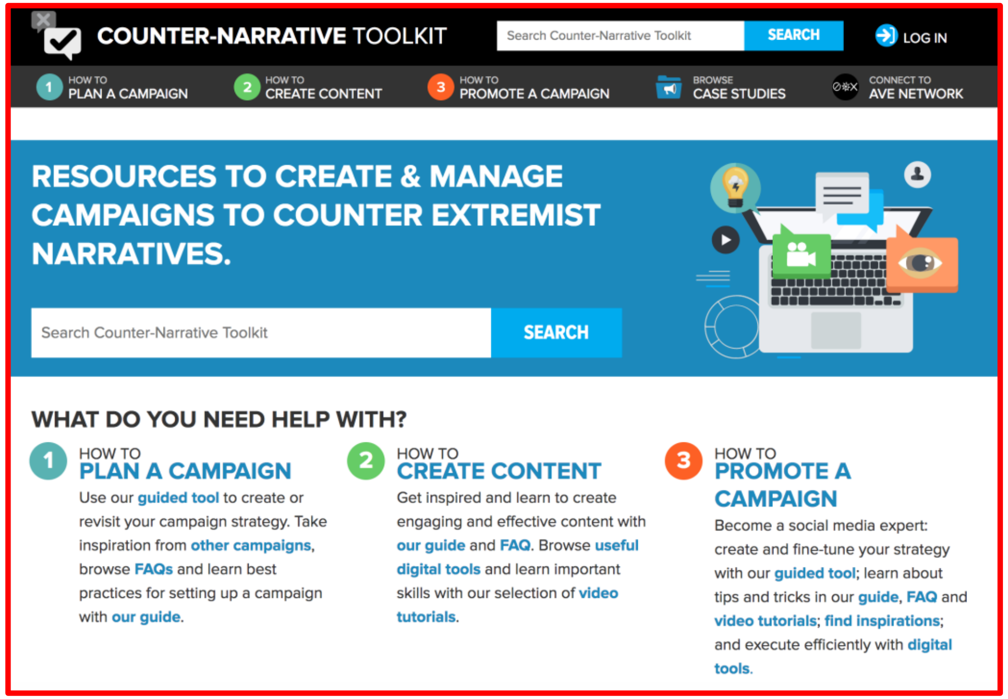
Blog Post *by* Guest Blogger for Adam Segal

June 26, 2017

The Budestag, the lower house of Germany's parliament on March 22, 2017. Hannibal Hanschke/Reuters

https://www.cfr.org/blog/germanys-misguided-social-media-law-minefield-us-tech

Case Study 2: Counter-Speech


COUNTER-NARRATIVE TOOLKIT
Search Counter-Narrative Toolkit
SEARCH
LOG IN
1 HOW TO PLAN A CAMPAIGN
2 HOW TO CREATE CONTENT
3 HOW TO PROMOTE A CAMPAIGN
BROWSE CASE STUDIES
CONNECT TO AVE NETWORK
Search Counter-Narrative Toolkit
SEARCH

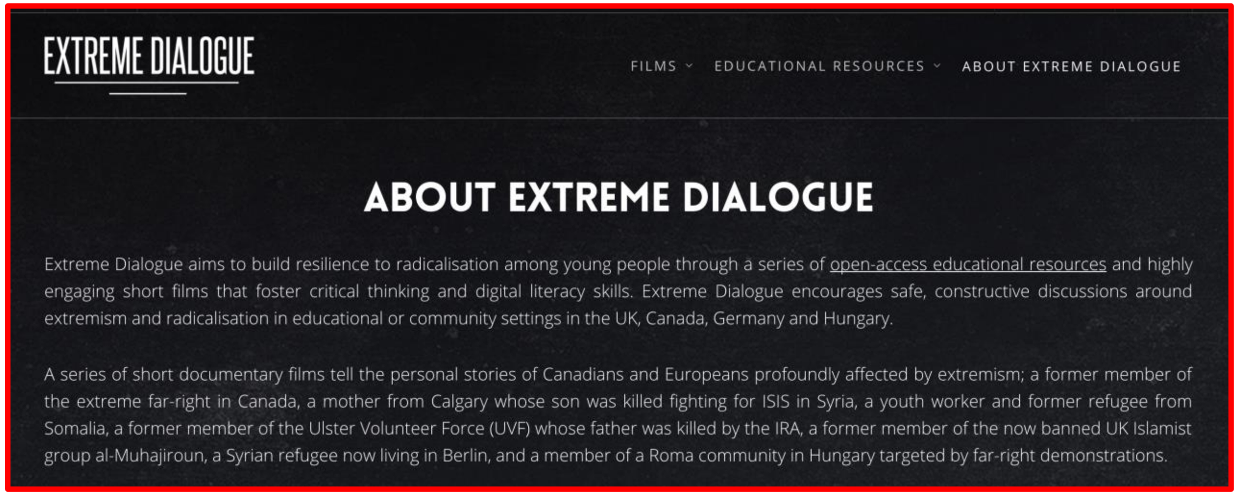
RESOURCES TO CREATE & MANAGE CAMPAIGNS TO COUNTER EXTREMIST NARRATIVES.

WHAT DO YOU NEED HELP WITH?

1 HOW TO **PLAN A CAMPAIGN**
Use our guided tool to create or revisit your campaign strategy. Take inspiration from other campaigns, browse FAQs and learn best practices for setting up a campaign with our guide.

2 HOW TO **CREATE CONTENT**
Get inspired and learn to create engaging and effective content with our guide and FAQ. Browse useful digital tools and learn important skills with our selection of video tutorials.

3 HOW TO **PROMOTE A CAMPAIGN**
Become a social media expert: create and fine-tune your strategy with our guided tool; learn about tips and tricks in our guide, FAQ and video tutorials; find inspirations; and execute efficiently with digital tools.



ABOUT EXTREME DIALOGUE

Extreme Dialogue aims to build resilience to radicalisation among young people through a series of open-access educational resources and highly engaging short films that foster critical thinking and digital literacy skills. Extreme Dialogue encourages safe, constructive discussions around extremism and radicalisation in educational or community settings in the UK, Canada, Germany and Hungary.

A series of short documentary films tell the personal stories of Canadians and Europeans profoundly affected by extremism; a former member of the extreme far-right in Canada, a mother from Calgary whose son was killed fighting for ISIS in Syria, a youth worker and former refugee from Somalia, a former member of the Ulster Volunteer Force (UVF) whose father was killed by the IRA, a former member of the now banned UK Islamist group al-Muhajiroun, a Syrian refugee now living in Berlin, and a member of a Roma community in Hungary targeted by far-right demonstrations.

http://www.counternarratives.org/

http://extremedialogue.org/about/

Reactions & Discussion

THE IMPACT OF COUNTER-NARRATIVES

Insights from a year-long cross-platform pilot study of counter-narrative curation, targeting, evaluation and impact

Tanya Silverman
Christopher J. Stewart
Zahed Amanullah
Jonathan Birdwell

Institute for Strategic Dialogue

www.againstviolentextremism.org

Against Violent Extremism

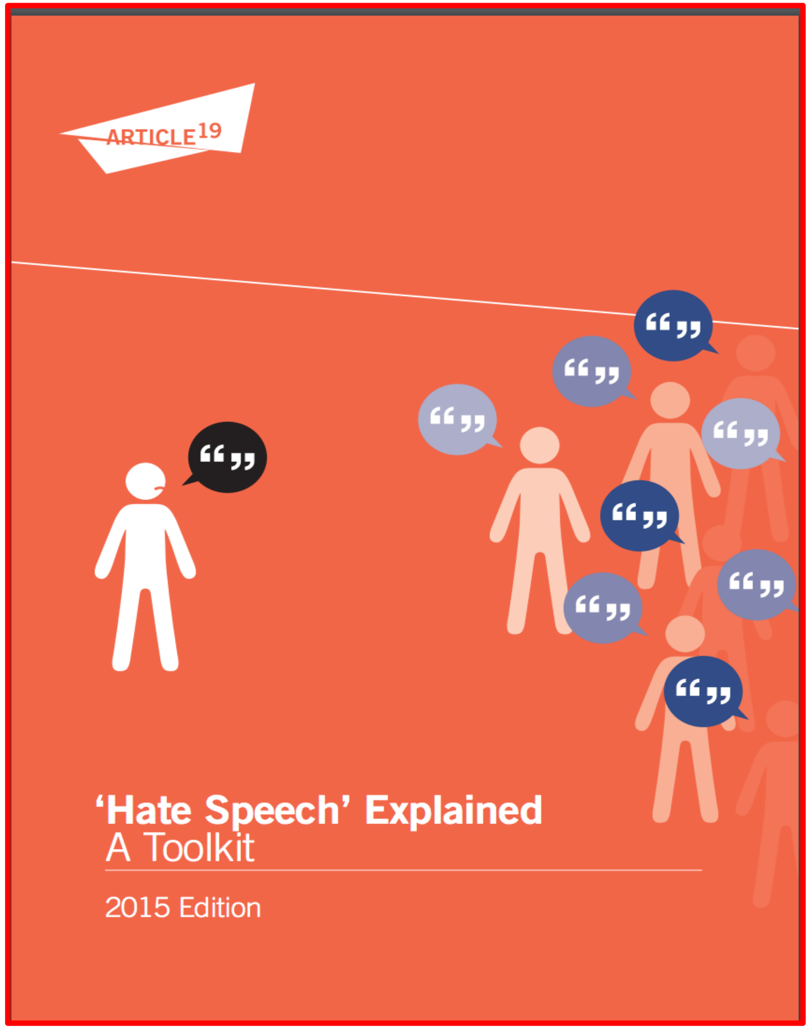
Conclusion

“By implementing a methodology that incorporates partnerships, curation, content creation, deployment, and evaluation, this study demonstrates that the use of counter-narrative messaging with measurable impact is replicable and scalable, though not without difficulty. Working with multiple partners and campaigns, we now have a much better idea of the interplay between key factors such as geography, language, ideology, audience, and media platforms.”

https://www.isdglobal.org/wp-content/uploads/2016/08/Impact-of-Counter-Narratives_ONLINE_1.pdf

Further Reading

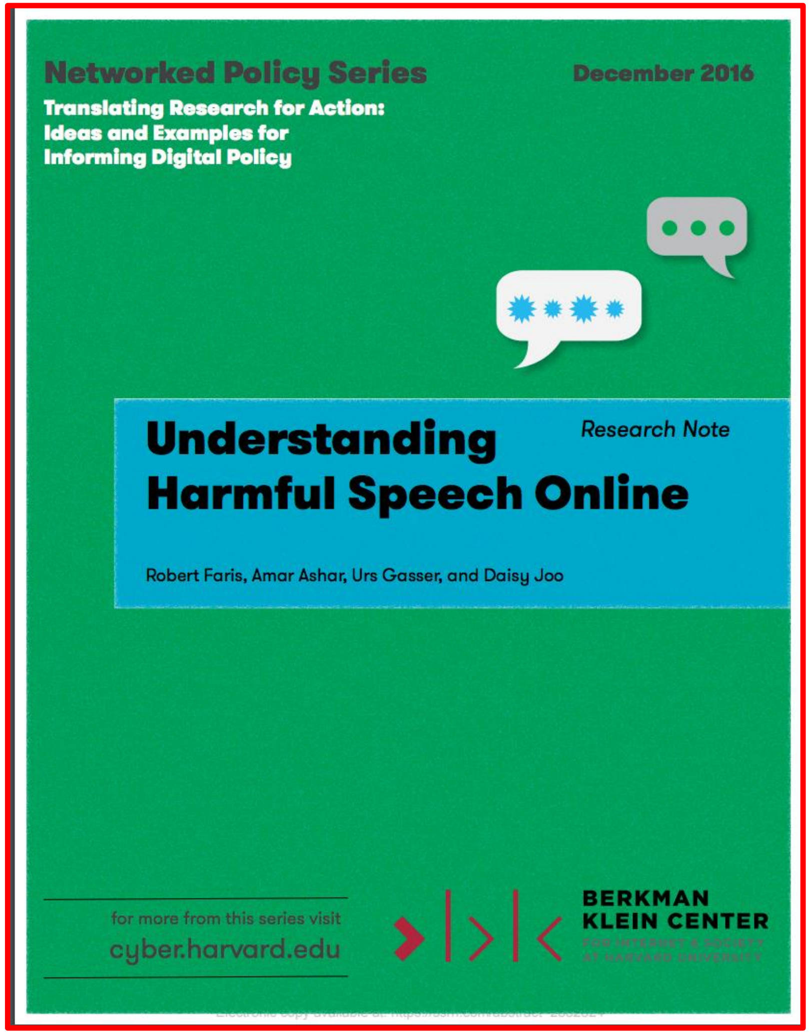
https://cyber.harvard.edu/research/harmfulspeech



ARTICLE 19

'Hate Speech' Explained
A Toolkit

2015 Edition



Networked Policy Series

December 2016

Translating Research for Action:
Ideas and Examples for
Informing Digital Policy

Understanding
Harmful Speech Online

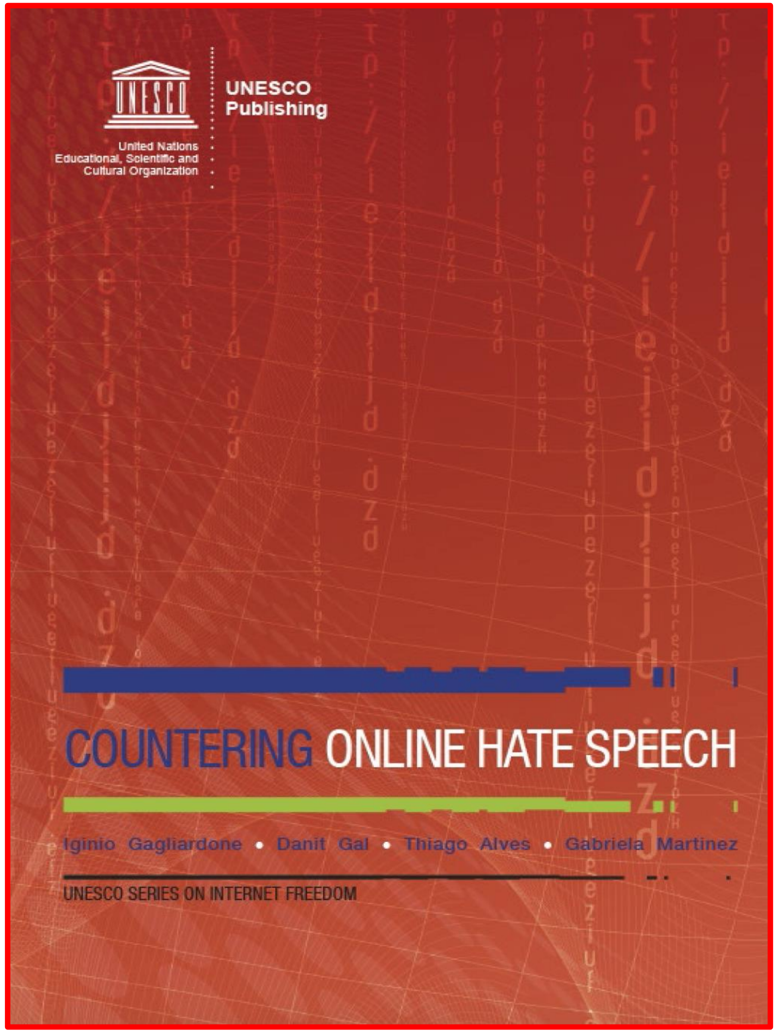
Research Note

Robert Faris, Amar Ashar, Urs Gasser, and Daisy Joo

for more from this series visit
cyber.harvard.edu

BERKMAN
KLEIN CENTER
FOR INTERNET & SOCIETY
AT HARVARD UNIVERSITY

Electronic copy available at: https://ssrn.com/abstract=2882824



UNESCO Publishing

United Nations
Educational, Scientific and
Cultural Organization

COUNTERING ONLINE HATE SPEECH

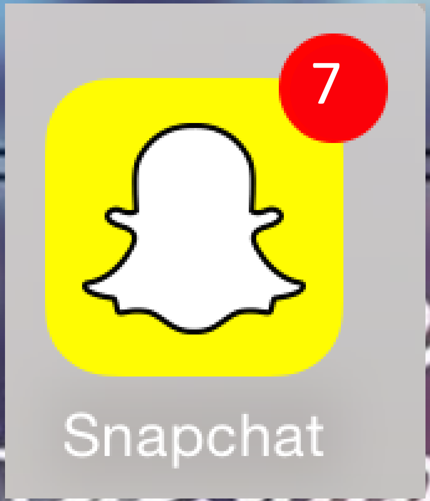
Iginio Gagliardone • Danit Gal • Thiago Alves • Gabriela Martinez

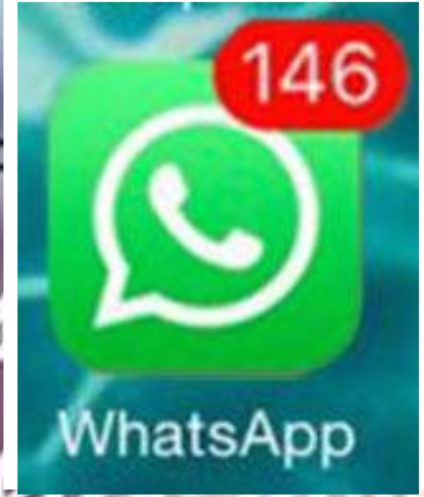
UNESCO SERIES ON INTERNET FREEDOM

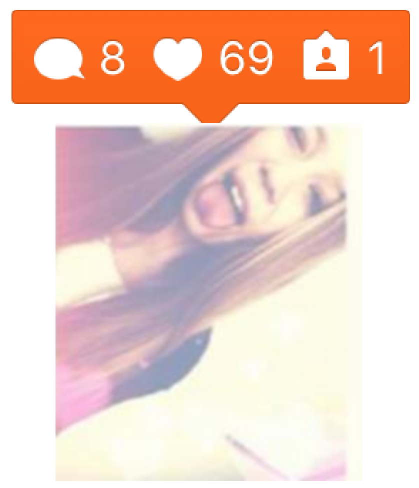
https://www.article19.org/data/files/medialibrary/38231/Hate_speech_report-ID-files--final.pdf

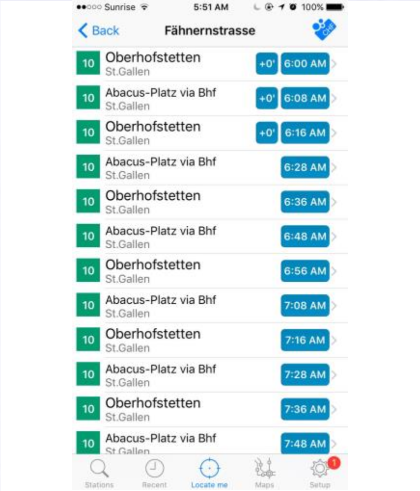
2 Digital Privacy

Example: Ananda (16 years)



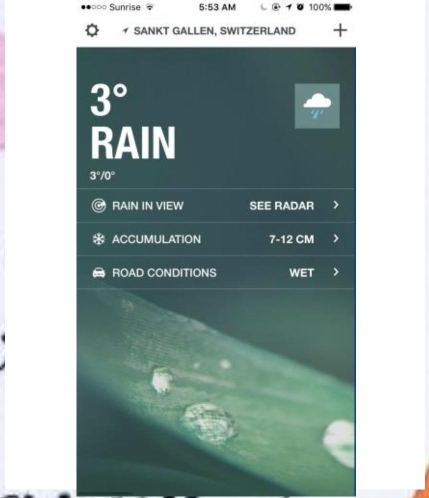






Fähnernstrasse

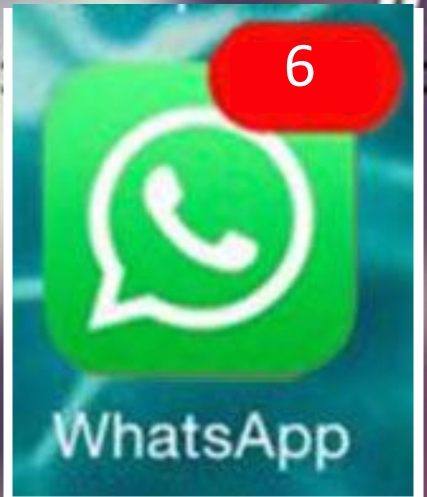
10	Oberhofstetten St.Gallen	+0'	6:00 AM
10	Abacus-Platz via Bhf St.Gallen	+0'	6:08 AM
10	Oberhofstetten St.Gallen	+0'	6:16 AM
10	Abacus-Platz via Bhf St.Gallen		6:28 AM
10	Oberhofstetten St.Gallen		6:36 AM
10	Abacus-Platz via Bhf St.Gallen		6:48 AM
10	Oberhofstetten St.Gallen		6:56 AM
10	Abacus-Platz via Bhf St.Gallen		7:08 AM
10	Oberhofstetten St.Gallen		7:16 AM
10	Abacus-Platz via Bhf St.Gallen		7:28 AM
10	Oberhofstetten St.Gallen		7:36 AM
10	Abacus-Platz via Bhf St.Gallen		7:48 AM

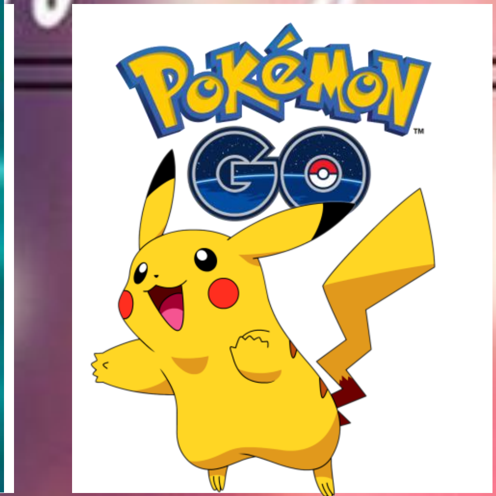


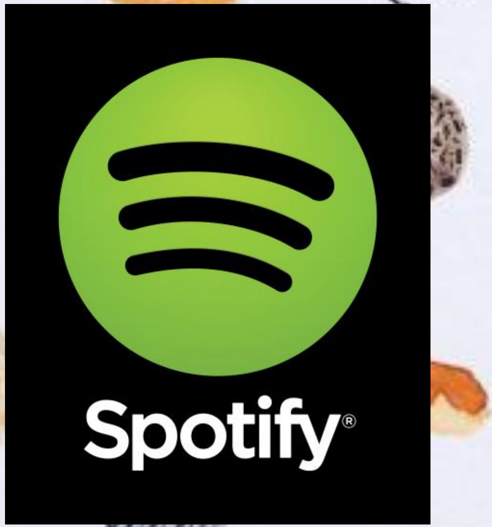
SANKT GALLEN, SWITZERLAND

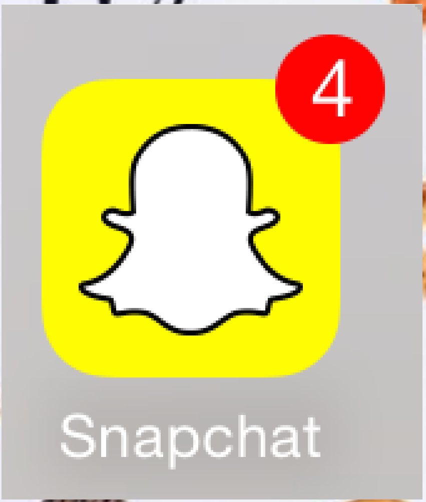
3°
RAIN
3°/0°

RAIN IN VIEW — SEE RADAR
ACCUMULATION — 7-12 CM
ROAD CONDITIONS — WET

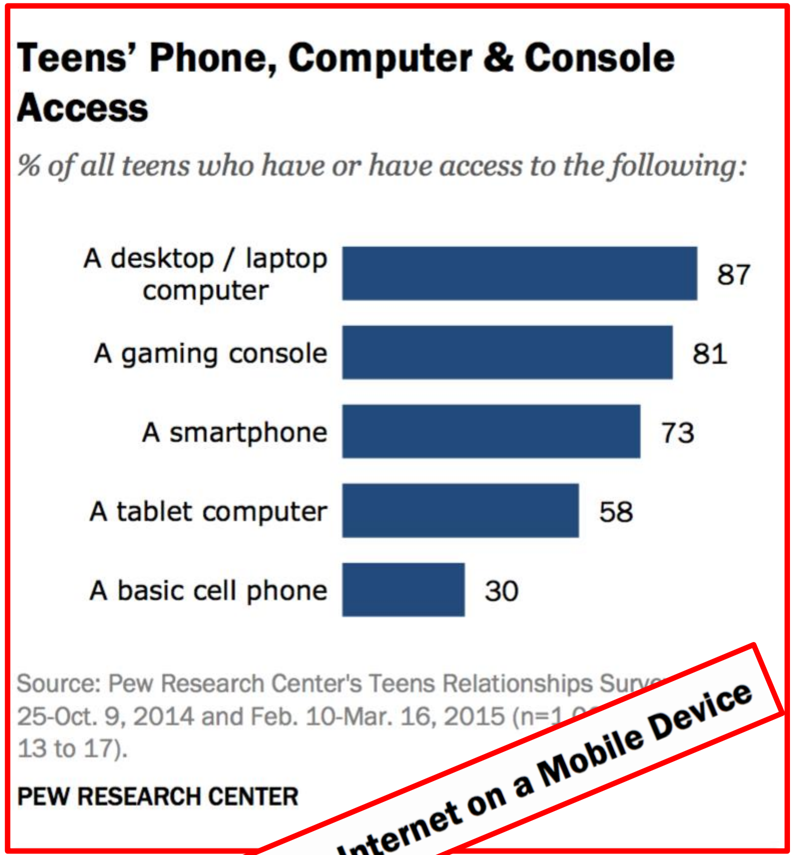








”Digital Natives” (Generational Shift)



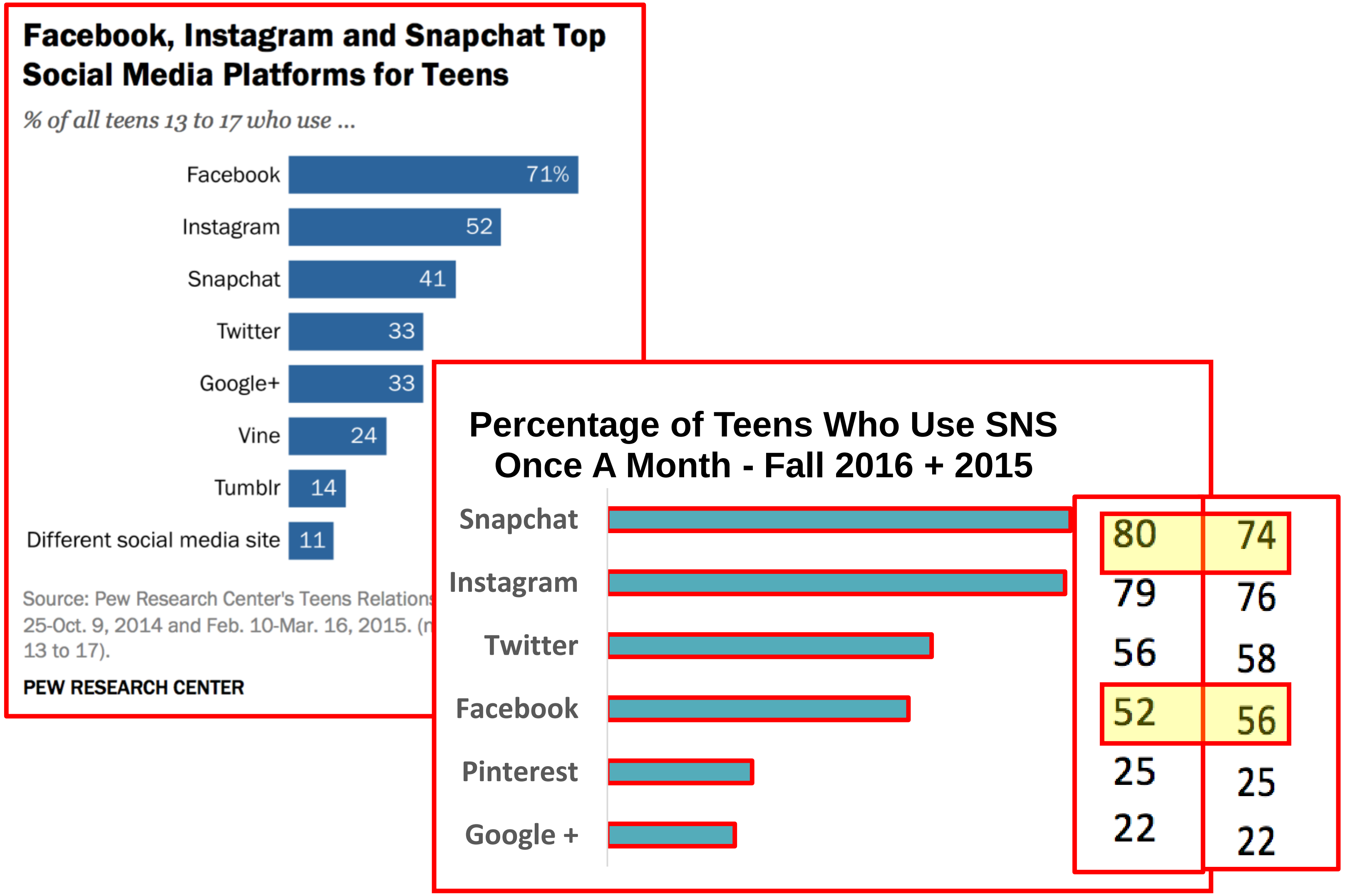
Teens’ Phone, Computer & Console Access

% of all teens who have or have access to the following:

Source: Pew Research Center's Teens Relationships Surve
25-Oct. 9, 2014 and Feb. 10-Mar. 16, 2015 (n=1,0
13 to 17).

PEW RESEARCH CENTER

91% of Teens Use the Internet on a Mobile Device



Facebook, Instagram and Snapchat Top Social Media Platforms for Teens

% of all teens 13 to 17 who use ...

Source: Pew Research Center's Teens Relation
25-Oct. 9, 2014 and Feb. 10-Mar. 16, 2015. (r
13 to 17).

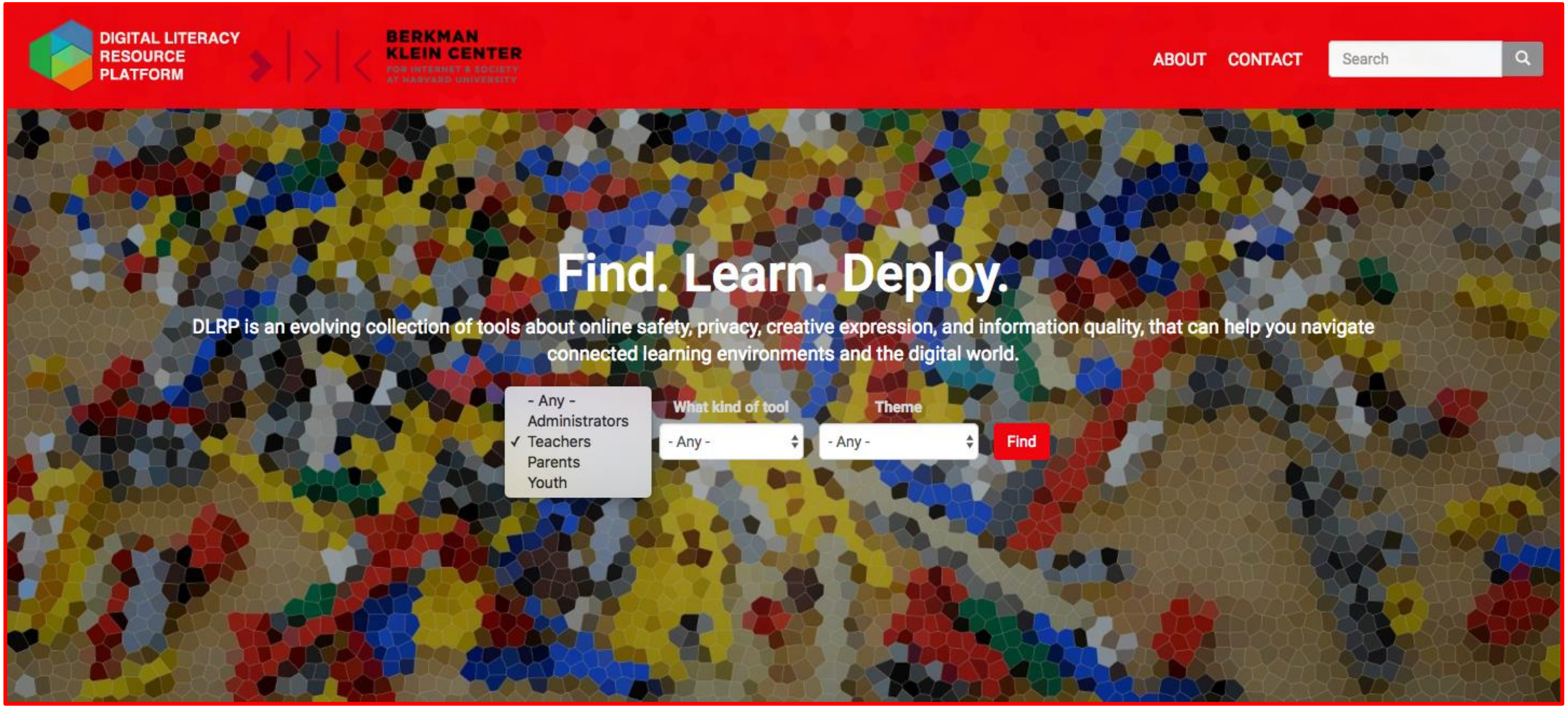
PEW RESEARCH CENTER

Percentage of Teens Who Use SNS Once A Month - Fall 2016 + 2015

Findings for Policymakers from Focus Groups

- *Semantic interoperability:* Use of term such as “privacy” means different things to different groups (e.g. youth = reputation, social dimension of privacy; adults = institutional dimension of privacy).
- *Perceived vs. real problem*: Adults worry about loss of privacy among youth based on sharing-behavior. Evidence shows much more nuance. But: commercial use of data as big blind spot among youth.
- *Importance of education*: Consider full range of approaches and tool, beyoned law, with an emphasis on education and digital literacy. Move towards human-centric approaches needed given speed of change in technology and markets.

Example: DLRP



Find. Learn. Deploy.

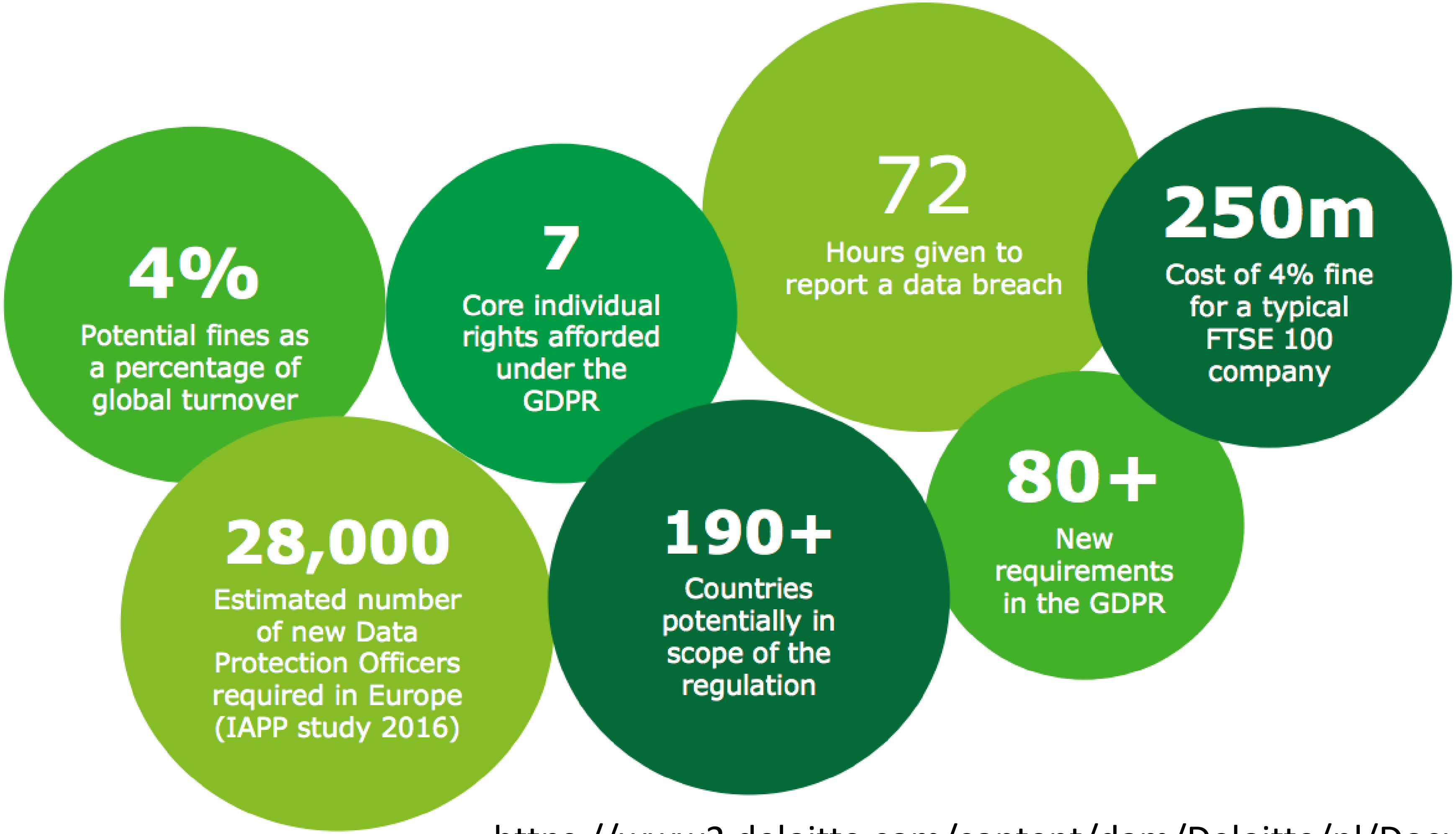
DLRP is an evolving collection of tools about online safety, privacy, creative expression, and information quality, that can help you navigate connected learning environments and the digital world.

http://dlrp.berkman.harvard.edu

Important Developments (EU): GDPR

- January 2012 reform announced to strengthen privacy rights and boost Europe's digital economy; GDPR Enacted on December 15, 2015; enforcement date: May 25, 2018
- Aims of the General Data Protection Regulation:
  - Supervisory Authorities
    - Harmonization and “one-stop shop” approach
    - Increased enforcement and sanctions
  - Strengthening Individual Control
    - Stricter consent forms & the right to withdraw consent at any time
    - Implied consent no longer a legal basis or when there is an imbalance between the data subject and controller
    - Right to access, correction and erasure in combination with the right to withdraw consent
    - Transparency principle requiring data collectors to implement transparent and easily accessible data processing policies
  - Increased Responsibility and Accountability of Data Processors and Controllers
    - Stricter “privacy by default”
    - Affirmative actions by data controllers required to protect the data
    - Notifications of data subjects and authorities in the case of a security breaches

GDPR – What Changes?



4%
Potential fines as a percentage of global turnover

7
Core individual rights afforded under the GDPR

72
Hours given to report a data breach

250m
Cost of 4% fine for a typical FTSE 100 company

28,000
Estimated number of new Data Protection Officers required in Europe (IAPP study 2016)

190+
Countries potentially in scope of the regulation

80+
New requirements in the GDPR

https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-gdpr-vision-approach.pdf

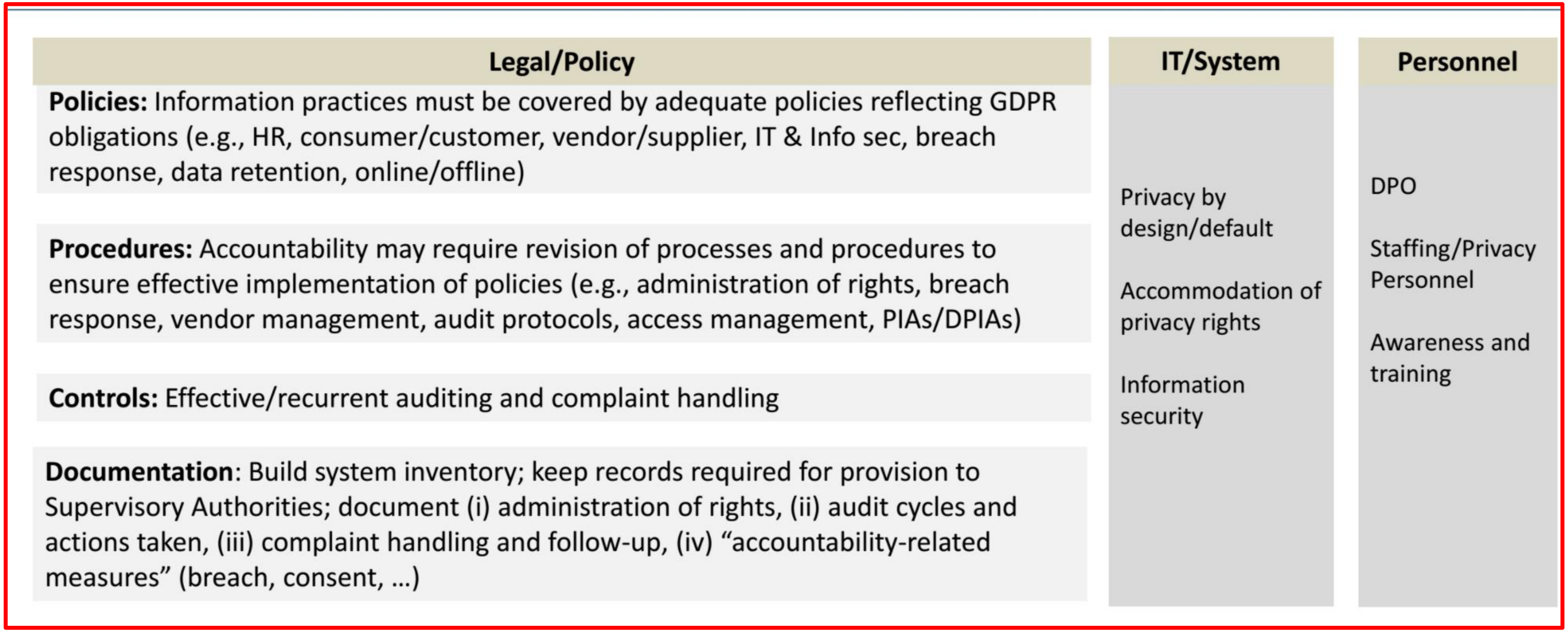
International Impact

- GDPR applies to data controllers and processors outside the EU whose processing activities relate to the offering of goods or services (even if for free) to, or monitoring the behavior (within the EU) of EU data subject (Art. 3(2)).
    - Offering goods or services" more than mere access to a website or email address. May include use of language or currency of a Member States with the possibility of ordering goods/ services there, and/or monitoring customers or users who are in EU
    - Example: Thai Controller targeting EU customers via website and sales in EURO = GDRP applies, even if site not hosted in the EU
    - "Monitoring of behavior" includes all types of Internet tracking and profiling
    - Example: Thai Controller placing tracking technology on hard-drives in the EU = GDRP applies (monitoring of behavior in the EU)
- GDPR Art. 27 requires designation of a representative of controllers or processors not established in the EU (some exceptions)
- SA may take action against EU-based representative, but not against the controller/processor in third country
    - But might cut off data flows (e.g. ordering local telco provider); representative might be sued and held accountable

GDPR: Accountability Requirements

- Data Protection Principles under GDPR similar as under DPD, but extensive new *accountability requirements* to demonstrate compliance (see Art. 5(2)).
- Includes requirement to maintain relevant documentation on processing activities; to conduct data protection impact assessment for risky processing; and implementation of privacy by design and by default (e.g. via data minimization).
    - *Documentation*: Develop personal data map and processing inventories (what data collected? For what purpose? How is data processed? Legal basis for each activity? Where is data stored? How long retained? Who has access? Transfers? Etc.); keep records of all processing (incl. breaches of vendors); implement appropriate and effective policies and processes.
    - *Privacy by design and default*: Consider data protection from start of project, assess privacy impact/risks; consider data minimization as default. Ensure that product design teams consider privacy.
    - *Data privacy impact assessment*: Required if using new technologies and processing is likely to result in high risks to the rights and freedoms of individuals (e.g. CCTV; profiling/predictive analytics w/ automated decision making).
    - *Data protection officers*: Required when company's core activities involve large-scale monitoring of individuals, or large scale processing of sensitive data.

Privacy Programs

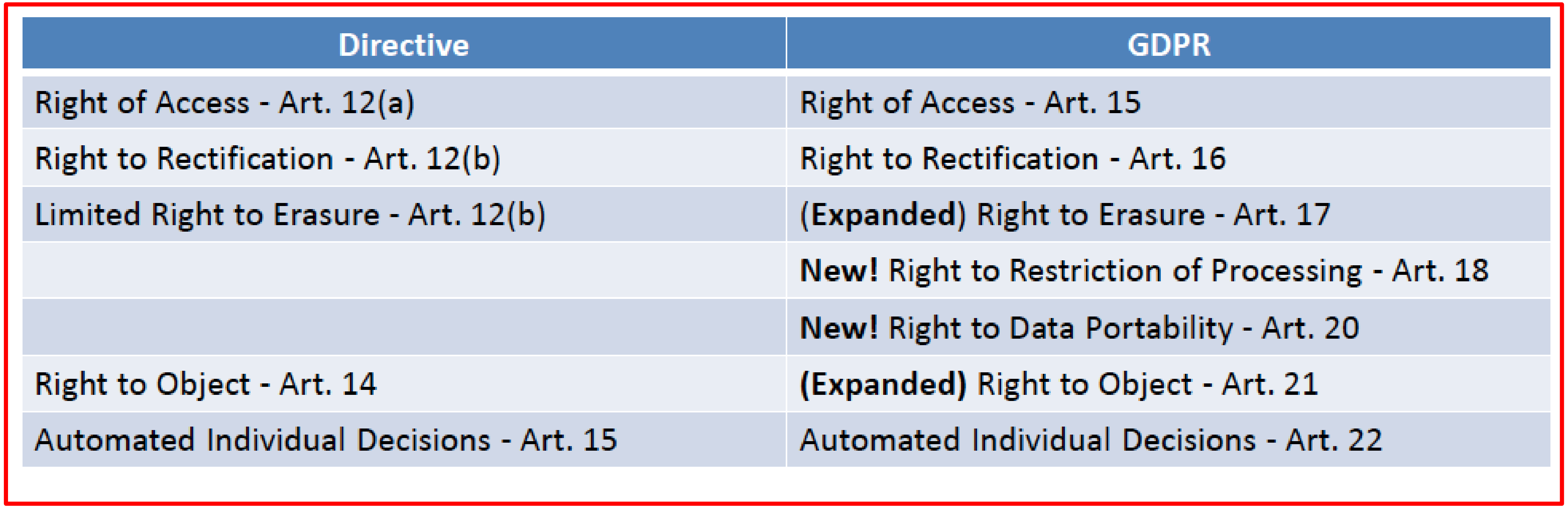


Legal/Policy	IT/System	Personnel
Policies: Information practices must be covered by adequate policies reflecting GDPR obligations (e.g., HR, consumer/customer, vendor/supplier, IT & Info sec, breach response, data retention, online/offline)	Privacy by design/default Accommodation of privacy rights Information security	DPO Staffing/Privacy Personnel Awareness and training
Procedures: Accountability may require revision of processes and procedures to ensure effective implementation of policies (e.g., administration of rights, breach response, vendor management, audit protocols, access management, PIAs/DPIAs)		
Controls: Effective/recurrent auditing and complaint handling		
Documentation: Build system inventory; keep records required for provision to Supervisory Authorities; document (i) administration of rights, (ii) audit cycles and actions taken, (iii) complaint handling and follow-up, (iv) "accountability-related measures" (breach, consent, …)		

Source: www.AlstonPrivacy.com

GDPR: Individual Rights (Overview)

- GDPR *strengthens* existing and creates *new rights* for individuals



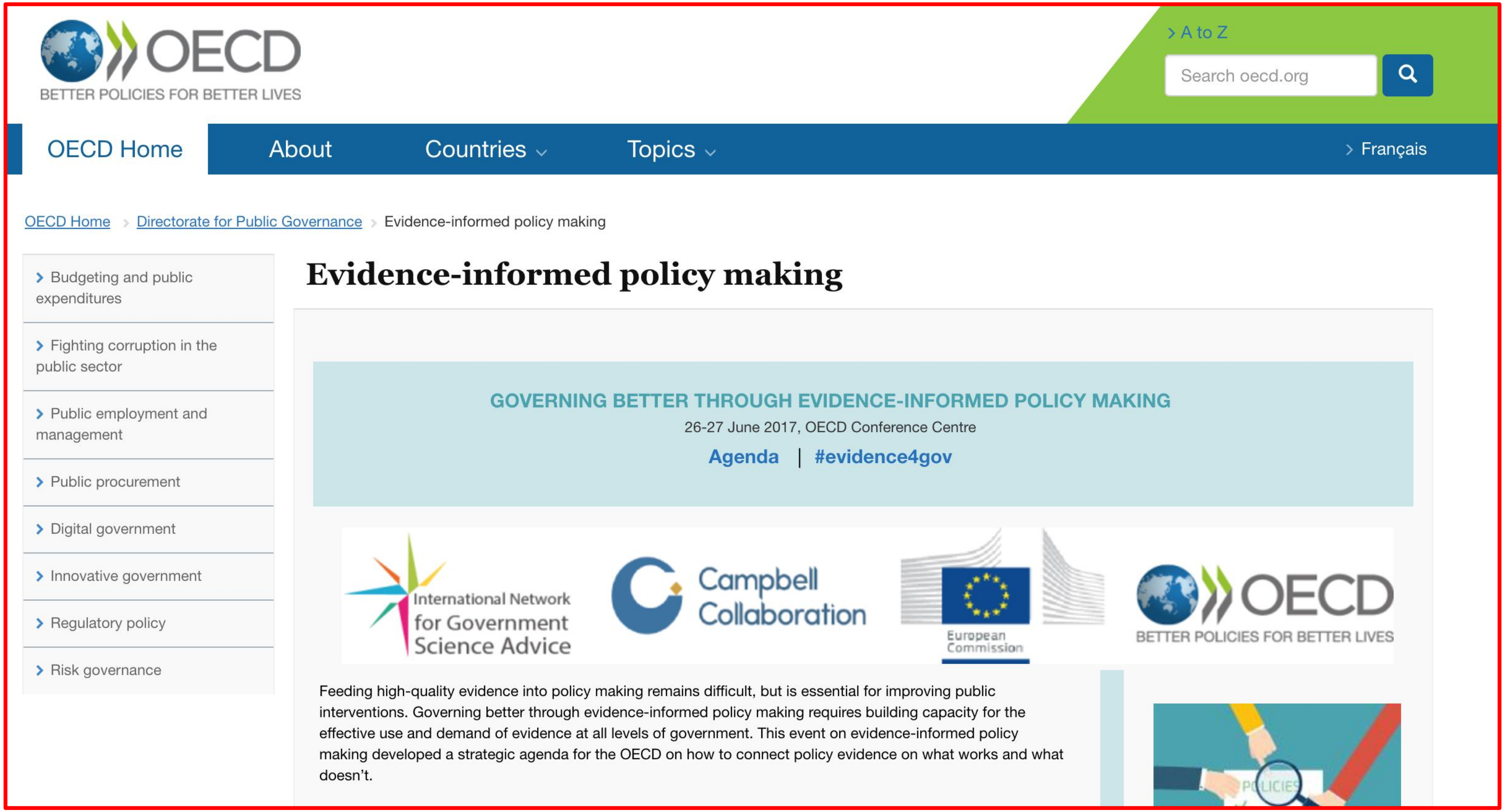
Directive	GDPR
Right of Access - Art. 12(a)	Right of Access - Art. 15
Right to Rectification - Art. 12(b)	Right to Rectification - Art. 16
Limited Right to Erasure - Art. 12(b)	**(Expanded)** Right to Erasure - Art. 17
	New! Right to Restriction of Processing - Art. 18
	New! Right to Data Portability - Art. 20
Right to Object - Art. 14	**(Expanded)** Right to Object - Art. 21
Automated Individual Decisions - Art. 15	Automated Individual Decisions - Art. 22

- *Expanded right to object*: Any processing based legitimate interest can be objected to by simply demanding a stop. Requires companies to map out what processing is conducted for what purposes; policies need to reflect interests that will override user objections. Marketing-related processing will always need to stop. Fraud/crime prevention likely to survive customer objection.

SEGMENT 3

1 Evidence-Informed Policymaking and Other Best Practices

Emerging Best Practices



OECD
BETTER POLICIES FOR BETTER LIVES
› A to Z
Search oecd.org
OECD Home
About
Countries ⌵
Topics ⌵
› Français

OECD Home › Directorate for Public Governance › Evidence-informed policy making

› Budgeting and public expenditures
› Fighting corruption in the public sector
› Public employment and management
› Public procurement
› Digital government
› Innovative government
› Regulatory policy
› Risk governance

Evidence-informed policy making

GOVERNING BETTER THROUGH EVIDENCE-INFORMED POLICY MAKING

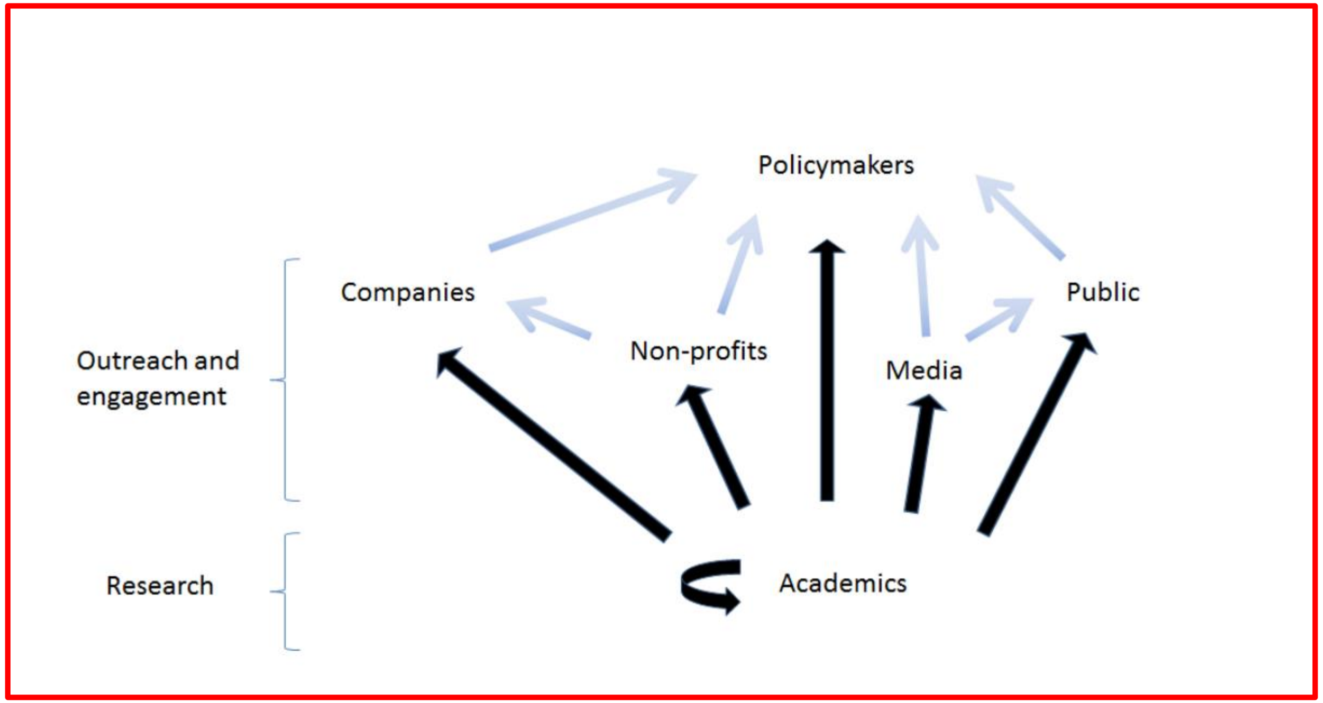
26-27 June 2017, OECD Conference Centre

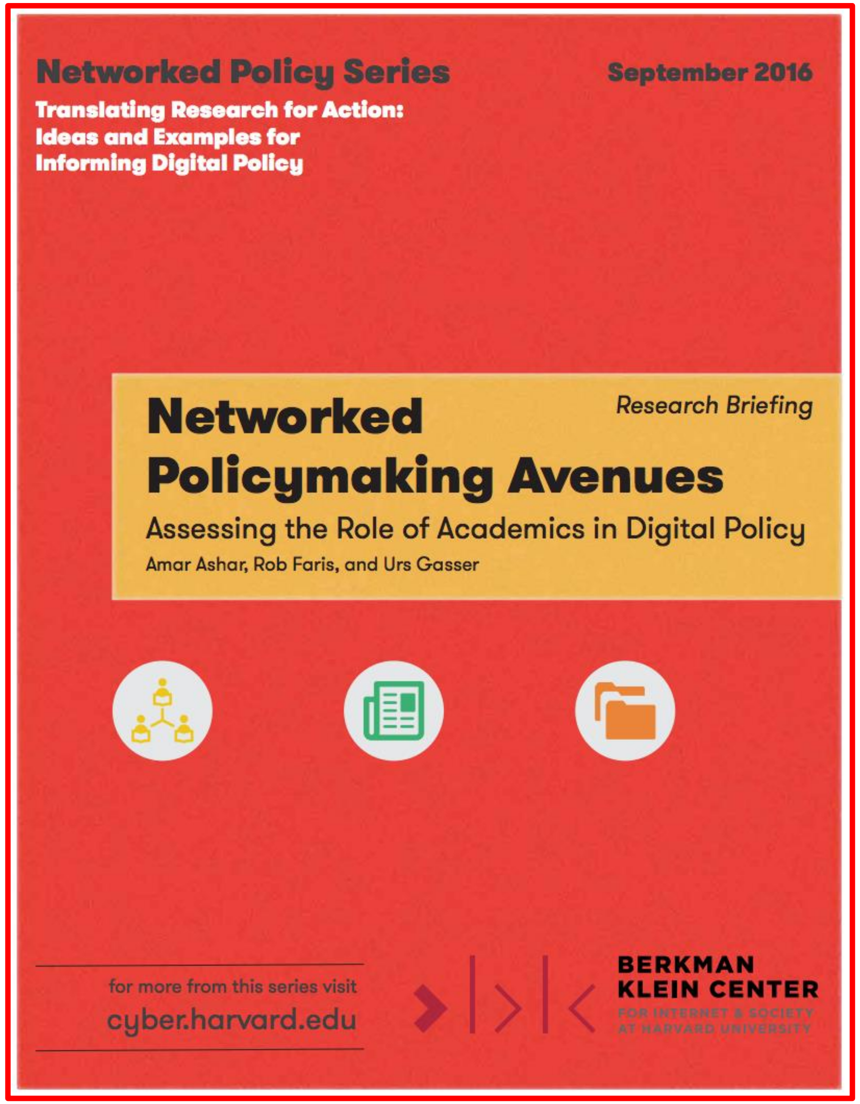
Agenda | **#evidence4gov**

International Network for Government Science Advice
Campbell Collaboration
European Commission
OECD
BETTER POLICIES FOR BETTER LIVES
POLICIES

Feeding high-quality evidence into policy making remains difficult, but is essential for improving public interventions. Governing better through evidence-informed policy making requires building capacity for the effective use and demand of evidence at all levels of government. This event on evidence-informed policy making developed a strategic agenda for the OECD on how to connect policy evidence on what works and what doesn't.

Building Interfaces





Networked Policy Series

September 2016

Translating Research for Action: Ideas and Examples for Informing Digital Policy

Networked Policymaking Avenues

Research Briefing

Assessing the Role of Academics in Digital Policy

Amar Ashar, Rob Faris, and Urs Gasser

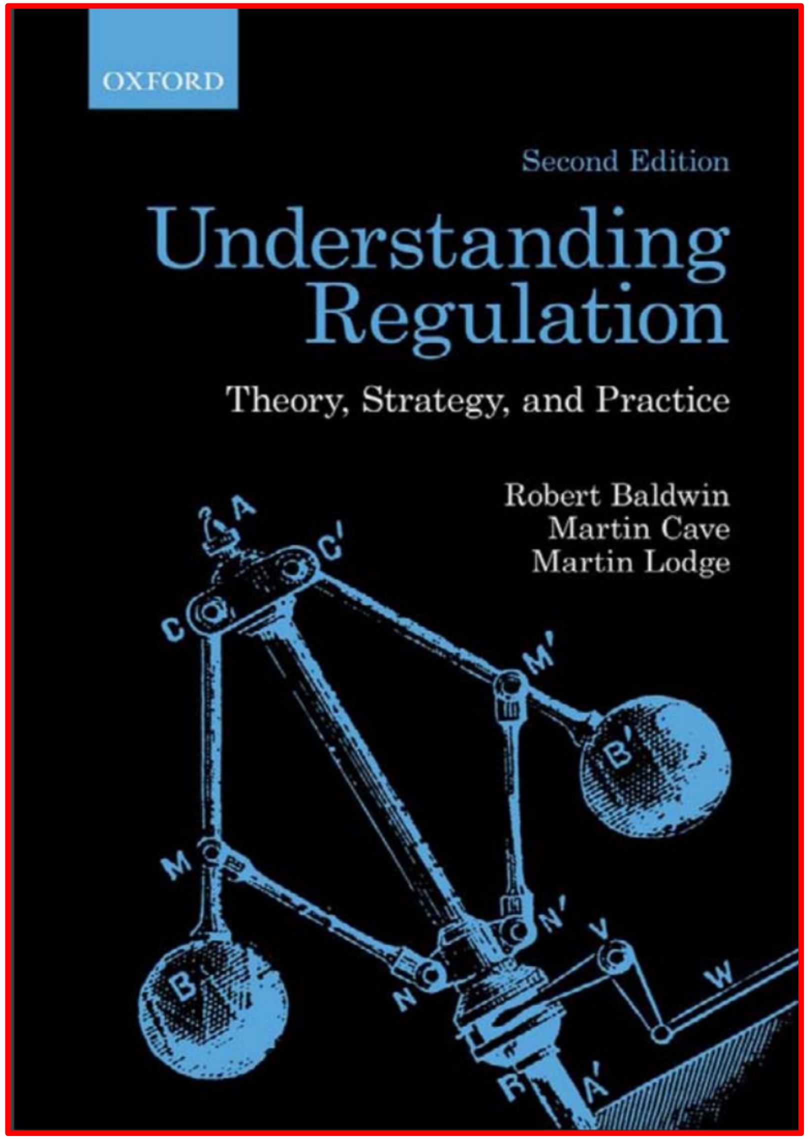
for more from this series visit
cyber.harvard.edu

BERKMAN KLEIN CENTER
FOR INTERNET & SOCIETY
AT HARVARD UNIVERSITY

https://cyber.harvard.edu/publications/2016/NetworkedPolicymaking

Criteria for Good Regulation

1. Is the action or regime supported by legislative authority?
2. Is there an appropriate scheme of accountability?
3. Are procedures fair, accessible, and open?
4. Is the regulator acting with sufficient expertise?
5. Is the action or regime efficient?



OXFORD

Second Edition

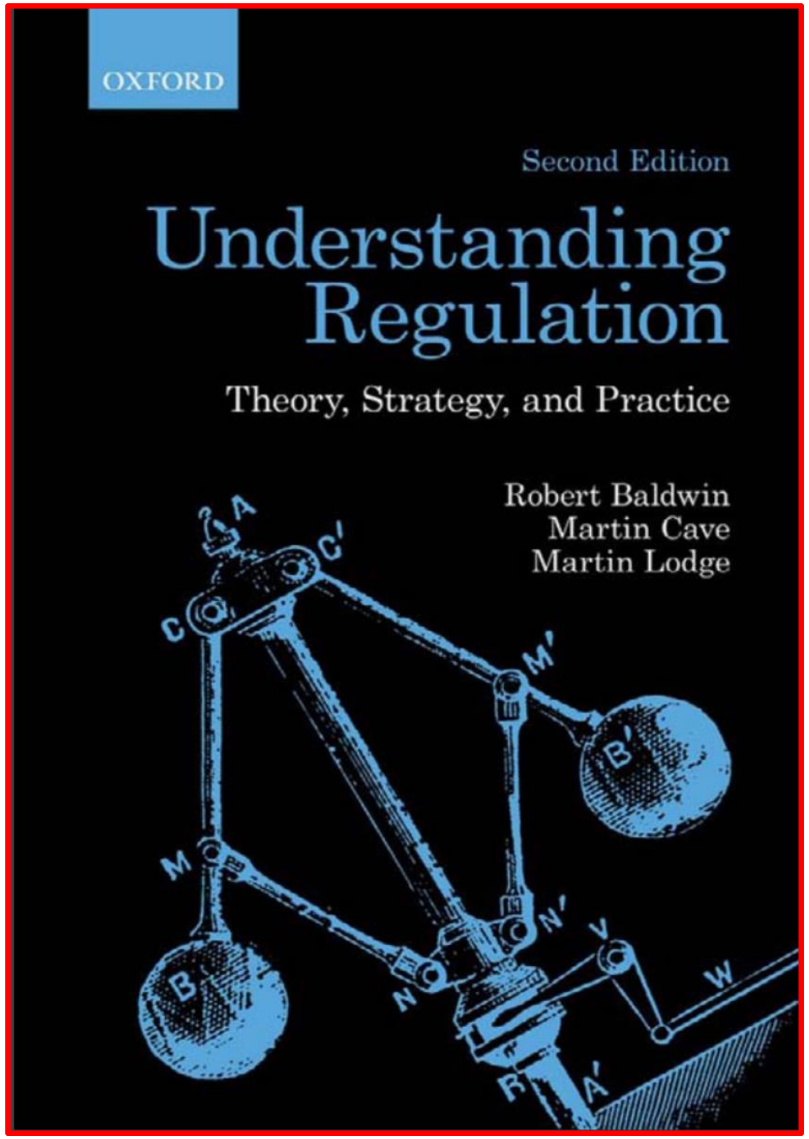
Understanding Regulation

Theory, Strategy, and Practice

Robert Baldwin
Martin Cave
Martin Lodge

Criteria for Good Regulation

1. Is the action or regime supported by legislative authority?
2. Is there an appropriate scheme of accountability?
3. Are procedures fair, accessible, and open?
4. Is the regulator acting with sufficient expertise?
5. Is the action or regime efficient?



OXFORD

Second Edition

Understanding Regulation

Theory, Strategy, and Practice

Robert Baldwin
Martin Cave
Martin Lodge

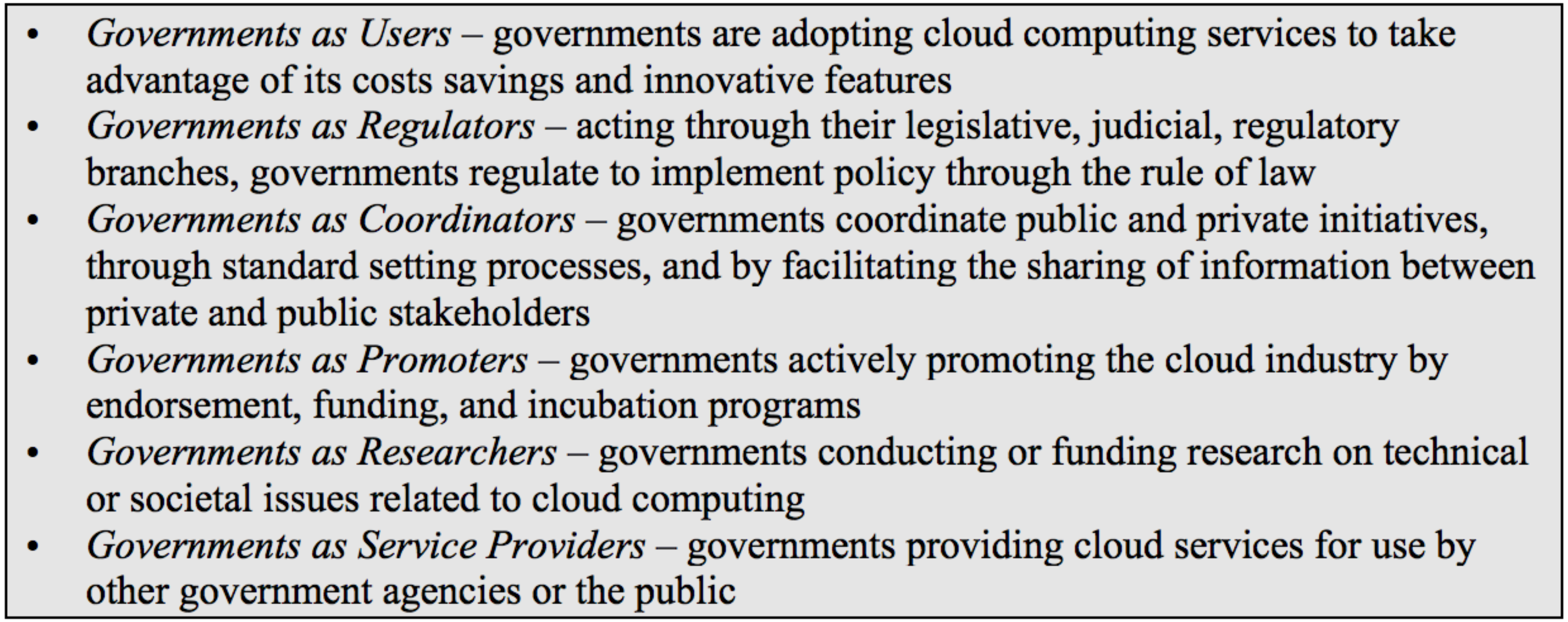
Learning Systems

- Even when pursuing an evidence-informed approach, law- and policymakers and regulators are often required to make decisions under uncertainty and complexity.
- Creates a structural need for learning (legal, regulatory) systems so that new knowledge can be incorporated when it comes available: Responsive regulation, smart regulation, etc.
- Institutional repertoire still relatively limited, incl.
  - Collaborative rulemaking
  - Periodic reviews
  - Sunset clauses
  - Backward planning method
  - Independent agency with decision-making power

2 National Digital Strategies

Introduction: Roles of Government

- Governments can play different roles when it comes to engagement with the digital economy, digital technology, and digital policy-making
- Example: Analysis of national Cloud Computing strategies highlights the following roles (Gasser & O'Brien, 2014):



- *Governments as Users* – governments are adopting cloud computing services to take advantage of its costs savings and innovative features
- *Governments as Regulators* – acting through their legislative, judicial, regulatory branches, governments regulate to implement policy through the rule of law
- *Governments as Coordinators* – governments coordinate public and private initiatives, through standard setting processes, and by facilitating the sharing of information between private and public stakeholders
- *Governments as Promoters* – governments actively promoting the cloud industry by endorsement, funding, and incubation programs
- *Governments as Researchers* – governments conducting or funding research on technical or societal issues related to cloud computing
- *Governments as Service Providers* – governments providing cloud services for use by other government agencies or the public

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2410270

Singapore: Leader in Digitization

- 100% connected homes and 150% device penetration.
- Strong digital government as a pillar, top leadership sponsorship & Singapore IDA.
- Evolving regulatory framework, strong user-centricity, incl. willingness of government to experiment and take risks and enter PPPs:
  - *Stage 1 - Automation and availability*: where government is very focused on digitizing its services and making it available on-line. Focus is mainly on citizens needs and engagements.
  - *Stage 2 - Mobility and simplicity* (single platform/portal): where government adopt a more integrated service delivery platform and portal to simplify user experience, targeting both citizens and enterprises.
  - *Stage 3 - Predictability, collaboration, and personalization*: where government becomes smarter about using customer data, rely more on AIto think ahead / anticipate things, and proactively provide personalized services. It also creates a fully open platform for citizens and enterprises to develop and customize their own services (digital communities).
- Major limitation of Singapore model's replication: small city-state with a single layer of government, which can instigate and implement such innovations very quickly.

Sweden: Low-Risk Entrepreneurship

- Sweden is the second-most productive tech hub in the world on a per-capita basis, after Silicon Valley, producing 6.3 billion-dollar companies per million people. One of the most open, competitive, and diverse economies in the world.
- Risk-friendly -- provided by the generous cradle-to-grave welfare system.
- Governmental support to access to personal computers and construction of ICT infrastructure during the late 1990s.
- Key takeaways:
  - Improvements of digital literacy need not solely be focused on the education system.
  - Achieving significant and sustainable impact from taxpayer-funded investments is likely to be a long-term play.
  - Given the dynamic nature of technology, it is important that politicians do not worry too much about trying to predict how investments might generate a return in the short term, but rather focus on longer-term capacity for innovation and entrepreneurship.

Brazil: Multi-Stakeholder Governance

- Brazilian Internet Steering Committee (CGI), comprised of 21 members from government, industry, technical and academic community.
- Unique Internet governance model for the effective participation of society in decisions involving network implementation, management, and use.
- Non-government members are democratically elected, no sector has majority.
- Responsible for Internet strategic planning, recommending standards for technical and operational procedures, and establishing guidelines to orient relationship between government and society.
- Challenge: Quest for consensus is never an organized or orderly process.

Further Reading (forthcoming)

Digital Policy Playbook

Approaches to National Digital Governance

(DRAFT FOR REVIEW)

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

July 2017

Discussion

- Which of these country examples are of particular interest in the context of Thailand?

- What are the core elements of the (future) digital strategy for Thailand? What’s the role of the government?

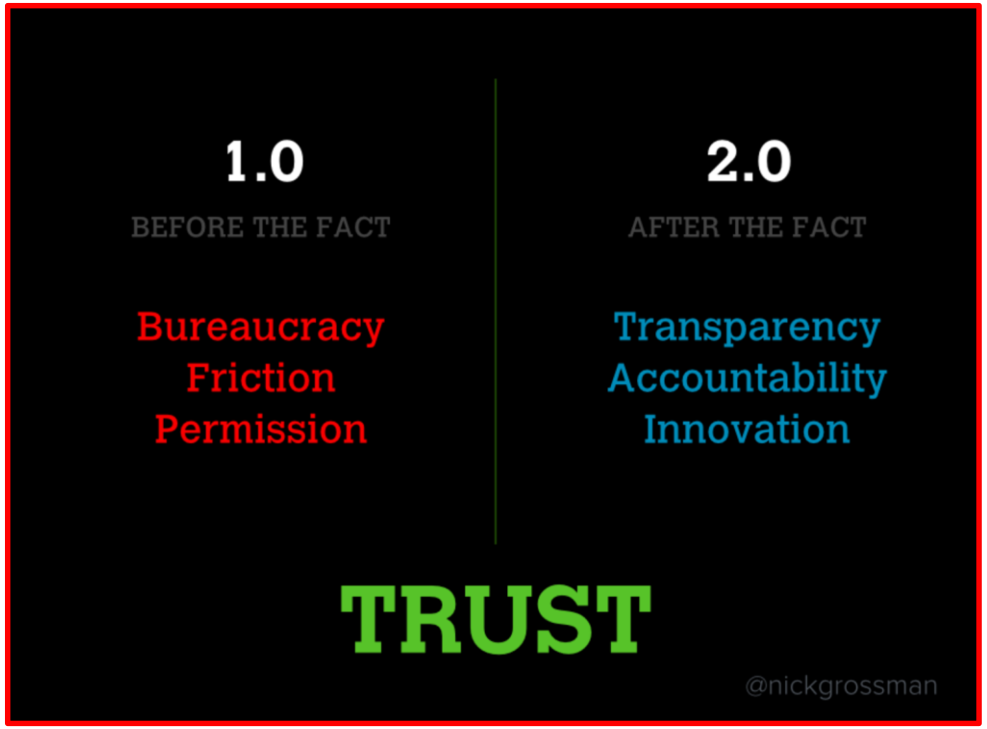
- What are lessons learned from Thailand with regard to law and policy of digital economy and technology?

3 Outlook and Some Concepts

Law and Regulation: Shifting Paradigm

- *Old paradigm*: Law is often seen in tension with digital technologies – technology as a "threat" and *problem.*
  - A cat and mouse game
  - Technology undermines privacy/security/labor/markets/… and law must respond, through subsumption, innovation, or gradual adjustments.
  - Historically this has been an accurate description of the progress of technology and law.
- Opportunity for a *new paradigm*: Disruptive technology can be harnessed to be a part of the *solution space* to privacy/security/labor/markets/… challenges.
  - Fusing computer science, law, policy, sociology, economic disciplines in a strategic way (incl. shared vocabulary for semantic interoperability).
  - Developing new types of technology to be deployed in collaboration with legal, regulatory, and policy changes.

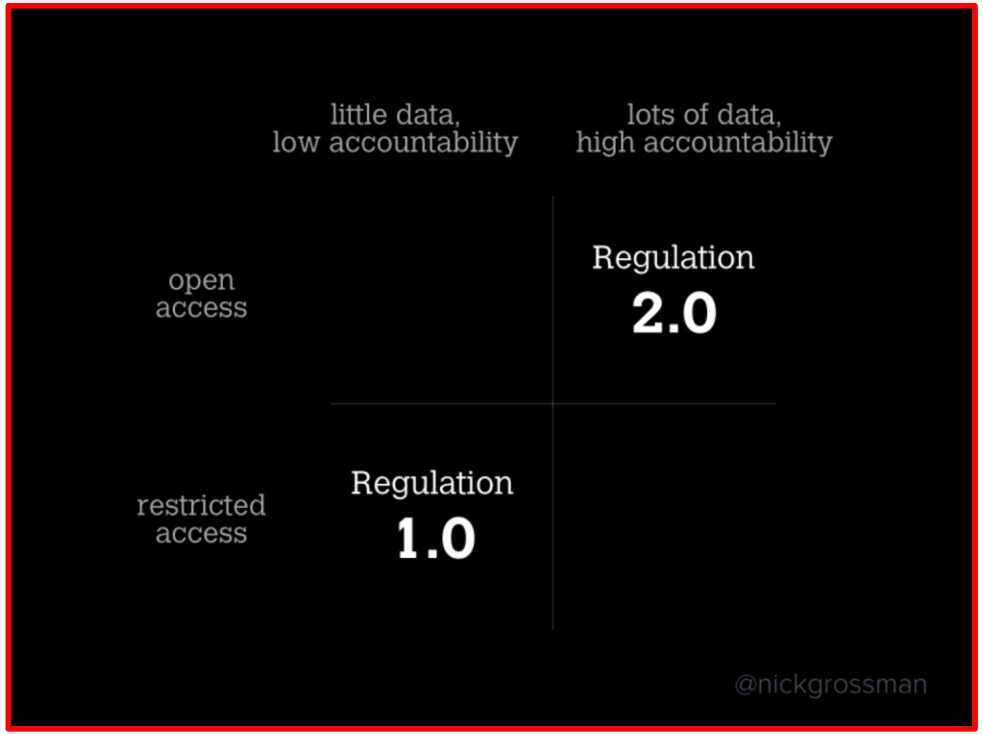
Example: Regulation 2.0



1.0	2.0
BEFORE THE FACT	AFTER THE FACT
Bureaucracy Friction Permission	Transparency Accountability Innovation

TRUST

@nickgrossman



	little data, low accountability	lots of data, high accountability
open access		Regulation 2.0
restricted access	Regulation 1.0	

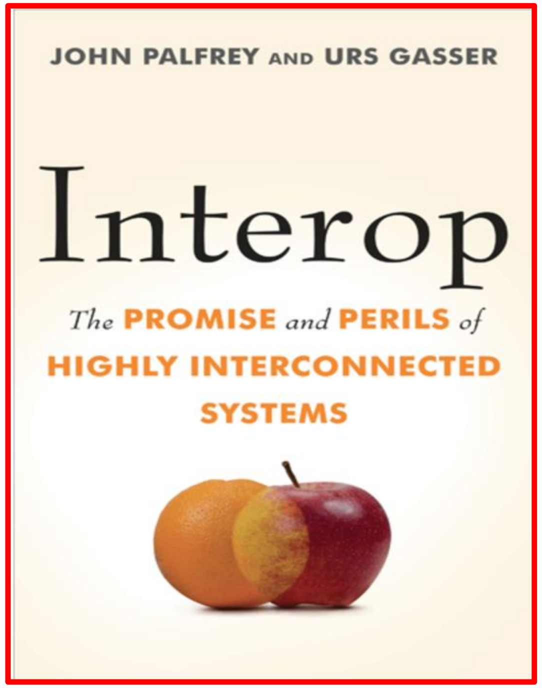
@nickgrossman

http://datasmart.ash.harvard.edu/news/article/white-paper-regulation-the-internet-way-660

Legal Interoperability

“Legal interoperability addresses the process of making legal rules cooperate across jurisdictions, on different subsidiary levels within a single state or between two or more states. Whether new laws should be implemented or existing laws adjusted or reinterpreted to achieve this interoperability depends on the given circumstances […].

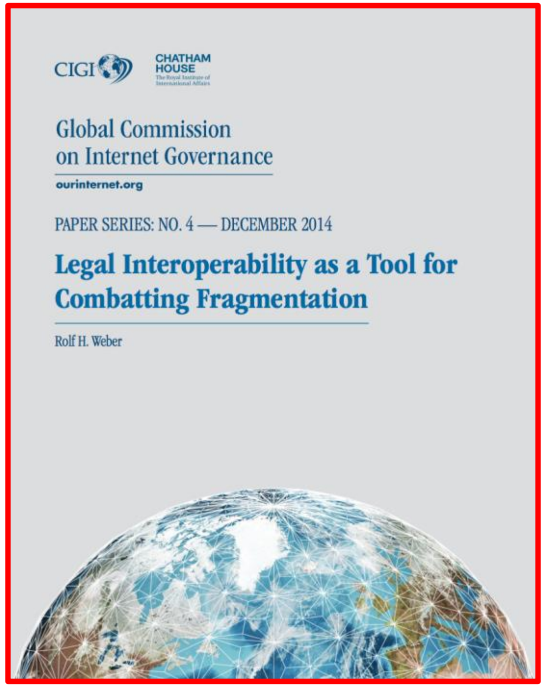
In view of the increasing fragmentation of the legal environment in cyberspace, efforts must be undertaken to achieve higher levels of legal and policy interoperability in order to facilitate global communication, to reduce costs in cross-border business, and to drive innovation and economic growth. Interoperable legal rules can also create a level playing field for the next generation of technologies and cultural exchange […]” (Weber 2014).



JOHN PALFREY AND URS GASSER

Interop

The PROMISE and PERILS of HIGHLY INTERCONNECTED SYSTEMS



CIGI CHATHAM HOUSE The Royal Institute of International Affairs

Global Commission on Internet Governance

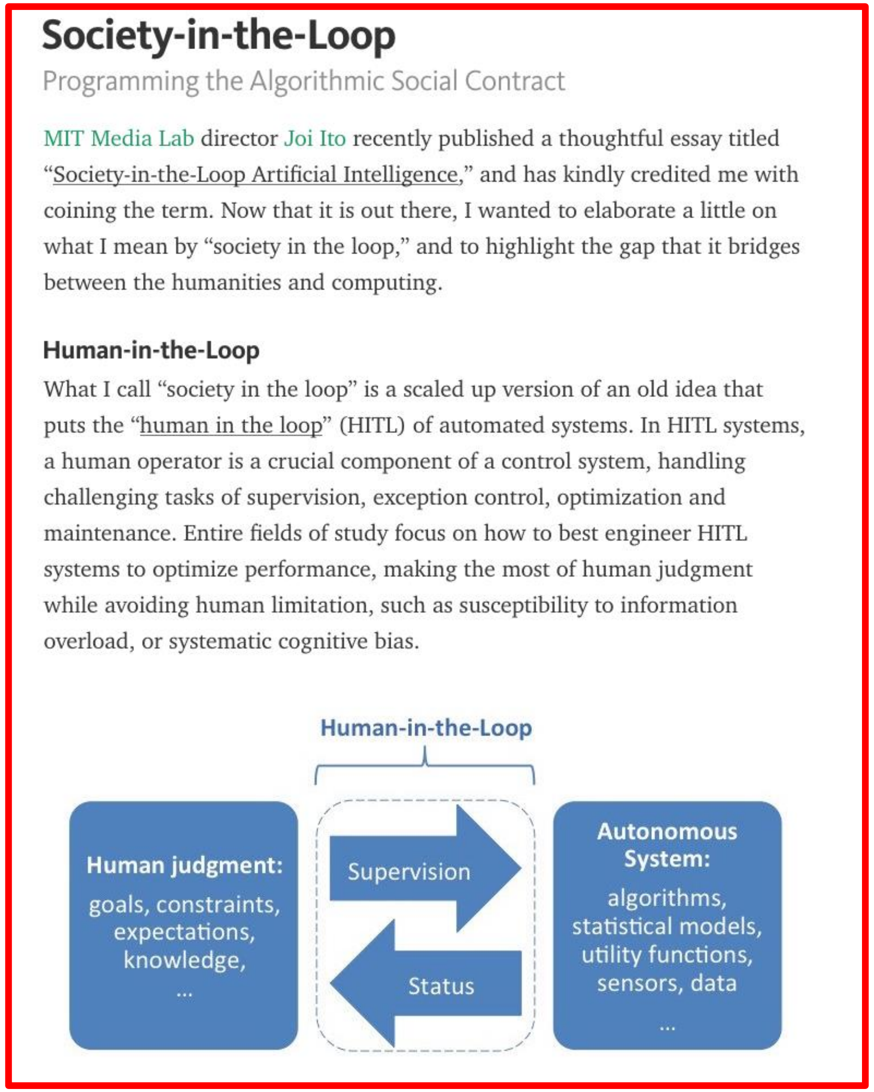
ourinternet.org

PAPER SERIES: NO. 4 — DECEMBER 2014

Legal Interoperability as a Tool for Combatting Fragmentation

Rolf H. Weber

Next Frontier: Artificial Intelligence



Society-in-the-Loop

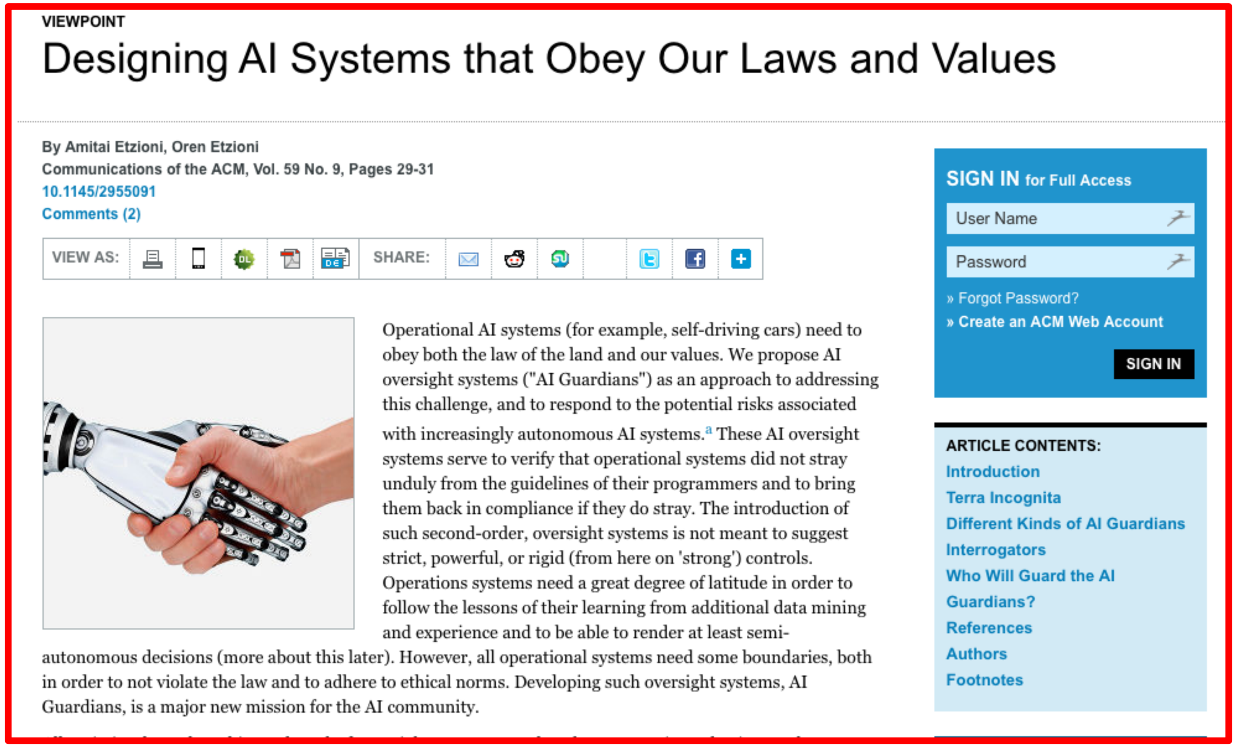
Programming the Algorithmic Social Contract

MIT Media Lab director Joi Ito recently published a thoughtful essay titled "Society-in-the-Loop Artificial Intelligence," and has kindly credited me with coining the term. Now that it is out there, I wanted to elaborate a little on what I mean by "society in the loop," and to highlight the gap that it bridges between the humanities and computing.

Human-in-the-Loop

What I call "society in the loop" is a scaled up version of an old idea that puts the "human in the loop" (HITL) of automated systems. In HITL systems, a human operator is a crucial component of a control system, handling challenging tasks of supervision, exception control, optimization and maintenance. Entire fields of study focus on how to best engineer HITL systems to optimize performance, making the most of human judgment while avoiding human limitation, such as susceptibility to information overload, or systematic cognitive bias.

Human-in-the-Loop
Human judgment:
goals, constraints, expectations, knowledge, …
Supervision
Status
Autonomous System:
algorithms, statistical models, utility functions, sensors, data
…



VIEWPOINT

Designing AI Systems that Obey Our Laws and Values

By Amitai Etzioni, Oren Etzioni
Communications of the ACM, Vol. 59 No. 9, Pages 29-31
10.1145/2955091
Comments (2)

Operational AI systems (for example, self-driving cars) need to obey both the law of the land and our values. We propose AI oversight systems ("AI Guardians") as an approach to addressing this challenge, and to respond to the potential risks associated with increasingly autonomous AI systems.[a] These AI oversight systems serve to verify that operational systems did not stray unduly from the guidelines of their programmers and to bring them back in compliance if they do stray. The introduction of such second-order, oversight systems is not meant to suggest strict, powerful, or rigid (from here on 'strong') controls. Operations systems need a great degree of latitude in order to follow the lessons of their learning from additional data mining and experience and to be able to render at least semi-autonomous decisions (more about this later). However, all operational systems need some boundaries, both in order to not violate the law and to adhere to ethical norms. Developing such oversight systems, AI Guardians, is a major new mission for the AI community.

ARTICLE CONTENTS:

Introduction
Terra Incognita
Different Kinds of AI Guardians
Interrogators
Who Will Guard the AI Guardians?
References
Authors
Footnotes

SEGMENT 4

Closing Exercise

In groups, please discuss on of the following questions:

1. Which of the current digital economy issues in Thailand would benefit from a multi-stakeholder approach?
2. Where can and should law play an enabling role in the future of Thailand’s digital economy?
3. How do you measure success when “regulating” the digital economy?

Q & A

Thank You

Email: ugasser@law.harvard.edu

Twitter: @ugasser