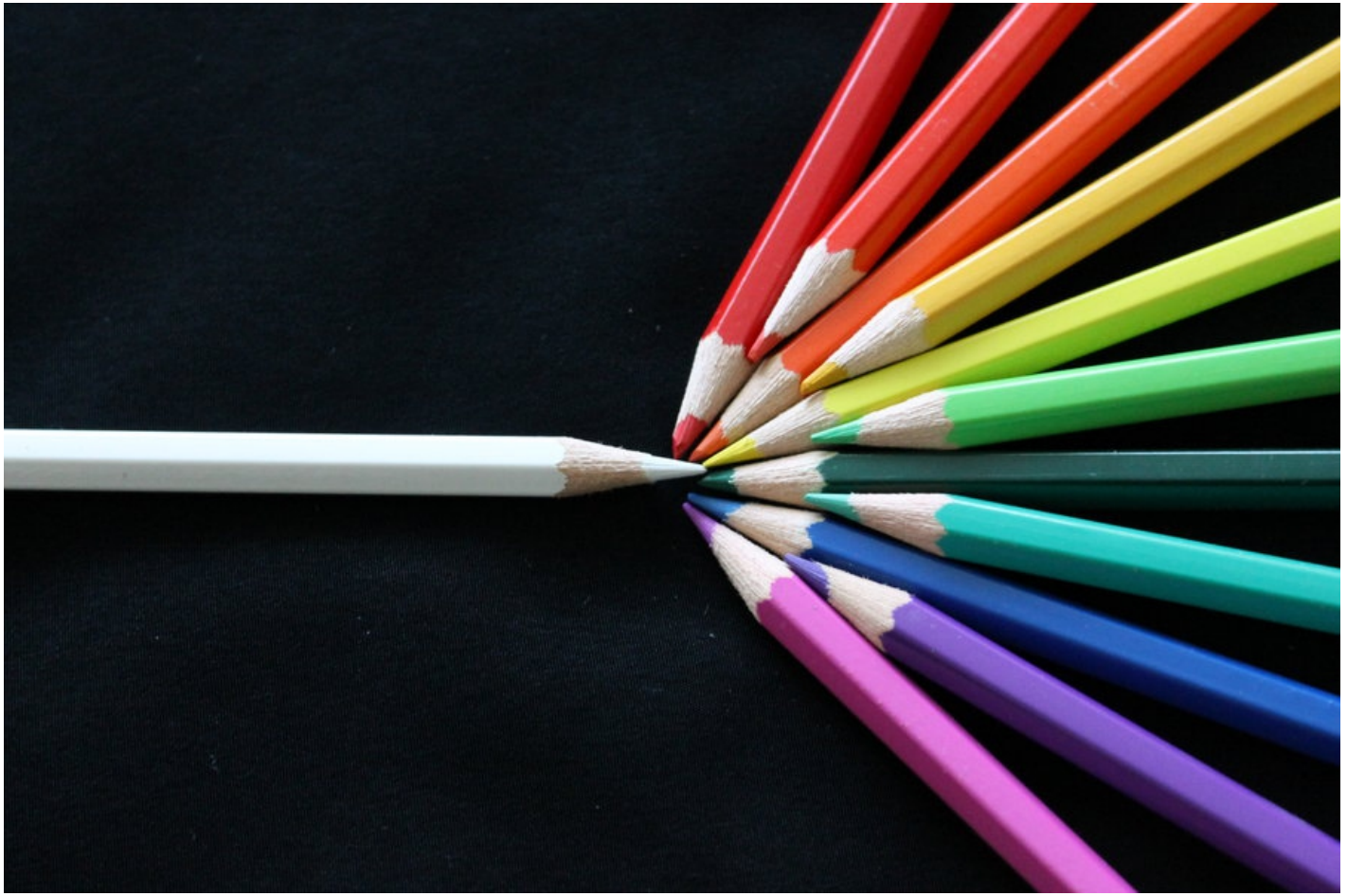
Any Colour You Like



The History (and Future?) of Communications Security Policy

NYU Security Seminar, New York 22.04.14
https://www.axelarnbak.nl
2013/14 Fellow Berkman Center & CITP, IviR University of Amsterdam

‘Obscured by Clouds’: Cloud Surveillance From Abroad

With Joris van Hoboken and Nico van Eijk
http://ssrn.com/abstract=2276103

‘Another Loophole in the Wall’: Traffic Shaping to Circumenvent 4th Amendment Protections for U.S. users

With Prof. Sharon Goldberg

Securing Communications through Law Increasingly Popular, at least in E.U.

...

What is 'security' as regulatory concept? How should regulators conceive it?

OUTLINE

Why Interested in Concepts?!

40 Years of (E.U.) Communications Security Policy

Two Claims: ‘Technical’ & ‘Political’ Security

New, Third Claim: 'Human Right'

Communications Security Amidst 3 Claims

OUTLINE

Why Interested in Concepts?!

40 Years of (E.U.) Communications Security Policy

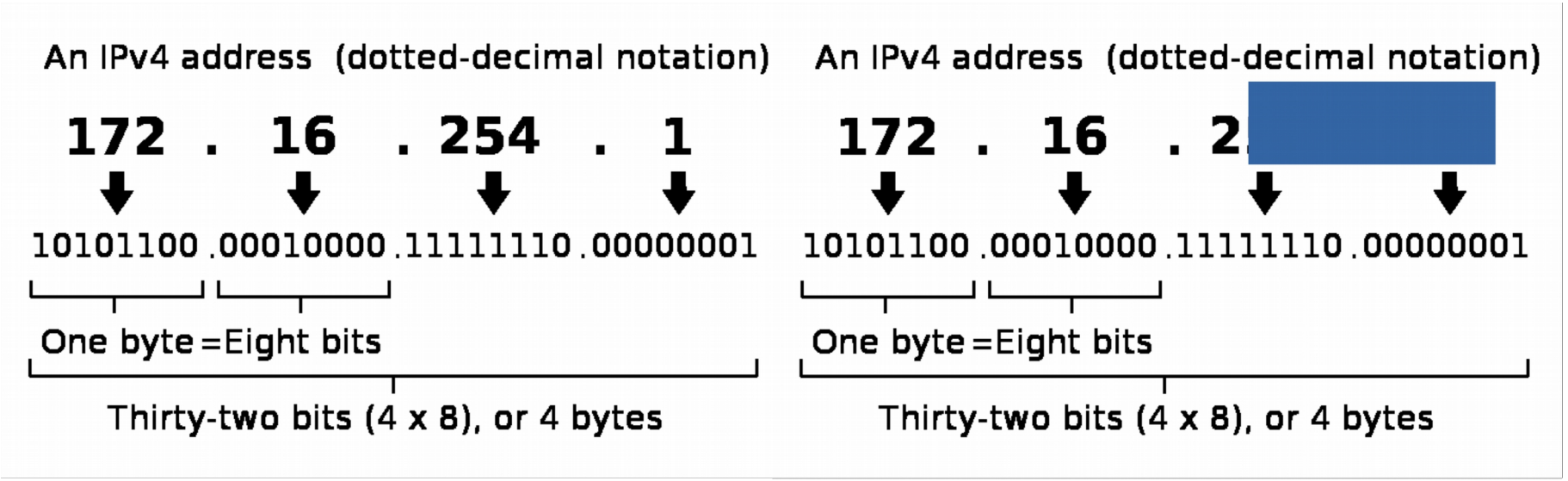
Two Claims: ‘Technical’ & ‘Political’ Security

New, Third Claim: 'Human Right'

Communications Security Amidst 3 Claims

Concepts Scope Regulation – Long Term Power Implications

15 years: IP-Address 'Personal Data' Definition?



New E.U. Proposal:[1] 'Pseudonimized' Data

E.U. Data Protection response to NSA? Lion's Share ≠ 'Personal Data'

OUTLINE

Why Interested in Concepts?!

40 Years of (E.U.) Communications Security Policy

Two Claims: ‘Technical’ & ‘Political’ Security

New, Third Claim: 'Human Right'

Communications Security Amidst 3 Claims

"In almost every issue of weekly [Computerworld] is an article detailing a case of computer fraud, embezzlement or sabotage (…). Over 100 different articles from mid 1971."

1.P. Browne, *Computer security: a survey,* ACM SIGMIS, vol. 4/3, 1972
2.A. Westin, *Databanks in a free society; computers, record-keeping, and privacy*, New York: Quadrangle Books 1972.

E.U. ‘Security’ Concepts: 5 Cycles Analyzed Definition & Scope

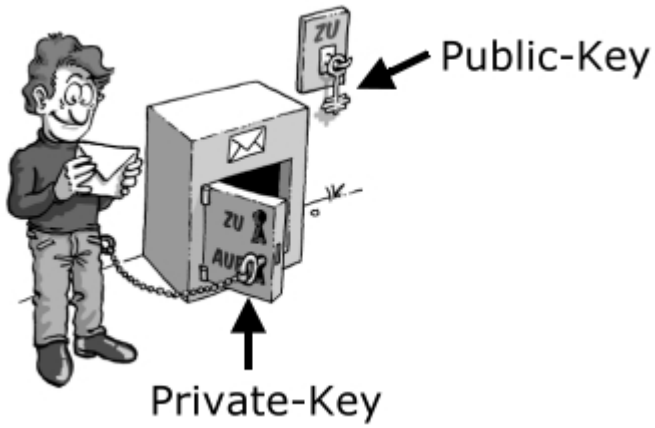
1. Data Protection
2. Telecommunications Law
3. Encryption: Signatures & Certificates
4. Cybercrime
5. ‘Network & Information Security’

You May Wonder, No National Security? Sole Competence E.U. Member States

History on One side of Coin:
E.U. Council / Members States
Re-frame it as National Security

Future on Other side of Coin?
Might enable focus on actually securing communications

Found some gems in mid 90s E.U. 'Security' Policymaking (paper)



General Observations E.U. Policies: Not About Communications Security

1. No conceptual clarity whatsoever
2. Data protection important normative influence
3. Lobbying very successful, legislator wary of additional regulatory burdens
4. Implicit, huge national security capture by E.U. Member States
5. Without E.U. constitutional framework, end user interests hardly observed

Comparison with U.S. Approach to Communications Security Concepts

"Secure Communications – Telecommunications deriving security through use of NSA-approved products"

NIST IR 7298, Revision 2, "Glossary of Key Information Security Terms", p. 171

Response to improving security

- For the past decade, NSA has lead an aggressive, multi-pronged effort to break widely used Internet encryption technologies
- Cryptanalytic capabilities are now coming on line
- Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable
- Major new processing systems, SIGDEV efforts and tasking must be put in place to capitalize on this opportunity

PTD "We penetrate targets' defences."

BULLRUN:
SUBVERTS HTTPS / SSL

(U) There is More Than One Way to QUANTUM

TS//SV//REL

Name	Description	Inception Date	Status	Operational Success
CNE				
QUANTUMINSERT	• Man-on-the-Side technique • Briefly hi-jacks connections to a terrorist website • Re-directs the target to a TAO server (FOXACID) for implantation	2005	Operational	**Highly Successful** (In 2010, 300 TAO implants were deployed via QUANTUMINSERT to targets that were un-exploitable by any other
QUANTUMBOT	• Takes control of idle IRC bots • Finds computers belonging to botnets, and hijacks the command and control channel	Aug 2007	Operational	**Highly Successful** (over 140,000 bots co-opted)
QUANTUMBISCUIT	• Enhances QUANTUMINSERT's man-on-the-side technique of exploitation • Motivated by the need to QI targets that are behind large proxies, lack predictable source addresses, and have insufficient unique web activity.	Dec 2007	Operational	**Limited success at NSAW due to high latency on passive access** (GCHQ uses technique for 80% of CNE accesses)
QUANTUMDNS	• DNS injection/redirection based off of A Record queries. • Targets single hosts or caching name servers.	Dec 2008	Operational	**Successful** (High priority CCI target exploited)
QUANTUMHAND	Exploits the computer of a target who uses Facebook	Oct 2010	Operational	**Successful**
QUANTUMPHANTOM	Hijacks any IP on QUANTUMable passive coverage to use as covert infrastructure.	Oct 2010	Live Tested	**N/A**
CNA				
QUANTUMSKY	Denies access to a webpage through RST packet spoofing.	2004	Operational	**Successful**
QUANTUMCOPPER	File download/upload disruption and corruption.	Dec 2008	Live Tested	**N/A**
CND				
QUANTUMSMACKDOWN	Pevents target from downloading implants to DoD computers while capturing malicious payload for analysis.	Oct 2010	Live Tested	**N/A**

TS//SV//REL

ANTUM: ~100.000 NETWORKS

~140.000 Botnets

Securing Communications through Law Increasingly Popular, at least in E.U.

...

What is 'security' as regulatory concept? How should regulators conceive it?

OUTLINE

Why Interested in Concepts?!

40 Years of (E.U.) Communications Security Policy

Two Claims: ‘Technical’ & ‘Political’ Security

New, Third Claim: Human Right to Data Security

Communications Security Amidst 3 Claims

Two Different Claims to 'Security': 'Technical' and 'Political'

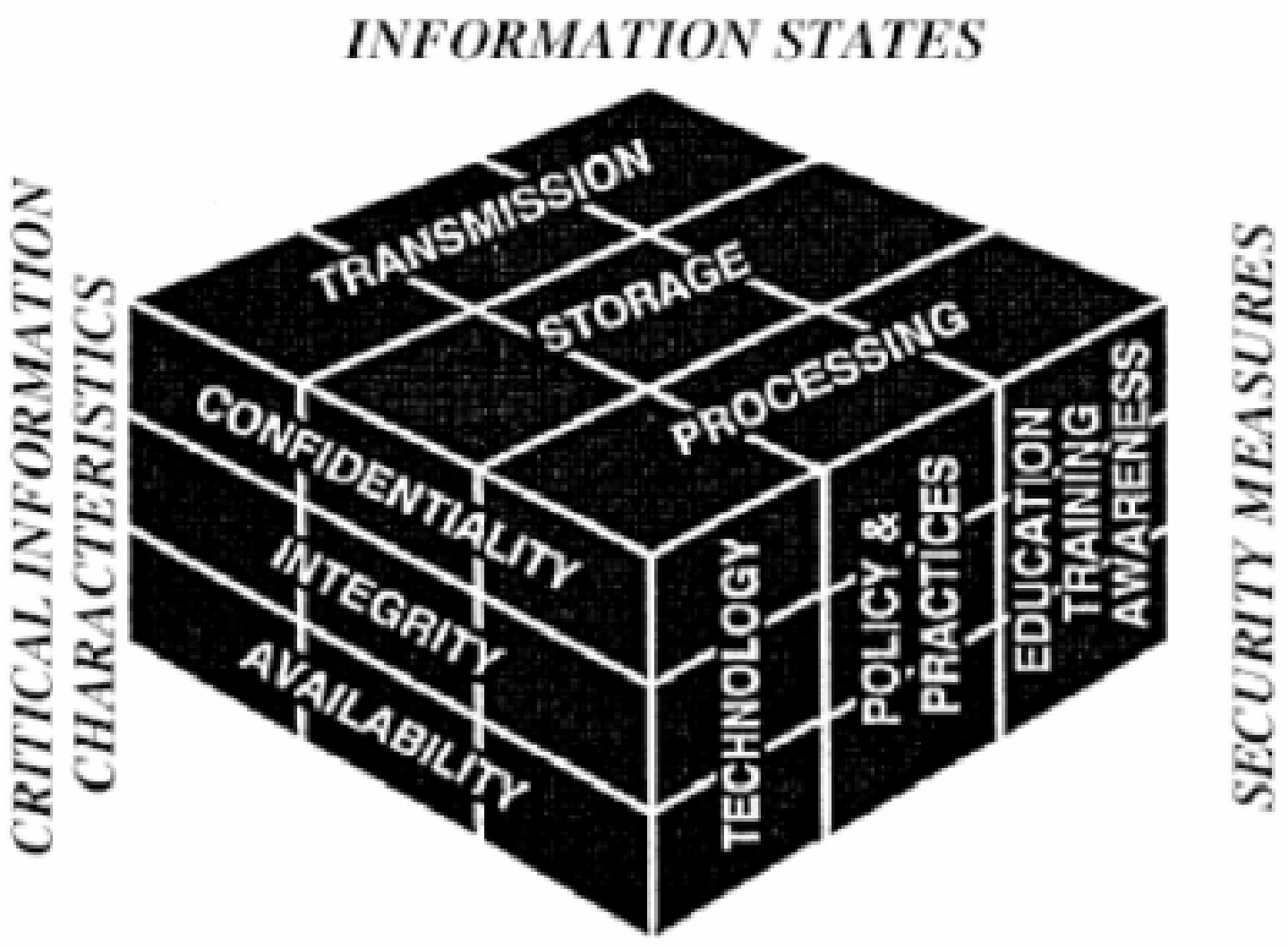
Where computer security meets national security[1]

Helen Nissenbaum
Department of Culture and Communication, New York University, NY, USA
E-mail: helen.nissenbaum@nyu.edu

Abstract. This paper identifies two conceptions of security in contemporary concerns over the vulnerability of computers and networks to hostile attack. One is derived from individual-focused conceptions of computer security developed in computer science and engineering. The other is informed by the concerns of national security agencies of government as well as those of corporate intellectual property owners. A comparative evaluation of these two conceptions utilizes the theoretical construct of "securitization," developed by the Copenhagen School of International Relations.

Key words: cyber-security, computer security, securitization

c.i.a.-Triad & McCumber Cube, 1991
Still part of training, standards, law



'Technical' Security: c.i.a.-Triad

Security protects

Confidentiality
Integrity
Availability

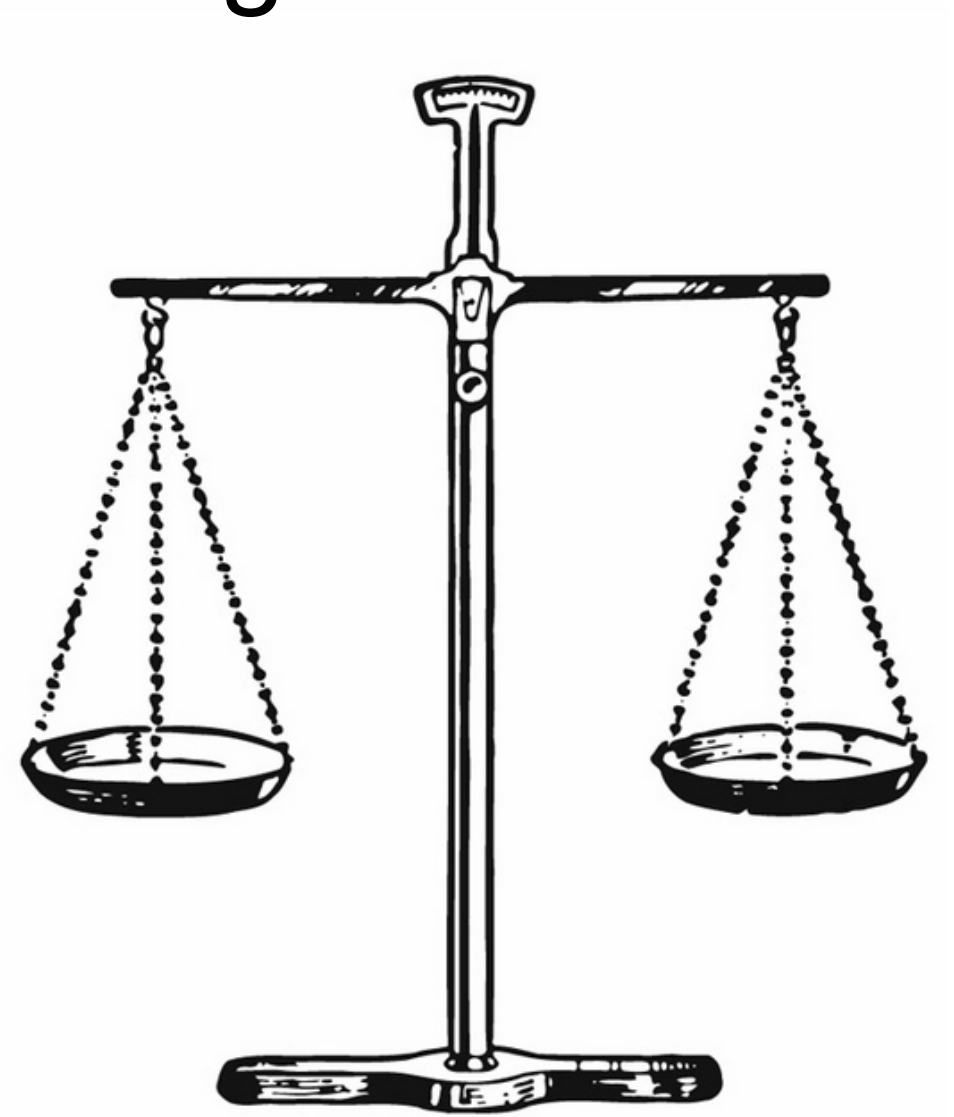
} of information transmitted through networks/systems

"the protection of information and information systems against unauthorised access or modification, whether in storage, processing, or transit, and against denial of service to authorised users"

Source: 'History of Information Security', Auerbach 2002, p.20.

RAND Report R-609 ("The Ware Report"), 1970
Calls to expand c.i.a. / to use 'Assurance' – Cherdantseva et al. (2013)

Central Concept: Authorization Role for Regulation



Complex c.i.a. trade-offs
Role for regulation/policy

DigiNotar Attack: Casualties? 600.000 Iranian IP Addresses

OUTLINE

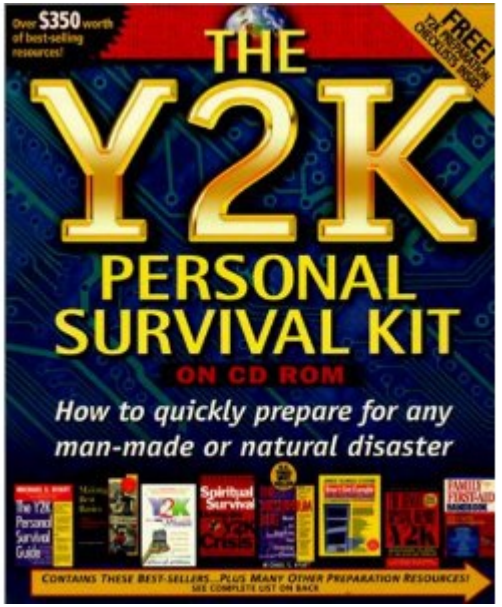
Why Interested in Concepts?!

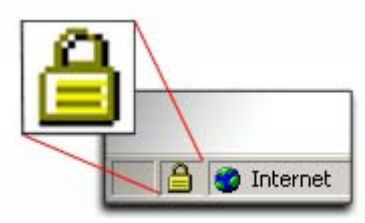
40 Years of (E.U.) Communications Security Policy

Two Claims: ‘Technical’ & **‘Political’ Security**

New, Third Claim: 'Human Right'

Communications Security Amidst 3 Claims





So 90's:
Users Connect
Tech Changes
Crypto Wars
IP Wars

Increased stakes in IT give rise to 'Political Security': Cybersecurity

Cybersecurity Securitization:

1. Urgent, imminent, existential **threat**
2. To a significant **collective**
3. By an accepted, powerful **agent**

The Copenhagen School
Nissenbaum (2009)

Cybersecurity Securitization: Securing Political Agenda's

Cybersecurity: the "Cyber Threat" to Monitor All Communications

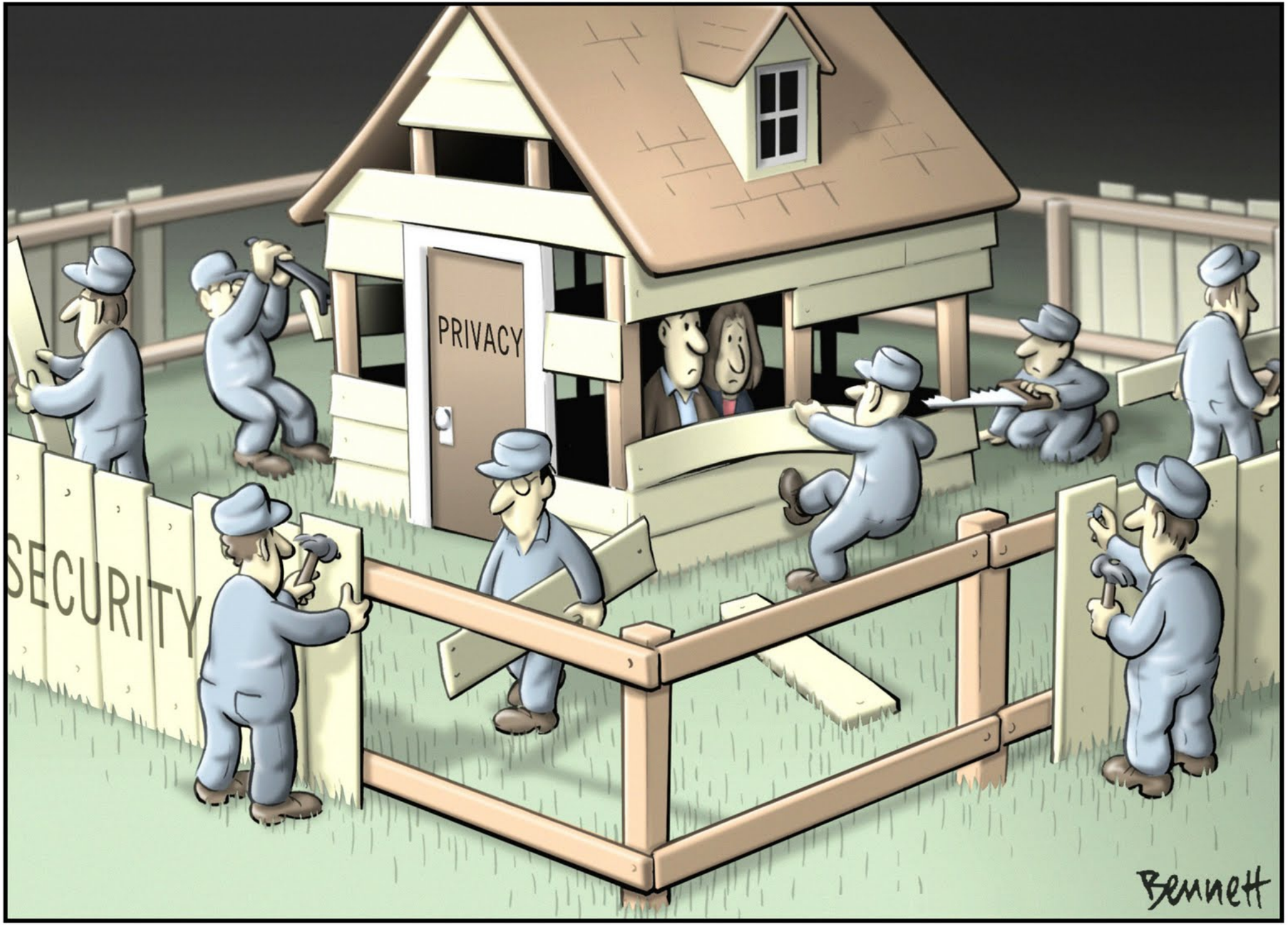
James Baker, former senior DOJ official on FISA:

"Let me repeat that: there are arguments that in order to defend ourselves, the government needs to be able to monitor all Internet communications. All of them.

Is this possible, even if it is necessary? Maybe. The key limiting factors are money and access. And you would need lots of both."

13 Sep '13, Constitution Day address, Dickinson College

http://clarke.dickinson.edu/wp-content/uploads/Dickinson-Constitution-Day-Talk-12-Sept-2013.pdf


PRIVACY
SECURITY
Bennett

OUTLINE

Why Interested in Concepts?!

40 Years of (E.U.) Communications Security Policy

Two Claims: ‘Technical’ & ‘Political’ Security

New, Third Claim: 'Human Right'

Communications Security Amidst 3 Claims

CONSEIL DE L'EUROPE

COUNCIL OF EUROPE

COUR EUROPÉENNE DES DROITS DE L'HOMME
EUROPEAN COURT OF HUMAN RIGHTS

FOURTH SECTION

CASE OF I v. FINLAND

(Application no. 20511/03)

Human Right to Data Security: States Obliged to Legislate and Enforce

JUDGMENT

STRASBOURG

17 July 2008

СЪД НА ЕВРОПЕЙСКИЯ СЪЮЗ
TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA
SOUDNÍ DVŮR EVROPSKÉ UNIE
DEN EUROPÆISKE UNIONS DOMSTOL
GERICHTSHOF DER EUROPÄISCHEN UNION
EUROOPA LIIDU KOHUS
ΔΙΚΑΣΤΗΡΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ
COURT OF JUSTICE OF THE EUROPEAN UNION
COUR DE JUSTICE DE L'UNION EUROPÉENNE
CÚIRT BHREITHIÚNAIS AN AONTAIS EORPAIGH
SUD EUROPSKE UNIJE
CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA

CVRIA
LUXEMBOURG

EIROPAS SAVIENĪBAS TIESA
EUROPOS SĄJUNGOS TEISINGUMO TEISMAS
AZ EURÓPAI UNIÓ BÍRÓSÁGA
IL-QORTI TAL-ĠUSTIZZJA TAL-UNJONI EWROPEA
HOF VAN JUSTITIE VAN DE EUROPESE UNIE
TRYBUNAŁ SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ
TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA
CURTEA DE JUSTIȚIE A UNIUNII EUROPENE
SÚDNY DVOR EURÓPSKEJ ÚNIE
SODIŠČE EVROPSKE UNIJE
EUROOPAN UNIONIN TUOMIOISTUIN
EUROPEISKA UNIONENS DOMSTOL

JUDGMENT OF THE COURT (Grand Chamber)

8 April 2014 *

(Electronic communications — Directive 2006/24/EC — Publicly available electronic communications services or public communications networks services — Retention of data generated or processed in connection with the provision of such services — Validity — Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union)

In Joined Cases C-293/12 and C-594/12,

REQUESTS for a preliminary ruling under Article 267 TFEU from the High Court (Ireland) and the Verfassungsgerichtshof (Austria), made by decisions of 27 January and 28 November 2012, respectively, received at the Court on 11 June and 19 December 2012, in the proceedings

Digital Rights Ireland Ltd (C-293/12)

8 apr, E.U. Court Data Retention Directive Void

Landmark ruling for 'data security': European Court of Justice, §66-68

§66: “no sufficient safeguards to ensure full confidentiality and integrity”

1. §66: Criteria when security measures need to go beyond general delegation to private sector:
   - Quantity Data
   - Sensitivity Data
   - Risk of Abuse
2. §67: DRD wrongly permits economic considerations for data security
3. §67: DRD has no explicit data destruction rules
4. §68: DRD does not prohibit storing data outside E.U., insufficient control over retained data

German Constitutional Court Hacking/Malware Surveillance

According to BVerfG, NJW 2008, 822 (849).

- IT-systems particularly sensitive
  - Separates systems, communication, data
  - Systems deserve particular protection
    - We structure our life
    - All-stop-shop for government access
  - Network, 'cloud‘ exacerbates privacy intrusion
    - 3rd parties & data centralised

- Hacking IT violates core of privacy, personality
  - Beyond 'Communication', Beyond the Home

Human Right:
Confidentiality & Integrity IT-Systems

- Broad scope: general storage device
  - Internet of Things, 'Cloud', RAM
  - Not on public device, but also on public wifi
  - Regardless of technical expertise user
- Integrity: manipulation of data also covered

- Not absolute, but strictest legal criteria
  - Stricter than house search
    - Exemption: 'Foundations of the State'
    - But: 'Concrete danger for life and other rights
  - Core of private life cannot be restricted
    - If such data found, immediate deletion!

What is 'security' as regulatory concept?
How should regulators conceive it?

Obligation for legislators in Europe:
Constitutional Criteria

European Constitutional Obligations: Establish Baseline Protection

1. ECHR '08: Not only own use, but state responsibility to ensure citizens enjoy secure systems
2. ECJ '14: broad understanding 'communications', part of data security
3. ECJ '14: first time develops parameters for human right, links to c.i.a.-triad
4. German Constitutional Court Leads Way, similar to data protection in 1983 ruling?

OUTLINE

Why Interested in Concepts?!

40 Years of (E.U.) Communications Security Policy

Two Claims: ‘Technical’ & ‘Political’ Security

New, Third Claim: 'Human Right'

Communications Security Amidst 3 Claims

Securing Communications through Law Increasingly Popular, at least in E.U.

...

What is 'security' as regulatory concept? How should regulators conceive it?

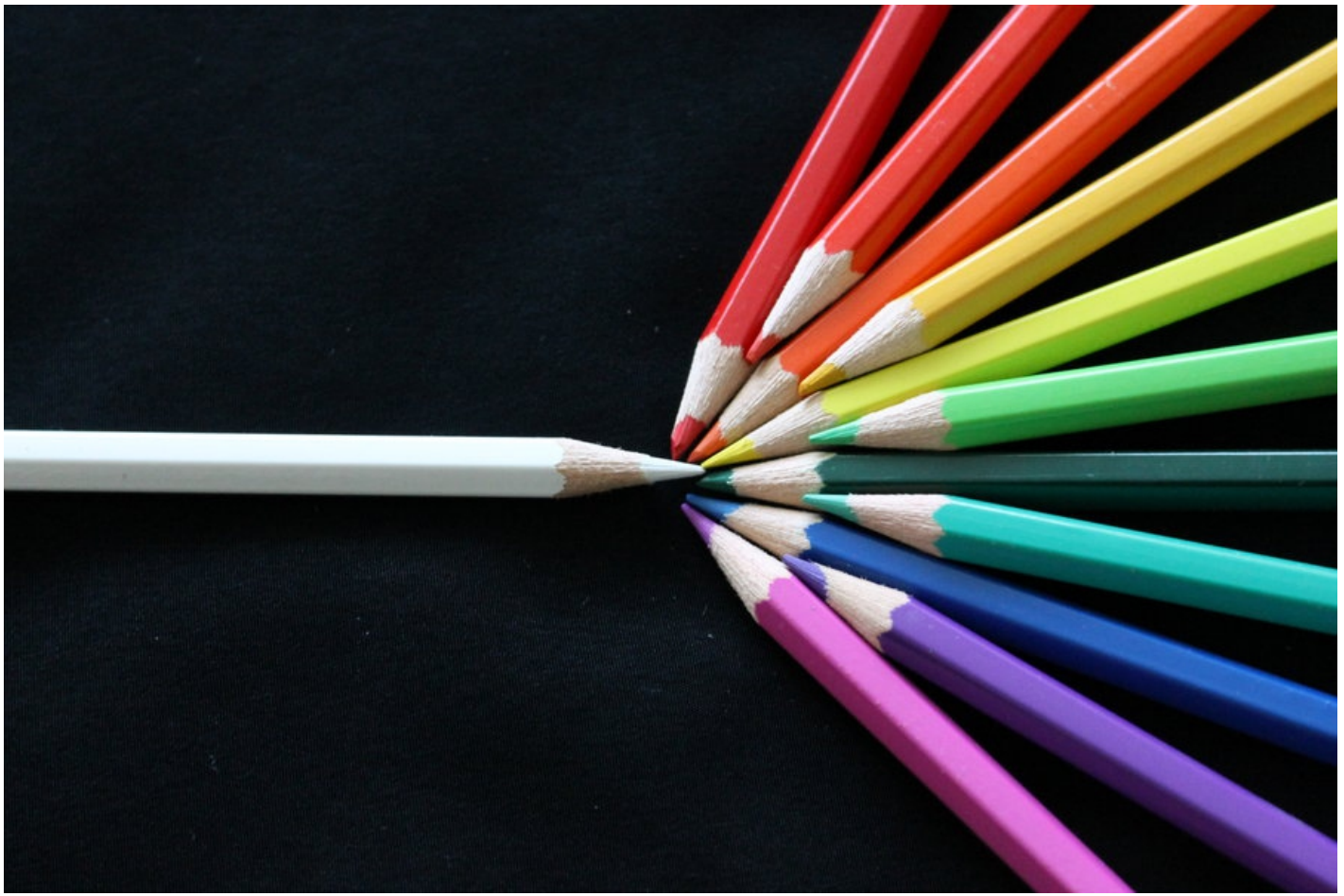
What Is "Communications Security" As a Regulatory Concept?

- Technical definition, and need to deepen conversation engineers and policymakers
- Infused with constitutional values
- Courts recognize need to counterbalance perverse economic and political incentives detrimental to the enjoyment of secure communications and fundamental rights

What Is “Communications Security” As a Regulatory Concept?

- Conceptual boundaries systems, networks and information blurring – also in regulation
- How to negotiate the authorized user depends on very specific circumstance, cf. HTTPS
- Within constitutional parameters, policymakers need to provide normative guidance:
  - Are you ensuring secure communications, or securing economic / political agenda's?

Any Colour You Like



The History (and Future?) of Communications Security Policy

Introduction to the Comsec Conceptualization Roundtable @ Berkman, Harvard 18.04.14

https://www.axelarnbak.nl

2013/14 Fellow Berkman Center & CITP