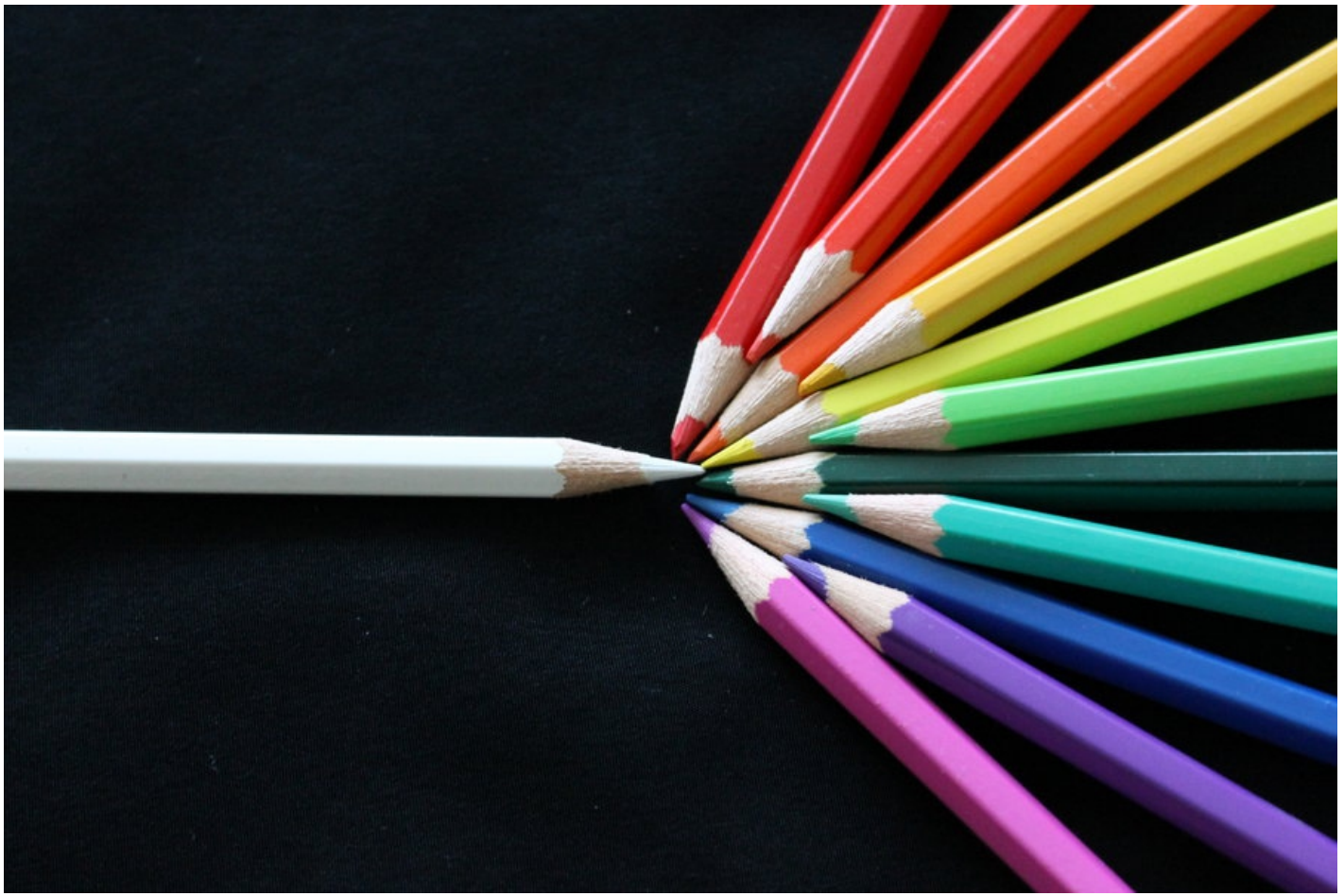
Any Colour You Like



The History (and Future?) of Internet Security Policy

Cyberscholars Workshop @ Berkman, Harvard 27.03.14

https://www.axelarnbak.nl
2013/14 Fellow Berkman Center & CITP

‘OBSCURED BY CLOUDS’: NSA SURVEILLANCE

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

‘ANOTHER LOOPHOLE IN THE WALL’: NSA TRAFFIC SHAPING TO CIRCUMVENT 4TH AMENDMENT

With prof. Sharon Goldberg

OUTLINE

Why Interested in Concepts?

Two Claims: ‘Technical’ & ‘Political’ Security

Policy: 40 Years of (E.U.) ‘Security’ Concepts

Research Agenda For Internet Security Policy

OUTLINE

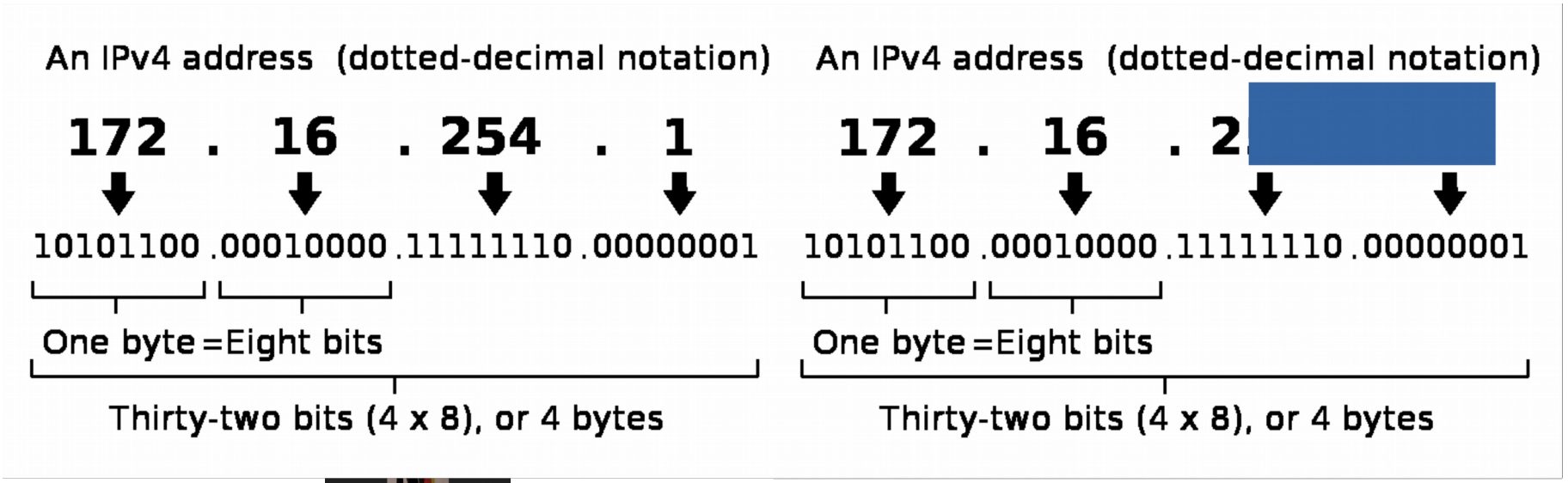
Why Interested in Concepts?

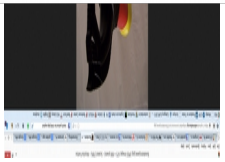
Two Claims: ‘Technical’ & ‘Political’ Security

Policy: 40 Years of (E.U.) ‘Security’ Concepts

Research Agenda For Internet Security Policy

‘Personal Data’ Definition: IP-Address? / ‘Pseudonimized Data?





Data Protection, Solution re: NSA?
Lion's Share ≠ Personal Data

OUTLINE

Why Interested in Concepts?

Two Claims: ‘Technical’ & ‘Political’ Security

Policy: 40 Years of (E.U.) ‘Security’ Concepts

Research Agenda For Internet Security Policy

Two Claims to Internet '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

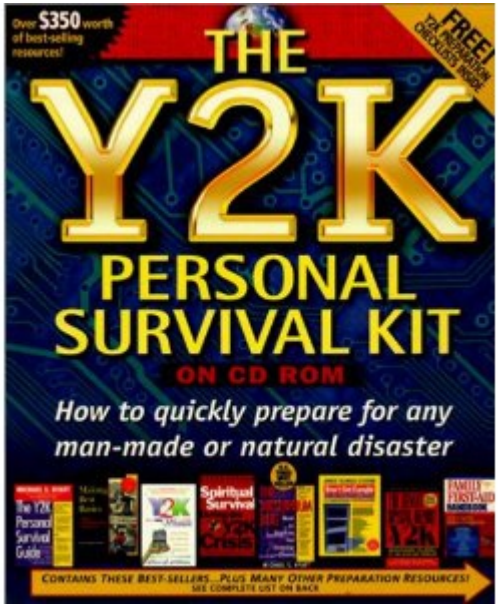
Abstract. This paper identifies two conceptions of security in contemporary concerns over the vulnerability of computers and networks to hostile attack. One is derived from individual-focused conceptions of computer security developed in computer science and engineering. The other is informed by the 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.

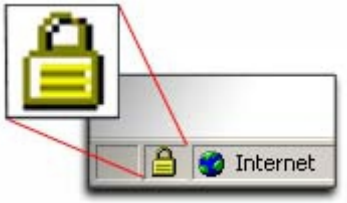
Key words: cyber-security, computer security, securitization

‘Technical Security’: c.i.a. Triad

McCumber Cube (1991)

Calls to Expand into Information Assurance – Cherdantseva et al. (2013)





So 90's:

Tech Change
Crypto Wars
IP Wars

‘Political Security’: Cybersecurity As a National Security Issue

Cybersecurity Securitization:

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

Nissenbaum (2009)

Cybersecurity Securitization: Trojan Horse for Exploitation

"CYBER-SECURITY" AND THE CYBER THREAT

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

OUTLINE

Why Interested in Concepts?

Two Claims: ‘Technical’ & ‘Political’ Security

Policy: 40 Years of (E.U.) ‘Security’ Concepts

Research Agenda For Internet Security Policy

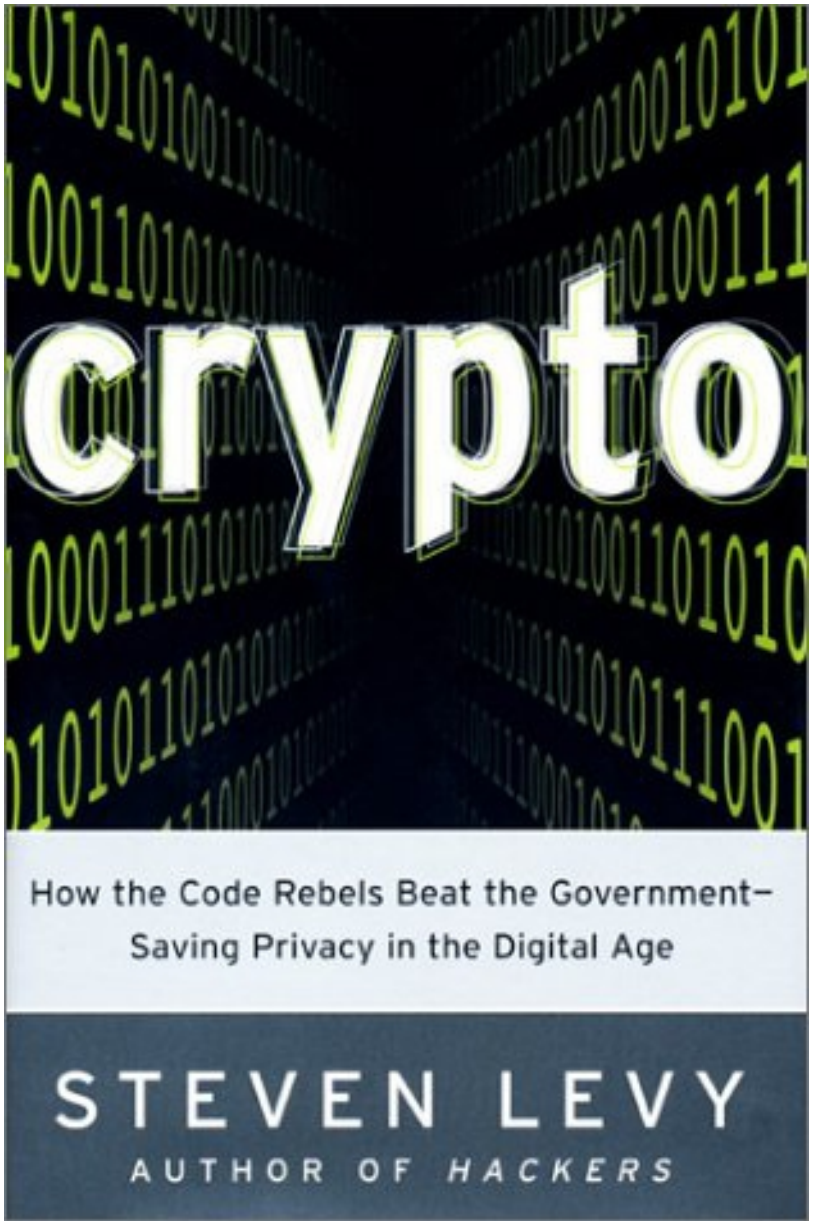
E.U. ‘Security’ Concepts: 5 Cycles Analyzed Definition & Scope

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

E.U. ‘Security’ Concepts: National Security? Member States!

Threat:
E.U. Council / States Re-framing into National Security Issue

Opportunity:
Focus on c.i.a.-Triad, Rather than “Cyber-Security”.
Internet Security For Everyone;



Definition Status Quo: Patchwork of Protection

	Confidentiality	*Integrity*	*Availability*
Data Protection	Personal data, may include network	Personal data, may include network	Personal data, may include network*
Telecoms Package	communications and information**	unclear, probably only personal data	priority issue, but phrased as 'integrity'
Encryption	undefined, linked to data protection	undefined, prioritized in Annexes	undefined, not covered
Cybercrime	undefined, but covered	undefined, but covered	undefined, but covered
"NIS"	yes, proposed Directive	adds 'authentiticity', proposed Directive	yes, proposed Directive

Definition Status Quo: Patchwork of Protection

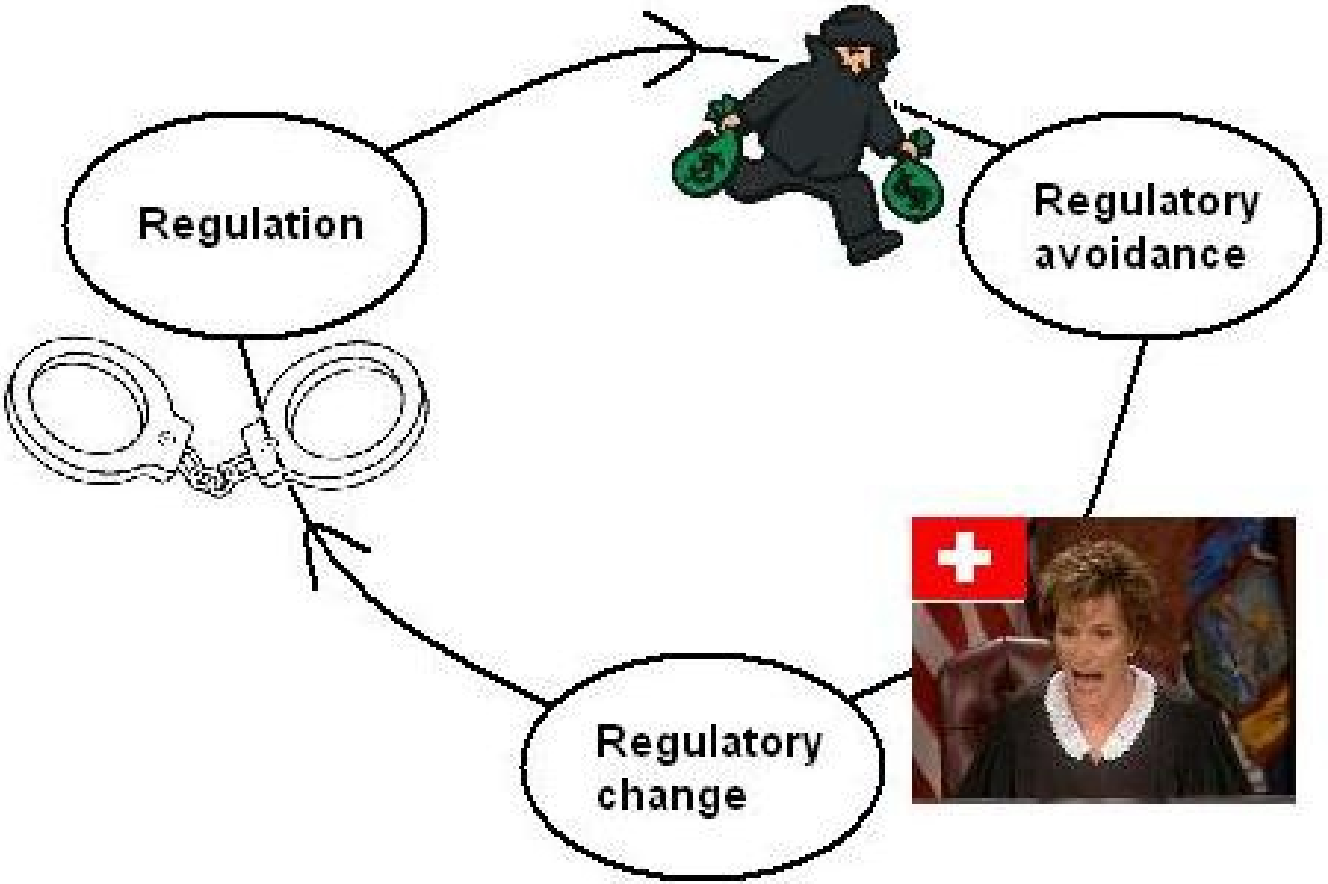
	Confidentiality	*Integrity*	*Availability*
Data Protection	Personal data, may include network	Personal data, may include network	Personal data, may include network*
Telecoms Package	communications and information**	unclear, probably only personal data	priority issue, but phrased as 'integrity'
Encryption	undefined, linked to data protection	undefined, prioritized in Annexes	undefined, not covered
Cybercrime	undefined, but covered	undefined, but covered	undefined, but covered
"NIS"	yes, proposed Directive	adds 'authentiticity', proposed Directive	yes, proposed Directive

Scope Status Quo: Laws Focus on Actor, rather than Function

at&t

regulated

Tech Turbulence Exacerbates Flawed Actor-Approach



OUTLINE

Why Interested in Concepts?

Two Claims: ‘Technical’ & ‘Political’ Security

Policy: 40 Years of (E.U.) ‘Security’ Concepts

Research Agenda For Internet Security Policy

The Major Research Question: A Directive for Internet Security?

Research Questions:

1. Computer Science
2. Political Science
3. Constitutional, European Law

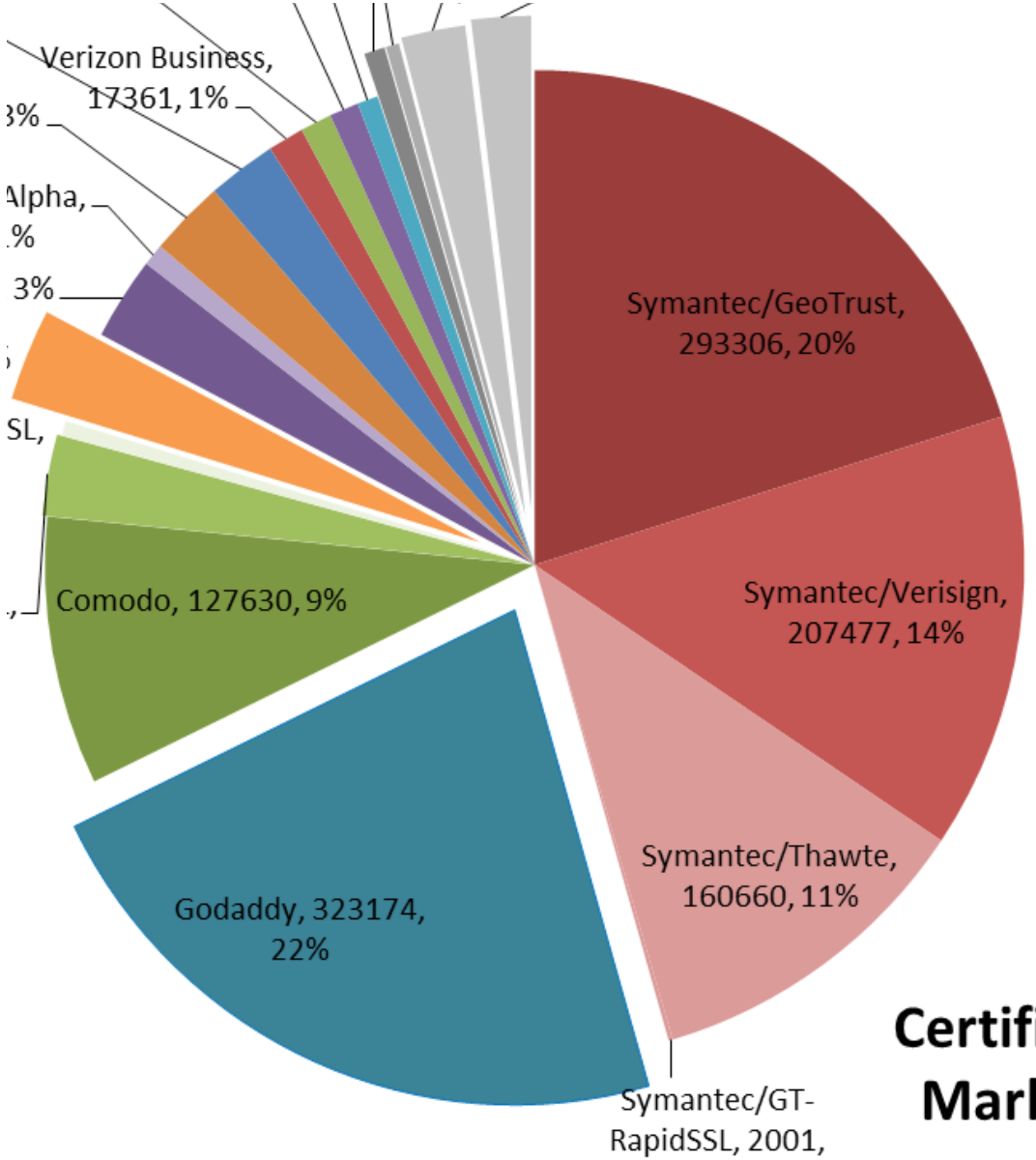
Technical Research Q's:

1. How timeless is the c.i.a.-Triad?
2. Security Requirements Engineering for Policy?
3. Is security a technical, or economic problem: empirical case studies on incentives?

Example:

Security Economics in the HTTPS Value Chain, with H. Asghari, M.J.G. van Eeten & N.A.N.M. van Eijk, Workshop on the Economics of Information Security 2013, 3 June 2013

Incentives: Internet markets tend towards 'winner take all'



Certificate Brand Market Shares

One of many examples:

- HTTPS market
- 3 CAs sell 75% certs
- 5 CAs sell 90% certs
- For top 1k, top 100k and top 1m domains

- **Across web, similar market dynamics**

With H. Asghari, M. van Eeten & N. van Eijk (WEIS 2013)
http://ssrn.com/abstract=2277806

ROOT CAUSES OF CYBERCRIME? GAME THEORY: LARGE SCALE VULNS

Where Do All The Attacks Go?

Dinei Florêncio and Cormac Herley
Microsoft Research
One Microsoft Way
Redmond, WA, USA

"Many attacks cannot be made profitable, even when many profitable targets exist."

Political Science Research Q's:

1. Call it 'security'? Or assurance, robustness?
2. Why subjective trumps objective security?
3. Securitization and regulatory capture?
4. Why deterrence opted over actual protection?

Chapter 3 thesis… Input more than welcome!

“We Must Do Something.
This Is Something.
Therefore, We Must Do It”

Re-framing Major Shifts Human Organization as Security Threat

“Transfer of Anxiety”
Bauman (1998)

5M. SECURITY CLEARANCE, 2 STAFF: ~15M OF 136M US WORKFORCE!

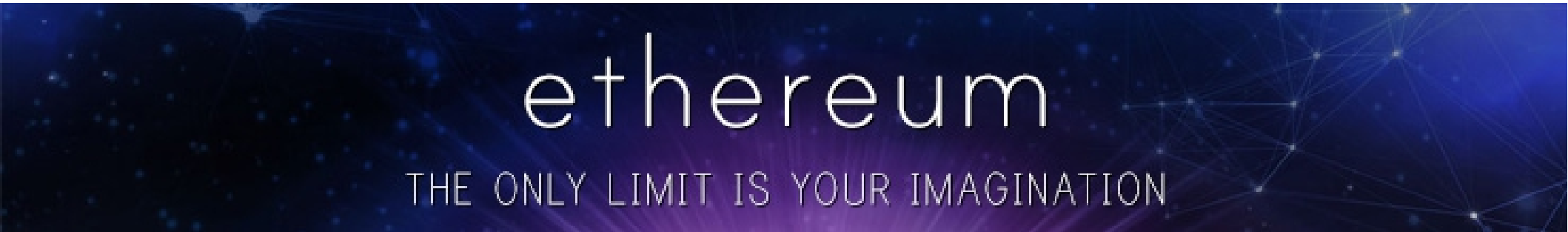
Here's the official Data, but nothing on national security:
http://www.bls.gov/news.release/empsit.t17.htm

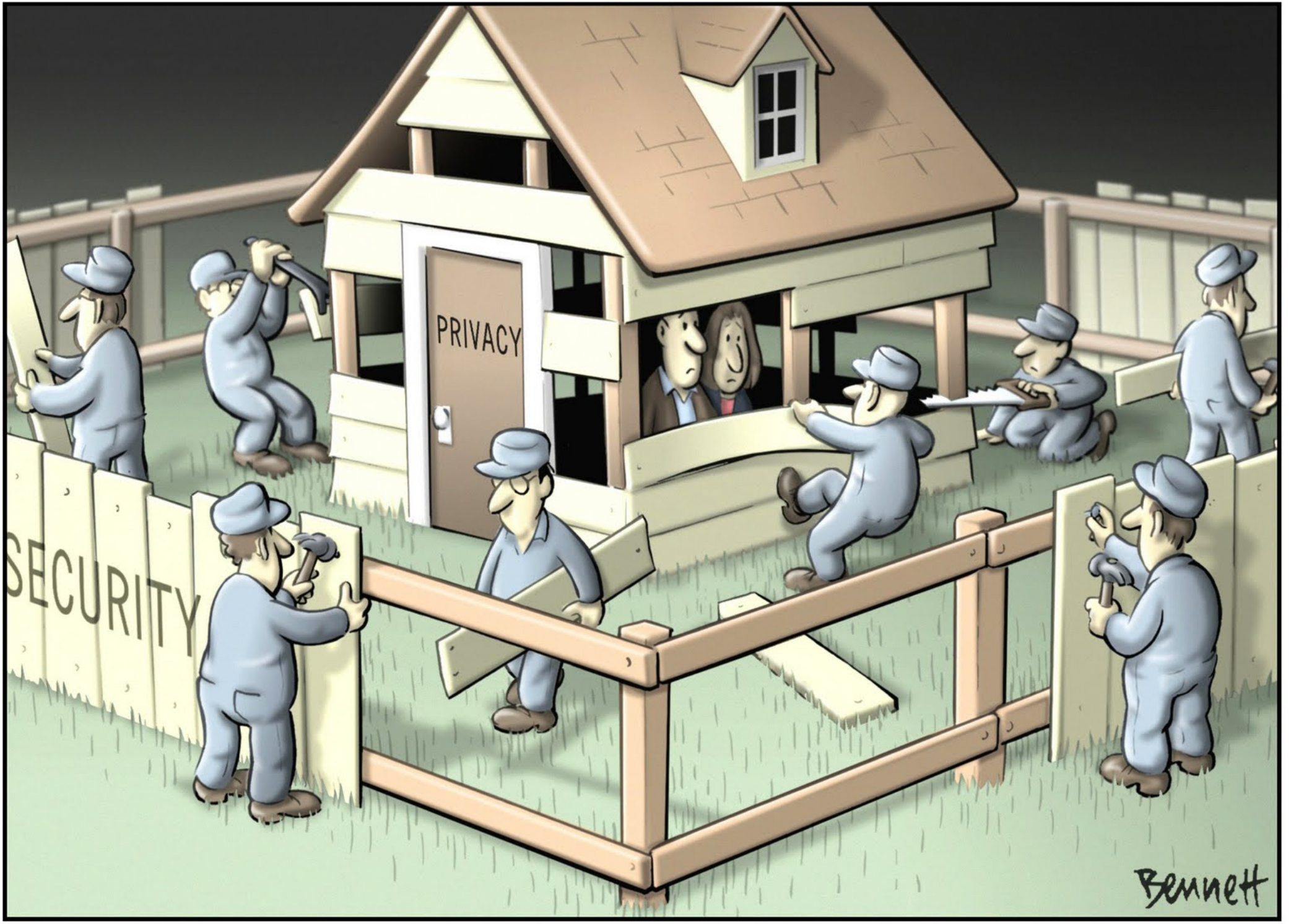
Constitutional, European Law Research Q's:

1. Constitutional elements of confidentiality, integrity and availability?
2. Constitutional Right to IT-Security?
3. Post-Lisbon Treaty, more leverage to secure the internet at the E.U. level?

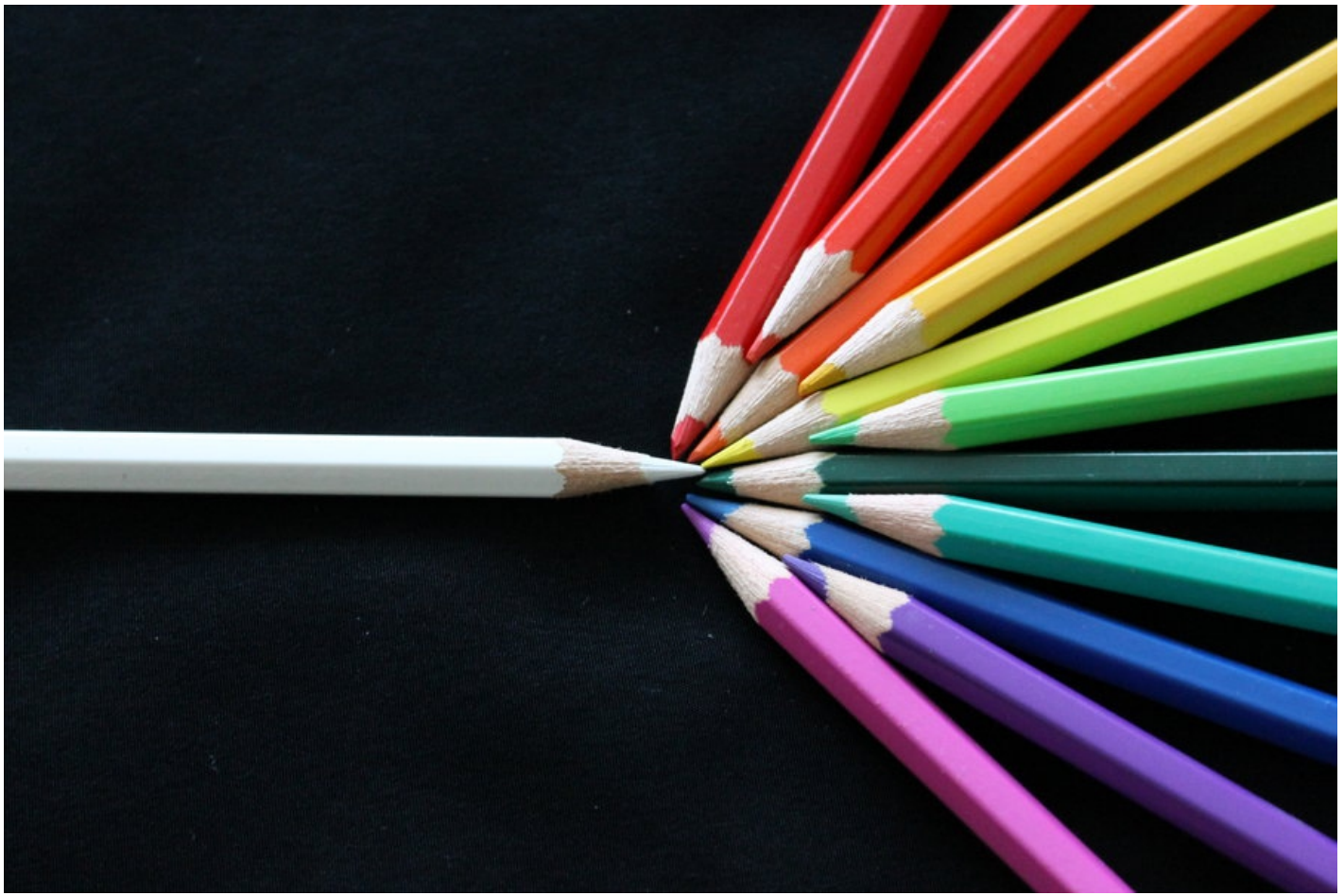
CONSTITUTIONAL COURT
GERMANY

HUMAN RIGHT IT-SECURITY: AGAINST COMPANIES?




PRIVACY
SECURITY
Bennett

Any Colour You Like



The History (and Future?) of Internet Security Policy

Cyberscholars Workshop @ Berkman, Harvard 27.03.14

https://www.axelarnbak.nl
2013/14 Fellow Berkman Center & CITP