



CAN
INTERNET
PROTOCOLS
AFFECT
HUMAN
RIGHTS?

IRTF RG
Human Rights Protocol Considerations
(hrpc)

IETF 98
Tuesday March 28 2017
13:00 - 14:30

Co-Chairs:
Niels ten Oever - Article19
Avri Doria - APC

Administrivia

Mailinglist

- <https://www.ietf.org/mailman/listinfo/hrpc>

Github

- <https://github.com/nllz/IRTF-HRPC>

- Meetecho (remote participation)

<http://www.meetecho.com/ietf98/hrpc/>

- Minutes

<http://etherpad.tools.ietf.org:9000/p/notes-ietf-98-hrpc>

- Intro website

<https://hrpc.io>

Agenda

- Beginning
 - Jabber scribe, note takers
 - Agenda Bashing
 - Notewell
 - Introduction
- Context of research
- Presentation + Q&A - Francesca Musiani on Distributed Architectures and Rights
- Presentation + Q&A - John Havens on:
 - The IEEE Global Initiative for Ethical Considerations in AI & AS
 - P7000 - Model Process for Addressing Ethical Concerns During System Design
- Presentation + Q&A - Giovane Moura on ['No domain left behind: is Let's Encrypt democratizing encryption?'](#)
- Presentation + Q&A - Adamantia Rachovitsa on ['Rethinking Privacy Online & Human Rights'](#)
- Discussion of draft-tenoever-hrhc-anonymity-00
- Discussion of draft-tenoever-hrhc-association-00
- Update of draft-irtf-hrhc-research
- Open discussion other drafts, papers, ideas
- Next steps
- AOB

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Document Review Request

- Document quality relies on reviews, please review documents in your working group and at least one other document from another working group.
- If you'd like documents you care about reviewed, put the effort in to review other documents.

Status of research group

- October, 27, 2014 - Publication of [Proposal for research on human rights protocol consideration](#)
- IETF91 - November, 13, 2014: Presentation during [saag session](#)
- March 9, 2015 - Publication of [Proposal for research on human rights protocol considerations - 01](#)
- January 2015 - Proposed research group in the IRTF
- IETF92 - March 22 to 27, 2015 - Session & Interviews with members from the community
- June 2015 - Interim Meeting
- July 2015 - Publication of [Methodology](#) and [Glossary](#) drafts
- IETF93 - July 2015 - Session
- IETF94 November 2015 - Screening of film Net of Rights, updates of [Glossary](#), [Methodology](#), [Report](#) drafts, [Users draft](#), [paper](#), session
- December 2015 - Research Group chartered
- IETF95 April 2016 - Session, new [Research draft](#), updated [Report](#) and [Censorship](#) draft, & 3 talks
- IETF96 July 2016 - Session, new Research Draft - road tests, reviews, text & 3 talks
- IETF97 November 2016 - Session, new Research Draft - reviews, talk
- February 2017 - Research Group Consensus on draft-irtf-hrpc-research-11
- IETF98 March 2017 - Session, two news drafts, four talks, plenary talk

Context and objective of the RG

- To expose the relation between protocols and human rights, with a focus on the rights to freedom of expression and freedom of assembly.
- To propose guidelines to protect the Internet as a human-rights-enabling environment in future protocol development, in a manner similar to the work done for Privacy Considerations in RFC 6973.
- To increase the awareness in both the human rights community and the technical community on the importance of the technical workings of the Internet and its impact on human rights.

Presentation + Q&A: Francesca Musiani on:
Distributed Architectures and Rights


The background features abstract, overlapping green geometric shapes in various shades, creating a modern and dynamic feel. The shapes are primarily triangles and polygons, some with thin white outlines, set against a white background.

Distributed architectures:

a few research paths
beyond engineering sciences

Francesca Musiani
Associate Research Professor
CNRS, France

- ▶ ADAM project (French National Agency for Research, 2010-2014)
- ▶ Exploring how the choice, by developers and engineers of Internet-based services, to develop distributed architectures instead of more centralized models has implications for the daily use of online services and for the rights of Internet users.

- 
- ▶ Centralization of the Internet and the surveillance excesses it appears to foster...
 - ▶ What is the place for user autonomy and empowerment at a time when infringements upon privacy and pervasive surveillance practices are often embedded in network architectures?
 - ▶ Are distribution and decentralization of network architectures the ways, as Philippe Aigrain (2010) suggested, to “reclaim” Internet services – instruments of ‘technical governance’ able to reconnect with the original organization of cyberspace?

A socio-legal approach to distributed architectures

- ▶ bearers of much more than the piracy vs. sharing opposition
- ▶ interesting “laboratory” where visions and implementations of alternative Internets were taking place – experiments of “governance by architecture” imbued with different, innovative ways of distributing authority, power, value, sense of community

Most recently, distributed architectures...

- ▶ Strictly linked to discussions of surveillance and privacy issues, and frequently associated to discussions about encryption
- ▶ increasingly seen as technologies of empowerment and liberation (WCNs, MESH...)
- ▶ but opposed to narratives of ‘terrorist technologies’
- ▶ What of the blockchain?

Four areas of (cross-cutting) reflection on distributed architectures


- ▶ The importance of being historical ...
- ▶ Heterogeneity of distributed architectures
- ▶ User empowerment(s)
- ▶ Law, responsibility and authority redistributed

(see Musiani & Méadel, 2016)

Recent interdisciplinary efforts

- ▶ P2Pvalue (H2020, CAPS, 2013-2016, <http://www.p2pvalue.eu/>)
- ▶ netCommons (H2020, CAPS, 2016- <http://netcommons.eu/>)
- ▶ NEXTLEAP (H2020, CAPS, 2016- <https://www.nextleap.eu/>)

- ▶ “Distributed Architectures for Decentralised Data Governance” call
<http://ec.europa.eu/programmes/horizon2020/en/news/eu-call-proposals-developing-blockchains-and-decentralised-data-architectures>

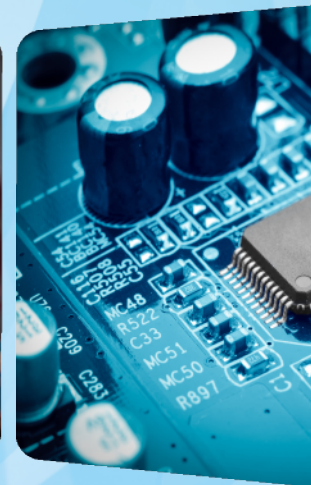
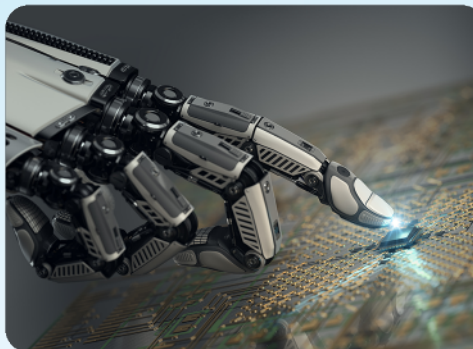
- 
- ▶ Architecture is politics, but it is not a substitute for politics (Agre, 2003)
 - ▶ Issues of intermediation and dis-intermediation, distribution of power, privatization of governance, privacy by design and by architecture, have hardly been more important in recent history than they are in our post-Snowden era
 - ▶ and reach out to the very ways in which Internet governance unfolds in our present times.

Thank you!

- ▶ Francesca.musiani@cnrs.fr
- ▶ @franmusiani
- ▶ <http://www.iscc.cnrs.fr/spip.php?article1960>

Presentation + Q&A: John Havens on:

- The IEEE Global Initiative for Ethical Considerations in AI & AS
- P7000 - Model Process for Addressing Ethical Concerns During System Design



The IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems

An introduction to *Ethically Aligned Design* and the Standards Working Groups inspired by our work

John C. Havens – Executive Director, The IEEE Global AI Ethics Initiative


The IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems


An incubation space for new standards and solutions, certifications and codes of conduct, and consensus building for ethical implementation of intelligent technologies




INDUSTRY CONNECTIONS

The IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems

ICAID 

Download the IEEE Global Initiative *Ethically Aligned Design* document 

Download the IEEE Global Initiative brochure 

NEWS AND EVENTS

ABOUT

The purpose of this Initiative is to ensure every technologist is educated, trained, and empowered to prioritize ethical considerations in the design and development of autonomous and intelligent systems.

- [View specifics regarding the Mission and deliverables for the Initiative.](#)
- [See a list of The Initiative's Executive and other Committees.](#)
- [Learn more from Frequently Asked Questions.](#)

Ethically Aligned Design, Version 1 - Request For Input

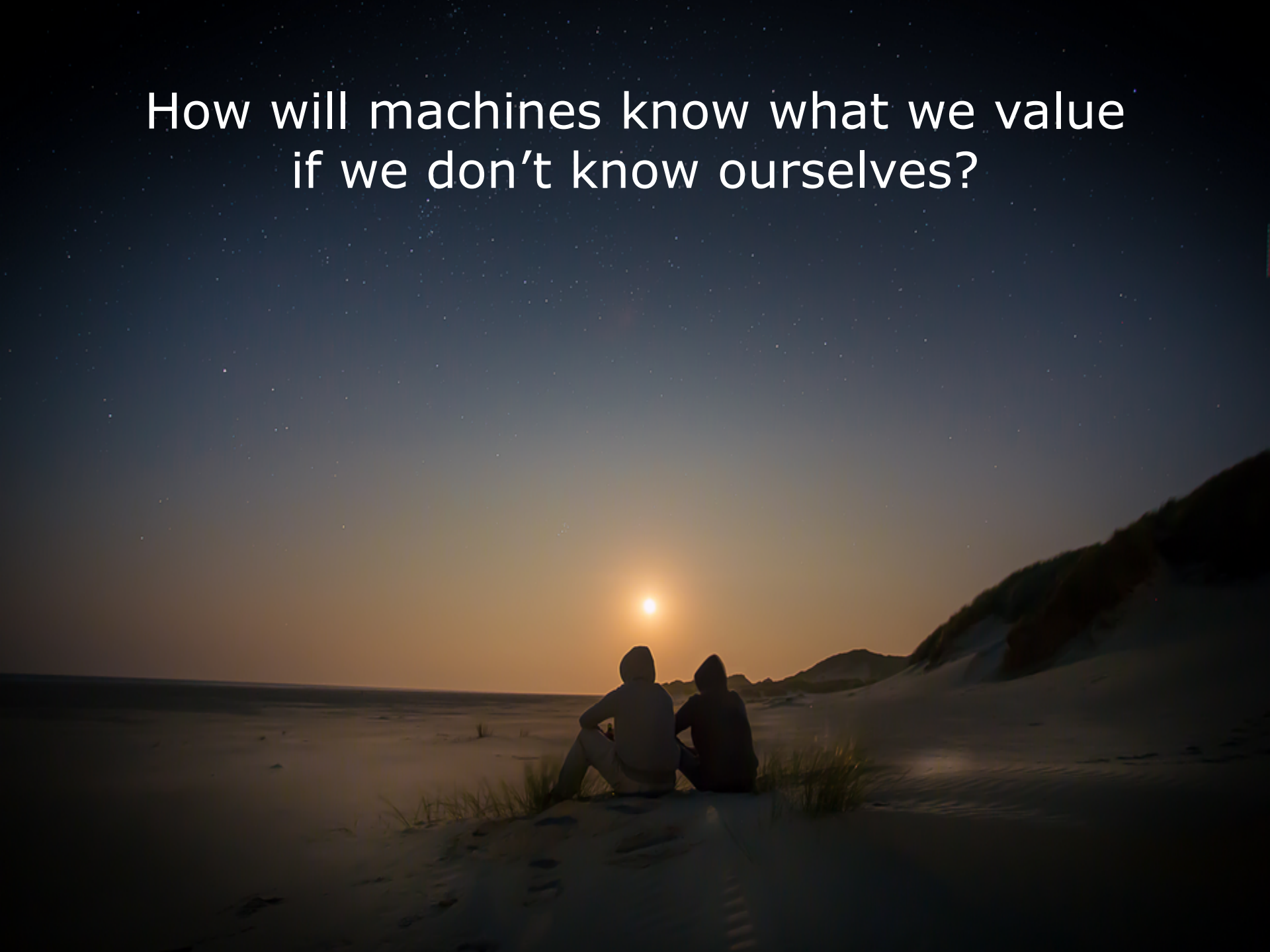
Ethically Aligned Design: A Vision for Prioritizing Human Wellbeing with Artificial Intelligence and Autonomous Systems represents the collective input of over one hundred global thought leaders from academia, science, government and corporate sectors in the fields of Artificial Intelligence, ethics, philosophy, and policy.



Ethics is the New Green



How will machines know what we value
if we don't know ourselves?

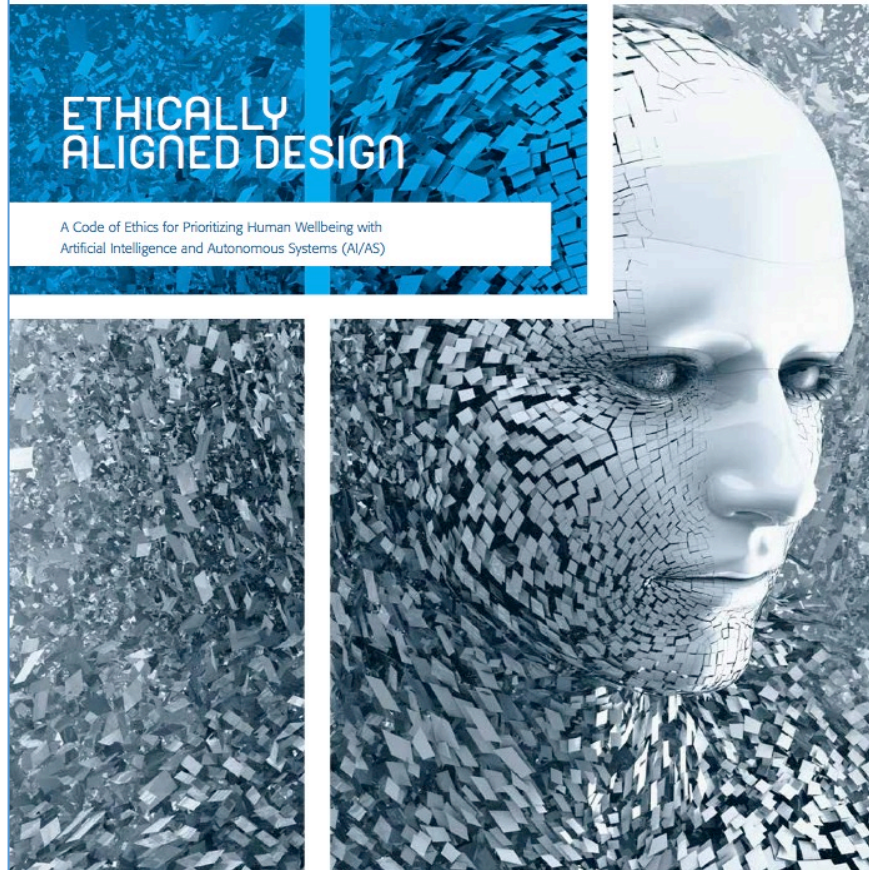


Version 1 - For Public Discussion



ETHICALLY ALIGNED DESIGN

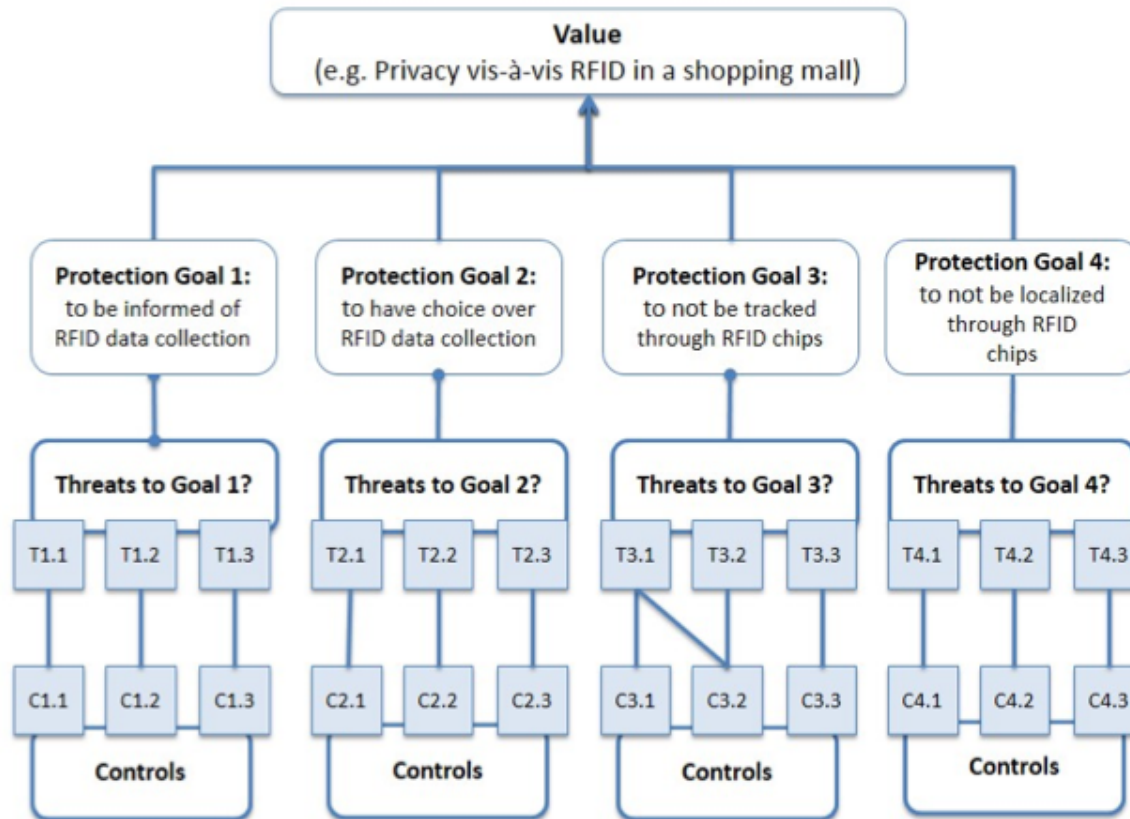
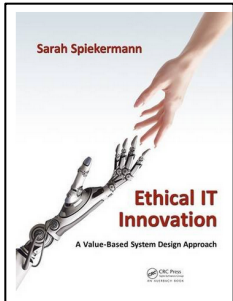
A Code of Ethics for Prioritizing Human Wellbeing with
Artificial Intelligence and Autonomous Systems (AI/AS)



IEEE-SA Standards Projects

- **IEEE P7000:** [Model Process for Addressing Ethical Concerns During System Design](#)
- **IEEE P7001:** [Transparency of Autonomous Systems](#)
- **IEEE P7002:** [Data Privacy Process](#)
- **IEEE P7003:** [Algorithmic Bias Considerations](#)
- **IEEE P7004:** Standard on Child and Student Data Governance
- **IEEE P7005:** Standard on Employer Data Governance
- **IEEE P7006:** Standard on Personal Data AI Agent Working Group

Values-Based Design





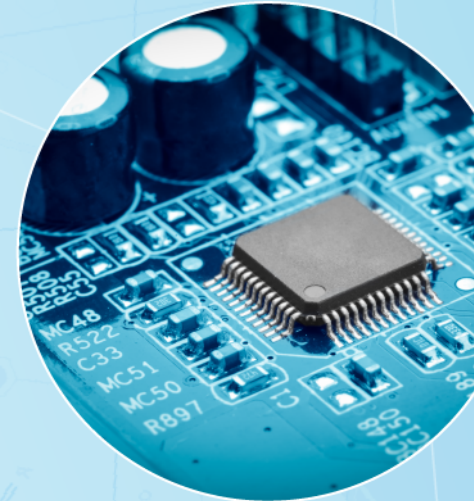
Thank you!



***The Global Initiative for Ethical Considerations
in Artificial Intelligence and Autonomous Systems***

Contact: John C. Havens, Executive Director

john.havens.us@ieee.org / 917-597-3323



Presentation + Q&A - Giovane Moura on:

'No domain left behind: is Let's Encrypt democratizing encryption?'

<https://arxiv.org/abs/1612.03005>

No domain left behind:
is Let's Encrypt democratizing encryption?

Maarten Aertsen¹, Maciej Korczyński², **Giovane C. M. Moura**³, Samaneh Tajalizadehkhoob², Jan van den Berg²

¹National Cyber Security Centre
The Netherlands

²Delft University of Technology
The Netherlands

³SIDN Labs
The Netherlands

IETF98 - IRTF - HRPC
Chicago, IL, April 28th, 2017

Disclaimer

- ▶ None of the authors is in any way affiliated with *Let's Encrypt*
- ▶ In other words: we do not speak for them
- ▶ But if you like their work, you may consider supporting them

The Encryption Rush

Ed Snowden NSA's revelations



- ▶ Massive, widespread surveillance
- ▶ Worst nightmares came true

The Encryption Rush

Ed Snowden NSA's revelations



- ▶ Massive, widespread surveillance
- ▶ Worst nightmares came true

Consequences:

- ▶ For many, it was a wake-up call (and panic)
- ▶ Market distrust in vendors
- ▶ Provided a great momentum for better security

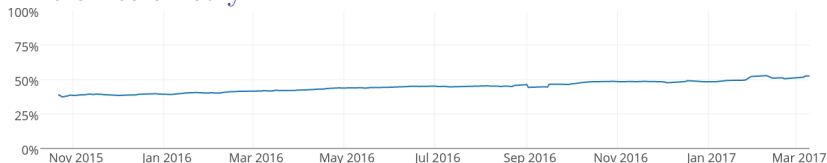
Reactions:

- ▶ IETF: RFC 7258, RFC 7624
- ▶ iOS/Android: mobile phone encryption by default
- ▶ Cloud providers enabling encryption everywhere
- ▶ ...

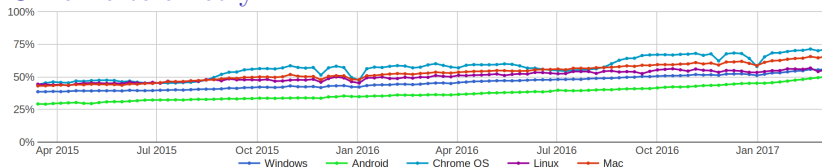
More than half of web traffic is encrypted nowadays

Yet that leaves out a lot of people without HTTPS

Firefox telemetry¹



Chrome telemetry²



¹ <https://telemetry.mozilla.org/>, based on *Let's Encrypt* stats page

² <https://www.google.com/transparencyreport/https/metrics/>

Certificates are required for encryption on the web

Barriers to ubiquitous web encryption (X.509 cert):

- ▶ **Cost:** purchase, deployment and renewal
- ▶ **Complexity:** request, deployment (at scale)

*Let's Encrypt*³ aims to make encrypted traffic ubiquitous

- ▶ Issue and re-issue costs: **\$0.00**
- ▶ Complexity mitigated by **automation**
 1. ACME protocol⁴
 2. and clients, e.g. Certbot⁵

³<https://letsencrypt.org>

⁴draft-ietf-acme-acme-latest → <https://ietf-wg-acme.github.io/acme/>

⁵<https://certbot.eff.org/>

No domain left behind

Is *Let's Encrypt* democratizing encryption?

Research question

“In its first year of certificate issuance, has Let's Encrypt been successful in democratizing encryption?”

Approach: measurements

- ▶ Analyze issuance in the first year of *Let's Encrypt*
- ▶ Show adoption trend from various perspectives
- ▶ Analyze coverage for the lower-cost end of the market

Methodology

- ▶ Period covered: Sept. 2015-2016 (1st year)
- ▶ Results based on FQDNs reduced to 2LD/3LD form
 - ▶ a.b.c.d.com → d.com

Datasets

Certificates →	Certificate transparency ⁶
Domain to IP mapping →	Farsight DNSDB ⁷
Organization mapping →	Methodology from previous work ⁸ , using <code>whois</code> data & Maxmind GEOIP2
Registration info →	.nl registry (SIDN)

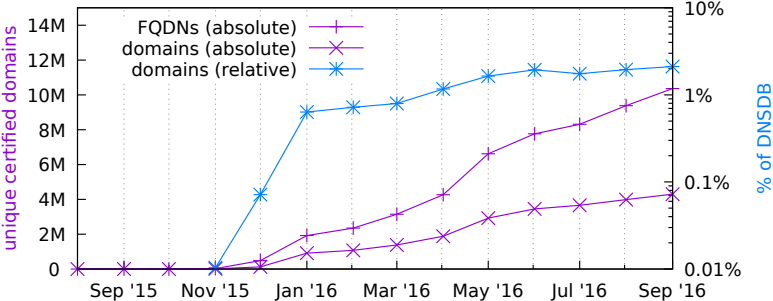
⁶ <https://www.certificate-transparency.org/known-logs>

⁷ <https://www.dnsdb.info/>

⁸ S. Tajalizadehkhoob et al., “Apples, oranges and hosting providers: heterogeneity and security in the hosting market,” IEEE NOMS 2016

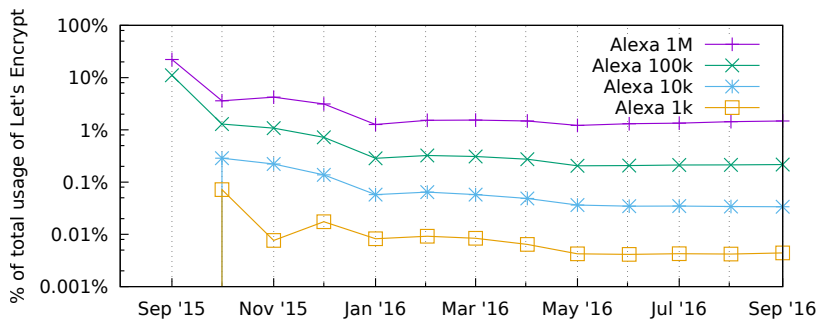
Let's Encrypt Adoption Rate

► Steady growth



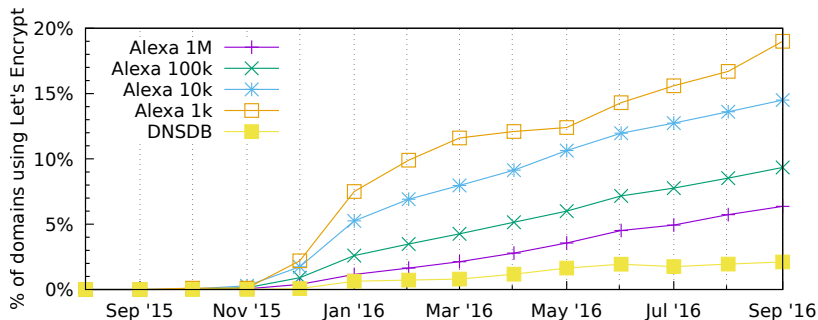
Who's using *Let's Encrypt* ?

- ▶ 98% of certificates are issued outside Alexa 1M ...



Who's using *Let's Encrypt* ?

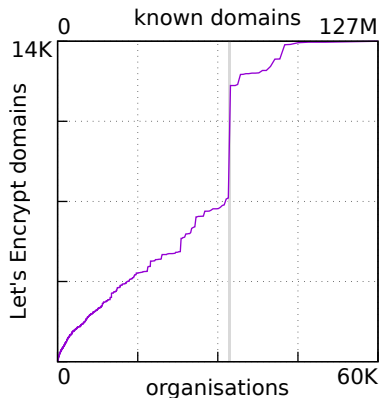
- ▶ ...yet issuance is not restricted to lower end of the market
 - ▶ meaning: big players also use in their subdomains



Growth is attributed to adoption by major players

3 hosting providers are responsible for 47% of the *Let's Encrypt* certified domains

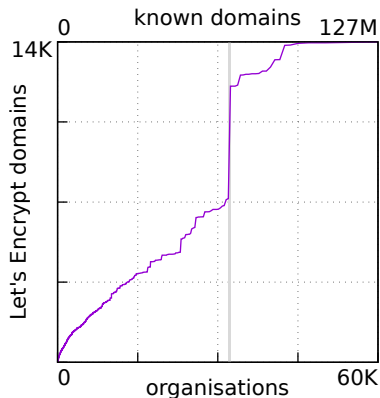
November 2015



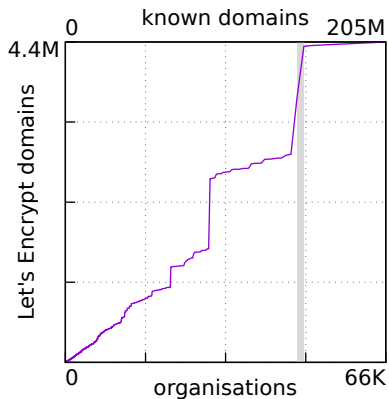
Growth is attributed to adoption by major players

3 hosting providers are responsible for 47% of the *Let's Encrypt* certified domains

November 2015



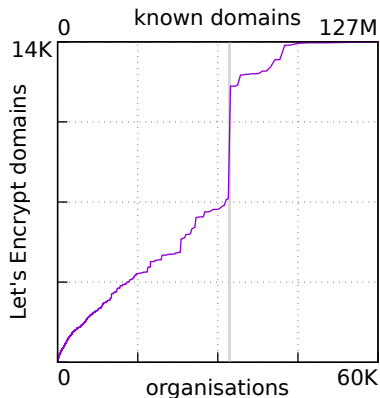
September 2016



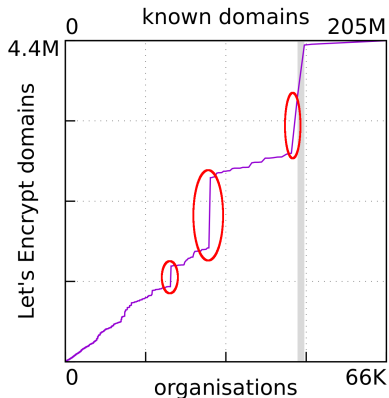
Growth is attributed to adoption by major players

3 hosting providers are responsible for 47% of the *Let's Encrypt* certified domains

November 2015



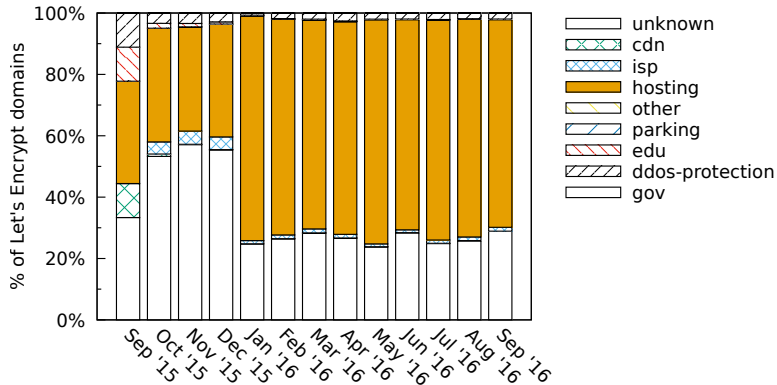
September 2016



Automation works!!

Issuance is dominantly for web hosting

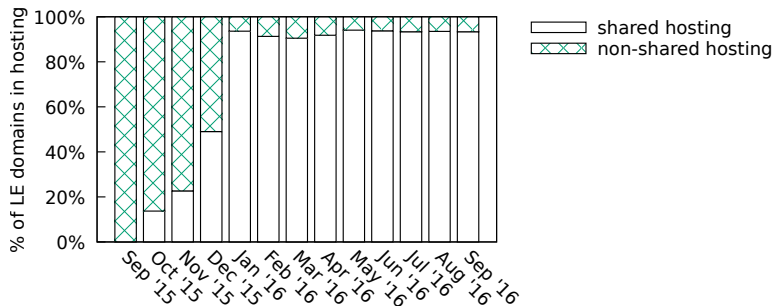
So far, no surprises



Over 90% of domains in hosting are on shared hosting

Issuance is dominantly for the lower-cost end of the market

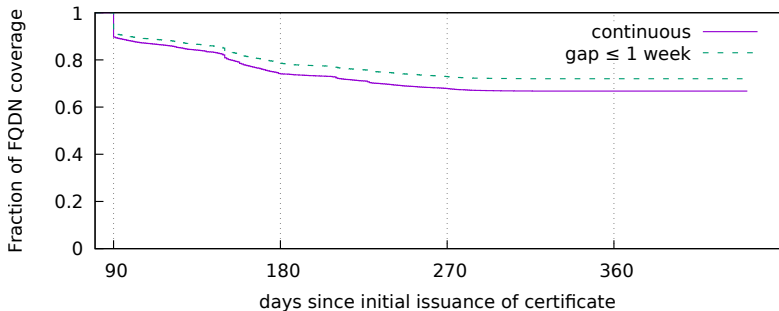
- ▶ Shared hosting = 10 domains/IP⁹
- ▶ *Let's Encrypt* reaches those with less incentive to encrypt



⁹S. Tajalizadehkhoob et al., "Apples, oranges and hosting providers: heterogeneity and security in the hosting market," IEEE NOMS 2016

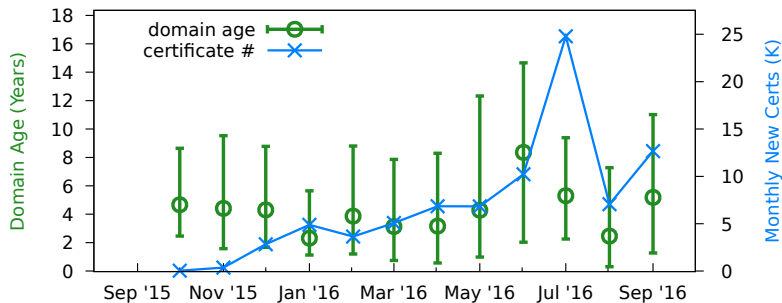
Let's Encrypt certificates are valid for 90 days

The majority of certificates are correctly renewed after their first expiration



Let's Encrypt : domain age use

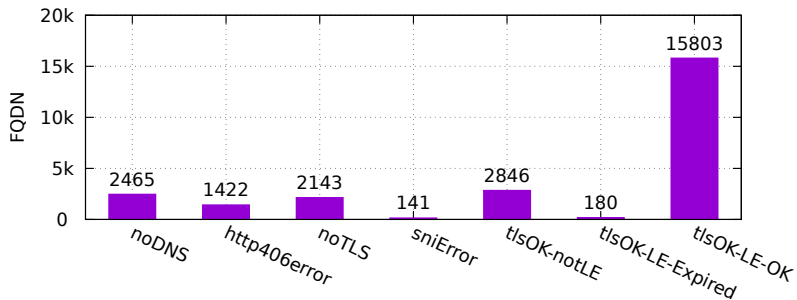
- ▶ Case study: .nl
- ▶ Determine the age of the domain when the cert was issued



Median, Q25, Q75 and number of monthly new certificates for .nl domains

Let's Encrypt : deployment

- ▶ https scans + cert processing (lower bound)
- ▶ 25K randomly chosen *Let's Encrypt* FQDN



Conclusions

We show that

- ▶ *Let's Encrypt* has been a success
 - ▶ Reduces costs & complexity
- ▶ Democratize encryption by covering low cost end of the market (shared hosting)
 - ▶ but big players also use it
- ▶ Automation works: *Let's Encrypt's* allows for bulk issuing
 - ▶ 3 hosting providers are responsible for 47% of the *Let's Encrypt* certified domains
- ▶ The majority of certificates are correctly renewed after their first expiration (90 days)

And find that

Let's Encrypt has indeed started to democratize encryption.

Future work

Future work

- ▶ extend measurement period
- ▶ issued versus deployed
 - ▶ active scans on shared hosting require prior knowledge of domains served (SNI)
- ▶ use by malicious actors

Contact details

Giovane C. M. Moura
`giovane.moura@sidn.nl`

Download our paper at:
<https://arxiv.org/abs/1612.03005>

Presentation + Q&A - Adamantia Rachovitsa on

'Rethinking Privacy Online and Human Rights: The Internet's Standardisation Bodies as the Guardians of Privacy Online in the Face of Mass Surveillance'

https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=2911978

Rethinking Privacy Online & Human Rights: The IETF as the Guardian of Privacy Online in the Face of Mass Surveillance

Dr. Mando Rachovitsa

Department of International Law, University of Groningen, NL

Main points

1. Internet standard-setting is informal law-making.
2. Informal international law-making (Internet standards) may not be legally binding but it can be legally & technically relevant.
3. Technically relevant: The IETF & human rights as technical issues
4. Legally relevant: What international human rights law can learn from the IETF.

Internet standards and international law/human rights interrelate in a dynamic way & may actively inform one another.

Internet standard-setting = informal law-making

(International) Law:

- ✓ produced by a specific actor
- ✓ following a specific process
- ✓ a specific final outcome

Informal law:

anything that de facto regulates and is being followed by actors, incl. States, individuals, industry etc.

Internet standards and protocols

- define how the Internet functions
- are a strong regulatory force complementing the law, market & social norms
- impose constraints to & shape the choices of the end-user
- are voluntarily implemented by all stakeholders

Therefore, Internet standard-setting constitutes international informal law-making.

The IETF & Human Rights



Let's keep calm and carry on...

The IETF & Human Rights

1. Is the IETF bound by human rights?

No, human rights concern only the relationship State-individual.

2. Does the IETF get involved with human rights?

Yes and No.

No, because it does not have the mandate to make standards *for* or *against* human rights.

Yes, because Internet standards define to a great extent the level of protection accorded to human rights.

3. Does it fall within the IETF's mandate to address and assess the impact of Internet standards to the human rights of the users?

[triggering the IETF's mandate]

Yes, if the impact on (human rights of the) users is such that it is related to

- retaining the trust of the users to the network; and
- making the Internet function better

e.g. mass surveillance & serious threats to the users' privacy are an attack to the network and the IETF thinks that it needs to defend the network against this attack.

Human Rights as Technical Issues

4. How will/should the IETF assess the impact of Internet standards on human rights of the users?

✓ Is the Internet-standard setting process receptive to non-technical considerations?

Yes. ➤ **assess the contribution of the standard to all affected parties and to the Internet** (one of the criteria for adopting an Internet standard)

✓ **Does this mean that the IETF will address and assess privacy or freedom of expression of user A in country X?**

No. It will assess through the (possible) impact of Internet standards to human rights.

This way **human rights** can be addressed in the IETF's work and process **as technical issues** - "translated" into the mentality and value-system of the IETF in order to be taken as a consideration when creating/updating standards.

Thinking Outside the IHRL Box

(or what international lawyers can learn from IETF's technical perspective)

Inside the IHRL box:

- ✓ Human rights are applicable online (e.g. freedom of speech, privacy)
- ✓ Existing human rights obligations need to be respected by States
- ✓ Mass/indiscriminate surveillance *may* be an arbitrary or disproportionate interference with the right to privacy
- ✓ We are not quite sure whether existing framework suffices or whether we need a new treaty or an OP or a new General Comment.

Outside the box:

How can the IETF's perception of privacy as a technical issue can inform an international lawyer's mindset as well as legal reasoning?

- How does the legal advisor argue for privacy?
- How the legislator articulates the interests at stake?
- How the academic and practitioner envisage privacy online?
- How national & international courts decide cases?

Thinking Outside the IHRL Box (cont)

Example 1

A rigorous understanding of the technical value of privacy online should update our perception of the complex relationship of
freedom of expression | privacy | national-network-individual security

In human rights law “offline” we are trained to think in terms of
conflict | tension | competing interests

e.g. **Freedom of expression vs. privacy** or **Privacy vs. security**

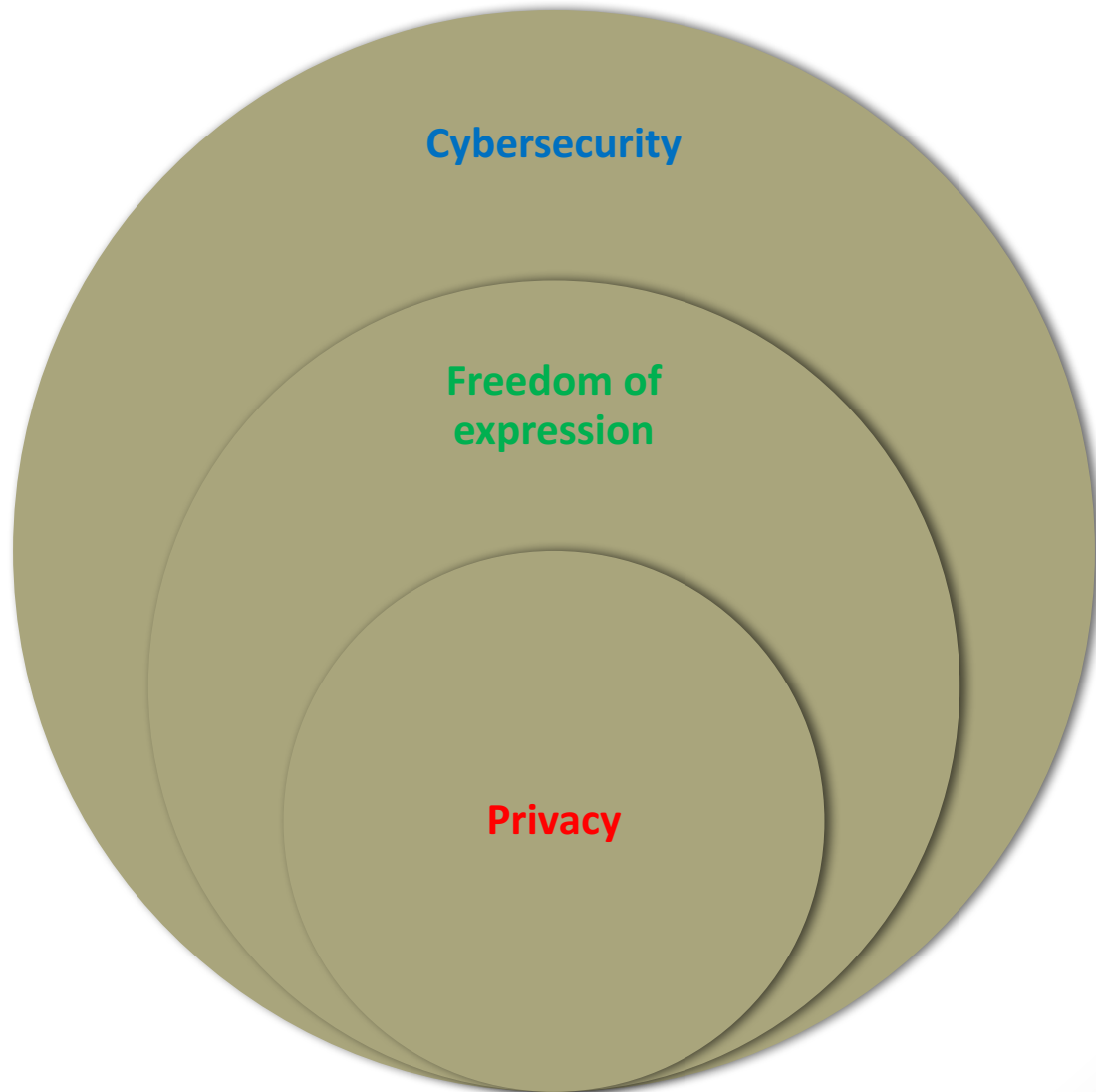
Instead we should learn to conceptualise and frame these relationships as
Symbiotic | Interdependent relationship | mutually supportive

Cybersecurity AND privacy

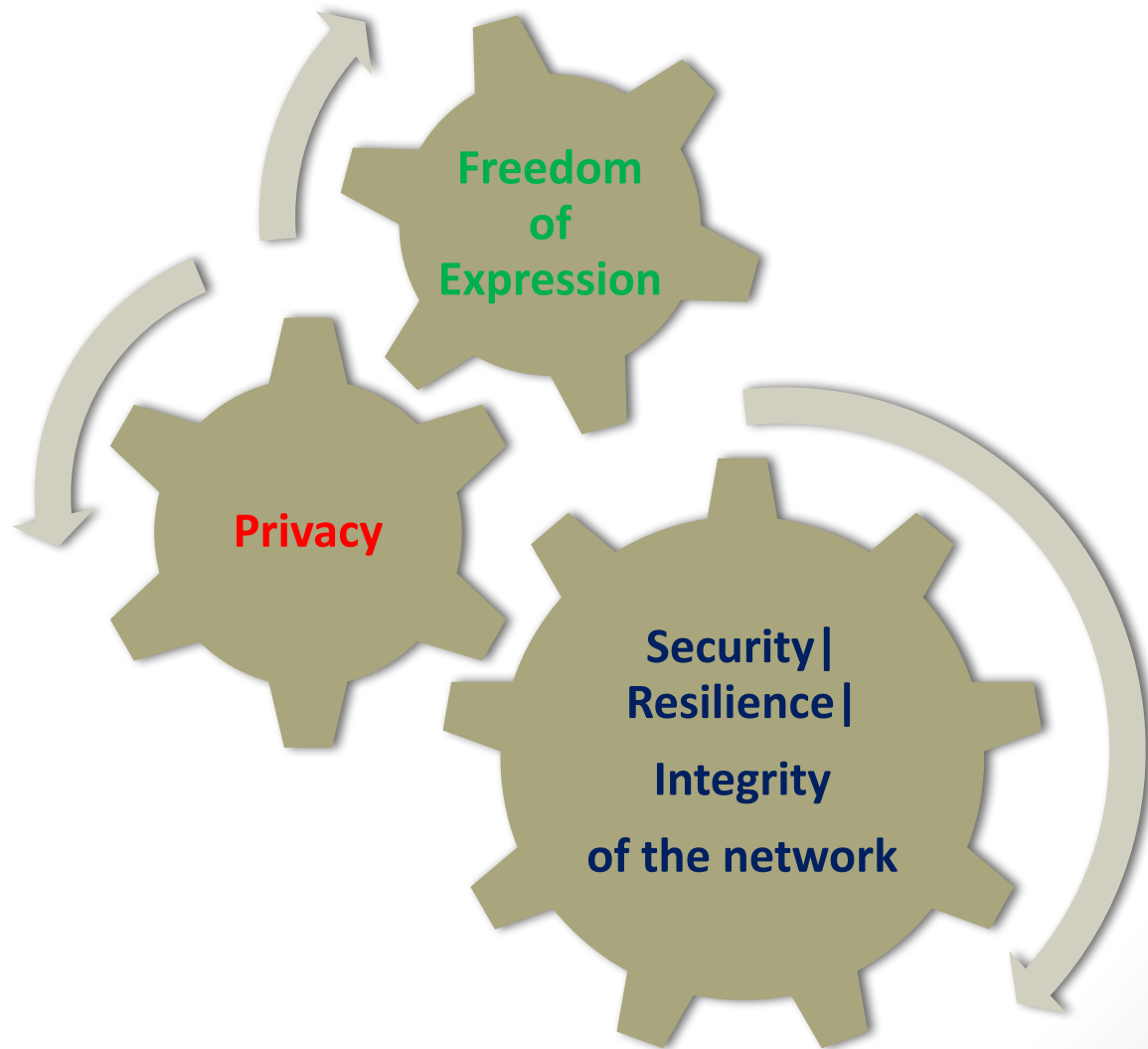
or privacy as a precondition to cybersecurity

e.g. weakening encryption leads to compromising human rights AND
weakening security.

Symbiotic | Mutually Supportive



Interdependent relationship (even in cases of tension)



Thinking Outside the IHRL Box (cont)

Example 2

Arguing for privacy as a technical issue – trust – digital economy can be more effective and persuasive to arguing for privacy as a human rights issue. This frame does not bring into surface cultural or values debates.

Example 3

From a technical point of view the nationality & location of individuals is irrelevant.

Human rights advocacy organisations are arguing before the UN Human Rights Council and US courts about:

“structural attacks to the network regardless of nationality or location”

“unintended detriment to the users, public trust to technology & digital security **around the globe**”

Thanks! Questions?



Discussion of draft-tenoever-hrpc-anonymity-00

This document aims to break down the different meanings and implications of anonymity on a mediated computer network

Research Questions

1. How anonymous is the end user to:

- local network operator
- other networks you connect to
- your communications peer on the other end of the pipe

2. How well can they distinguish my identity from somebody else (with a similar communication) (ie linkability)

3. How does the protocol impact pseudonymity?

- in case of long term pseudonymity
- in case of short term pseudonymity

4. How does the protocol, in conjunction with other protocols, impact pseudonymity?

5. Could there be advice for protocol developers and implementers to improve anonymity and pseudonymity?

Way forward for draft-tenoever-hrpc-anonymity-00

- Is thing interesting and/or relevant?
- Are these the rights questions?
- Co-authors?
- Pull requests?

Freedom of Association and Internet Infrastructure

draft-tenoever-hrpc-association-00

Gisela Pérez de Acha – Derechos Digitales

Niels ten Oever – Article 19

How it came up: If DDoS is not a legitimate form of protest using the Internet infrastructure (BCP72, draft-irtf-hrpc-research-11), then what is?

Objective: to document forms of protest, association and assembly that do not have a negative impact on the Internet infrastructure.

Central question:

How does the Internet architecture enable and/or inhibit freedom of association and assembly?

Assembly & Association

1. Assembly: an intentional and temporary gathering of a collective in a private or public space for a specific purpose.
2. Association: a group of individuals or entities formally brought together to collectively act, express, promote, pursue or defend a field of common interest.

Both rights protect the possibility to join or leave a group of choice.

Can the Internet be considered as an assembly itself?

Or even an association?

Cases and examples

A. Communicating

- Mailing lists
- Multi party video conferencing and risks
- Reaching out
- Working together (peer production)
- Version control

B. Grouping together (identities)

- DNS
- ISPs

What are we missing?

Update on the status of draft-irtf-hrpc-research

- Document authors: N. ten Oever & C. Cath
- Document shepherd: A. Doria
- Last call held on Rev 7
 - Extended length of call- 4 Dec 2016 – 9 Jan 2017, one review as late as 4 Feb
 - Extended call beyond the research group including academic & advocacy experts
 - Limited response from not RG, but some
 - Multiple Substantive Comments
- Draft was updated and discussed; substantive changes were made
- A second Last Call was held on Rev 10
 - Length of call: 2 weeks - 8 Feb – 24 Feb
 - Several issues discussed during the last call and a clean draft addressing those comments was put out.
 - Believe there is RG rough consensus on sending the draft to IRSG with request for publication as Informational
- After current submission moratorium for change of IRTF chair, request will be made for IRSG review and approval on Rev 11

- Open discussion other drafts, papers, ideas
- Next steps
- AOB

```
if write code(protocols):
    consider human rights implications
elif run internet infrastructure:
    respect human rights
elif engage in internet governance:
    build in human rights protections
else
    carry on and use FLOSS
```