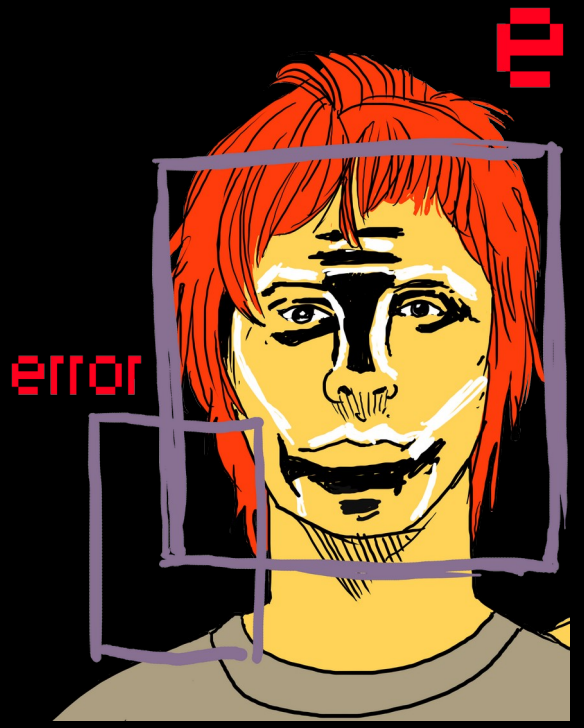
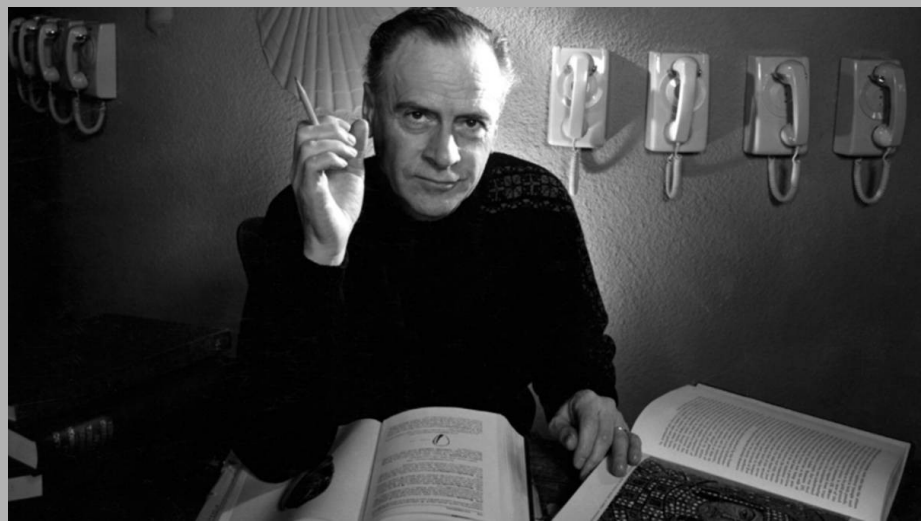
Niels ten Oever
PhD candidate
DATACTIVE Research Group
University of Amsterdam

E: mail@nielstenoever.net
T: @nielstenoever
PGP : 8D9F C567 BEE4 A431 56C4 678B 08B5 A0F2 636D 68E9



The medium is the message

– Marshall McLuhan



We shape our tools
and thereafter they shape us.

–John Culkin

the uses made of technology are largely determined by the structure of the technology itself

– Neil Postman

Technology is neither good nor bad;
nor is it neutral.

– Melvin Kranzberg

Technology is a very human activity
– and so is the history of
technology.

– Melvin Kranzberg

Infrastructure sets the invisible rules that govern the spaces of our everyday lives

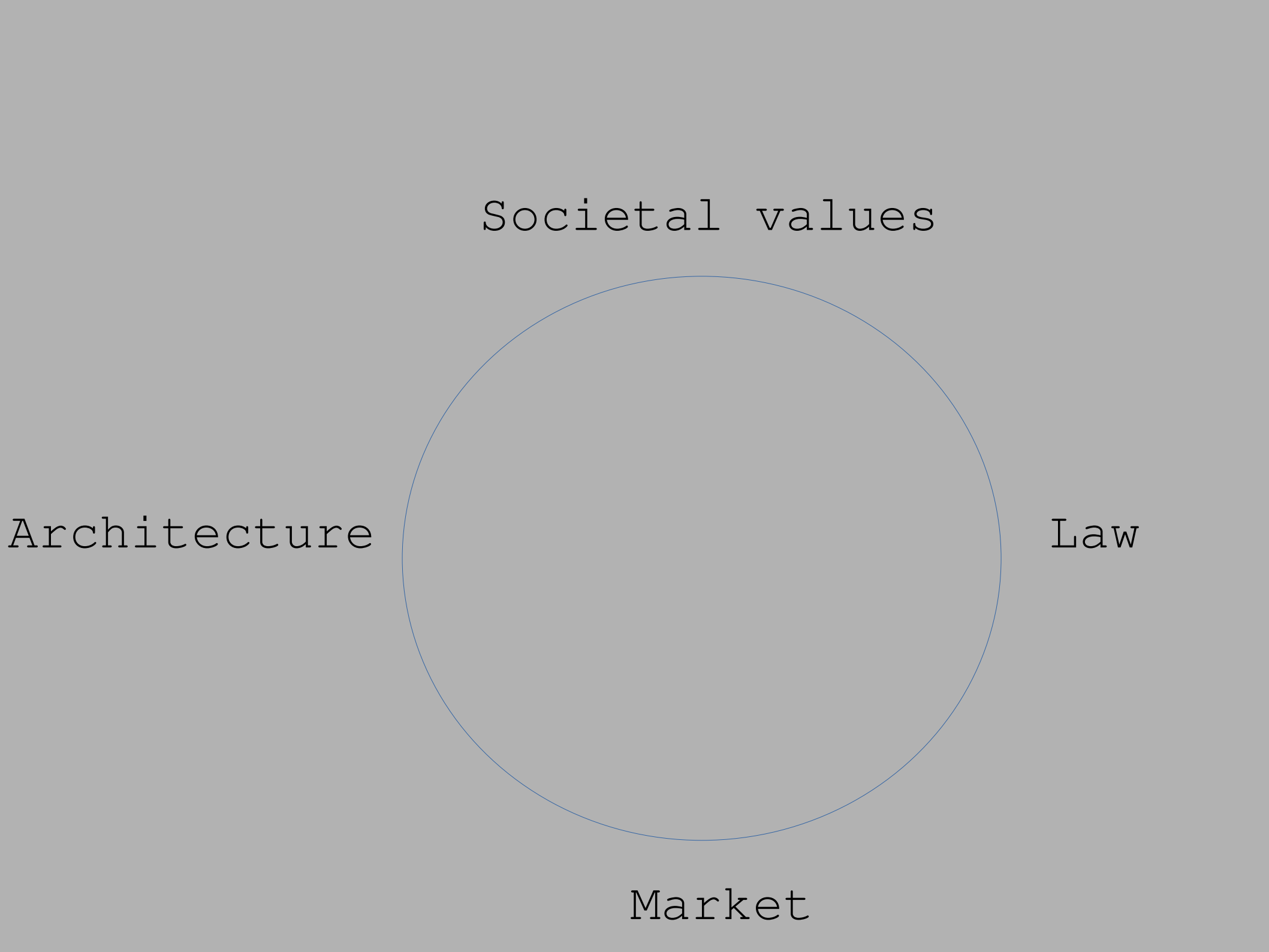
– Keller Easterling

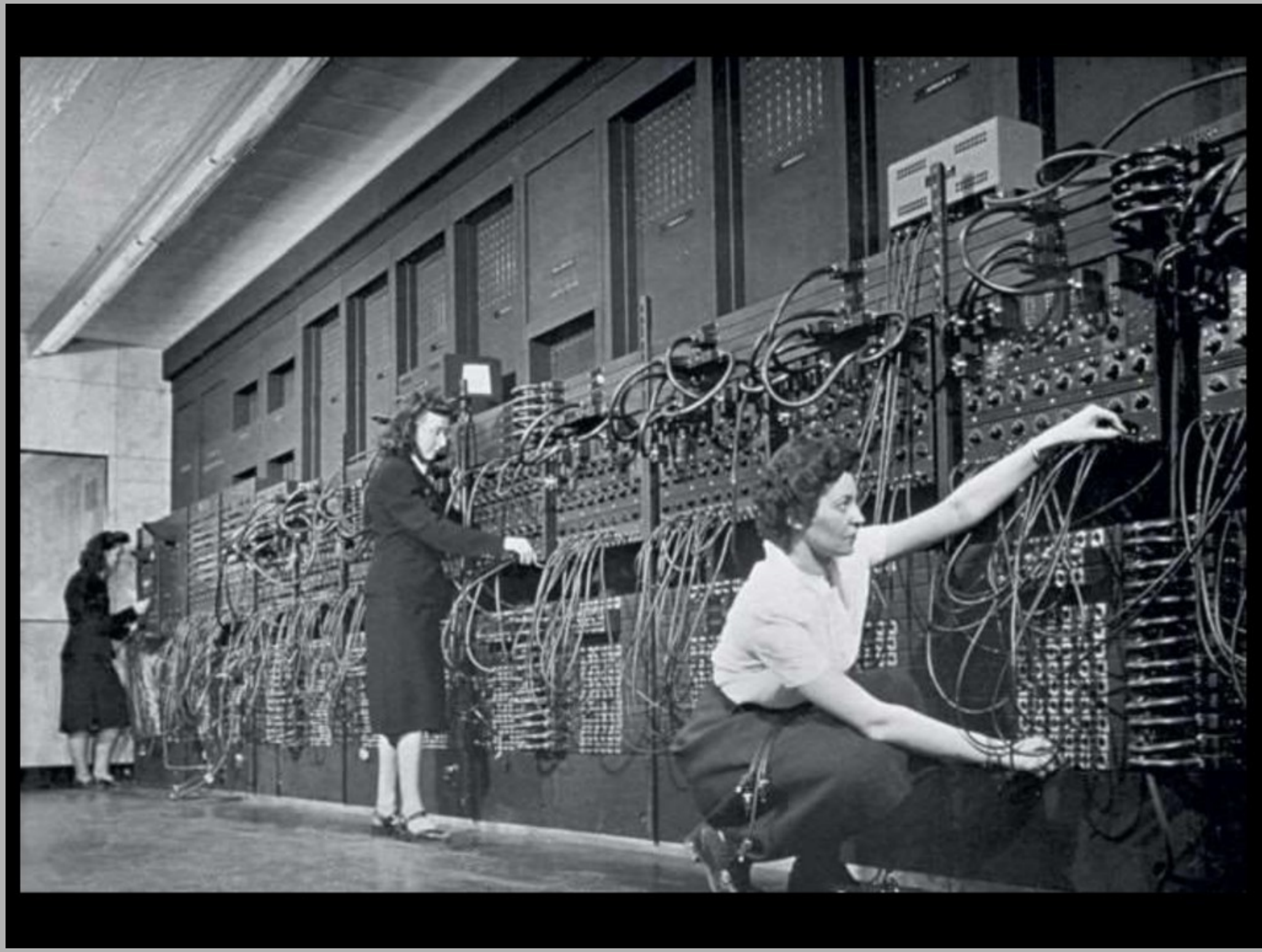
Infrastructure is both relational and ecological

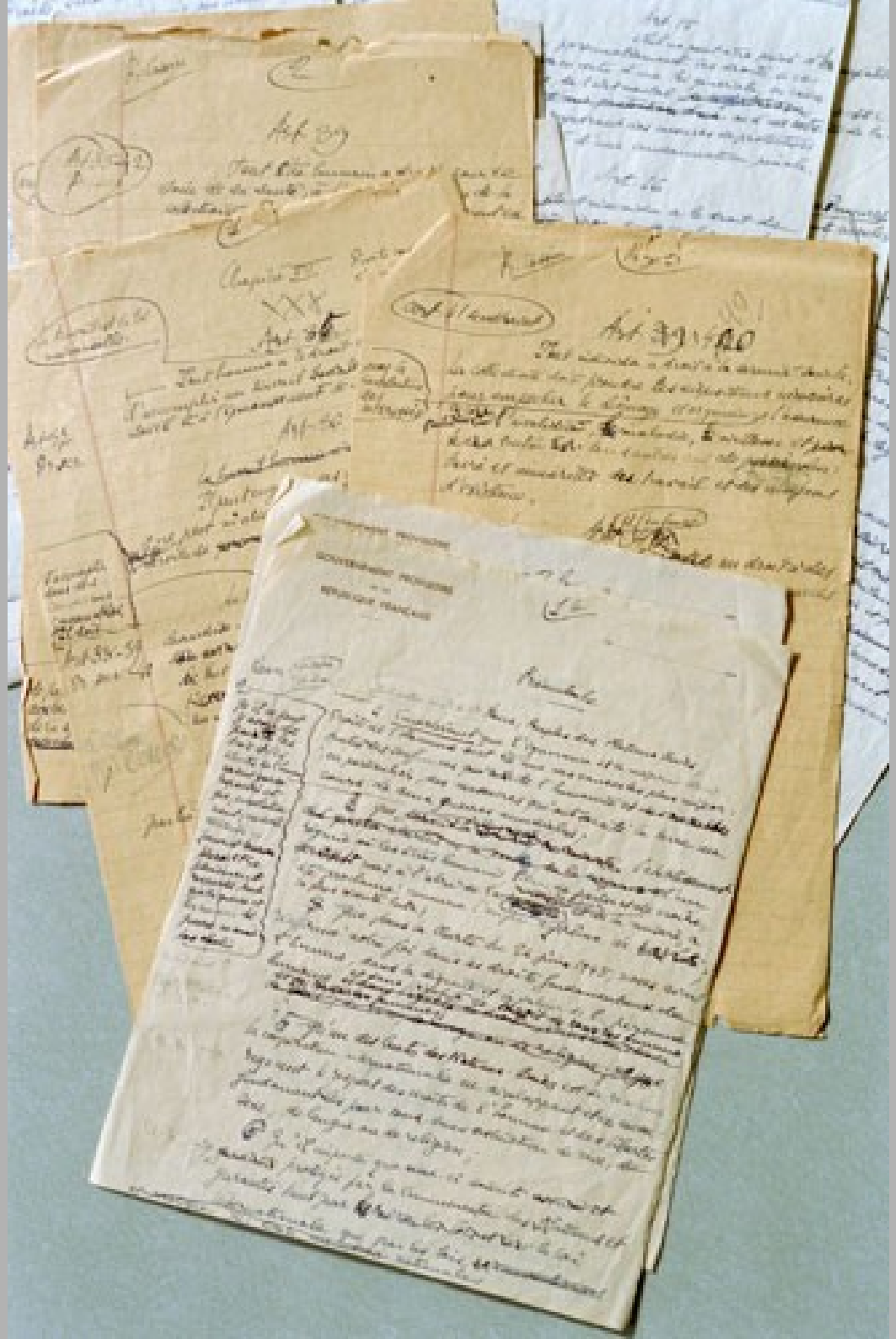
– Susan Leigh Star

Standard setting is a wild mix of politics and economics

– Shapiro and Varian


Societal values
Architecture
Law
Market






UNITED NATIONS


Universal Declaration of Human Rights
International Covenant on Civil and Political Rights (ICCPR) 1966
International Covenant on Economic, Social and Cultural Rights (ICESCR) 1966
International Convention on the Elimination of All Forms of Racial Discrimination (ICERD) 1965
Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) 1979
Convention on the Rights of Persons with Disabilities (CRPD) 2006

UNITED NATIONS GUIDING PRINCIPLES ON BUSINESS & HUMAN RIGHTS

THREE PILLARS of the UN GUIDING PRINCIPLES

HUMAN RIGHTS

PROTECT

STATE

duty to
protect

RESPECT

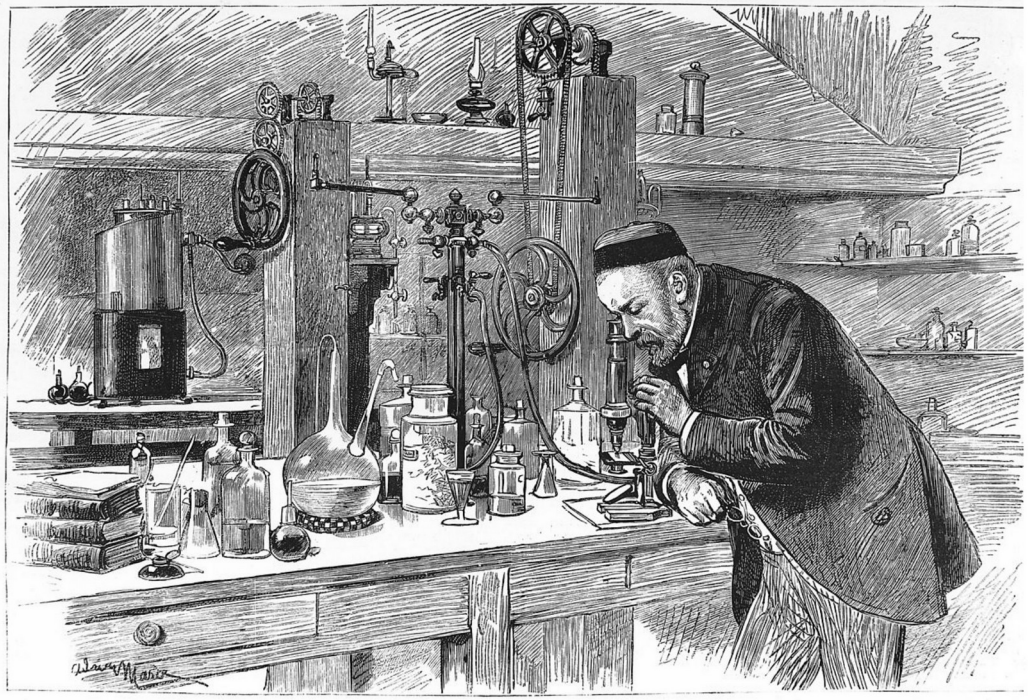
CORPORATE

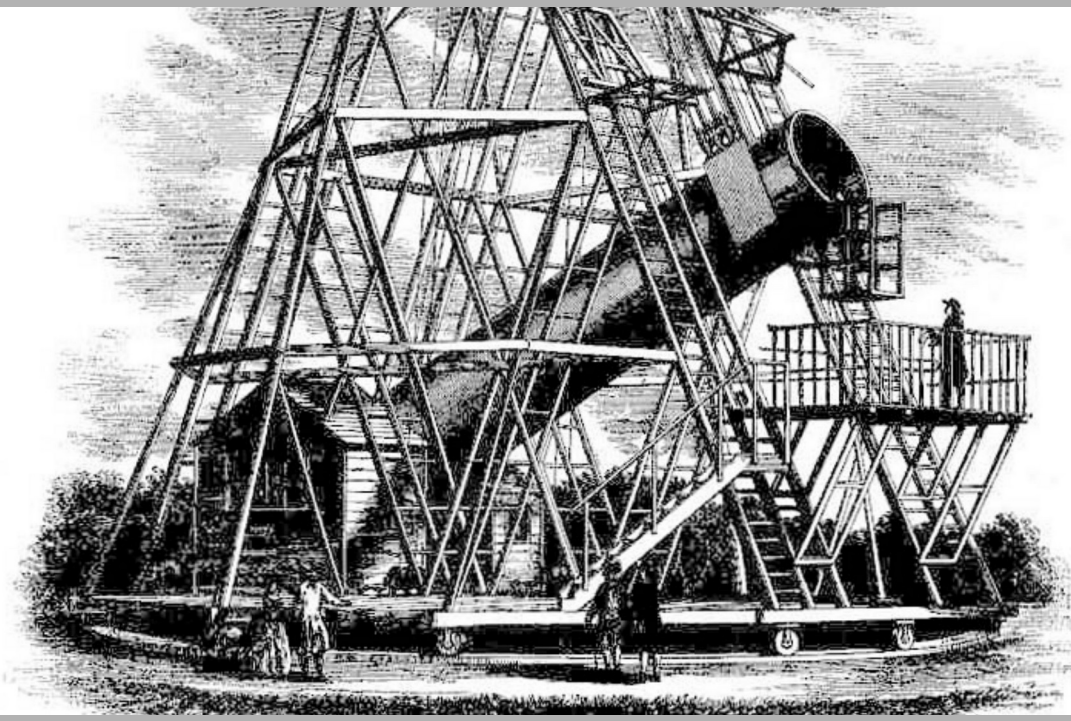
responsibility
to respect

REMEDY

VICTIMS

access to
effective remedy



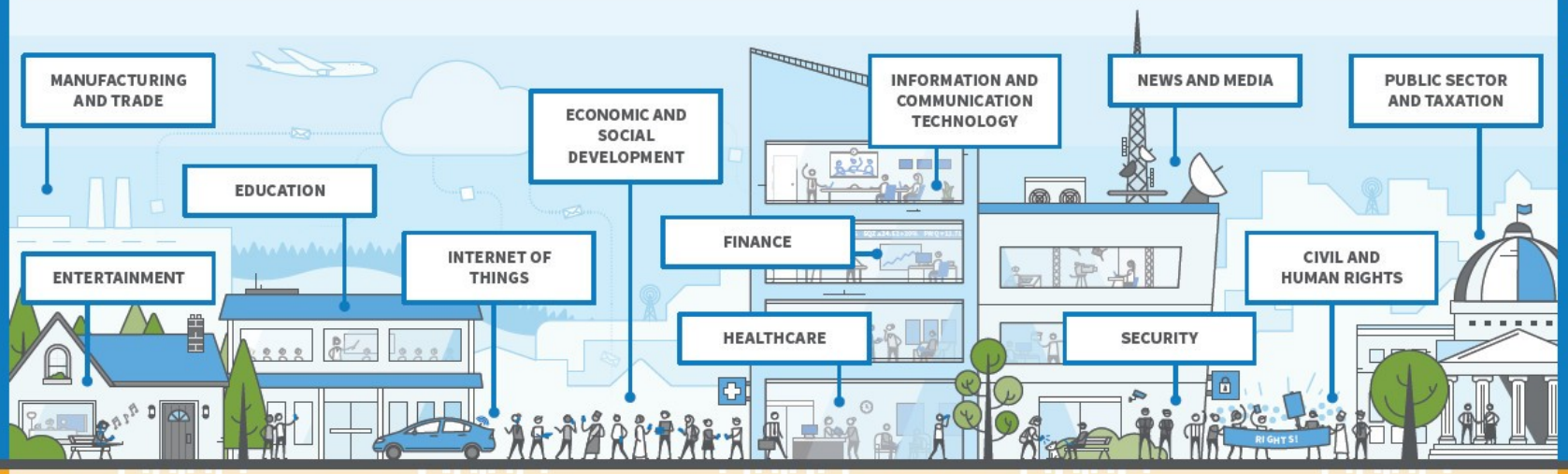


THE THREE LAYERS OF DIGITAL GOVERNANCE

No one person, government, organization, or company governs the digital space. Digital Governance may be stratified into the three layers depicted here: Infrastructure, Logical, Economic and Societal. Solutions to issues in each layer include policies, best practices, standards, specifications, and tools developed by the collaborations of stakeholders and experts from actors in business, government, academia, technical, and civil society. For a map of Digital Governance Issues and Solutions across all three layers, visit https://map.netmundial.org.

DIGITAL GOVERNANCE ACTORS

ECONOMIC AND SOCIETAL LAYER

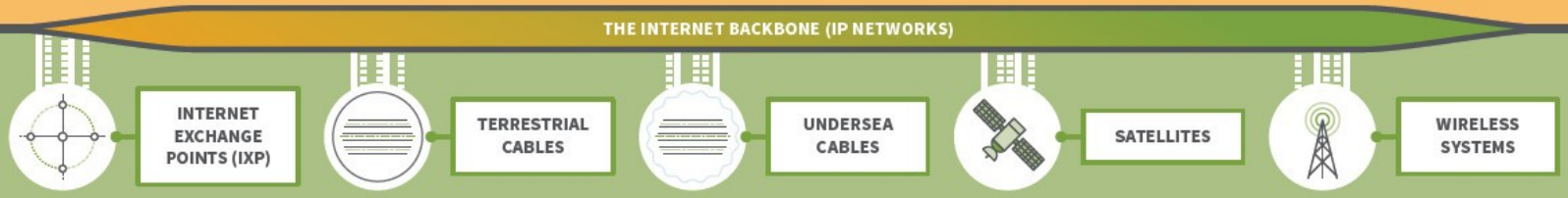


- IGF
- World Economic Forum
- NETmundial Initiative
- W3C
- Industrial Internet Consortium
- ISOC
- National Governments
- Private Sector (ex.: Facebook, Google, Sony, Alibaba)
- Inter-governmental Organizations (ex.: OECD, UNESCO, WTO, WIPO)
- Civil Society (ex.: Human Rights Watch, APC)
- Academia
- Law Enforcement Agencies (ex.: INTERPOL, FBI)

LOGICAL LAYER

- ICANN / IANA
- IETF
- NRO / RIRs
- ISO
- ETSI
- TLD Operators
- Domain Name Registrars
- IEEE
- W3C

INFRASTRUCTURE LAYER



- GSMA
- IEEE
- IETF
- ITU
- National ICT Ministries
- National Regulators
- Network Operators


human
governance
transparency
internet
freedom
openness
icann
cybersecurity
access
privacy
social
iana
open
security
expression
multi-stakeholder
multistakeholder
democracy
neutrality
principles
participation
rights
accountability
cybercrime
global
roadmap
surveillance
multistakeholderism

WSIS > Tunis Agenda

42. We reaffirm our commitment to the **freedom to seek, receive, impart and use information**, in particular, for the creation, accumulation and dissemination of knowledge. We affirm that measures undertaken to ensure Internet stability and security, to fight cybercrime and to counter spam, must protect and respect the provisions for privacy and freedom of expression as contained in ***the relevant parts*** of the **Universal Declaration of Human Rights and the Geneva Declaration of Principle**

UN Human Rights Council 2012

1. Affirms that the **same rights that people have offline must also be protected online**, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights;

UN General Assembly 2013

4. Calls upon all States:

(a) To respect and protect the right to privacy, including in the context of digital communication;

(b) To take measures

(c) To review their procedures, practices and legislation

5. Establish Special Rapporteur for Privacy

NETmundial

Human rights are universal as reflected in the ***Universal Declaration of Human Rights*** and that should underpin Internet governance principles.

Rights that people have offline must also be protected online, in accordance with international human rights legal obligations, including the ***International Covenants on Civil and Political Rights*** **and** ***Economic, Social and Cultural Rights***, **and the** ***Convention on the Rights of Persons with Disabilities***.

UN Special Rapporteur FoE

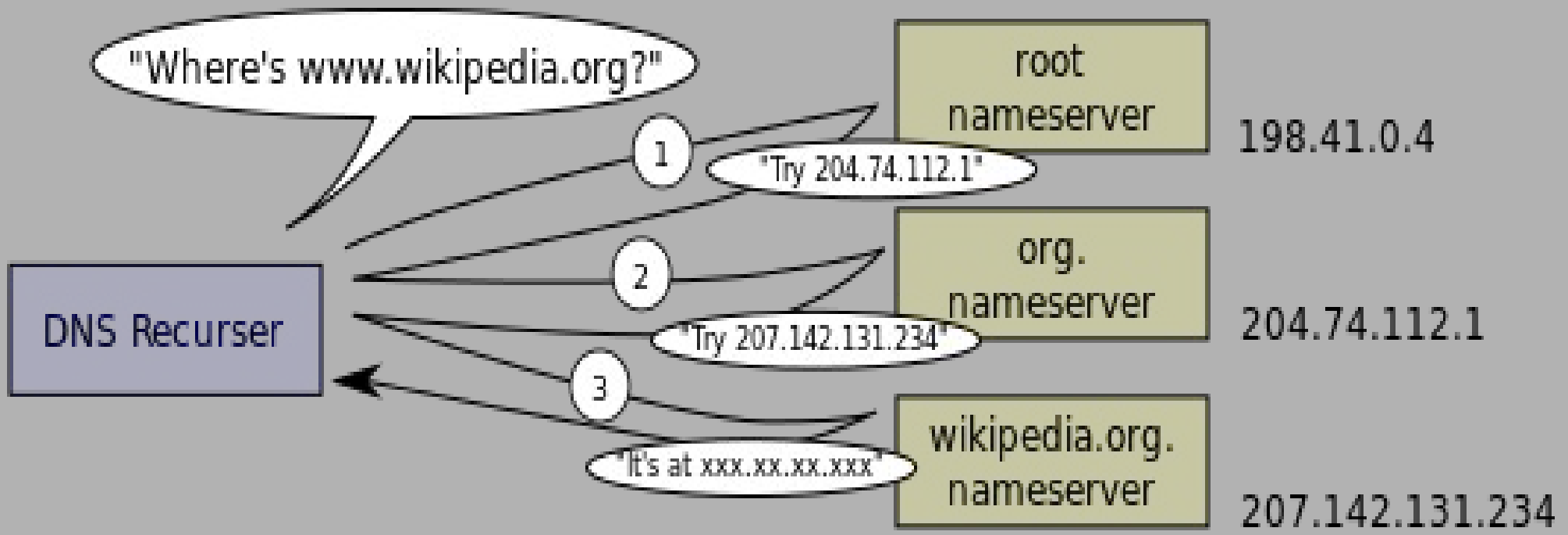
2015 report:

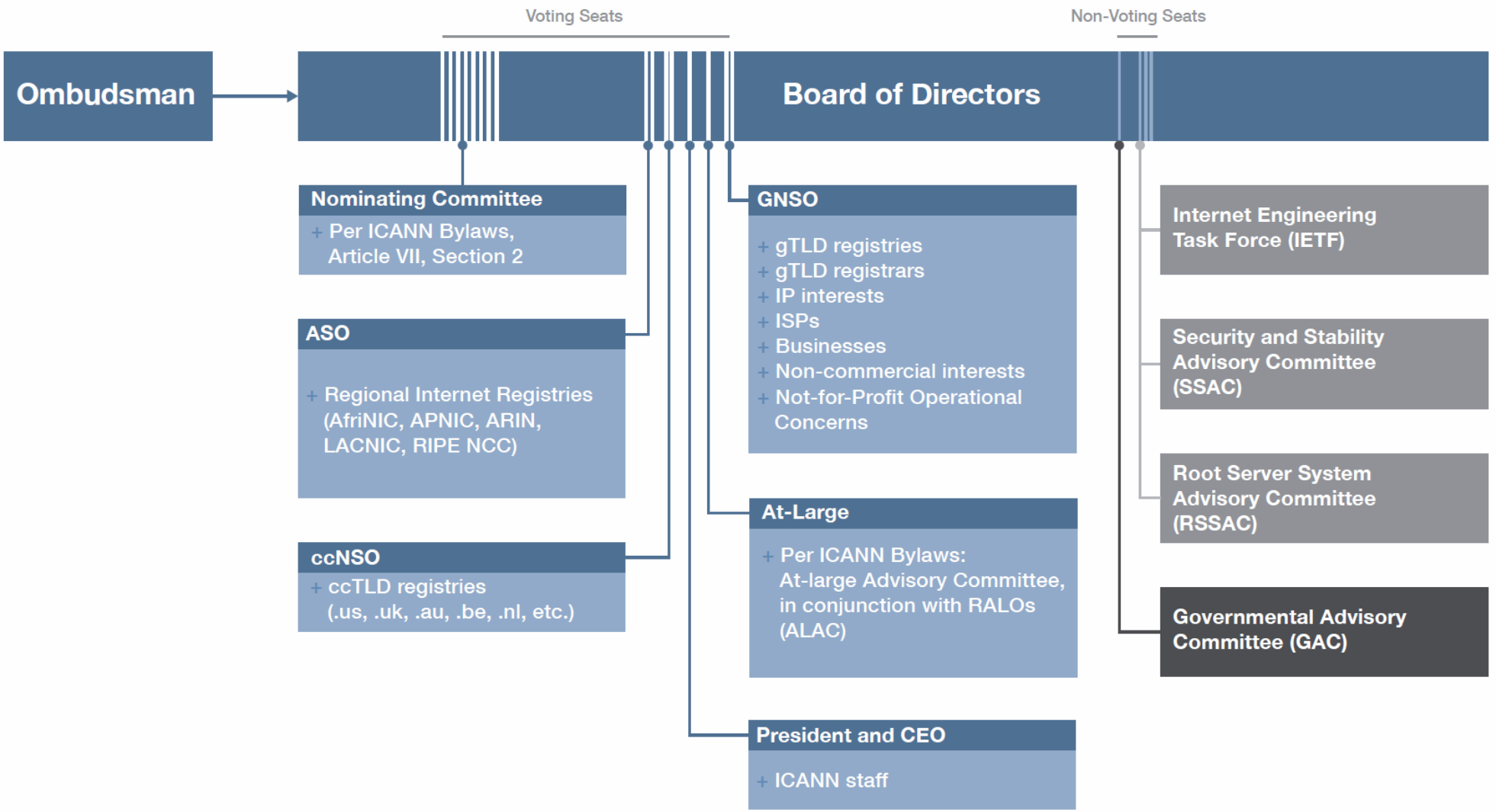
Governments should promote the use of strong encryption and protect anonymous expression online

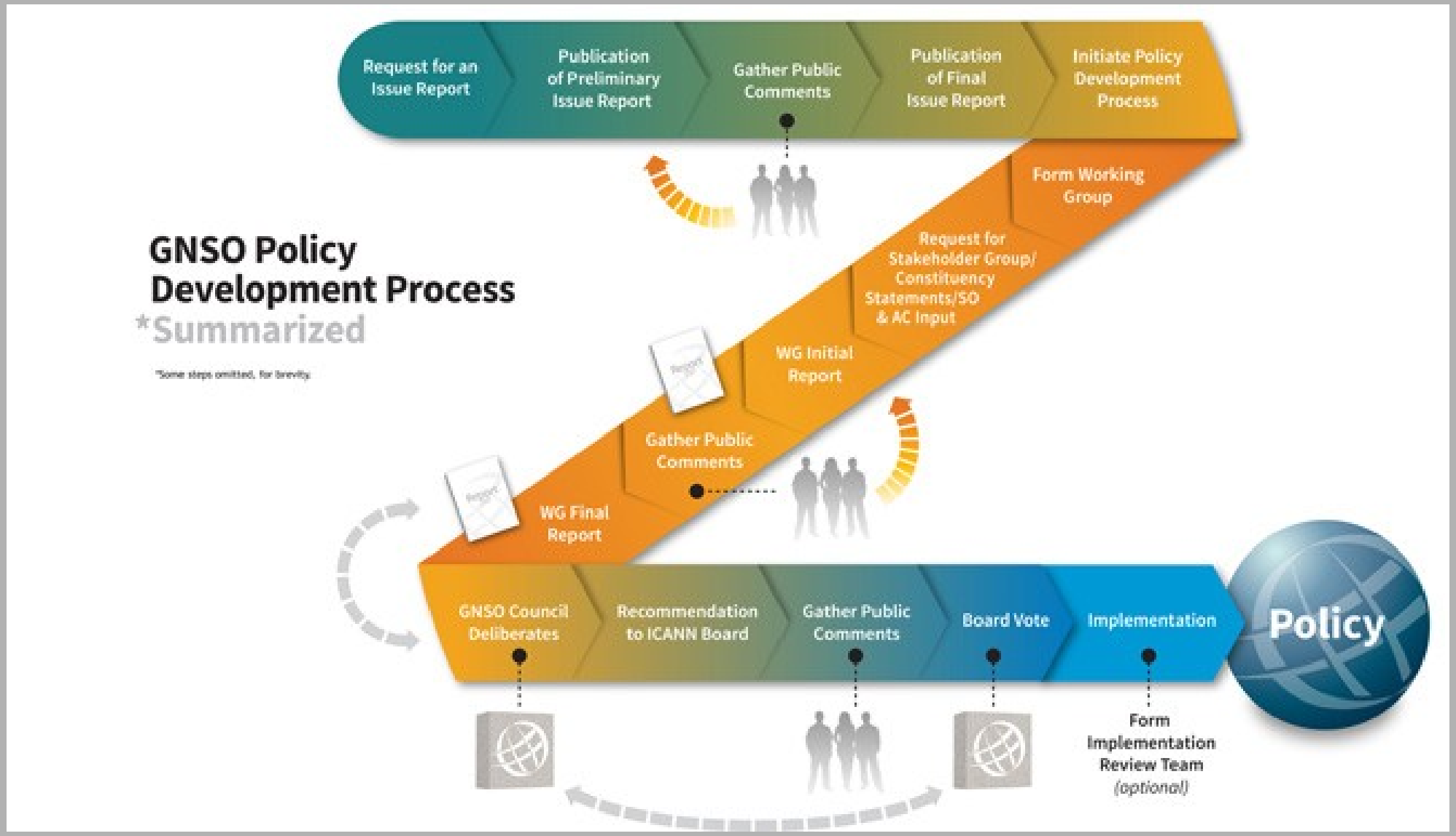
2016 report:

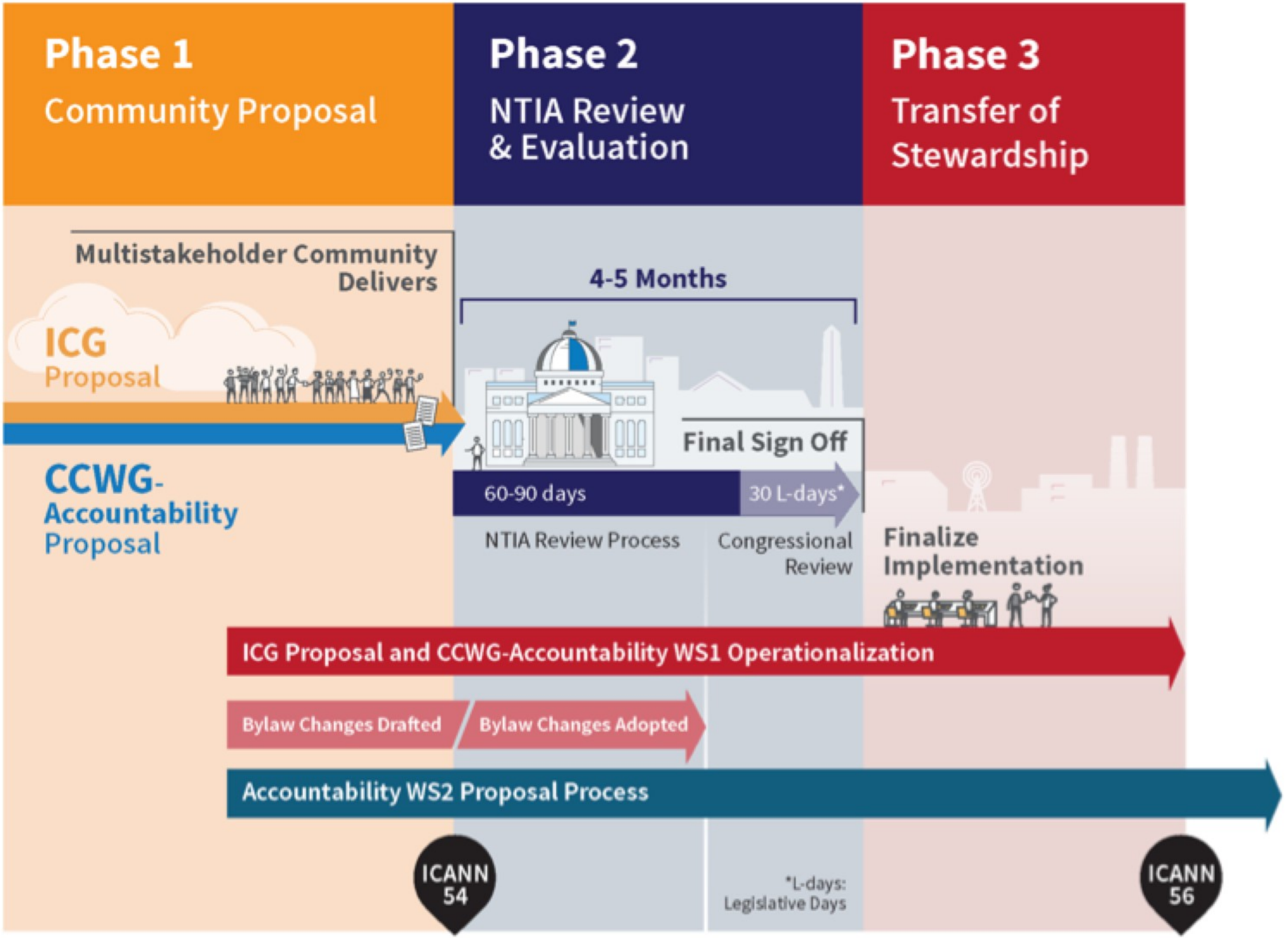
- Intermediary liability
- Private entities should ensure the greatest possible transparency in their policies, standards and actions that implicate the freedom of expression and other fundamental rights.
- Private entities should also integrate commitments to freedom of expression into internal policymaking, product engineering, business development, staff training and other relevant internal processes.


ICANN'T EVEN


"Where's www.wikipedia.org?"
DNS Recurser
1
2
3
root nameserver
198.41.0.4
"Try 204.74.112.1"
org. nameserver
204.74.112.1
"Try 207.142.131.234"
wikipedia.org. nameserver
207.142.131.234
"It's at xxx.xx.xx.xxx"


Voting Seats
Non-Voting Seats
Ombudsman
Board of Directors
Nominating Committee
+ Per ICANN Bylaws, Article VII, Section 2
ASO
+ Regional Internet Registries (AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC)
ccNSO
+ ccTLD registries (.us, .uk, .au, .be, .nl, etc.)
GNSO
+ gTLD registries
+ gTLD registrars
+ IP interests
+ ISPs
+ Businesses
+ Non-commercial interests
+ Not-for-Profit Operational Concerns
At-Large
+ Per ICANN Bylaws: At-large Advisory Committee, in conjunction with RALOs (ALAC)
President and CEO
+ ICANN staff
Internet Engineering Task Force (IETF)
Security and Stability Advisory Committee (SSAC)
Root Server System Advisory Committee (RSSAC)
Governmental Advisory Committee (GAC)


GNSO Policy Development Process
*Summarized
*Some steps omitted, for brevity.
Request for an Issue Report
Publication of Preliminary Issue Report
Gather Public Comments
Publication of Final Issue Report
Initiate Policy Development Process
Form Working Group
Request for Stakeholder Group/ Constituency Statements/SO & AC Input
WG Initial Report
Gather Public Comments
WG Final Report
GNSO Council Deliberates
Recommendation to ICANN Board
Gather Public Comments
Board Vote
Implementation
Policy
Form Implementation Review Team
(optional)


Phase 1
Community Proposal
Phase 2
NTIA Review & Evaluation
Phase 3
Transfer of Stewardship
Multistakeholder Community Delivers
ICG
Proposal
CCWG-
Accountability
Proposal
4-5 Months
Final Sign Off
60-90 days
30 L-days*
NTIA Review Process
Congressional Review
Finalize Implementation
ICG Proposal and CCWG-Accountability WS1 Operationalization
Bylaw Changes Drafted
Bylaw Changes Adopted
Accountability WS2 Proposal Process
ICANN 54
*L-days: Legislative Days
ICANN 56

Internationalization vs privatization

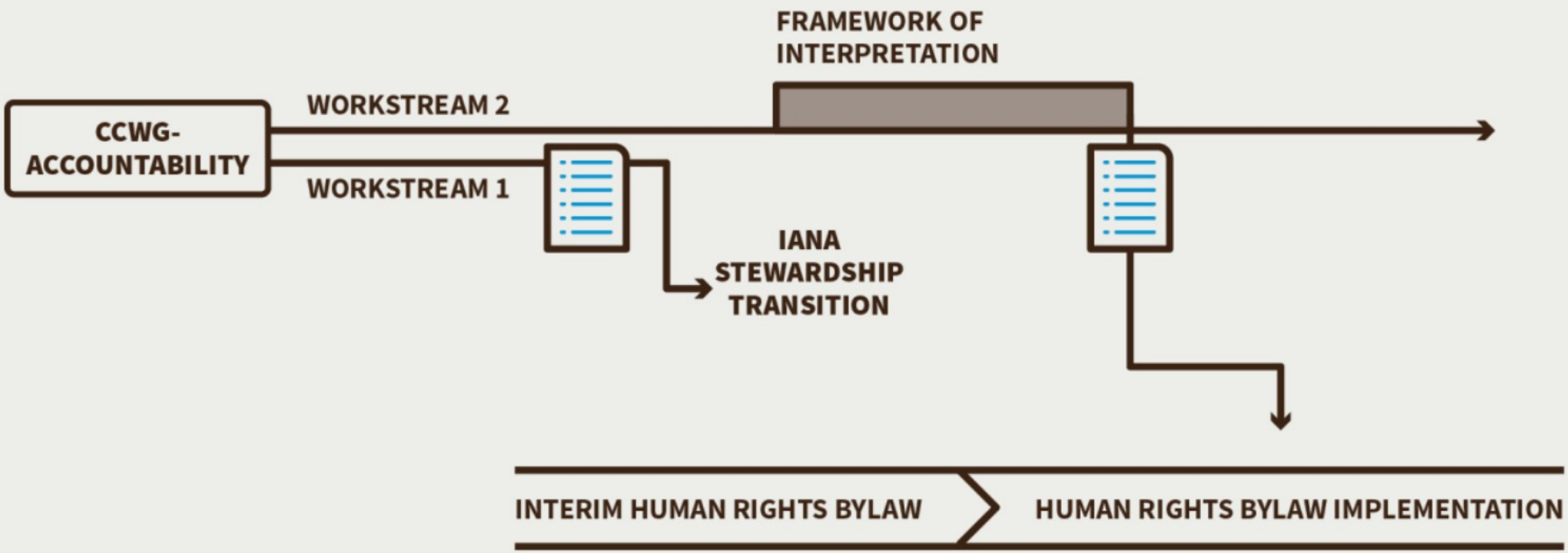
the government of the United States "is committed to a transition that will allow the private sector to take leadership for DNS management."

– NTIA

The Internet "is built on the principles that define America: free enterprise and limited government.”

– Steve Crocker

Human Rights



ICANN

POLICIES AND HUMAN RIGHTS

ICANN

The Internet Corporation for Assigned Names and Numbers coorinates the policy making and distribution of domain names and IP numbers. It therefore is often dubbed as the 'telephone book of the Internet'.

ICANN GLOSSARY

DANE: DNS-based Authentication of Named Entities

DCND: Defined conditions of nondisclosure

DIDP: Documentary Information Disclosure Policy

DNSSEC: Domain Name System Security Extensions

GAC: Governmental Advisory Committee

GNSO: Generic Names Supporting Organization

gTLD: Generic top-level domain

IDNs: Internationalized Domain Names

IGOs: Inter-Governmental Organisations

INGOs: International Non-Governmental Organizations

IRP: Independent Review Panel

PDP: Policy Development Process

RDAP: Registration data access protocol

RPMs: Rights Protection Mechanism (as related to Intellectual Property Rights)

WHOIS: an Internet service that provides information about a domain name or IP address

HUMAN RIGHTS PRINCIPLES

INHERENT: human rights derive from the humanity of each person.

UNIVERSAL: all human beings have the same human rights.

INALIENABLE: human rights cannot be given up.

INDIVISIBLE: there are no conflicts between rights and no priorities among rights. There will be situations or occasions where rights must be balanced and prudent decisions taken about how all rights can best be protected and promoted.

INTERDEPENDENT AND INTERRELATED: the enjoyment and fulfilment of any right depends on the enjoyment and fulfilment of other rights.

EQUALITY AND NON-DISCRIMINATION: all individuals are equal as human beings and by virtue of the inherent dignity of each human person.

PARTICIPATION AND INCLUSION: all people have the right to participate in and access information relating to the decision-making processes that affect their lives and well-being.

ACCOUNTABILITY AND RULE OF LAW: States and other duty-bearers are answerable for the observance of human rights. In this regard, they have to comply with the legal norms and standards enshrined in international human rights instruments.

Universal Declaration of Human Rights

Treaties

- International Covenant on Civil and Political Rights (ICCPR) 1966
- International Covenant on Economic, Social and Cultural Rights (ICESCR) 1966
- International Convention on the Elimination of All Forms of Racial Discrimination (ICERD) 1965
- Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) 1979
- Convention on the Rights of Persons with Disabilities (CRPD) 2006

Guidelines

- UN Guiding Principles on Business and Human Rights (2011)
  - Protect (states)
  - Respect (non state actors)
  - Remedy
- UN Global Compact (2000)

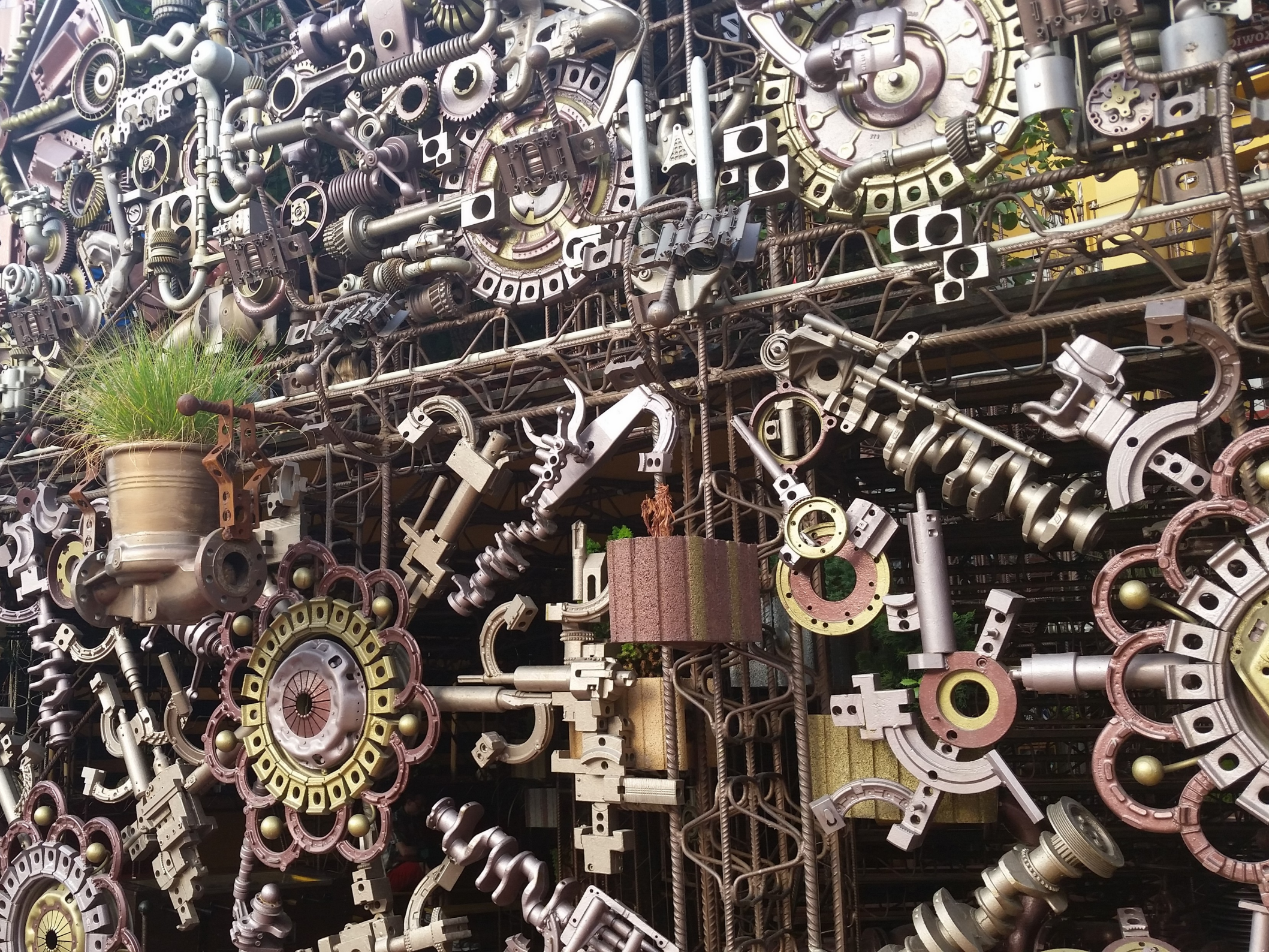
Scoping the relation between ICANN and Human Rights

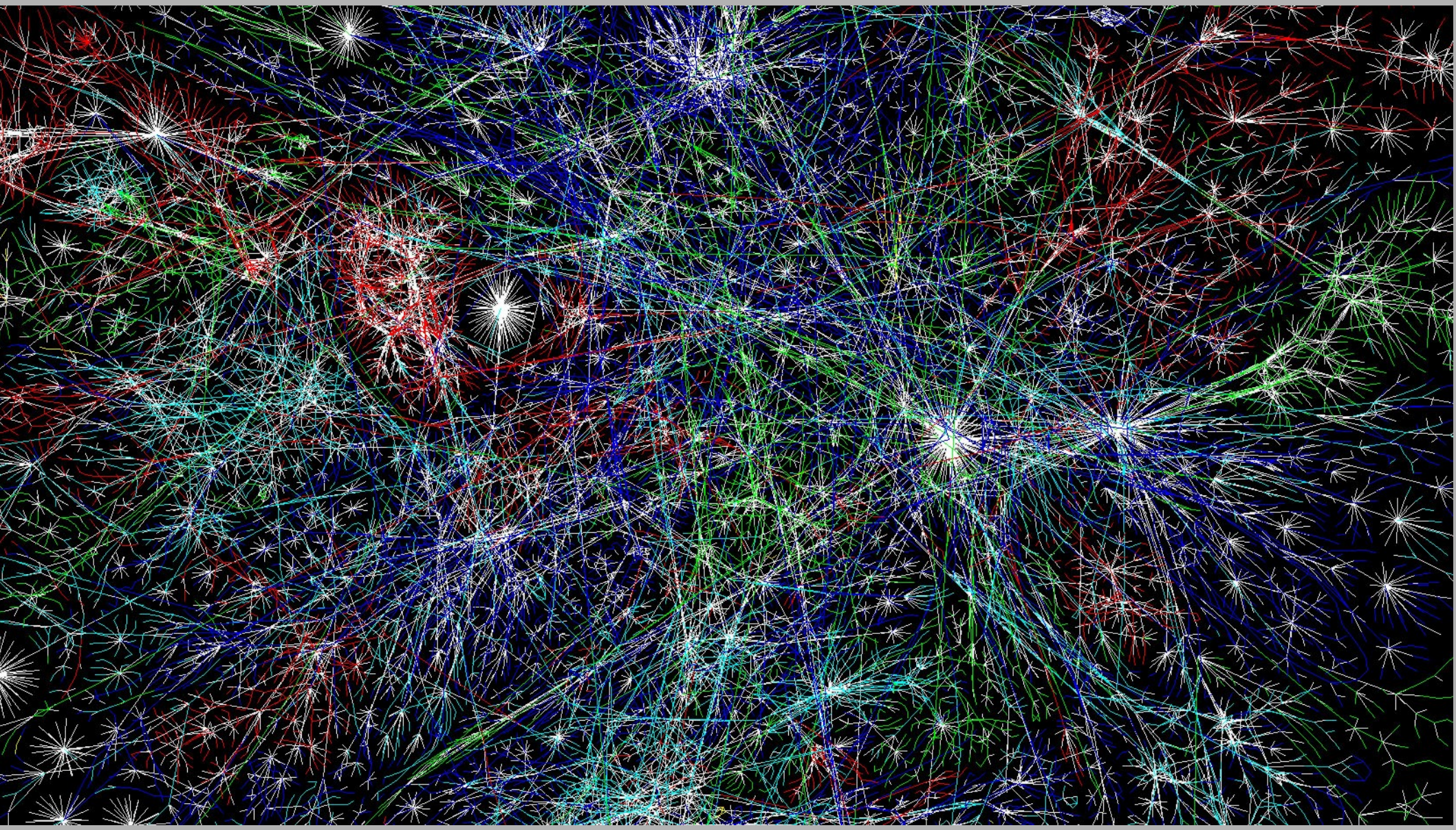
RIGHTS INVOLVED	THEME	ICANN POLICY OR PROCESS
RIGHT TO PRIVACY	Documentary Information Disclosure Policy	Defined conditions of non-disclosure
	2014 Registrar Accreditation Agreement	Data escrow provider financial support
	2013 Registrar Accreditation Agreement	WHOIS accuracy specification requirement
	WHOIS	Thick WHOIS implementation review team
		Next generation gTLD registration directory service
		RDAP changes and privacy
RIGHT TO FREEDOM OF ASSOCIATION	New gTLD subsequent procedures WG	Applicant guidebook — Community based TLD
ECONOMIC, SOCIAL AND CULTURAL RIGHTS	New gTLD subsequent procedures WG	Application fees
		Registrar accreditation process & insurance requirements
		GNSO new gTLD auctions proceeds drafting team
	IP addresses	Coordination and distribution of IP addresses
	Free and fair use of domain names	The right to use all words and names in domain names
RIGHT TO FREEDOM OF EXPRESSION	New gTLD subsequent procedures WG	Content-based gTLD String Evaluations
		Applicant guidebook — Sensitive strings; Community based TLD
	Internationalized Domain Names	Implementation of Internationalized Domain Names
	Rights Protection Mechanisms	Review of protection IGO/NGO names in all gTLDs
		Review of curative rights protections in IGO/INGOs in gTLDs
		New gTLDs subsequent round WG
		PDP to review RPMs in all gTLDs
RIGHT TO SECURITY	DNSSEC	Implementation of DNSSEC
		Implementation of DANE
PARTICIPATION, INCLUSION, EQUALITY AND NON-DISCRIMINATION	Protection of rights to fair and equal treatment	Awareness of Ombudsman office for complaint
DUE PROCESS	PDP procedure	GNSO PDP improvements discussion group
	GAC early warning	
	Reconsideration Request	Effect of failure and the use of the Ombudsman
	IRP Process	
	All Dispute Resolution processes within ICANN	Need to ensure that parties know about Ombudsman for unfair process
	Documentary Information Disclosure Policy	Documentary Information Disclosure Policy requests

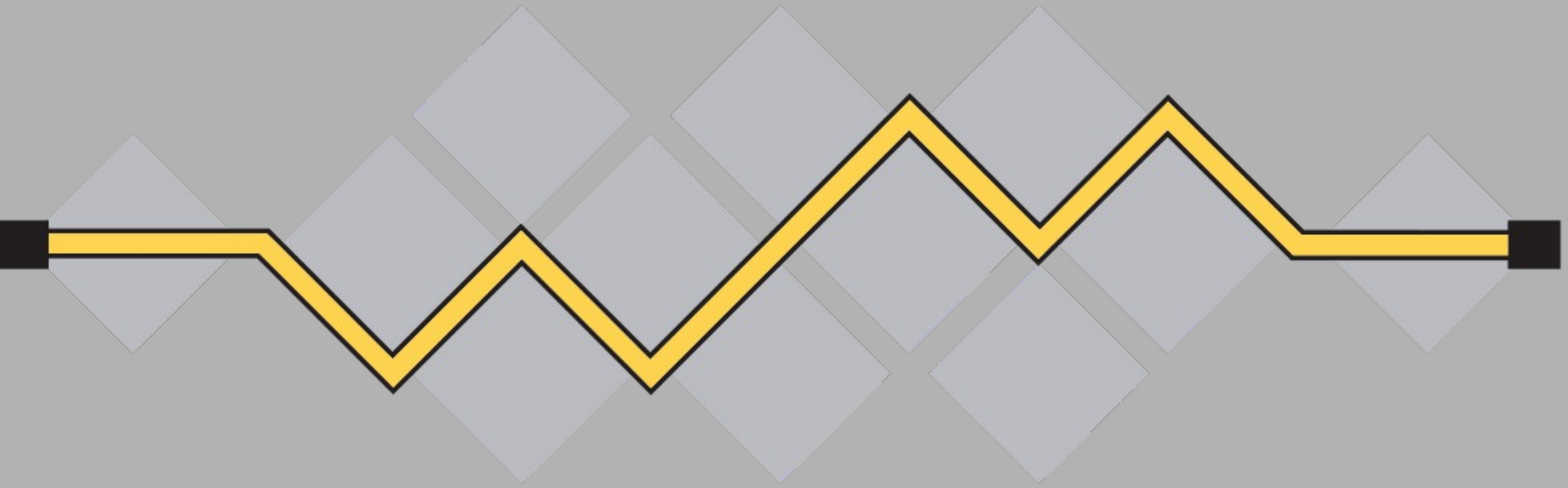
This illustration has been produced by the Cross Community Working Party on ICANNs Corporate and Social Responsibility to Respect Human Rights

This is a preliminary scoping, pending a full Human Rights Impact Assessment


ICANN







IETF®

Internet Architecture Imaginary (1)

- End-to-end principle
  - Intelligence at the edges
  - Network only provides datagram transport
  - Low complexity
  - High robustness

  But...

The purpose of this document is not, therefore, to lay down dogma about how Internet protocols should be designed, or even about how they should fit together. Rather, it is to convey various guidelines that have been found useful in the past, and that may be useful to those designing new protocols or evaluating such designs.

A good analogy for the development of the Internet is that of constantly renewing the individual streets and buildings of a city, rather than razing the city and rebuilding it. The architectural principles therefore aim to provide a framework for creating cooperation and standards, as a small "spanning set" of rules that generates a large, varied and evolving space of technology.

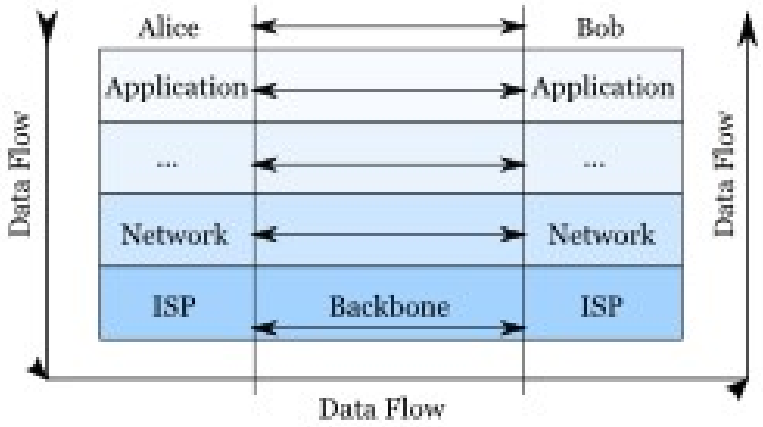
Some current technical triggers for change include the limits to the scaling of IPv4, the fact that gigabit/second networks and multimedia present fundamentally new challenges, and the need for quality of service and security guarantees in the commercial Internet.

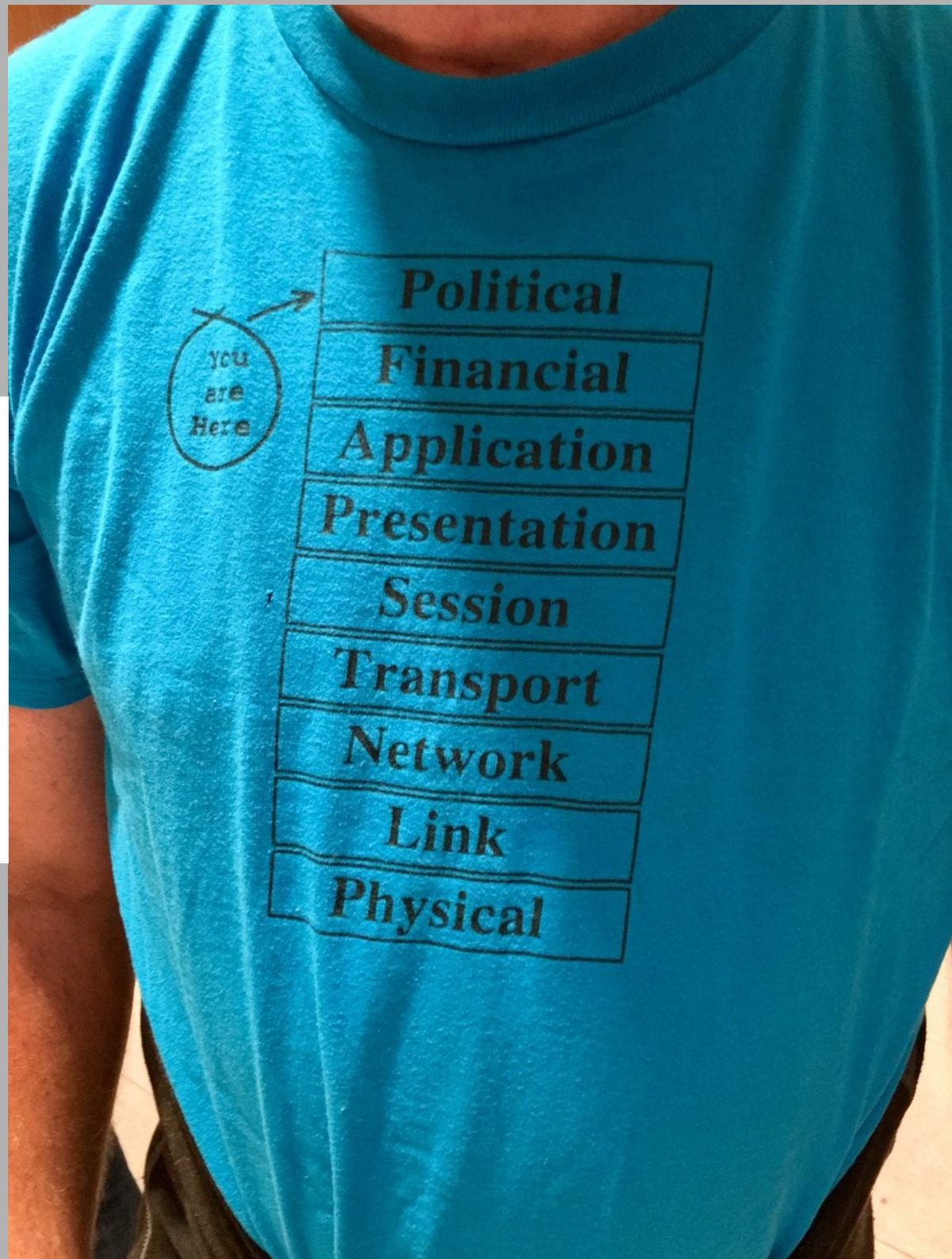
As Lord Kelvin stated in 1895, "Heavier-than-air flying machines are impossible." We would be foolish to imagine that the principles listed below are more than a snapshot of our current understanding.

2. Is there an Internet Architecture?

2.1 Many members of the Internet community would argue that there is no architecture, but only a tradition, which was not written down for the first 25 years (or at least not by the IAB). However, in very general terms, the community believes that the goal is connectivity, the tool is the Internet Protocol, and the intelligence is end to end rather than hidden in the network.

End-to-end principle





(Another step is to choose leaders that we trust to exercise their good judgement and do the right thing. But we're already trying to do that.)

4. Issues with Scoping the IETF's Mission

4.1. The Scope of the Internet

A very difficult issue in discussing the IETF's mission has been the scope of the term "for the Internet". The Internet is used for many things, many of which the IETF community has neither interest nor competence in making standards for.

The Internet isn't value-neutral, and neither is the IETF. We want the Internet to be useful for communities that share our commitment to openness and fairness. We embrace technical concepts such as decentralized control, edge-user empowerment and sharing of resources, because those concepts resonate with the core values of the IETF community. These concepts have little to do with the technology that's possible, and much to do with the technology that we choose to create.

Internet Architecture Imaginary (2)

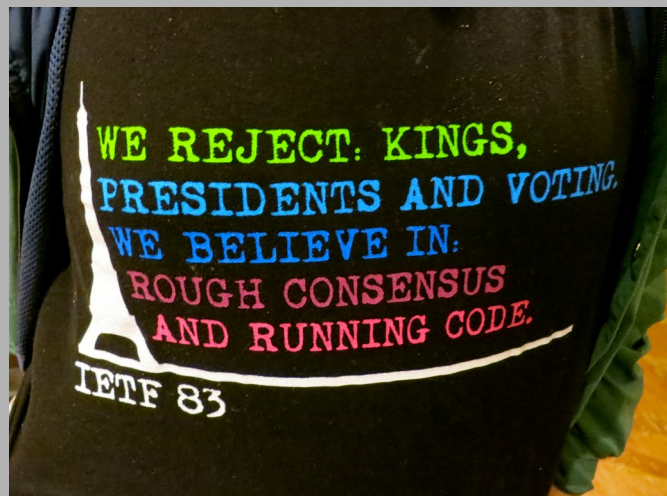
- Permissionless innovation
  - No barriers for deployment of new protocols
  - No need to negotiate with entities in the middle of the network
  - Response to Telco era (and perhaps Acceptible Use Policy of ARPANET & NSFnet)

Internet Architecture Imaginary (3)

- Openness (network)
  - Reach any endpoint on the Internet without being hampered, altered or stopped
  - Ability to add new endpoints to the network
- Open standards
  - Voluntary
  - Freely accessible
- Open governance
  - Transparent
  - Open participation
  - Open archives

We reject: kings,
presidents and voting.
We believe in: rough consensus
and running code.

- Quote from Dave Clarke in the Tao of the IETF



Explicit discussions about rights and freedoms, as well as social impact of technology have featured in RFCs since their beginnings

-Sandra Braman

Commercialization & Privatization (end 80s, early 90s)

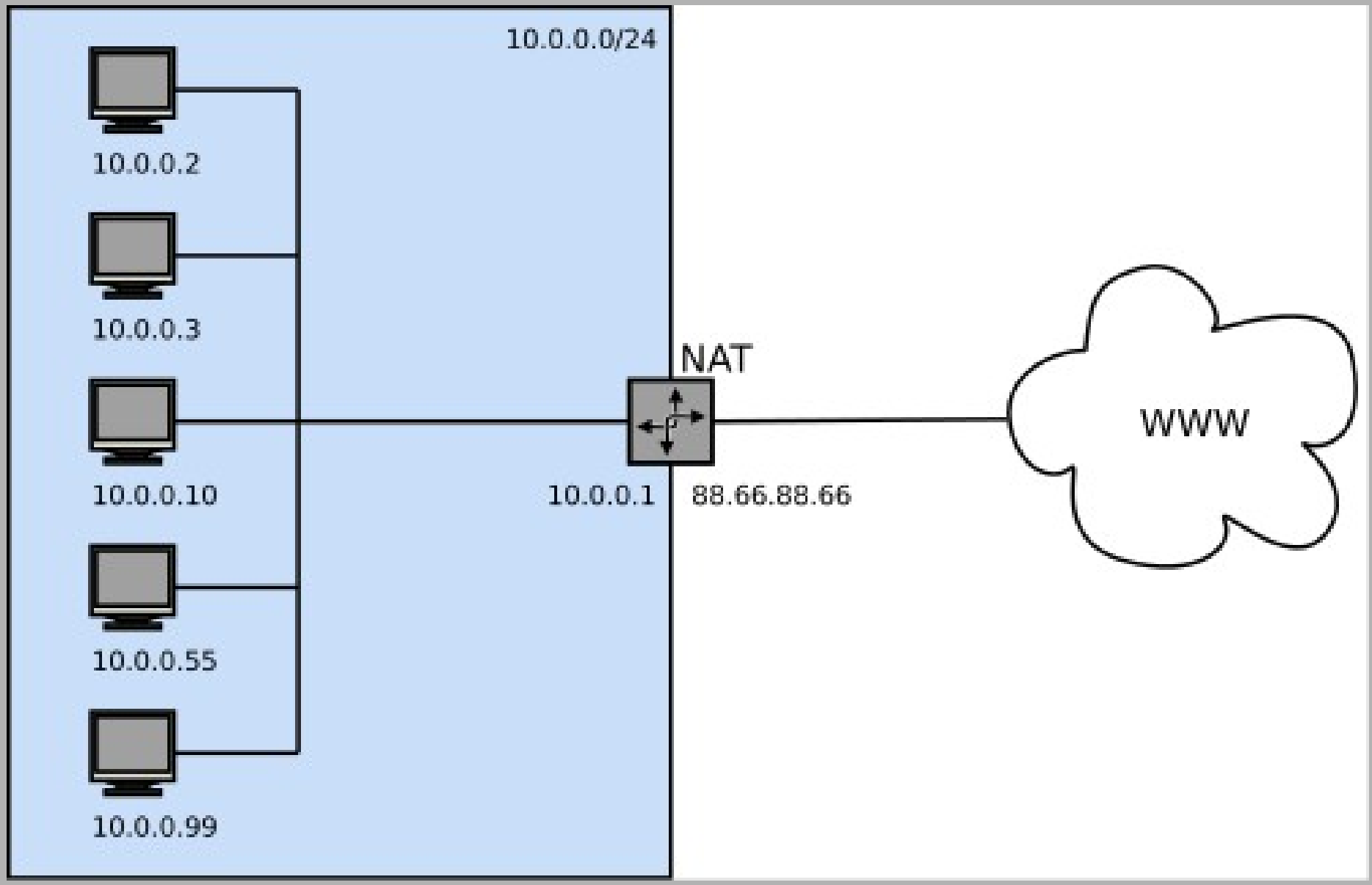
- US government cedes direct control:
  - ARAPNET (Dept of Defense)
  - NSFNET (Dept of Education)
  - ESNET (Dept of Energy)
- Establishment of Commercial Internet Exchanges
- Formal institutionalization of:
  - Internet Engineering Taskforce
  - Internet Society
  - Regional Internet Registries

Crack in the imaginary: Rise of the Middlebox

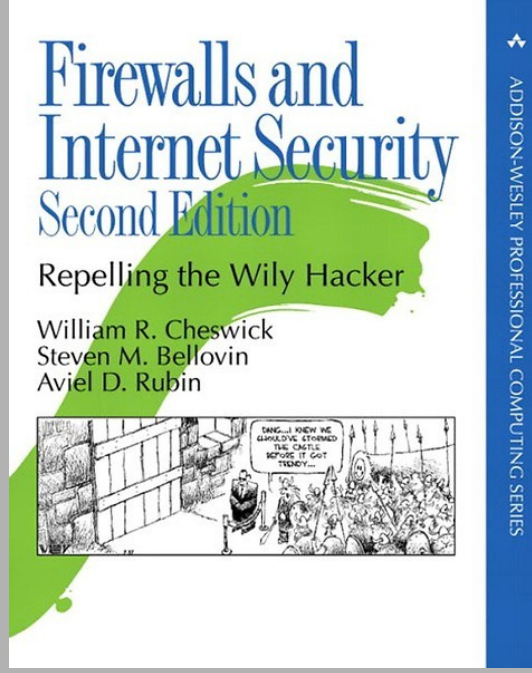
- IPv4 running out
  - ‘only’ 4.3 billion IP addresses
  - No replacement done yet
- Security considerations
  - Internet was no longer comprised of trusted actors
- Perceived need from network operators differentiate business models

(RFC3725)

Network Address Translation



Firewalls



- Security
- Administrative control

‘a lot of networks do a lot of bad things to peer-to-peer traffic’

‘firewalls didn't serve only a security purpose, they also served an administrative control purpose, that's a third party in the midst of the peers who are talking to each other. So it's been difficult for Internet peer to peer things to take off. ‘

Security technologies do not just make the internet more or less secure. They redistribute power relationships among actors. New gatekeepers might be established, some people lose access to information, while others gain it, and so on.

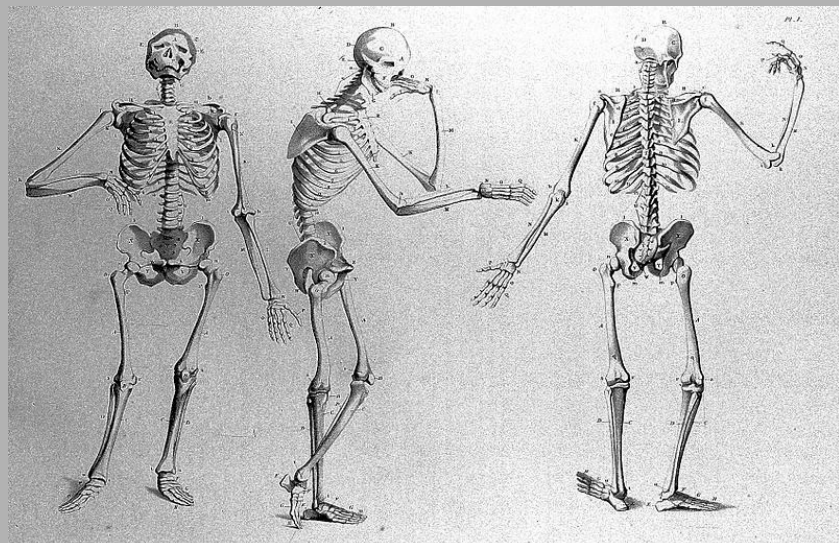
– Milton Mueller

Network management

- Quality of service
- Caching
- Prioritization of services

Rise of the Middlebox (4)

- Added functionality to the network
- Not at the edges, but in the network
- This led to ‘ossification’
- Introduced directionality, created users and producers
- Created a new **affordance structure** in the Internet architecture



Example 1 : TLS1.3

If a server established a TLS connection with a previous version of TLS and receives a TLS 1.3 ClientHello in a renegotiation, it MUST retain the previous protocol version. In particular, it MUST NOT negotiate TLS 1.3.

Structure of this message:

```
   uint16 ProtocolVersion;
   opaque Random[32];

   uint8 CipherSuite[2];    /* Cryptographic suite selector */

   struct {
       ProtocolVersion legacy_version = 0x0303;    /* TLS v1.2 */
       Random random;
       opaque legacy_session_id<0..32>;
       CipherSuite cipher_suites<2..2^16-2>;
       opaque legacy_compression_methods<1..2^8-1>;
       Extension extensions<8..2^16-1>;
   } ClientHello;
```

Example 2: Stream Control Transmission Protocol

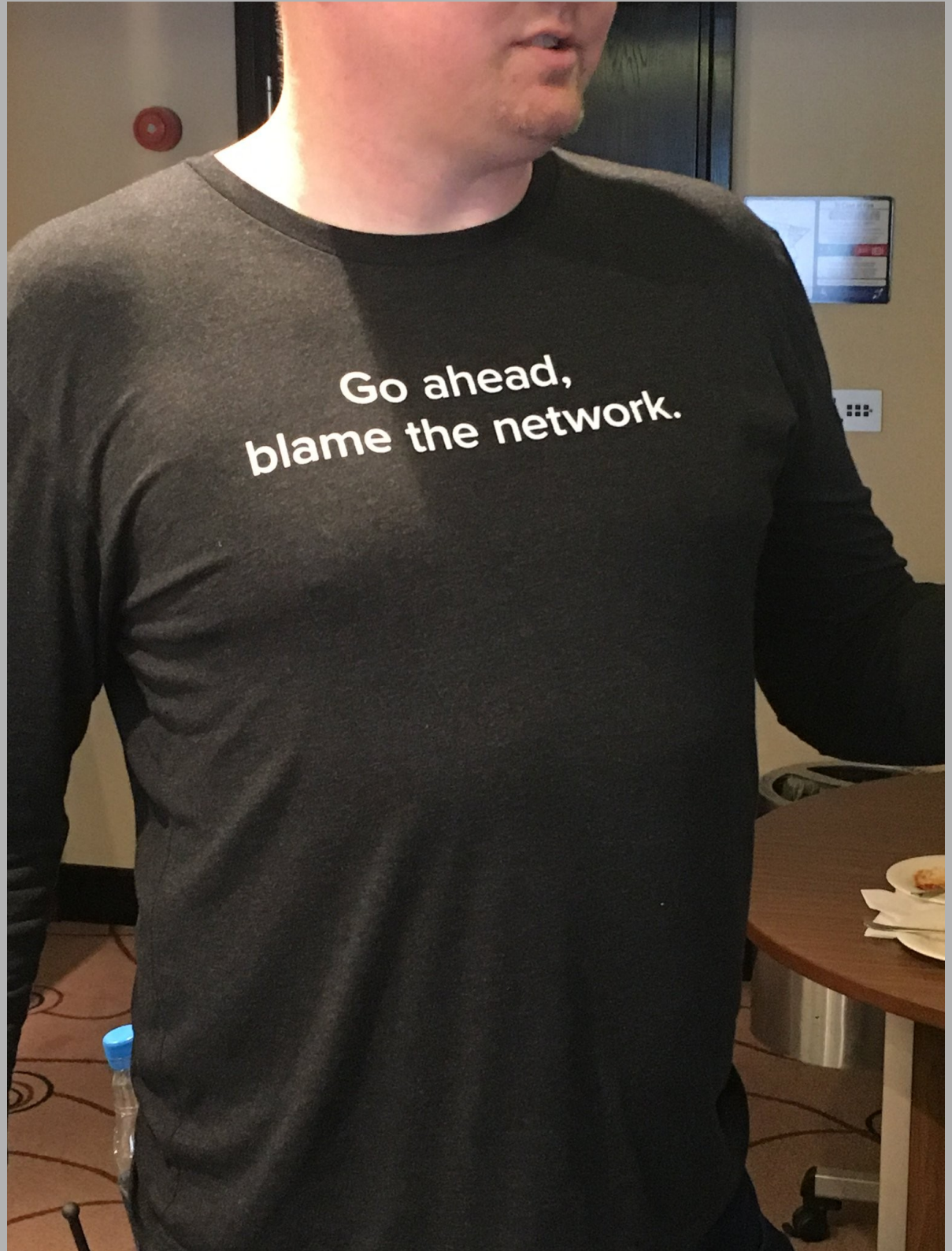
- Transport layer replacement for TCP
- Multiple streams
- Multiple transmission paths
- No head of line blocking
- Described in 39 (!) RFCs
- Worked perfectly in the lab
- Blocked by many NATs
- Never reliably worked on the Internet
- Because of reordered affordances

First RFC:
April 2002

Last RFC:
November 2017

Protocol
Failure

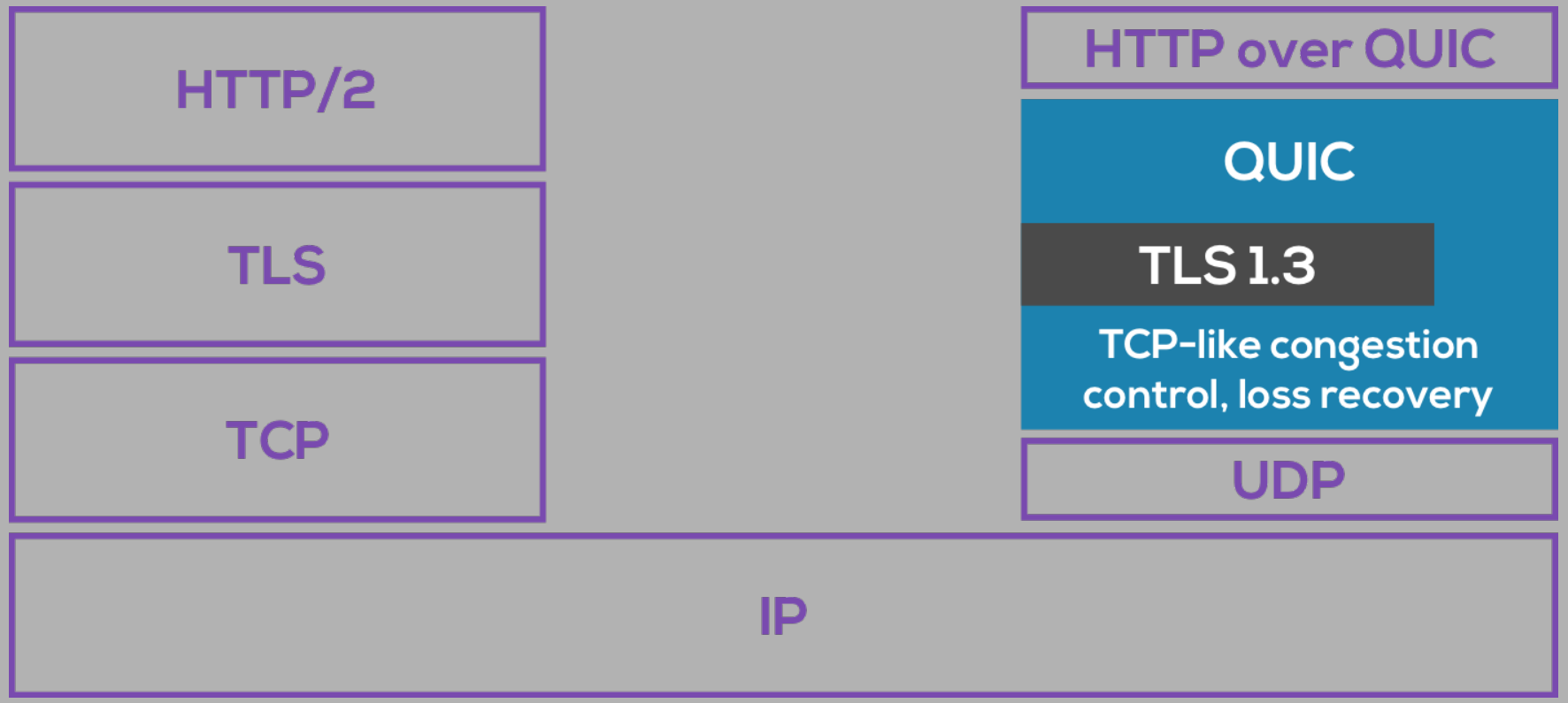
- RFC8261: Datagram Transport Layer Security (DTLS) Encapsulation of SCTP Packets
- RFC8087: The Benefits of Using Explicit Congestion Notification (ECN) informational
- RFC7829: SCTP-PF: A Quick Failover Algorithm for the Stream Control Transmission Protocol
- RFC7765: TCP and Stream Control Transmission Protocol (SCTP) RTO Restart experimental
- RFC7605: Recommendations on Using Assigned Transport Port Numbers bcp
- RFC6951: UDP Encapsulation of Stream Control Transmission Protocol (SCTP) Packets for End-Host to End-Host Communication
- RFC6633: Deprecation of ICMP Source Quench Messages
- RFC6526: IP Flow Information Export (IPFIX) Per Stream Control Transmission Protocol (SCTP) Stream
- RFC6525: Stream Control Transmission Protocol (SCTP) Stream Reconfiguration
- RFC6458: Sockets API Extensions for the Stream Control Transmission Protocol (SCTP) informational
- RFC6096: Stream Control Transmission Protocol (SCTP) Chunk Flags Registration
- RFC6084: General Internet Signaling Transport (GIST) over Stream Control Transmission Protocol (SCTP) and Datagram Transport Layer Security (DTLS) experimental
- RFC6083: Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)
- RFC6053: Implementation Report for Forwarding and Control Element Separation (ForCES) informational
- RFC5923: Connection Reuse in the Session Initiation Protocol (SIP)
- RFC5827: Early Retransmit for TCP and Stream Control Transmission Protocol (SCTP) experimental
- RFC5811: SCTP-Based Transport Mapping Layer (TML) for the Forwarding and Control Element Separation (ForCES) Protocol
- RFC5062: Security Attacks Found Against the Stream Control Transmission Protocol (SCTP) and Current Countermeasures informational
- RFC5061: Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration
- RFC5043: Stream Control Transmission Protocol (SCTP) Direct Data Placement (DDP) Adaptation
- RFC4960: Stream Control Transmission Protocol
- RFC4895: Authenticated Chunks for the Stream Control Transmission Protocol (SCTP)
- RFC4820: Padding Chunk and Parameter for the Stream Control Transmission Protocol (SCTP)
- RFC4666: Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) - User Adaptation Layer (M3UA)
- RFC4460: Stream Control Transmission Protocol (SCTP) Specification Errata and Issues informational
- RFC4233: Integrated Services Digital Network (ISDN) Q.921-User Adaptation Layer
- RFC4168: The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)
- RFC4166: Telephony Signalling Transport over Stream Control Transmission Protocol (SCTP) Applicability Statement informational
- RFC4138: Forward RTO-Recovery (F-RTO): An Algorithm for Detecting Spurious Retransmission Timeouts with TCP and the Stream Control Transmission Protocol (SCTP) experimental
- RFC3873: Stream Control Transmission Protocol (SCTP) Management Information Base (MIB)
- RFC3868: Signalling Connection Control Part User Adaptation Layer (SUA)
- RFC3807: V5.2-User Adaptation Layer (V5UA)
- RFC3758: Stream Control Transmission Protocol (SCTP) Partial Reliability Extension
- RFC3708: Using TCP Duplicate Selective Acknowledgement (DSACKs) and Stream Control Transmission Protocol (SCTP) Duplicate Transmission Sequence Numbers (TSNs) to Detect Spurious Retransmissions experimental
- RFC3554: On the Use of Stream Control Transmission Protocol (SCTP) with IPsec
- RFC3436: Transport Layer Security over Stream Control Transmission Protocol
- RFC3331: Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) - User Adaptation Layer
- RFC3286: An Introduction to the Stream Control Transmission Protocol (SCTP) informational
- RFC3257: Stream Control Transmission Protocol Applicability Statement informational


Go ahead,
blame the network.

The return of the strong endpoints: The Rise of QUIC

- Quick UDP Internet Protocol (QUIC)
- Stream-based protocol
- Similar to SCTP, but..
  - Developed by Google
    - Communicate between Google servers (CDNs) and browsers (mainly Chrome)
    - Experimental A/B testing
- Fallback to TCP

Includes encryption by default...

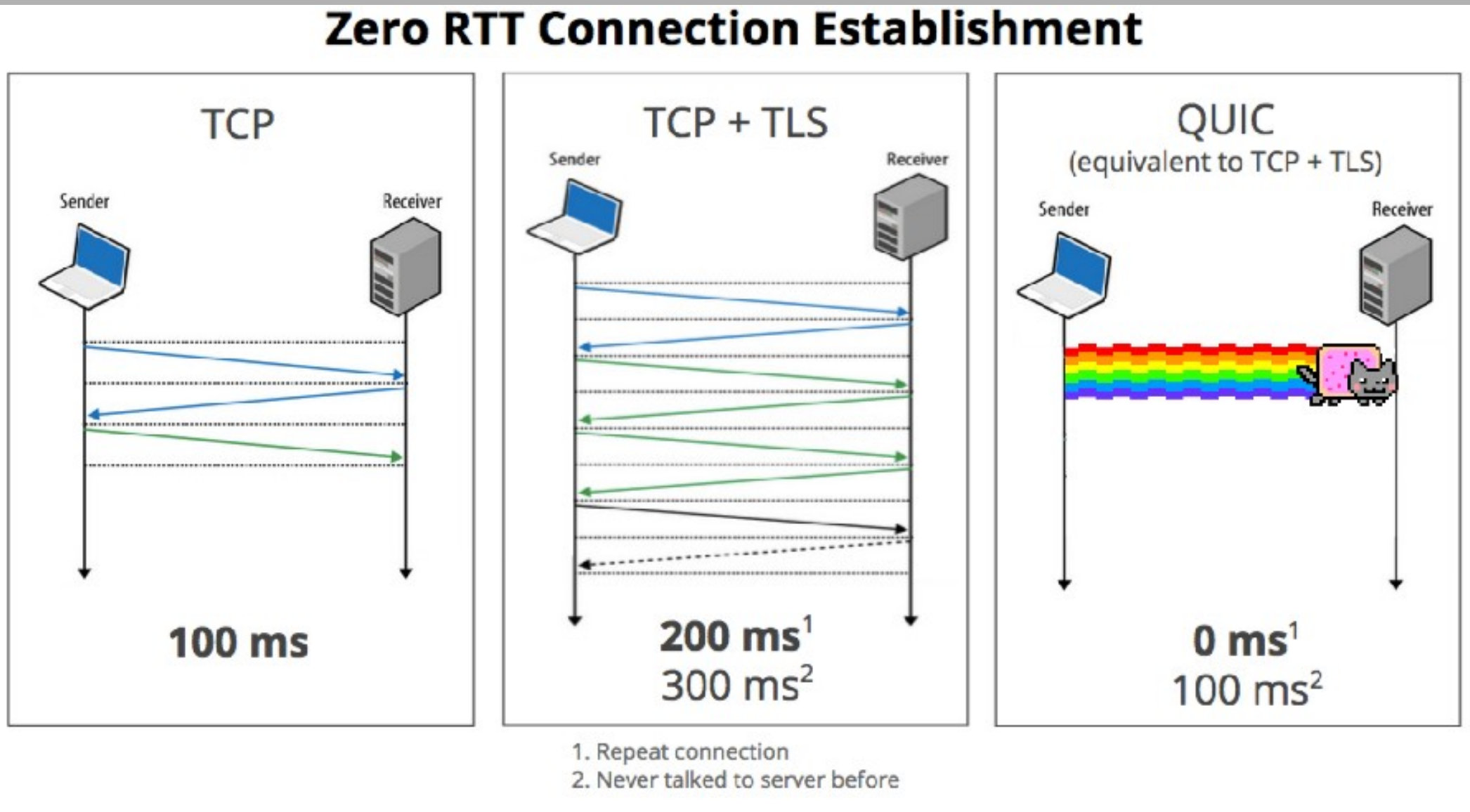


...as much as possible

“Let’s not share anything [with the network] unless we really need to because I don't care whether it’s ossified or whether it’s not. We’ve tried this in the past and we’ve failed because people ossify whatever is visible. I don't care what they can and cannot use it for. I just don't want to share it unless there is…

The burden of proof, in my opinion, is on the operators to say we really, really, really can’t run our networks unless we see this one bit. And if they can prove that, then maybe it’s fine at that point.”

Latency wins

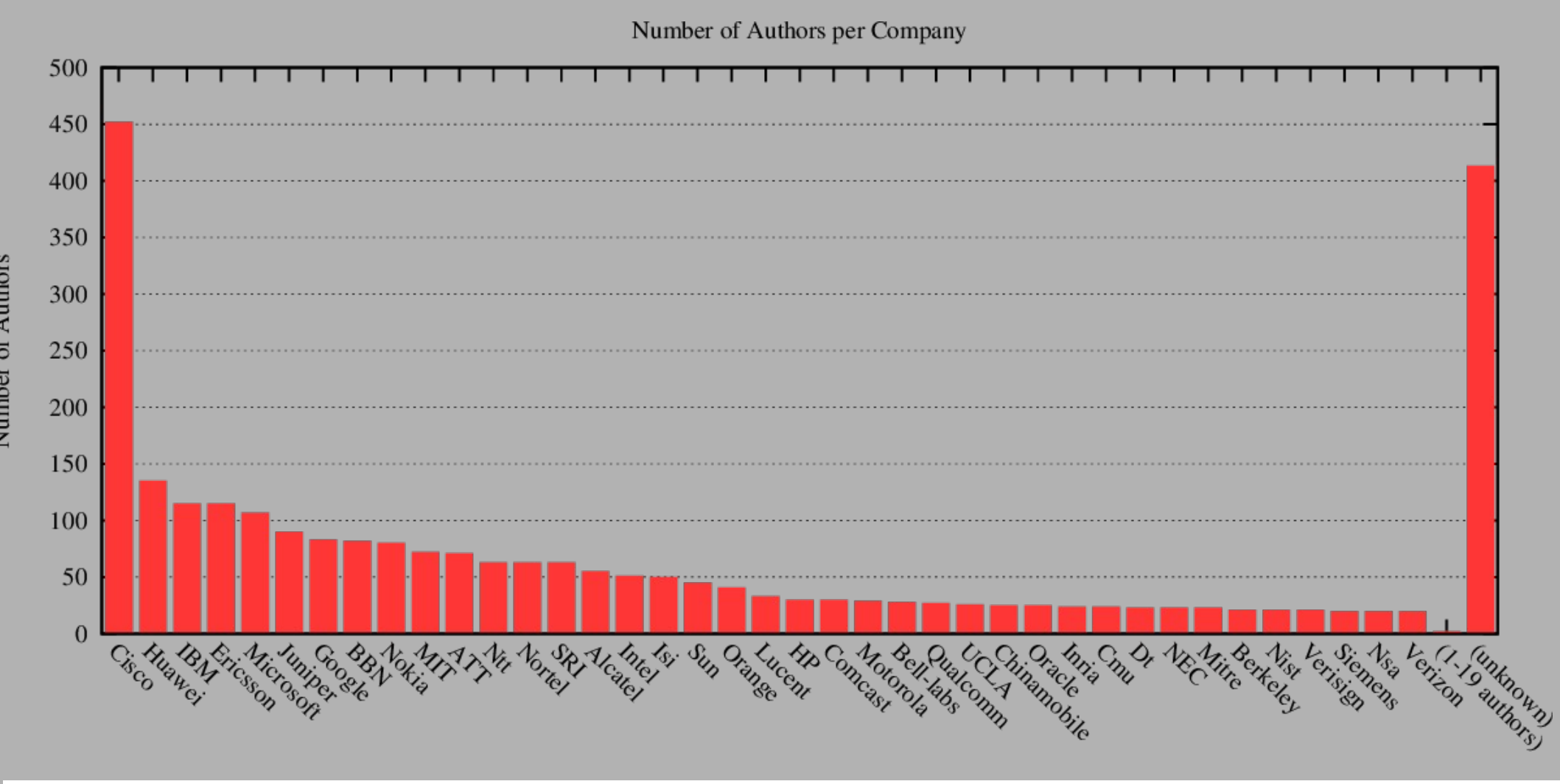


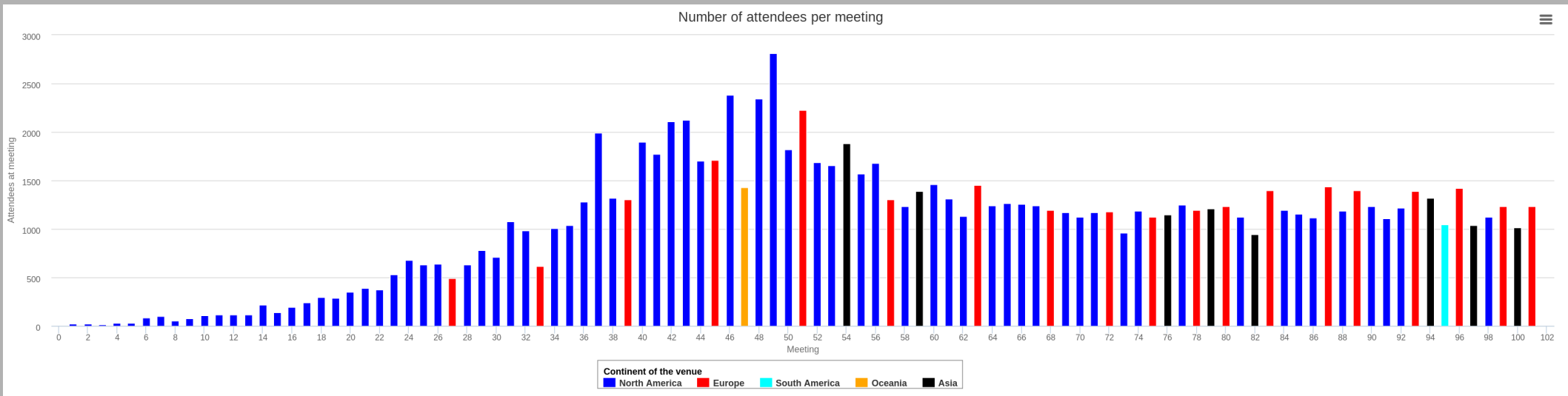
All's well that end(-to-end)s well?

- Only large effort by a transnational corporation with significant control of the network could make this evolution, and change affordance structure
- NAT directionality is still in place, equality of nodes is by no means restores
- With ubiquitous encryption it is harder to analyze on the network (for researchers as well)
- Network operators are not pleased

Imaginaries They Are A-Changin’

‘you need to play in some of the operators or vendors earning models in order to get something deployed’


Number of Authors per Company
Number of Authors
500
450
400
350
300
250
200
150
100
50
0
Cisco
Huawei
IBM
Ericsson
Microsoft
Juniper
Google
BBN
Nokia
MIT
ATT
Ntt
Nortel
SRI
Alcatel
Intel
Isi
Sun
Orange
Lucent
HP
Comcast
Motorola
Bell-labs
Qualcomm
UCLA
Chinamobile
Oracle
Inria
Cmu
Dt
NEC
Mitre
Berkeley
Nist
Verisign
Siemens
Nsa
Verizon
(1-19 authors)
(unknown)


Number of attendees per meeting
Attendees at meeting
3000
2500
2000
1500
1000
500
0
0 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50 52 54 56 58 60 62 64 66 68 70 72 74 76 78 80 82 84 86 88 90 92 94 96 98 100 102
Meeting
Continent of the venue
North America
Europe
South America
Oceania
Asia

‘[m]yths are important for what they reveal (including a genuine desire for community and democracy) and for what they conceal (including the growing concentration of communication power in a handful of transnational media businesses)’

– Vincent Mosco

Conclusions (1)

The sociotechnical Internet architecture imaginary and its self-regulatory governance model have **not been able to safeguard freedom and equality** of researchers, small companies or individuals to innovate on the Internet protocol level.

Permissionless innovation, for the purpose of retaining openness, has undermined itself and the end-to-end principle.

Conclusions (2)

Corporate interests have become a first-order consideration for protocols to be adopted and implemented

Political conceptions of the architectural imaginary are fading into the background.

Conclusions (3)

Explicit values, such as human rights, are only inscribed and upheld in the Internet infrastructure, through its transnational governance, if the value is:

1. *Translatable to the social worlds of all of the significantly represented groups in the governance body, and;*
2. *In the interest of significantly represented groups in the governance body.*

Bonus

$$\left\{\begin{array}{l}\left(\begin{array}{c}interoperability\\resilience\\reliability\\robustness\end{array}\right)=connectivity\\ \left(\begin{array}{c}resilience\\reliability\\confidentiality\\anonymity\\authenticity\end{array}\right)=security\\ privacy\\ content\ agnosticism\\ internationalization\\ censorship\ resistance\\ open\ standards\\ heretogeneity\ support\end{array}\right\}=freedom\ of\ expression$$

$$\left(\begin{array}{c} \textit{connectivity} \\ \textit{decentralization} \\ \textit{censorship resistance} \\ \textit{pseudonomity} \\ \textit{anonymity} \\ \textit{security} \end{array}\right) = \text{right to } \textit{freedom of assembly} \text{ and } \textit{association}$$

$$\begin{pmatrix} anonymity \\ privacy \\ pseudonymity \\ content\ agnosticism \end{pmatrix} = non-discrimination$$

$$\begin{pmatrix} content\ agnosticism \\ security \end{pmatrix} = equal\ protection$$

$$\begin{pmatrix} anonymity \\ privacy \\ security \end{pmatrix} = \text{right to } be\ presumed\ innocent$$

$$\begin{pmatrix} accessibility \\ internationalization \\ censorship\ resistance \end{pmatrix} = \text{right to } political\ participation$$

Internet Research Task Force (IRTF)
Request for Comments: 8280
Category: Informational
ISSN: 2070-1721

N. ten Oever
ARTICLE 19
C. Cath
Oxford Internet Institute

October 2017

Research into Human Rights Protocol Considerations

Abstract

This document aims to propose guidelines for human rights considerations, similar to the work done on the guidelines for privacy considerations (RFC 6973). The other parts of this document explain the background of the guidelines and how they were developed.

This document is the first milestone in a longer-term research effort. It has been reviewed by the Human Rights Protocol Considerations (HRPC) Research Group and also by individuals from outside the research group.

2.1.2.1.5. Internationalization

Question(s): Does your protocol have text strings that have to be understood or entered by humans? Does your protocol allow Unicode encoded in UTF-8 only? If other character sets or encodings are allowed, does your protocol mandate a proper tagging of the charset? Did you have a look at [RFC6365]?

Explanation: Internationalization refers to the practice of making protocols, standards, and implementations usable in different languages and scripts. (see Localization). In the IETF, internationalization means to add or improve the handling of non-ASCII text in a protocol. [RFC6365] A different perspective, more appropriate to protocols that are designed for global use from the beginning, is the definition used by W3C:

> "Internationalization is the design and development of a product, application or document content that enables easy localization for target audiences that vary in culture, region, or language." {{W3Ci18nDef}}

Many protocols that handle text only handle one charset (US-ASCII), or leave the question of what CCS and encoding are used up to local guesswork (which leads, of course, to interoperability problems). If multiple charsets are permitted, they must be explicitly identified [RFC2277]. Adding non-ASCII text to a protocol allows the protocol to handle more scripts, hopefully representing users across the world. In today's world, that is normally best accomplished by allowing Unicode encoded in UTF-8 only.

Example: See localization Impacts:

- Right to freedom of expression
- Right to political participation
- Right to participate in cultural life, arts and science
- Right to political participation

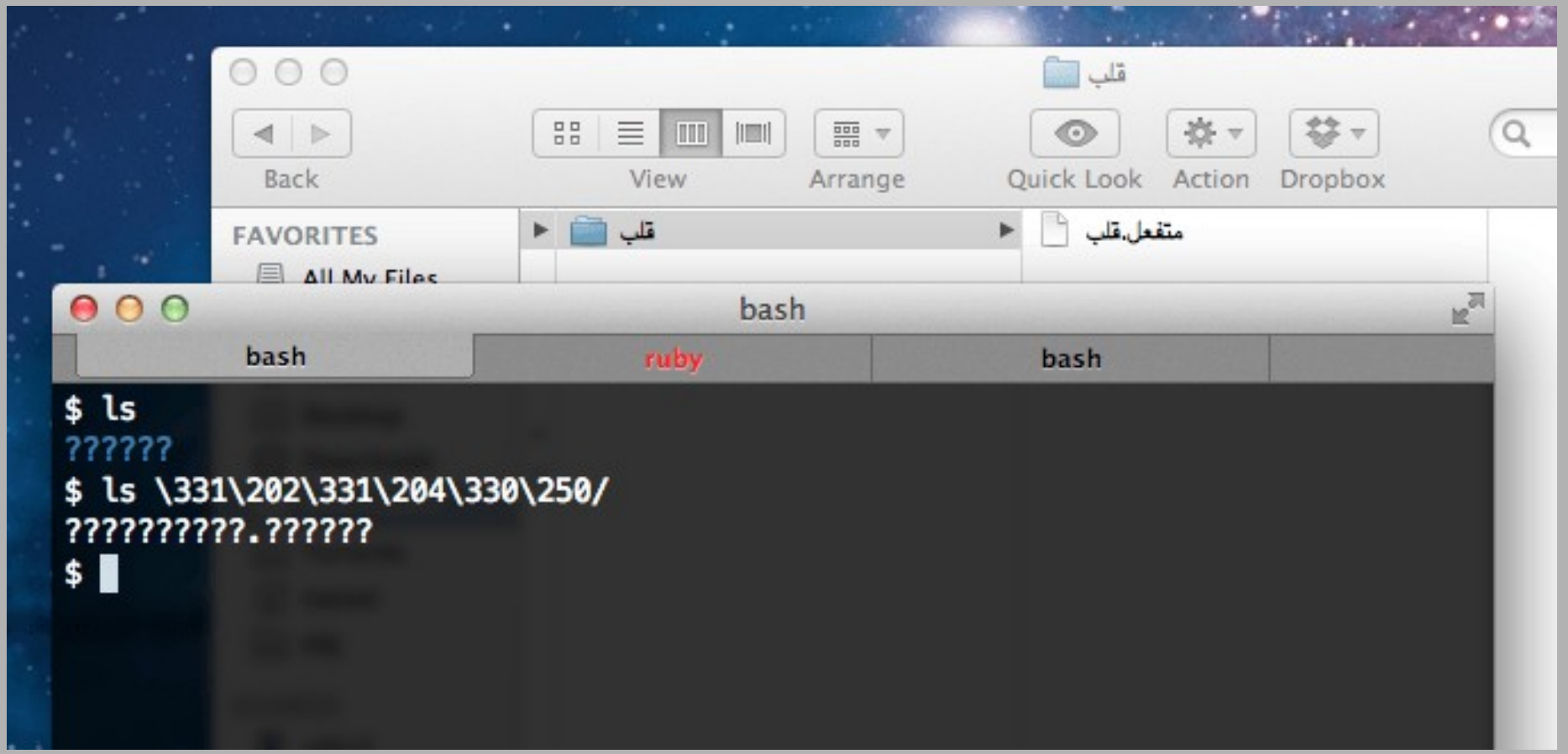
```
; لعبة بونج
; رمزي ناصر، ٢٠١٤
(ابدأ-رسم ٨٠٠ ٦٠٠)
(طريقة-رسم-مستطيلات "وسط")

(حدد نتيجة-لاعب١ ٠)
(حدد س-لاعب١ (طرح (عرض-الرسم) ٢٠))
(حدد ص-لاعب١ (قسم (طول-الرسم) ٢))

(حدد نتيجة-لاعب٢ ٠)
(حدد س-لاعب٢ ٢٠)
(حدد ص-لاعب٢ (قسم (طول-الرسم) ٢))

(حدد س-كرة (قسم (عرض-الرسم) ٢))
(حدد ص-كرة (قسم (طول-الرسم) ٢))
```

Repository Name

قلب

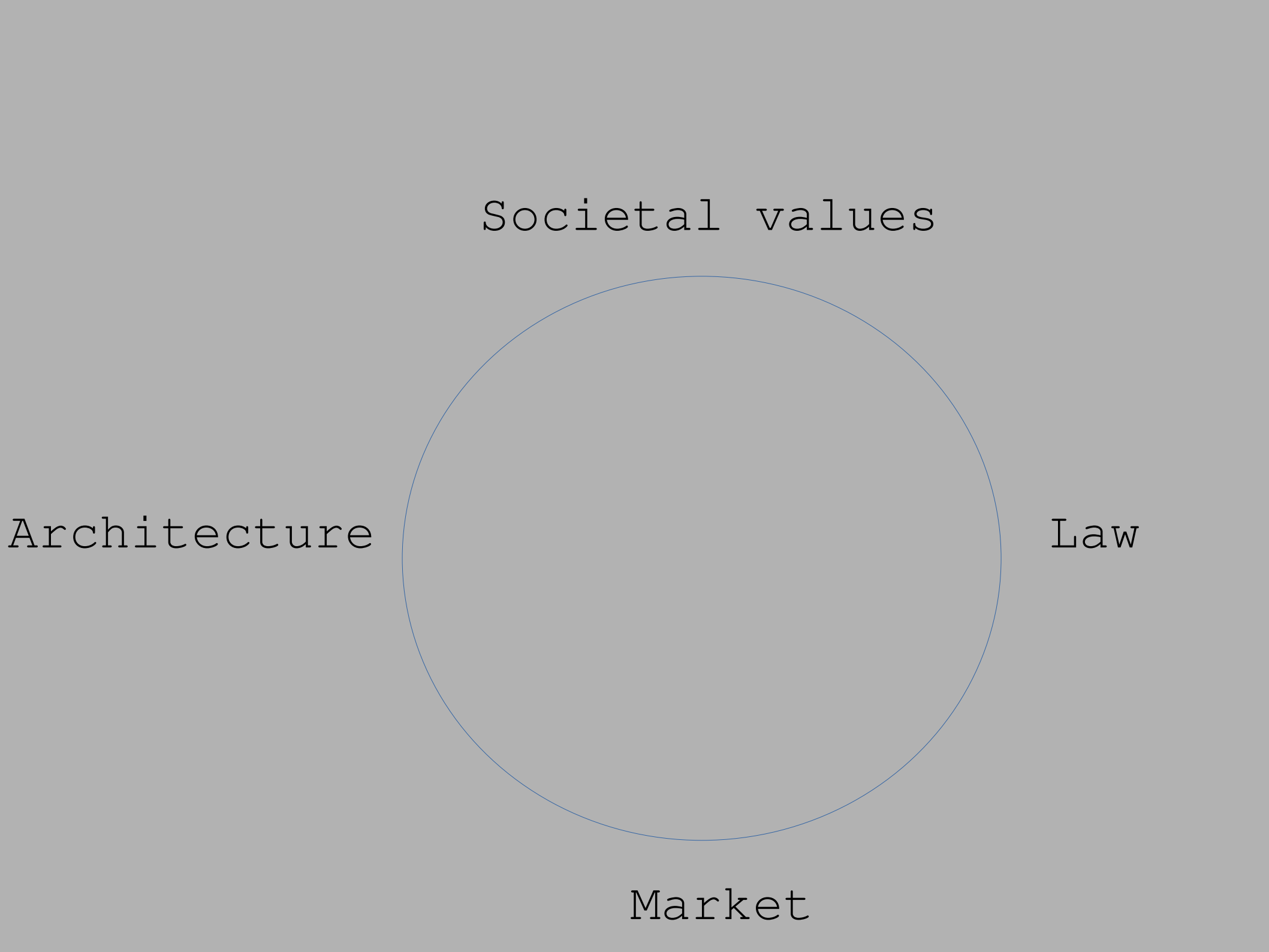
Rename

Will be created as ---



You can and must understand computers NOW.

COMPUTER


Societal values
Architecture
Law
Market

```
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
```