

Can Technology Solve Governance?

Jeffrey Hunker
GTIP
7 December 2010

Jeffrey Hunker Associates © 2010

1

This workshop is about the governance of information in the context of technology (and choices about technology) and policy choices. I'm going to focus on issues of governance of the Internet and inter-networked computer systems, rather than the broader – and more intractable – issues of information governance writ large.

This discussion addresses an issue which I perceive as being either assumed or ignored in discussions of governance.

Some discussions assume that technology will magically provide a path forward for any issue.

Other discussions seem to make an almost opposite assumption – that whatever the Internet protocols do, or don't do (attribution, security) are fixed like laws of nature.

I would challenge both views.

Governance

Definition:

Government

Authoritative direction or control

Webster's New Collegiate Dictionary

Jeffrey Hunker Associates c. 2010

2

Always good to start out with a basic definition.

The point is, we lack authoritative direction or control over the Internet. Whether this is good or bad is a subject of considerable controversy.

Internet IS a City

Vancouver
Circa 2010



3

The Internet has been described in many ways, but it really is a cyber city. We have addresses there, and conduct business and social discourse. Goods move in and out. It has neighborhoods.

We'd like to think of the Internet city as a progressive place.

Internet IS a City

LONDON
Circa 1830



In fact the Internet is a city much like London was in the 1830's --- a vibrant, exciting city, rapidly growing, driven by new technologies.

Early Victorian London was a phenomenon unimagined and unseen ever before – growing from a few hundred thousand population in the late 1700's to several millions in a few decades. It's very size amazed observers – famously one person went up in a balloon to see where London ended and the country began, and couldn't see its edges. This was a shocking realization.

The speed of its growth and transformation was unprecedented in history.

It also was disease ridden, filled with criminals, and both dangerous and smelly. It had no organized police force, and no unified government.

In short, the Internet today is the cyber equivalent to London of this era.

Lessons

Then: Issues of public health, morals, safety

Today: Different stakeholders have interests that conflict (so different from then?)

Technical architecture governs some aspects

Institutional infrastructure and incentives govern other aspects

We have choices about both.

Jeffrey Hunker Associates c. 2010

5

Londoner's were not blind to the problems of the city then, but the proposed solutions were just as controversial then as any discussion of Internet governance today.

Whatever choices we make, however, two observations are relevant.

The technical architecture of our 'city' governs some aspects of its functioning. In London, the absence, and subsequent construction, of a sewer system to replace latrines did much to reduce disease and filth.

Institutional infrastructure and incentives matter too – technical architecture does not solve all problems. London had to create a unified city government, create a police force, and create a public health service, as well as subsequently build the transit system (along with many other changes, such as building codes) in order to become the city we take for granted today.

These observations are relevant for the Internet today.

Technical Architecture Shapes Governance e.g., Security

From DARPA Request for Ideas

DARPA Internet
design principles

Information Assurance Implications

The Internet

must support
multiplexed
utilization of
existing
interconnected
networks.

Interconnectivity and assurability are inherently at odds and must be balanced deliberately, but this topmost priority does not explicitly consider the tradeoff. Moreover, because legacy networks must be incorporated into the design, the required security mechanisms are driven by the limitations of the least capable legacy network.

Internet
communication
must continue
despite loss of
networks or
gateways.

To speak of lost gateways and networks oversimplifies the nature of modern threats. Robustness must be redefined in terms of cyber attack as well as external physical attack or failure. Signals intelligence, infiltration, exfiltration, and malicious control are as important to consider as outright infrastructure loss.

Jeffrey Hunker Associates c2010

6

The Internet protocols used today reflect design choices that were appropriate for its original use. TCP/IP was designed for use by a commune – a community of university researchers who for the most part literally knew each other.

Hence, security of packets, or the attribution of messages were not part of what TCP/IP was designed to care about. As Dave Farber notes, 'we weren't blind to the importance of stuff like security, it's just that we were so focused on getting the damn thing to work at all that the other stuff just wasn't important.'

Technical Architecture Shapes Governance
e.g., Security can be more than window bars



Jeffrey Hunker Associates c 2010

7

Hence, like in 1830's London, Internet security is mostly about putting bars on windows (intrusion detection, firewalls, virus scans) or going about town highly protected (encrypting packets).

Technical Architecture Shapes Governance Desirable Network Capabilities, e.g., ...

- **Addressing (DNS) separates 'trademark' issues from 'addressing' issues**
- **Choice of routing for backbone**
- **Attribution framework for choice**
- **Better facilitates control over access to your resources (security)**
- **Pay for what you use**

Jeffrey Hunker Associates c. 2010

8

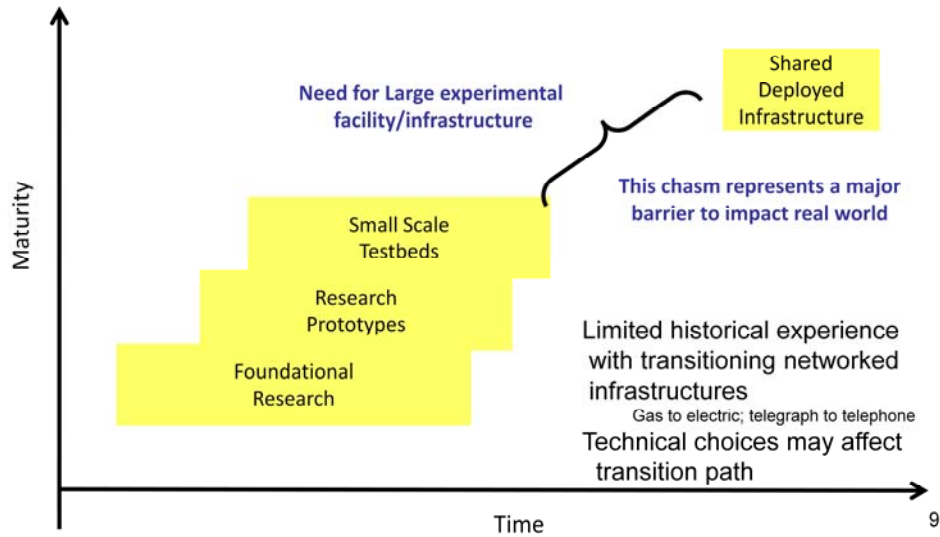
Here are several capabilities that the Internet does not have built in that I (Jeffrey Hunker) would find desirable.

For instance, in the physical world most postal addresses have little or no commercial value (physical location does affect value, but we're talking about the postal address). But on the Internet the equivalent postal address (e.g., sex.com, which apparently just set a record for its value when auctioned) does have potentially enormous value.

Conflicts over the value of Internet addresses would be simpler to deal with if network addressing paralleled that of the physical world – separating the trademark from the actual address.

Or a framework that provided users with a choice as to whether their message would be sufficiently attributed to the sender would then parallel what telephone service offers with caller ID, and caller ID blocking.

Technical Architecture Shapes Governance Build a new Network (1)



Jeffrey Hunker Associates c2010

Today there are numerous R&D programs examining future internetworking protocols, but these initiatives have not spanned the gap towards a system at scale.

Technical Architecture Shapes Governance New Infrastructures Require Vision



 conEdison

Jeffrey Hunker Associates c 2010

10

Along with the history of how the Internet was launched, we have a few examples of how a networked infrastructure actually is rolled out. Edison's leadership in creating what is now the electric grids is a good example.

The lesson is that networked infrastructures do not 'evolve' or grow by individual choice until a certain minimum scale is achieved. Someone (Edison) or some institution (DARPA) has to have the vision and the resources to 'get the infrastructure over the hump' before it has the presence so that individuals can then decide to link to it.

Technical Architecture Shapes Governance Build a New Network (2)

Western Nations Should Build It Out



Edison's Grid



Emergence of State Cyber Power Will Force Action

Jeffrey Hunker Associates c2010

11

I am a strong proponent that a new internetworking infrastructure should be launched to provide users who require security and attribution choice those capabilities.

This new internetworking would not be a replacement for the Internet, but run in parallel.

The national defense communities of the 'Five I's' (US, Canada, UK, Australia, New Zealand) is my proposed community to launch, at scale, a new internetworking. Critical infrastructure providers would be a logical next community to join the new network.

Technical Architecture Shapes Governance Build a New Network (3)

Key Design Principles



- **Modularize along boundaries of potential governance conflict**
- **Design for choice**
 - Make choice visible?

Jeffrey Hunker Associates c. 2010

12

There will always be potential conflicts over network use. In order to make these conflicts more transparent and manageable, governance conflicts should be made explicit (modularized) and the potential for choice – as opposed to hardwiring the technology for one particular governance option – should be provided.

For instance, rather than hardwiring one particular attribution mode (e.g., all messages have x level of attribution) a better system design would provide the sender/receiver pair (or all interested parties) with the opportunity to negotiate or choose among different attribution modes.

An interesting question is whether such choices should be made visible to other network users.

Lessons

Then: Issues of public health, morals, safety

Today: Different stakeholders have interests that conflict (so different from then?)

Technical architecture governs some aspects

Institutional infrastructure and incentives govern other aspects

We have choices about both.

Jeffrey Hunker Associates c 2010

13

Choices of technical architecture may solve some issues, and provide structured choices for others, but do not address all governance issues.

Institutional infrastructure and incentives are, broadly speaking, the way in which societies express and enforce/encourage appropriate choices of behavior.

In the non-cyber world, we have incentives to pay our taxes or obey speed limits (avoid the penalty). We also have the institutional infrastructure (IRS, police) to enforce these incentives.

On a more positive note, we have incentives (the social contract) to wash our hands before eating or handling food, though it is usually only for restaurant employees that these incentives are backed by law.

When considering the governance of the Internet, we have choices about institutional infrastructure and incentives.

Institutional Infrastructure and Incentives Y2K Fix Provides Partial Model

- **No regulations but....**
- **Requirements for public companies to report on their preparations**
- **Widespread high level awareness**
- **True government-private sector command center**



Jeffrey Hunker Associates c2010

14

Preparation for the Y2K event in 1999-2000 rollover was a good instance demonstrating that institutional infrastructure and incentives are not just about the dreaded 'heavy handed government regulation.'

In the run-up to Y2K for instance the US Securities and Exchange Commission (SEC) required only that publicly traded companies report to investors what if any efforts they were making to prepare for Y2k. The SEC did not require any particular action – only that whatever was or was not being done be reported publicly.

As a result of investor concern, most companies took Y2k seriously.

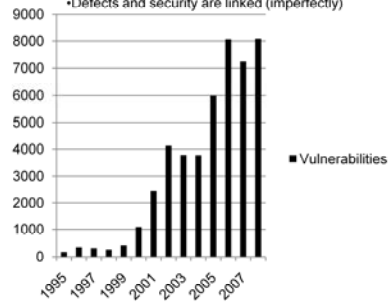
In addition, the US Federal government created a command center staffed by industry representatives as well as Federal officials to monitor, and if necessary coordinate responses to any Y2k events. Participation by industry was voluntary but enthusiastic.

Institutional Infrastructure and Incentives More Secure Software

We KNOW How to Build Better Software

Anecdotal and otherwise, software quality is a problem

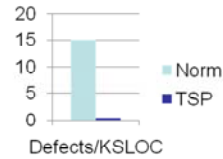
• Defects and security are linked (imperfectly)



Source: CERT/CC

Techniques for defect reduction exist

• Not widely adopted in North America



Source: Software Engineering Institute

Options:

- Federal procurement
- Market based incentives (seals, rating information)
- Regulation

**PRODUCT LIABILITY WOULD
ENCOURAGE BETTER SOFTWARE**

Caution – imperfect knowledge of how to produce quality software
• Microsoft Vista

Jeffrey Hunker Associates c 2010

15

Mistakes or bad design choices in software are a leading cause of cyber insecurity. Mistakes or bad design sometimes leads to security vulnerabilities; in other instances they lead to system failure or unexpected results.

We know how to build better software. That better software is not being produced results from 'the market' as it currently operates not valuing, or being perceived as not valuing, higher quality software.

Policy choices by governments, industry standards boards, and insurers can alter the market.

Governance
Technical Infrastructure
Institutional Infrastructure and Incentives

- Internet today like Dicken's London
- Different stakeholders have interests that conflict
- Technical architecture shapes some aspects
- Institutional infrastructure and incentives shapes others
- We have a choice about both

16

Jeffrey Hunker Associates c 2010

To summarize.

Governance An End to Intellectual Dalliance?

**State sponsored disruptive cyber attacks
becoming a reality**

Not cyber war – CYBER POWER

Implications

- **driver for change (like it or not)**
- **Think about governance in terms of discouraging Chinese actions?**

Jeffrey Hunker Associates © 2010

17

Choices about changes in Internet governance have been talked about, but there has been little or no change in the past decade.

State sponsored disruptive cyber attacks (e.g., against Estonia in 2007) are not new news, and we cannot 'prove' in the public record that they are state sponsored, but the evidence is clear.

It is also clear that these state sponsored attacks will become a more prominent part of the Internet world. Stuxnet illustrates a new phase of such attacks.

The rise of cyber power (state sponsored disruptive cyber attack or the threat of its use) will, I suggest, make changes in Internet governance a matter of national security.

Thus, our window of what I call intellectual dalliance about Internet governance is closing. If we don't choose our future, someone else will.

Governance Good Sources

Code and Other Laws of Cyberspace

**Lawrence Lessig
Basic Books, 1999**

Tussle in Cyberspace: Defining Tomorrow's Internet

**David Clark, Karen Sollins et. Al
SIGCOMM '02. August 2002**

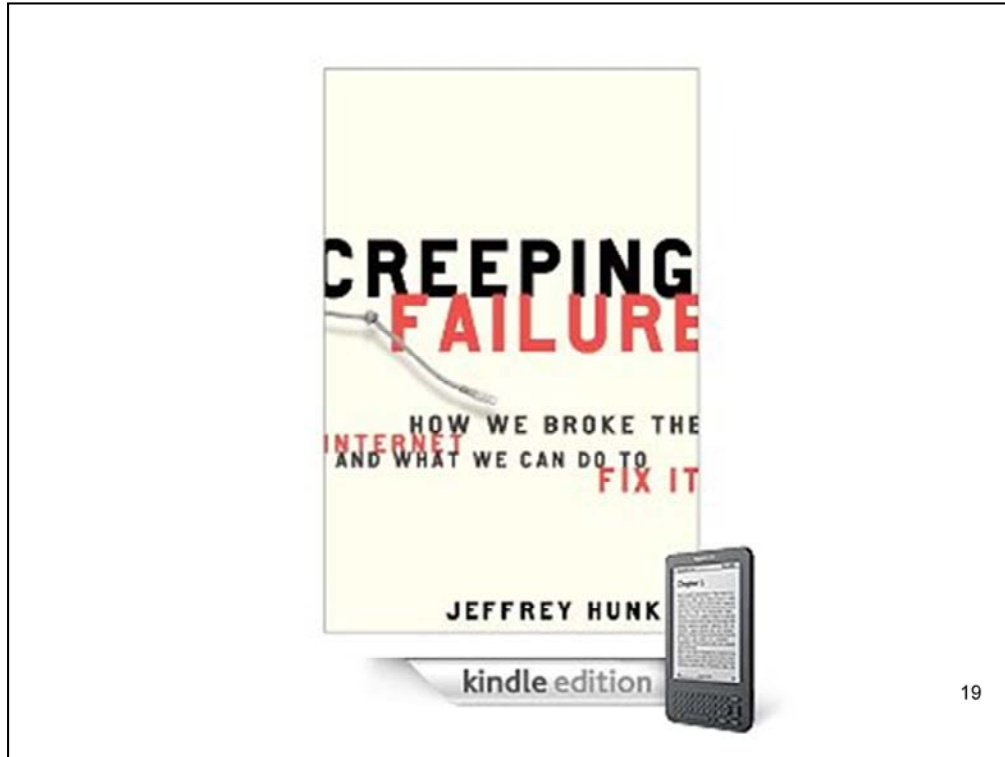
Creeping Failure: How We Broke the Internet and What We Can Do to Fix It

**Jeffrey Hunker
McClelland and Stewart, 2010**

Jeffrey Hunker Associates © 2010

18

Here are good sources on Internet governance that have shaped my thinking, or in the case of my own book (which I recommend that you buy and read) express more fully my own thoughts.



Creeping Failure is available electronically through Amazon Kindle, Kobobooks.com, and Sony Reader Store. It is also available in print.

Published by McClelland and Stewart (Canada) and Random House (US), 2010.

Contact

Professor Jeffrey Hunker

hunker@jeffreyhunker.com

202 257 7778 (mobile)

412 683 7909 (office)

Jeffrey Hunker Associates c2010

20

I'm always happy to talk with you.