Future of the Internet: A Political Perspective

David D. Clark

MIT CFP

October, 2010

Background

- I have talked about non-technical drivers of Internet evolution.
  - A past focus on economic issues and industry structure.
- I want to broaden this discourse.
  - Look at political issues and matters of state.
  - Example: a past talk of mine predicted that ISPs would more and more become the Internet police.

A way to map political concerns

- Three top-level baskets of concerns.
  - Security
  - Economic
  - Social/Community
- Within each basket you find different scopes.
  - Individual
  - Collective
  - State
  - International
  - Global

The map

Basket	Considerations
Security	
Economics	
Social	

Scope	Considerations
Individual	
Collective	
State	
International	
Global	

Using that map

- When you look at a particular problem (e.g. spam, broadband access) or a particular mechanism (e.g. address allocation, freegate), ask what the implications are in each box of that cross-product.

Spam

Basket	Considerations
Security	Nuisance
Economics	Crime, cure is business opportunity
Social	Erosion of trust, email is unreliable

Scope	Considerations
Individual	Get a spam filter
Collective	Move off email
State	Pass a law
International	Discuss at ITU
Global	Private sector institution

Spamhaus

- A private sector, trans-national, bottom-up organization (weakly institutionalized) that has defined and implemented an approach, in cooperation with other organizations (email operators).
- How is this different from vigilantism?
  - Oddly extra-judicial.

Making predictions about outcomes

- Look at examples from history.
- U.S. policy on encryption.
  - NSA blocked export of crypto to slow deployment (security)
  - Privacy folks act out (Zimmerman is threatened with arrest)
  - Commercial interests advocate for encrypted e-commerce (NSA folds).
- Lesson:
  - Economic > security > social in the U.S.

Still true today

- Obama administration on cyber-security
  - Makes cyber-security a campaign plank.
  - Hires Larry Summers.
  - Degrades cyber-czar position to avoid any impact on economic recovery.
  - Disheartened cyber-folks leave Washington
  - Beltway bandits still expect lots of money.

Other example

- Proposed legislation to mandate increased powers to carry out lawful intercept.
- "The bill, which the Obama administration plans to submit to lawmakers next year, raises fresh questions about how to balance security needs with protecting privacy and fostering innovation."
  - NYT, 27 Sept 2010

Larry Lessig Thesis

- Economic + security >> social
- The alignment of economic and security objectives will combine to shift the nature of the Internet to a more controlled and controlling context, at the cost of many social values.
  - See his book Code.

What is going on in Washington

- The not-dead “reasonable network management” debate.
- Spectrum (stay tuned).
- Public sector investment in access.
- Use of deterrence.
- Demand for attribution.
- Rage over industrial espionage.
- Rage over theft of IP (e.g. music).

Deterrence

- A natural reaction.
  - Create a ecosystem that dissuades bad folks from acting.
  - Two approaches (in general)
    - Find them and punish them.
    - Make their behavior unrewarding.

Catch the bad guys…

- "[W]e need to reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment -- who did it, from where, why and what was the result -- more manageable."
  - Mike McConnell, "Mike McConnell on How to Win the Cyberwar We're Losing," Washington *Post,* February 28, 2010.

Attribution

- Key to finding and punishing “bad guys”.
- Leads to calls in D.C. (and elsewhere) for “an accountable Internet”.
  - A idea based on a natural instinct but a serious misunderstanding of technology.
    - “Why don’t packets have license plates?”
  - See a recent paper by Susan Landau and me for a full discussion of this point of view.
- Will present this at panel tomorrow.

Key conclusions

- Packet level personally identifiable information (PLPII) is not useful.
- The important attacks are multi-stage.
  - Need multi-stage traceback.
- Packet addresses are more useful than is sometimes thought.
  - Consider the “copyright police”.
- Cross-jurisdiction issues are central.
  - This is *not* a simple technical problem.

Making attacks unrewarding

- It depends on the motivation of the attacker, of course.
  - Economic (e.g. classic crime).
  - Espionage (can be economic or national advantage)
  - Intentional attacks
    - War, sabotage, terror.

Crime (economic) may be a good target

- Bot-nets are used by criminals
  - DDoS extortion attacks, spam campaigns
- Erode utility of bot-nets.
  - A statistical approach will work.
  - Make it harder to
    - Create zombies
    - Keep control of zombies
    - Send malicious traffic from zombies.

The evil bit—take two

- In 2003, Steve Bellovin wrote an RFC that suggested that all packets sent with malicious intent have a bit in the header that signaled this fact.
  - This was written on first of April.
  - But wait a minute…
- The sender would not do this, but why not the ISP?

The good bit (or the bad bit)

- If an ISP sees that a customer is engaging in inappropriate behavior, it tags its traffic with the “bad” bit.
  - It still sends it.
- Others can choose to discard or limit such traffic.
  - Again, a division of responsibility.
- What if an ISP will not cooperate?
  - Mark all of its traffic as bad.

Design of incentives

- Create an incentive structure that motivates all the actors to do “the right thing”.
- Creates a tool of discipline less drastic than disconnection.
  - Would probably require some discussion at the global level to create an agreement that this was reasonable behavior.

Other forms of discipline

- How could one ISP impose a burden on another apart from disconnecting it?
  - Force it to enumerate all its hosted AS blocks and only accept traffic from those blocks.
    - Need to do this in a way that the "bad" ISP carries all the operating costs.
  - Impose some sort of routing restrictions?
- This sort of thinking is the exact opposite of what we have trained ourselves to do.

Copyright

- Again, the ISPs are being told to be the police/punishers.
  - Three strike rules.
  - Force revelation of identity.
- Tension between the economic and social framing.
- Tension between the collective and the state (or international) scope.
  - Limits to the right of free association.

What is Washington *not* talking about?

- Privacy and individual rights.
  - A bit surprising, given the emerging recognition of behavioral tracking.
- A tension between the economic and the social framing, of course.
  - With respect to advertizing, not yet an international matter.
  - A hint for ISPs: frame their role in positive economic terms.