



Redesigning the Internet: Anonymity or Accountability?

Ira Rubinstein

Senior Fellow, Information Law Institute

NYU School of Law

Center for Cybercrime Studies, John Jay College

November 30, 2009

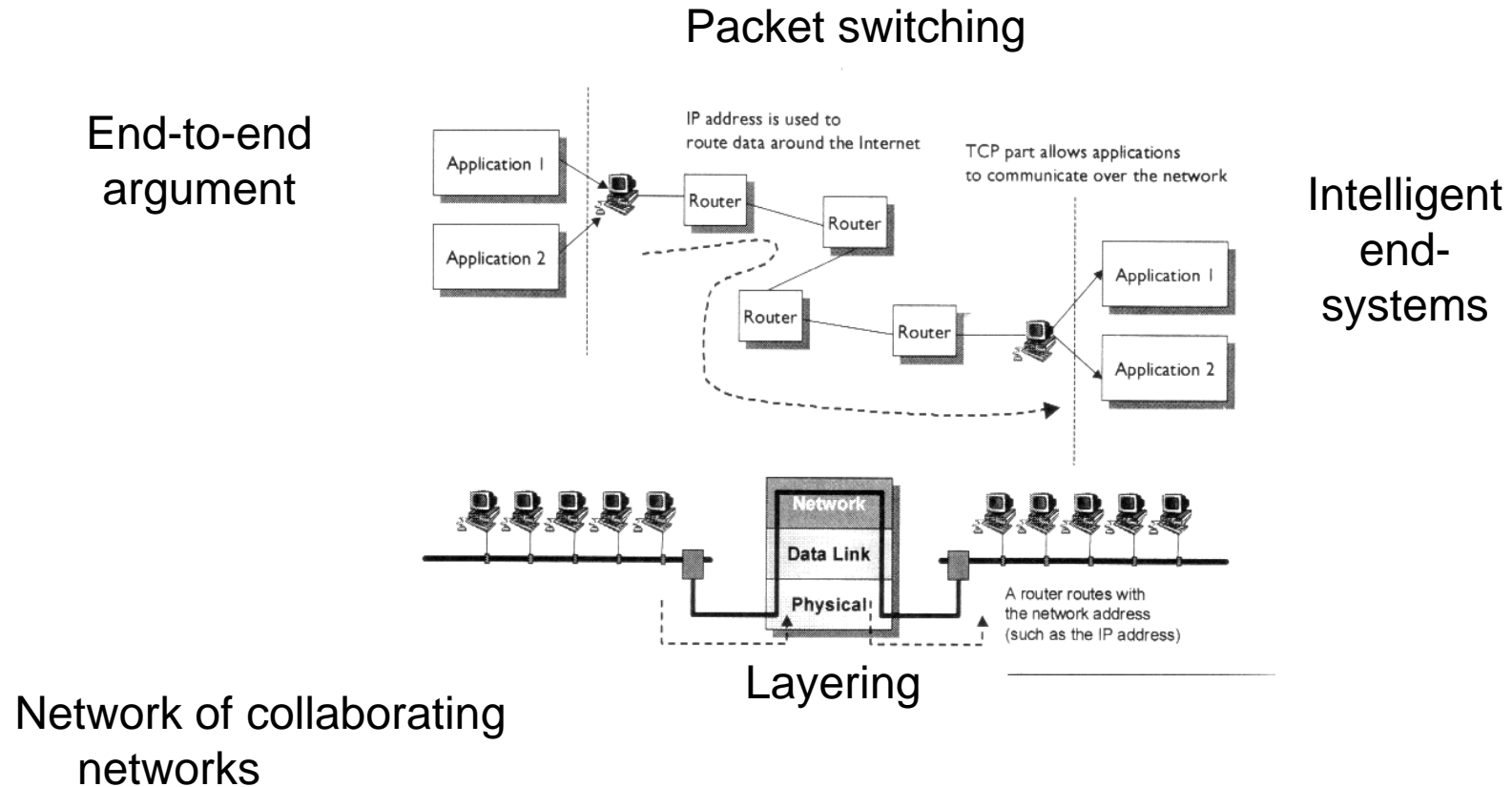


Overview

- Early Internet
- The Evolving Internet
- Accountability in a Future Internet
 - David Clark's Work
- Overcoming Some Objections
 - Lessig
 - Zittrain
 - Privacy and Free Speech Concerns
- Next Steps

Early Internet

- Basic Goal: Connectivity
- Design Principles:





Lack of Security

- Protocols designed for benign and trustworthy environment
- Protocol design assumed that end-points would cooperate to achieve goals
 - Security not “designed in”
 - Little authentication of packets or people
 - Weak identity
- Various efforts to “bolt on” security but with limited success
- Current status:
 - End-host security is weak and end-points are untrustworthy
 - Entire system vulnerable to exploits and attacks



The Social and Political Overlay

- *Open*: Access to all devices, users, services; open standards/open source
- *Innovative*: New (and unanticipated) applications, services, infrastructure
- *Free*: Freedom of expression; no centralized control of services or products
 - Also, specific views on limited government controls and IP rights
 - Often associated with “free software” and “free culture” movements
- *Anonymous?*
 - Anonymity is the given, the default, the substrate
 - Meaning of anonymity
 - Absence of name and address
 - Identity-anonymity continuum
 - Internet anonymity: Levels of privacy protection



Lessig's Regulability Argument

- Code is law--meaning that Internet architecture regulates and constrains its use
- For Lessig, TCP/IP is an “architecture of liberty”
 - This is partly due to the design of TCP/IP, which “reflects both a political decision about disabling control and a technological decision about the optimal network design.”
 - But Lessig fears that business and government will make the Internet more regulable by moving from “a default of anonymity to a default of identification”
 - Why?
 - TCP/IP is “identity-ignorant”
 - But commerce requires security in the form of a trust system (PKI), and government will leverage this change for control purposes of its own
 - So Lessig (writing in 1999) fears an inevitable shift to an “architecture of control”



The Evolving Internet

- Changing Circumstances
 - Vast scale and reliance on Internet as critical infrastructure
 - Lack of security
 - Spam, phishing, DDoS, botnets
 - New threat resources: organized crime, terrorists, state actors
- New requirements
 - Security, reliability and availability
 - “Accountability” and what this means:
 - Common structure consists in three necessary elements: information, standards, and sanctions; also, no accountability without identity.
 - Anonymity minimizes or eliminates accountability
 - Other requirements
- Future Internet
 - Incremental vs. clean slate approach



Accountability via Incremental Approach

- Prevent spoofing
 - Ingress filtering and source-based accountability
 - Host authentication
- Tracking and tracing
 - Use IP addresses to track and trace compromised hosts
 - Data retention
- Revocable anonymity
- Replace IP protocol with Accountable IP (AIP)
 - Self-certifying addresses



Accountability via Clean-Slate Approach

- Future Internet Design (NSF-funded FIND project)
 - Treats security as fundamental
 - Rejects “band-aid” approach and recommends including “appropriate” identity mechanisms
 - Flexible architecture that makes identity available at packet level or end-points as needed
- Next Generation Secure Internet (NGSI)
 - When should identity be visible at the packet level?
 - One approach: Make available an identity field but with no fixed specification



David Clark's work

- Redesign of Internet characterized by “tussles” including anonymity vs. accountability
 - Design should permit variations in outcome
- Mechanisms needed that regulate interactions based on mutual trust
 - Permit users to choose with whom they interact*
 - Permit users to choose the level of transparency
 - Reframe the end-to-end argument in terms of trust (where and between whom trust exists) rather than in terms of physical location
 - Rely on trusted third parties to manage identity, protect end-users from attack or unwanted content, provide mutual assurances, and so on
 - Design for delegation so that end-user controls trust decisions

*See Johnson, Crawford and Palfrey, *The Accountable Internet* (“connect only with...those who have shown they are worthy of your trust”).



Clark on Identity

- Need new role for identity
 - Identity (knowing whom one is communicating with) key to deciding on appropriate level of trust
 - Many design questions for identity at both the network level and the application level
- Preliminary ideas
 - Avoid a single (universal) identity scheme but instead create a framework for talking about identity
 - Permit anonymity but make it visible or at least hard to disguise



Teasing Out the Policy Issues


- Redesigned internet protocols would give a new role to identity and thereby challenge long held views about the relationship between architecture and social and political values
 - Entrenched view (Lessig/Zittrain):
 - Identity undermines civil liberties by enhancing regulability
 - Security enhancements threaten innovation
 - Anonymity highly desirable in preserving/achieving free speech and privacy
 - Emerging view (Clark et al):
 - Accountability is necessary aspect of re-designed Internet
 - Early design principles require certain modifications
 - Goal is to make necessary changes while preserving privacy and free speech



Lessig Redux: Problems

- *Code 2.0* (2006)
 - Lessig reaffirms his argument that “the Net will become increasingly controlled and regulable through digital identity technologies”
 - Notes in passing that recent work on a new identity layer is very promising but this does not allay his fears of increasing regulability
- Problems
 - The design of TCP/IP is *not* the result of any political decision
 - Lessig’s account of TCP/IP as “identity-ignorant” is almost entirely lacking in historical context
 - The default condition of the Internet is *not* anonymity, but weak identity
 - Lessig views security almost entirely through the lens of its secondary effects on regulability, and never as a serious problem in its own right
 - In addressing why government has yet to transform the Net into a regulable space, Lessig mainly defers to Zittrain

Zittrain's "Generative Dilemma"

- Shares Lessig's views on anonymity and regulability but takes security far more seriously
- Primary concern is that malware and related security issues will trigger a fatal shift:
 - *Generative Internet*  *appliance networks*
 - Generativity: "The capacity of technology to produce unprompted change driven by large, varied and uncoordinated audiences."
 - The Internet & PCs are generative; tethered appliances and software –as-service are not
 - Appliances are optimized for specific apps and restrict user and 3rd party modifications, thus permitting "perfect enforcement" and security via "lockdown"
- On this account, security is inversely related to generativity, hence the dilemma



Problems with Zittrain's Resolution

- Either/or analysis
 - Generativity *or* appliances
- But roposed solutions are inadequate
 - Peer-based solutions premised on collaborative action and self-ordering norms: the Wikipedia model
 - Make the Internet more stable for ordinary users
 - Deploy community-based tools
 - Examples:
 - Red-green virtual machines? No
 - StopBadware? Closer to the mark.
 - But unlike Wikipedia, the Internet at large lacks a common ethos and is highly vulnerable to asymmetric threats
- Security that passes a “least harm to generativity” test still may fail at protecting hosts against attack and meeting availability requirements



Other Objections to Re-Designing Network Protocols: Privacy

- Anonymity protects privacy
 - PII/non-PII distinction
 - Anonymity tools combat surveillance
- Counter-arguments
 - Incomplete conception of privacy
 - “Ring of Gyges” scenarios
 - Anonymity tools have very mixed record of success
 - Privacy by design is a better approach
 - This includes “user-centric” identity systems



Other Objections to Re-Designing Network Protocols: Free Speech

- 1st Amend. protects anonymity including anonymous political speech conducted online
 - *McIntyre*: “An author’s decision to remain anonymous,...is an aspect of the freedom of speech protected by the First Amendment.”
 - *McIntyre* in cyberspace
 - Subpoena cases: Unmasking anonymous defendants
 - CDA/COPA
 - False identity cases
 - *ACLU v. Miller*
 - *Jaynes v. Comm. of Virginia*



Counter-arguments

- *McIntyre*
 - Language of opinion is equivocal
 - Anonymity or pseudonymity?
 - Confronting the enforcement dilemma
- *McIntyre* in cyberspace
 - Subpoena cases rely on balancing tests
 - CDA/COPA cases consider impact of age verification devices on free speech w/o recognizing right to anonymity
 - *Miller* construes a badly drafted statute
 - *Jaynes* misconstrues the relevant technology and arguably uses the wrong standard of review
- State action issue
 - What if re-design of Internet results from open standards process rather than government mandate?



Conclusion: A Few Next Steps

- Treat security as a core aspect of any future Internet design; this includes acknowledging a new role for identity
- Evaluate any identity-based solutions against the following criteria:
 - Are there equally effective alternative solutions that avoid the privacy/free speech concerns associated with identity?
 - If a solution requires identity, do identity applications suffice or is it necessary to build identity into the network?
 - If a solution relies on identity at the network level, what are the social implications?
 - How does any new identity-based capability play out in both democratic and repressive societies?
 - How do these capabilities fare against Zittrain's perfect enforcement scenarios?



Bibliography

- S. Bellovin, D. Clark, A. Perrig and D. Song, Clean Slate design for the Next-Generation Secure Internet (2005)
- M. Blumenthal and D. Clark, Rethinking the Design of the Internet: The End to End Arguments vs. the Brave New World, *ACM Transactions on Internet Technology (TOIT)*, v.1 n.1, p.70-109 (Aug. 2001)
- David D. Clark, Marjory S. Blumenthal End-to-end Arguments in Application Design: The Role of Trust (2004)
- David D. Clark, Requirements for a Future Internet: Security as a Case Study, (December 2005)
- Anja Feldmann, Internet Clean-Slate Design: What and Why? *ACM SIGCOMM Computer Communication Review*, July 3, 2007
- D. Johnson, S. Crawford & J. Palfrey, Jr. The Accountable Internet: Peer Production of Internet Governance, 9 *Va. J. L. & Tech.* 9 (2004)
- Lawrence Lessig, *CODE AND OTHER LAWS OF CYBERSPACE (1999) and CODE 2.0 (2006)*
- Jonathan Zittrain, *THE FUTURE OF THE INTERNET AND HOW TO STOP IT (2008)*