ARTICLE

# TRUST AND ONLINE INTERACTION

JUSTIN (GUS) HURWITZ[†]

[†] Fellow, Center for Technology, Innovation and Competition, University of Pennsylvania Law School. This project has benefitted from the input of several individual and workshop commentators. Particular thanks are due to Jerry Kang, Peter Swire, and the editors of the *University of Pennsylvania Law Review*. The initial idea for this project stems from conversations with Christopher Yoo about the noncontractability of nonverifiable interactions. All errors or omissions are of course my own, unless they can be unprovably attributed to an unaccountable online intermediary.

## INTRODUCTION

> Of all the changes that are transforming the Internet, the loss of trust may be the most fundamental. . . . [T]he simple model of the early Internet—a group of mutually trusting users attached to a transparent network—is gone forever.[1]

The Internet's early architecture was built on a foundation of trust. From its inception in the 1960s through commercialization in 1993, the Internet was a relatively simple network that was designed, constructed, and used by a relatively small community of research and governmental institutions with broadly aligned incentives. In the decade following commercialization, even as these institutions gave way to diverse commercial interests, trust remained an organizing principle—the personal ties of technologists and their largely shared vision of a technological future drove use, investment, and research.

This trust-based architecture is quickly giving way to a post-trust future, however. As the Internet has matured, its architecture, uses, and the interests of its architects and users have become increasingly diverse and complicated. During the Internet's early development, a meaningful number of its users knew and cared how the Internet worked. They were vested in contributing to its development. This is no longer the case. Rather, the Internet now facilitates myriad private interests that may or may not be aligned with the social interests of the developing Internet architecture.

This transition from the Internet as a community with a common purpose to the Internet as a platform that supports myriad, often conflicting, private interests is not necessarily a bad thing. Many communities are founded with a common purpose that allows their members to rely on informal, trust-based mechanisms to respond to, or avoid the need to respond to, conflicts. As these communities grow, their informal mechanisms give way to more formal ones. It is unsurprising that the Internet would follow a similar trajectory.

This Article considers one of the challenges of this evolution: the role of intermediaries' liability for the harm they cause to users. All online interactions

[1] Marjory S. Blumenthal & David D. Clark, *Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World*, 1 ACM TRANSACTIONS ON INTERNET TECH. 70, 93 (2001).

are conducted through intermediaries—the routers, servers, applications, services, and switches that make up the Internet's "core." In the era of the trust-based Internet, intermediaries were largely passive participants in the technological ecosystem. This limited both the harm they could cause and the basis for liability against them. In today's Internet, intermediaries are increasingly active; they make real-time decisions about how to handle user data, and they have the ability to store or share that data for private purposes. In the post-trust Internet, intermediaries can cause real harm. Without trust, it remains unclear which institutions, if any, safeguard users from such harm.

This Article's focus differs from that of previous work in this area. Many scholars have considered the role of liability for Internet intermediaries, but their work has generally focused on using intermediaries to redress harms *caused by users*.[2] For instance, to what extent should an intermediary be considered a speaker for moderating (or not) harmful speech? Or, should intermediaries be vicariously or indirectly liable for the illegal acts of users? Should payment intermediaries be liable for curtailing certain classes of illegal activity? Scholars have previously addressed questions such as these when considering intermediary liability.

As the role of active intermediaries continues to expand, liability for harm that intermediaries themselves cause is increasingly significant. There are two basic reasons for this. First, users lacking the ability to seek recourse may demand that active intermediation *not* be used. Regulatory and proposed statutory responses to network neutrality and privacy concerns are early examples of such demands. If the technology can, in users' estimation, harm them in ways against which they cannot protect themselves, users will be reluctant to embrace such technology—even if it is otherwise beneficial.

Second, the dearth of non–trust based enforcement mechanisms will reduce the supply of active intermediation technologies. This is a second-order effect driven by a lack of demand: if users are unable to hold intermediaries accountable for harms they may cause, users will be less willing to

[2] *See generally* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221 (2006); Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 WM. & MARY L. REV. 239 (2005); Joel R. Reidenberg, *States and Internet Enforcement*, 1 U. OTTAWA L. & TECH. J. 213 (2003–2004); Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653 (2003). Peter Swire's work is one exception, but this Article's analysis, unlike that of Professor Swire, does not consider the role of intermediaries with respect to the viability of bilateral negotiations between users. *See generally* Peter P. Swire, *Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet Privacy*, 54 HASTINGS L.J. 847 (2003).

use those intermediaries' services. This reduces demand, and therefore will reduce the quantity of active intermediation services offered, including research and development of new services.

Both of these problems are rooted in the transition away from trust-based interactions. In the trust-based Internet, there was little concern that active intermediation would be used to users' detriment. In the post-trust Internet, users cannot embrace active intermediaries without assurances that their data will be handled in accordance with their expectations. This Article argues that the availability of legal recourse plays an important role in establishing such assurances, both by providing an avenue of redress when expectations are frustrated and by creating incentives to develop technologies that enable lower-cost mechanisms to this end.

Whatever the form taken by the role of liability, its transformation complements ongoing efforts to address the concerns generated by active intermediation. Both regulation and ongoing technological development shape what intermediaries can do as well as what they actually do. But it is doubtful that regulation and technology alone can protect users from harmful intermediation; adding recourse to the courts may help to advance the goal of protecting users from harmful intermediation.

This Article proceeds in four parts. Part I considers the role of trust in the early Internet, how the evolving Internet is moving away from this trust-based model, and how the loss of trust affects and limits online institutions.

The Internet is not the only institution that operates without trust. Many institutions already operate in such an environment. Part II looks to how other institutions function absent trust. These institutions' approaches fall into three categories: vertical integration; reliance on internal mechanisms to enable trust-like interactions (e.g., reputation, encryption); and reliance on external mechanisms to enable trust-free interactions (e.g., legal institutions).

Part III considers the limitations and lessons from these standard approaches and synthesizes them into a set of principles for establishing intermediaries' liability. Each approach suggests ways that a post-trust Internet might operate, but the Internet's architectural characteristics also present certain challenges. The Internet is designed to accommodate myriad independent actors, making widespread integration among intermediaries unviable. Those intermediaries are also supposed to operate transparently to users, which presents additional challenges to legal institutions. These two design principles—independence and transparency[3]—present fundamental technical challenges to any mechanism designed to facilitate interactions between parties that do not trust each other.

The institutional constraints that result from the Internet's architectural characteristics suggest two separate goals for the law: (1) establishing liability for intermediaries that may cause harm to users and (2) creating incentives to influence the ongoing evolution of underlying technology in ways that may overcome these fundamental technical challenges. Part IV considers both of these goals and presents a framework to assess which legal rules should apply based upon the capabilities of the underlying technology. Under this framework, today's intermediaries would be governed by broad liability rules with the burden on intermediaries themselves to prove that they have not harmed users. As technology develops, however, this framework may give users greater control over how their data is used, such that intermediaries would be better governed by property rules with burdens placed on users to control their own data. Such an approach provides technologists with a menu of options, enabling them to understand the legal consequences that may follow from technical design decisions.

## I. TRUST LOST

This Part considers three topics: the role of trust in the early Internet, how the evolving Internet is moving away from this trust-based model, and how the loss of trust affects and limits online institutions.

### A. *What is Meant by Trust*

Scholars of various stripes often speak about the role of trust on the Internet.[4] In this and other areas of scholarship, the term "trust" often goes

[3] Blumenthal and Clark's article captures the role of transparency. *See supra* note 1, at 93. Independence follows from the Internet's design as an "internetwork" or "network of networks." *See generally* Brian Carpenter, *Architectural Principles of the Internet*, (Internet Eng'g Task Force (IETF) Network Working Grp., Request for Comments (RFC) No. 1958, 1996), *available at* http://www.rfc-editor.org/rfc/pdfrfc/rfc1958.txt.pdf. *See also* Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME L. REV. 815, 819, 878 (2004) (discussing the centrality of transparency to the Internet); Richard S. Whitt, A Deference to Protocol: Fashioning a Three-Dimensional Public Policy Framework for the Internet Age at 20-26 (Sept. 17, 2012) (unpublished manuscript) (on file with author) (discussing Internet design principles including how end-to-end design and connectivity demonstrate independence while modularity and layering demonstrate transparency).

[4] *See generally* Blumenthal & Clark, *supra* note 1; Ed Gerck, *Trust as Qualified Reliance on Information*, COOK REP. ON INTERNET PROTOCOL, Jan. 2002, at 19; David R. Johnson, Susan P. Crawford & John G. Palfrey, Jr., *The Accountable Internet: Peer Production of Internal Governance*, 9

undefined.[5] Despite this trend, it is useful to consider the meaning of trust at the outset of this discussion.

In its most pithy form, this Article takes trust to mean "reliance without recourse." That is, one person trusts another when she relies on that other person in a way that exposes her to harm, but does so under circumstances where she has no recourse available should that harm come to pass. This meaning falls within a core concept of trust common to many authors.[6]

More importantly, this definition captures the idea animating most discussions of online trust—an intangible and important coordinating

VA. J.L. & TECH. 1 (2004); Helen Nissenbaum, *Securing Trust Online: Wisdom or Oxymoron?*, 81 B.U. L. Rev. 635 (2001).

[5] Blumenthal & Clark, *supra* note 1; David D. Clark et al., *Tussle in Cyberspace: Defining Tomorrow's Internet*, 13 IEEE/ACM TRANSACTIONS NETWORKING 462 (2005); Johnson et al., *supra* note 4. The greatest exception is those articles that do take the meaning of trust, as opposed to the role of trust, as their primary topics. As discussed generally by Rebecca Bratspies,

> In light of the vast number of trees killed to publish psychological, economic, and sociological studies on the topic, trust's continued elusiveness seems surprising. Part of the problem may be that the term is used colloquially in many different contexts, and researchers from many different fields rely on an intuitive understanding of the term. . . . Indeed there is an ongoing debate within scholarly circles over the meaning of the term "trust," and there is still no consensus definition.

Rebecca M. Bratspies, *Regulatory Trust*, 51 ARIZ. L. REV. 575, 588-89 (2009); *see also* Gerck, *supra* note 4, at 21 (noting that "there are also 'poetic' or 'everyday' uses of the word trust that permeate some [computer] security work and Internet communication protocols"); Oliver E. Williamson, *Calculativeness, Trust, and Economic Organization*, 36 J.L. & ECON. 453, 453, 463-69 (1993) (observing that "'trust' is a term with many meanings" and examining the relationship between trust and commercial exchange).

[6] *See* Bratspies, *supra* note 5, at 589 (identifying scholarly convergence on a definition of trust as "a willingness to accept vulnerability under conditions of uncertainty"); L. Jean Camp et al., *Trust: A Collision of Paradigms* ("People's decisions to trust computers may be affected by their perceptions of the difference between computers and humans in error making and acting with guile. It is a commonly held belief that computers only replicate human error and that computers can be easily monitored to find the source of error. Also, most individuals do not perceive computers are able to act with guile."), *in* FINANCIAL CRYPTOGRAPHY: 5TH INTERNATIONAL CONFERENCE, 2001, at 91, 97 (Paul F. Syverson ed., 2001); Nissenbaum, *supra* note 4, at 643-46 (warning that without sufficient trust in online services, people will be reluctant to make use of such resources in part due to the increased exposure to harm); Larry E. Ribstein, *Law v. Trust*, 81 B.U. L. REV. 553, 555, 556-58 (2001) (defining trust as "the willingness to make oneself vulnerable to another without costly external constraints"); *see also* JAMES S. COLEMAN, FOUNDATIONS OF SOCIAL THEORY 111 (1990) ("[I]t is to the trustor's interest to create social structures in which it is to the potential trustee's interest to be trustworthy, rather than untrustworthy."); Timothy L. Fort & Liu Junhai, *Chinese Business and the Internet: The Infrastructure for Trust*, 35 VAND. J. TRANSNAT'L L. 1545, 1551 (2002) ("Trust always entails at least one party being vulnerable to the actions of another, and that party therefore depends upon, relies on, or trusts the other party not to exploit that vulnerability."); Russell Hardin, *The Street-Level Epistemology of Trust*, 21 POL. & SOC'Y 505, 505 (1993) ("[Y]ou trust someone if you have adequate reason to believe it will be in that person's interest to be trustworthy in the relevant way at the relevant time.").

principle that facilitated interactions on the early Internet, but one that is decreasingly viable as a coordinating principle today. Trust was the factor that, in the "simple model of the early Internet," allowed "a group of mutually trusting users attached to a transparent network" to work as a community toward the common goal of developing the network—and this is the thing that "is gone forever."[7] In the early iteration of the Internet as described by David Clark, users could rely on one another without fear of being harmed; they had no need to consider whether avenues of recourse were available. Similarly, users were sufficiently aware of the relatively simple network's operational principles so that they did not fear harm from the network itself.

However, as the network has grown in complexity and as users' interests have grown more diverse, the possibility of harm has grown as well. As harm has become a concern, so too has the need for protection from that harm. Absent the availability of recourse against such harms, users must alter their behavior to protect against them.

Trust is therefore a variable on two sides of an equation. Users' trust in the Internet affects their willingness to rely on the Internet. The extent of that trust mirrors their ability to secure recourse against harm: recourse increases users' willingness to accept the risk of incurring those harms. Increasing trust decreases the need for available avenues of recourse, while decreasing trust decreases the extent to which users will rely on the Internet if there is no offsetting increase in the reach of available recourse.

### B. *The Early Internet*

The early Internet was developed by a small community of researchers with a common goal: to make the technology work.[8] Protocols and applications were

[7] Blumenthal & Clark, *supra* note 1, at 93; *see also* J. Kempf & R. Austein, *The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture* 6 (IETF Network Working Grp. RFC No. 3724, 2004), *available at* http://www.rfc-editor.org/pdfrfc/rfc3724.txt.pdf ("Blumenthal and Clark . . . make the point that the Internet originally developed among a community of like-minded technical professionals who trusted each other, and was administered by academic and government institutions who enforced a policy of no commercial use. The major stakeholders in the Internet are quite different today."); Christopher S. Yoo, *Beyond Coase: Emerging Technologies and Property Theory*, 160 U. PA. L. REV. 2189, 2213 (2012) ("Commentators widely recognize that the universe of Internet users can no longer be characterized as the type of 'close-knit community' needed for social norms to arise.").

[8] *See Internet Governance Not Scaling Well*, 6 COOK REP. ON INTERNET PROTOCOL, Sept. 1997, at 1, 1 ("In the 1970s and 80s American researchers developed a technology to support the functioning of an arcane computer network. It was a small community where everyone knew each other. For twenty five years it did things with a hand shake and a documentation system that supported a rough consensus of its engineers as the direction in which to push further development.

developed to accomplish technical ends without thought to securing them against malicious use. In general, the idea that the technology had to be secured against such misuse was secondary, if present at all.[9] The reason for this is simple: while such misuse could happen, there was no concern it that *would* happen.

This mentality thrived—and helped the Internet thrive—throughout most of its early history. The scale of the network aided this mentality. Throughout most of the 1980s, there were fewer hosts connected to the entire Internet than computers connected to the internal networks of many companies today.[10] By the late 1980s, there were only a few hundred networks connected to the Internet backbone, then operated by the National Science Foundation (NSF) as NSFNET.[11] Any problems that occurred could be handled by individuals who knew each other professionally and sometimes even socially.[12]

Similarly, the Internet's early technology and architecture were simpler. Most of the Internet's history has been dominated by two basic types of applications: data transfer and text-based interactive communication. These applications have relatively straightforward technical requirements, and

They called it the Internet."); *see also* KAREN D. FRAZER, NSFNET: A PARTNERSHIP FOR HIGH-SPEED NETWORKING, FINAL REPORT (1987-1995) at 20-26 (1996), *available at* http://www.merit.edu/documents/pdf/nsfnet/nsfnet_report.pdf (detailing the history behind the creation of a national backbone service).

[9] Security has often been an afterthought in the development of new technology. *See, e.g.*, United States v. Morris, 928 F.2d 504, 505 (2d Cir. 1991) (discussing the 1988 Morris Worm where "[t]he goal of this program was to demonstrate the inadequacies of current security measures"); W. Eddy, *TCP SYN Flooding Attacks and Common Mitigations* 2 (IETF Network Working Grp. RFC No. 4987, 2007), *available at* http://www.rfc-editor.org/rfc/pdfrfc/rfc4987.txt.pdf ("The TCP SYN flooding weakness was discovered as early as 1994. . . . Unfortunately, no countermeasures were developed within the next two years."); KEMPF & AUSTEIN, *supra* note 7, at 6 ("Because the end users in the Internet of 15 years ago were few, and were largely dedicated to using the Internet as a tool for academic research and communicating research results[,] . . . trust between end users . . . and between network operators and their users was simply not an issue in general."); *see also* Ashwin Jacob Mathew & Coye Cheshire, The New Cartographers: Trust and Social Order Within the Internet Infrastructure (2002) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1988216 ("Since network administrators often knew one another personally, and trusted their peers . . . there was no need anticipated for security in the protocol."); Tim Moors, A Critical Review of "End-to-End Arguments in System Design" (2002) (unpublished manuscript), *available at* http://www2.ee.unsw.edu.au/~timm/pubs/02icc/published.pdf (discussing congestion, "it is naive in today's commercial Internet to expect end-points to act altruistically").

[10] *Internet Host Count History*, INTERNET SYSTEMS CONSORTIUM, https://www.isc.org/solutions/survey/history (last visited Apr. 10, 2013).

[11] *See* FRAZER, *supra* note 8, at 25 (noting that in 1988, there were approximately 170 networks connected online); *see also id.* at 5 (noting that there were 217 networks connected in July of 1988).

[12] *See* Mathew & Cheshire, *supra* note 9, at 9-12 ("The social groups . . . were tightly knit.").

neither is extremely sensitive to minor variations in performance: where problems did arise, they could be addressed by simply increasing the capacity of congested links.[13] At the same time, the architecture of the early Internet was relatively simple. As of 1988, for example, the NSF provided a single, nationwide Internet backbone that interconnected regional networks at a small number of network access points.[14] This presented a straightforward, hierarchical model of the Internet—one that remained dominant during the Internet's commercialization in 1993 and transition away from NSFNET in 1995.[15]

Like a simple machine in which one can see all the moving parts, it was relatively easy for users to trust this basic model of the Internet. It was simple enough that almost any engineer could understand it, and when problems occurred, they were relatively easy to identify and address. If these problems required the help of others, that help would be forthcoming, in part because the hierarchical structure of the network created a clear division of responsibility, and in part simply because everyone shared the common goal of making the network function.

In fact, trust was a necessity in the early days of the Internet. Many of the current tools used in response to trust-related concerns were not viable in the early days of the Internet. For instance, the encryption technology that is used to secure online transactions ("public-key" encryption) was unknown to the public before 1976.[16] And, prior to the 1990s, even to the

[13] *See, e.g.,* Susan R. Harris & Elise Gerich, *Retiring the NSFNET Backbone Service: Chronicling the End of an Era*, CONNEXIONS, April 1996, at 2, 3-9 (discussing the upgrade of the NSFNET backbone from T1 to T3 circuits in order to increase the capacity on the backbone connections). It was not until the rise of high-bandwidth interactive applications, such as interactive voice, massively multiplayer online gaming, or video-on-demand services, that something more than additional capacity was necessary to ensure the network provided sufficient resources to all applications sharing it. *See infra* notes 27, 53 and accompanying text.

[14] *See, e.g.*, Harris & Gerich, *supra* note 13, at 2 ("The first NSFNET . . . backbone . . . linked the six nationally funded supercomputer centers and seven mid-level networks.").

[15] *See id.*

[16] The current version of the Internet Protocol used across most of the Internet, IPv4, was developed from 1977 through 1981. *See* Jon Postel, *Internet Protocol: DARPA Internet Program Protocol Specification* 1-3 (IETF Def. Advanced Research Projects Agency RFC No. 791, 1981), *available at* http://www.rfc-editor.org/rfc/pdfrfc/rfc791.txt.pdf (describing the Internet system developed by the Department of Defense and citing to sources from the late 1970s). This system built upon the work of Vinton G. Cerf and Robert E. Kahn. *See* Vinton G. Cerf & Robert E. Kahn, *A Protocol for Packet Network Intercommunication*, 22 IEEE TRANSACTIONS ON COMM. 637 (1974). The principles underlying public-key encryption were first publicly disclosed in Whitfield Diffie and Marlin E. Hellman's *New Directions in Cryptography*, IEEE TRANSACTIONS ON INFO. THEORY 644 (1976), followed shortly thereafter by R.L. Rivest, A. Shamir, and L. Adleman's *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, 21 COMM. ACM 120 (1978).

extent that the technology was widely known, it was too resource-intensive to be widely used.[17]

### C. *Losing Trust*

The Internet's character began changing in the early 1990s. During the NSFNET era, the NSFNET backbone was the only game in town, and its rules limited use of the Internet to research and education applications.[18] The creation of the Commercial Internet eXchange (CIX) in 1991, however, signaled the beginning of a period of transformation for the Internet.[19] In 1992, Congress passed legislation that allowed the NSF to permit non-research and educational uses, provided that such use would "tend to increase the overall capabilities of the networks to support such research and education activities"—i.e., commercial traffic.[20]

In conjunction with this legislative change, in 1992, NSFNET began winding down its role as the primary Internet backbone provider.[21] In 1993, NSFNET solicited bids from firms to build a nationwide backbone network on a commercial basis, the construction of which began in 1994.[22] On April 30, 1995, the NSFNET backbone was officially shut down.[23]

The decommissioning of NSFNET was part of a broader explosion of the Internet. As the Internet was commercialized, the number of service

[17] *See* Ashar Aziz, *Draft: Simple Key-Management for Internet Protocols* (SKIP) 2 (IETF 1994), *available at* http://tools.ietf.org/pdf/draft-ietf-ipsec-aziz-skip-00.pdf ("[B]oth the protocol and computational overhead of [state-of-the-art encryption] is very high."); *see also* S. Kent & R. Atkinson, Security Architecture for the Internet Protocol 42-43 (IETF Network Working Grp. RFC No. 1825, 1998), *available at* http://www.rfc-editor.org/rfc/pdfrfc/rfc2401.txt.pdf (noting the costs associated with increased security measures); George Apostolopoulos et al., *Securing Electronic Commerce: Reducing the SSL Overhead*, IEEE NETWORK, July/Aug. 2000, at 8, 10-13 (discussing the high overhead of encryption efforts); Diffie & Hellman, *supra* note 16, at 653 ("For cryptographic purposes, typical computational costs must be considered.").

[18] *See* OFFICE OF INSPECTOR GEN., NAT'L SCI. FOUND., REVIEW OF NSFNET 38 (1993), *available at* http://www.nsf.gov/pubs/stis1993/oig9301/oig9301.txt (chronicling the National Science Foundation's regulation of NSFNET).

[19] *See Fallout from the ANS "Proposal" of January 1991*, COOK REP. ON INTERNET PROTOCOL (1993), http://www.cookreport.com/p.part3.shtml (describing the agreement announced at the Internet Service Provider's Workshop held at the United States Congress Office of Technology Assessment on February 14, 1991, regarding the formation of the Commercial Internet eXchange).

[20] Scientific and Advanced-Technology Act of 1992, Pub. L. No. 102-476, sec. 4, § 3, 106 Stat. 2297, 2300 (codified at 42 U.S.C. § 1862(g) (2006)).

[21] *See* Harris & Gerich, *supra* note 13, at 3-4 (chronicling the gradual demise of the NSFNET backbone).

[22] *Id.* at 4.

[23] *Id.* at 4-6.

providers, services, and users grew exponentially.[24] There was also a boom on the equipment side of the business. NSFNET had interconnected networks using general-purpose IBM mainframes with multiple network interfaces.[25] The new Internet was being built on specialized equipment called routers[26]—as the technology continued to evolve, this equipment increasingly included specialized features.[27]

In addition to these technological changes, the most obvious change to the Internet following commercialization of the backbone was the growth in the number of users and uses. The Internet went from adding tens of thousands of users per month to hundreds of thousands of users, driven by an increasing range of applications.[28] Perhaps the most notable of these applications was the World Wide Web, released in 1993.[29] The Web represented two fundamental shifts in Internet use: First, it had mass appeal—anyone could use the Web. Second, it embraced the interconnected nature of the Internet on an unforeseen scale. A single web page could easily pull information from dozens of sources—using dozens of connections—in ways entirely transparent to the user.[30]

The emerging form of the Internet was precisely the Internet that its designers had hoped to prove would be possible. This was only the tip of

[24] *See* FRAZER, *supra* note 8, at 5 ("From 217 networks connected in July of 1988 to more than 50,000 in April of 1995 when the NSFNET backbone service was retired, the NSFNET's exponential growth stimulated the expansion of the worldwide Internet . . . .").

[25] *See id.* at 7-11 (highlighting the contributions of the corporate partners to the NSFNET backbone, particularly the fact that IBM "provide[d] the computing systems for the network, including hardware and software, and MCI . . . provide[d] the underlying telecommunications circuits for the NSFNET").

[26] *See id.* at 18 (recalling the need for "appropriate hardware and software" to supplement the NSFNET backbone, including the need for routers).

[27] *See* James Aweya, *On the Design of IP Routers, Part 1: Router Architectures*, 46 J. SYSTEMS ARCHITECTURE 483, 483-508 (2000) (offering a detailed examination of routers and identifying trends in router design); András Császár et al., *Converging the Evolution of Router Architectures and IP Networks*, IEEE NETWORK, Aug. 2007, at 8, 9-11 (reviewing the architectural developments leading to modern routers); Jim Duffy, *Evolution of the Router*, NETWORK WORLD (Feb. 9, 2009), http://www.networkworld.com/slideshows/2009/020909-evolution-router.html (providing a pictorial account of the development of the router).

[28] *See Internet Host Count History*, *supra* note 10 (enumerating the number of Internet hosts since August 1981).

[29] The technologies underlying the Web were developed over a period of years, but the web's release into the public domain in 1993 is recognized as its birth year. *See* Press Release, W. Hoogland, Dir. of Research, & H. Weber, Dir. of Admin., Eur. Org. for Nuclear Research, Statement Concerning CERN W3 Software Release into Public Domain (Apr. 30, 1993), *available at* http://tenyears-www.web.cern.ch/tenyears-www/Welcome.html (announcing public access to the World Wide Web).

[30] *See* Solum & Chung, *supra* note 3, at 835-42 (discussing "the transparency of the network to applications" despite the "layered architecture" of the Internet).

the iceberg, moreover: over the following decade, driven partially by the growth of consumer grade, high-speed Internet access, the Internet grew in size and complexity at a break-neck pace.[31]

This move away from a network built on "mutually trusting users attached to a transparent network" has continued unabated up to the present moment. The greatest technological change to the Internet architecture during the 1990s was the rise of active intermediaries. Every part of the Internet architecture—from the routers and switches, to the applications and services occupying the edges of the network—is increasingly interconnected. The result, and purpose, of these interconnections is to allow for active intermediation of user data. Routers no longer passively forward datagrams from one network interface to another; they decide to which interface to forward datagrams, and with what priority, based upon the contents, context, or even prior existing state of the packet.[32] Servers no longer provide deterministic responses to client requests, but rather evaluate myriad data, much of which is unavailable to the client, in order to determine which response to provide.[33]

Typical end users seem unaware or unconcerned by the changes discussed above. This is because end-user perception of the Internet's trustworthiness lags behind the network's actual trustworthiness. There are two explanations of this phenomenon. First, sociological literature has found that humans are predisposed to trust impersonal interactions, such as those that occur on the Internet.[34] This predisposition has certainly been a significant factor in facilitating the Internet's current reach. But it is possible, even likely, that the post-trust Internet will disabuse users of this predisposition over time. When the curtain is pulled back, so to speak, it is

[31] *See* Császár et al., *supra* note 27, at 8 ("The elementary network architecture of the ARPANET . . . has grown into a complex network of autonomously operated domains interconnected by a sophisticated inter-domain control infrastructure."); K.G. Coffman & Andrew Odlyzko, *The Size and Growth Rate of the Internet*, FIRST MONDAY (Oct. 5, 1998), *available at* http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/rt/printerFriendly/620/541 (charting the trajectory of public use of the Internet during the 1990s, which included an approximately one-hundred percent annual growth rate).

[32] *Id.* at 9-11.

[33] *See generally* David Plans Casal, Advanced Software Development for Web Applications (unpublished manuscript), *available at* http://www.jisc.ac.uk/uploaded_documents/jisctsw_05_05pdf.pdf. (describing the sophistication of web application frameworks); Barry Doyle & Cristina Videira Lopes, Survey of Technologies for Web Application Development (2008) (unpublished manuscript), *available at* http://arxiv.org/pdf/0801.2618v1.pdf (exploring the development of technologies for the Web and concluding that the lack of uniformity therein stems from the lack of a singular model for such development).

[34] Camp et al., *supra* note 6, at 97 ("Previous research has supported the hypothesis that people are more trusting of computers than of other people.").

unclear what will replace trust in allowing users to feel confident in the network.

Second, the growth of the Internet to date has benefitted greatly from investors' and firms' belief in the platform and their concomitant willingness to shield users from trust-eroding concerns. For instance, average credit card loss rates are about 0.07% for all transactions, but over 1% for online transactions—roughly fifteen times higher.[35] And this problem is likely to get worse over time.[36] Online e-retail transactions represent only about 5% of total domestic retail transactions, a number that is growing at approximately 15% per year.[37] As the volume of transactions continues to grow, so too will the incentives for fraud. It is less clear that Internet-based firms and intermediaries will continue to subsidize these losses.[38]

A converse implication of investors' and firms' belief in the platform is an expectation that the platform will be profitable. To be sure, their interest in developing and operating intermediaries is not altruistic. This marks a fundamental change in the nature of the Internet architecture—prior to commercialization, intermediaries were not operated with a profit motive.[39]

[35] *Compare* Julia S. Cheney et al., *The Efficiency and Integrity of Payment Card Systems: Industry Views on the Risks Posed by Data Breaches*, ECON. PERSP., Fourth Quarter 2012, at 130, 132 (noting loss rates between 0.05% and 0.09% for all transactions), *with* CYBERSOURCE, 2012 ONLINE FRAUD REPORT 1 (approximating 1% loss rates for e-retail transactions). For a comparison of U.S. fraud statistics with those of other nations, see Richard J. Sullivan, Econ. Research, Fed. Reserve Bank of Kansas City, Presentation to the Conference on the Role of Government in Payments Risk and Fraud: Payments Fraud Statistics (Nov. 17, 2011), http://www.frbatlanta.org/documents/news/conferences/11rprf/11rprf_Sullivan.pdf.

[36] *See* Sullivan, *supra* note 35.

[37] Press Release, U.S. Census Bureau, Quarterly Retail E-Commerce Sales: 3rd Quarter 2012 tbl.1 (Nov. 15, 2012), *available at* http://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf.

[38] This is particularly true for two reasons. First, credit card fraud detection efforts do not scale well. They involve substantial manual review and processing. Fraud activity, on the other hand, scales quite well. Credit card account information is readily sold online for as little as one dollar per card (for ordinary credit cards), and between five and twenty dollars per card (for higher-end cards, depending upon spending limits). Second, interchange reform efforts, such as those reflected in the Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010) (to be codified at 12 U.S.C. § 5301 *et seq.*), and recent antitrust settlements with Visa and Mastercard, *see, e.g.*, Jessica Silver-Greenberg, *MasterCard and Visa Will Pay Billions to Settle Antitrust Suit*, N.Y. TIMES, July 14, 2012, at B1, are likely to usher in an era of higher prices for credit cards as opposed to debit cards. Debit transactions, however, are not subject to the protections of the Truth in Lending Act, Pub. L. No. 90-321, 82 Stat. 146 (1968) (codified as amended at 15 U.S.C. 1601 *et seq.* (2006)). It is thus far harder to recover money lost to fraudulent debit card transactions than to credit card transactions. *Compare* 15 U.S.C. § 163(a) (limiting the liability of credit card holders to charges over $50 under certain conditions), *with* 15 U.S.C. § 1693g (allowing either uncapped liability or liability up to $500, but placing greater burdens on the cardholder).

[39] *See* KEMPF & AUSTEIN, *supra* note 7, at 7 ("Academic and government institutions ran the Internet of 15 years ago. These institutions did not expect to make a profit from their investment

The incentives of intermediaries and users were thus typically aligned. In the wake of commercialization, intermediaries increasingly face conflicting incentives and this creates a fault line between the interests of intermediaries and those of users.

### D. *The Post-Trust Internet*

These changes have ushered in the era of a brave new Internet—one in which many new social and economic institutions seem at first blush wondrous and vital, but on deeper inspection may be built upon questionable foundations. Users' ability to trust other users and the architecture of the early Internet helped define that Internet's institutional equilibria. But as the users and architecture continue to change, and especially as users begin to question whether the Internet is a trustworthy platform, so, too, will these equilibria change.

The remainder of this Section considers reasons that these social and economic institutions may not be sustainable in the post-trust Internet. The basic concern is that the Internet architecture, which in the early Internet age allowed users to interact in new and positive ways, can now be turned against users in ways that harm them. Active intermediaries now are capable of using and manipulating user data in ways that were never before possible, and the danger is exacerbated because there is increasing incentive for data to be used in harmful ways. Absent a mechanism to prevent such use—or, in the language of trust, "recourse"—we can expect users to resist active intermediation. Indeed, this is precisely what we have witnessed in the cases of network neutrality and online privacy.[40]

Users can be harmed online through many vectors. The best-known concern is harm from other users. Harm from other users can come in many forms, for instance: hackers breaking into computers, online bullying or the spread of harmful information, the dissemination of disturbing or disruptive information such as spam, or outright fraudulent activity.[41] Much ink has been spilled over these issues, often with a focus on how intermediaries can be harnessed to help protect users from harm caused by other users.[42]

in networking technology. In contrast, the network operator with which most Internet users deal today is the commercial ISP . . . [whose] investors rightly expect . . . to turn a profit."); *see also* OFFICE OF INSPECTOR GEN., *supra* note 18, at 28-30 (describing the onset of commercial investment in the Internet).

[40] *See infra* notes 58-62 and accompanying text.

[41] These are the sorts of concerns animating calls for intermediaries to be liable for user conduct, as discussed by the sources in *supra* note 2.

[42] For examples of authors arguing for various forms of direct and vicarious liability, *see supra* note 2.

But as intermediaries have come to play an active role in the processing and transmission of data online, they also have become a vector for harming end users. Routers and switches, for instance, can prioritize data for certain users and applications.[43] This basic concern is familiar in the context of network neutrality—though network neutrality concerns are generally limited to routers and switches located near the edges of the network (e.g., those hosted by users' Internet Service Providers (ISPs)). User- and applications-based prioritization can occur throughout the Internet, from the data link layer up through the application layer.[44] Similarly, active intermediaries can collect and manipulate user information in ways that are entirely transparent to users. These two concerns may be joined together, with intermediaries collecting user data to identify favored (e.g., more profitable) or disfavored users, and offering them better or worse service.

The aforementioned examples envision intermediaries acting deliberately. Active intermediation also increases the likelihood and prospective extent of inadvertent harms. The complexity of the Internet makes it difficult to properly configure intermediaries.[45] For instance, there have been multiple cases over the past few years where certificate authorities[46] have themselves fallen prey to security vulnerabilities, allowing their systems to be used to issue forged security certificates.[47] Similarly, there have been cases, again in just the past year or two, where routers were misconfigured to transfer data

[43] Császár et al., *supra* note 27.

[44] For an explanation of layering, see Solum & Chung, *supra* note 3, at 817-18.

[45] For example, the more active the intermediary, the more complicated it is to configure correctly. *See* Theophilus Benson, Aditya Akella & Aman Shaikh, Demystifying Configuration Challenges and Trade-offs in Network-based ISP Service (2011) (unpublished manuscript), *available at* http://conferences.sigcomm.org/sigcomm/2011/papers/sigcomm/p302.pdf (exploring the increasing complexities of service configurations over time); Theophilus Benson, Aditya Akella & David Maltz, Unraveling the Complexity of Network Management (unpublished manuscript), *available at* http://pages.cs.wisc.edu/~akella/papers/complexity-nsdi.pdf (analyzing network complexity based on a host of "complexity models" developed by the authors).

[46] Certificate authorities are intermediaries responsible for issuing and managing the encryption keys that allow users to securely send encrypted information to known counterparties over the Internet.

[47] *See* Byron Acohido, *Trust in the Internet Falters After DigiNotar, Comodo Hacked*, THE LAST WATCHDOG ON INTERNET SECURITY (Sept. 28, 2011), http://lastwatchdog.com/trust-internet-wavers-diginotar-comodo-hacked ("Digital certificates enable consumers to submit information that travels through an encrypted connection between the user's web browser and a website server. The certificate assures the web page can be trusted as authentic. But the unprecedented attacks against [certificate authorities] shows how fragile that trust can be."); Peter Bright, *Comodo Hacker: I Hacked DigiNotar Too; Other CAs Breached*, ARS TECHNICA (Sept. 6, 2011), http://arstechnica.com/security/2011/09/comodo-hacker-i-hacked-diginotar-too-other-cas-breached (warning of future attacks and discussing purported "stopgap solutions").

from U.S.-based senders to U.S.-based receivers along a path that traversed routers in China, Indonesia, and Pakistan.[48]

Both of these examples—and there is an alarming number of additional ones[49]—demonstrate two types of potential intermediary-based harm to end users: harm caused by negligence, or harm caused by malicious third-parties taking control of active intermediaries. Most important, this sort of harm is possible only because these are active intermediaries. In the earlier era of the Internet, built upon a network of passive intermediaries, those passive intermediaries lacked the sophistication necessary to harm (or to be used to harm) individual users.[50]

[48] *See, e.g.*, Matt Brian, *Routing Error Momentarily Sends AT&T Facebook Data Via China*, THE NEXT WEB (Mar. 23, 2011), http://thenextweb.com/facebook/2011/03/23/routing-error-momentarily-sends-att-facebook-data-via-china (quoting a security researcher as stating that "Chinese authorities were likely to monitor unencrypted traffic" passing through their network even though no "sensitive information was compromised"); Martin A. Brown, *Pakistan Hijacks YouTube: A Closer Look*, CIRCLE ID (Feb. 25, 2008, 12:17 PM PST), http://www.circleid.com/posts/82258_pakistan_hijacks_youtube_closer_look (suggesting that the hijacking problem "remains one of transitive trust"); Barrett Lyon, *Hey AT&T Customers: Your Facebook Data Went to China and S. Korea This Morning . . .*, BLYON (Mar. 22, 2011, 12:45 PM), http://www.blyon.com/hey-att-customers-your-facebook-data-went-to-china-and-korea-this-morning (questioning whether this incident involved a data breach or was "just the way the Internet functions"); Ram Mohan, *Routing on the Internet: A Disaster Waiting to Happen?*, SECURITY WEEK (Dec. 1, 2001), http://www.securityweek.com/routing-internet-disaster-waiting-happen (warning against the "rapid growth and fragmentation of core routing tables" as "one of the most significant threats to the long-term stability and scalability of the Internet"); Tom Paseka, *Why Google Went Offline Today and a Bit About How the Internet Works*, CLOUDFLARE, (Nov. 6, 2012), http://blog.cloudflare.com/why-google-went-offline-today-and-a-bit-about (describing outages at Google due to the routing of information through Indonesia and Pakistan); *YouTube Hijacking: A Ripe NCC RIS Case Study*, RIPE NCC (Mar. 17, 2008), http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study (concluding that unauthorized announcements by foreign networks can be prevented from spreading by "appropriate routing configuration of operators of Autonomous Systems").

[49] Consider, for instance, accounts showing that routers and switches are susceptible to attack. *See, e.g.*, Siobhan Gorman, *China Tech Giant Under Fire—Congressional Probe Says Huawei Poses National-Security Threat to the U.S.*, WALL ST. J., Oct. 8, 2012, at A1, ("[A] year-long investigation by the House intelligence committee concluded [two Chinese telecommunications corporations] pose security risks to the U.S. because their equipment could be used for spying on Americans."); Dan Goodin, *Secret Account in Mission-Critical Router Opens Power Plants to Tampering*, ARS TECHNICA (Sept. 4, 2012) http://arstechnica.com/security/2012/09/secret-account-in-mission-critical-router-opens-power-plants-to-tampering (contextualizing a warning issued by the Department of Homeland Security that "power utilities, railroad operators, and other large industrial players [face] a weakness in a widely used router that leaves them open to tampering by untrusted employees"); Darren Pauli, *Hardcoded Passwords Leave Telstra Routers Wide Open*, SC MAG. (Nov. 13, 2012), http://www.scmagazine.com.au/News/322729,hardcoded-passwords-leave-telstra-routers-wide-open.aspx (describing a patch issued by an Internet provider to prevent the likelihood of hacking due to a network glitch).

[50] To be sure, passive intermediaries can fail, or be used improperly, in ways that could harm users. *See, e.g.*, J.H. Saltzer, D.P. Reed & D.D. Clark, *End-to-End Arguments in System Design*, 2

Vint Cerf explains that "[e]very layer of the Internet's architecture is theoretically accessible to users and, in consequence, users (and abusers) can exploit vulnerabilities in any of the layers."[51] In an Internet of passive intermediaries, most layers of the Internet contained insufficient logic to be meaningfully exploited; in a network of active intermediaries, the network itself can be exploited and turned against its users.

Despite these concerns, active intermediation is not entirely detrimental (to the contrary, active intermediation has the potential to add substantial value to the Internet value chain[52]) to the ability to combine data from multiple sources over a single communications channel.[53] This creates value because it allows many users to efficiently share resources that would otherwise lie fallow. Many active intermediation technologies are an evolution of earlier technologies that enable this sharing, working to more efficiently squeeze the value out of the network infrastructure.[54] Indeed, whereas earlier technologies statistically multiplexed data along a bandwidth dimension, one way of understanding technologies like prioritization, quality of service (QoS), and active queue management (AQM) is that they enable statistical multiplexing along a second (temporal) dimension.[55]

Another form of active intermediation is tailoring the online experience to individual users. This is most familiarly seen in targeted advertising.

ACM TRANSACTIONS ON COMPUTER SYS. 277, 280 (1984) (discussing the "[t]oo-[r]eal [e]xample" of a transient bit-flipping error in a network gateway's memory). But such harm would occur stochastically, and would generally be visible to a broad range of users.

[51] Vint Cerf, *Internet Governance: A Centroid of Multistakeholder Interests*, *in* MIND CO:LLABORATORY DISCUSSION PAPER SERIES NO. 1: INTERNET POLICYMAKING (Sept. 2011), at 74, 76.

[52] As one example, the most basic technological premise of the Internet is statistical multiplexing.

[53] Damon Wischik et al., *The Resource Pooling Principle*, 38 ACM SIGCOMM COMPUTER COMM. REV. 47, 48 (2008) ("Statistical multiplexing through packet switching is the most fundamental concept in the Internet architecture.").

[54] Today, we are seeing substantial investment in private networks to bypass large parts of the Internet for content-delivery purposes. From the perspective of the traditional Internet, this is harmful, because these content-delivery networks allow firms to place more data on the network without allowing other users to opportunistically share any new capacity when the network is unused. But this approach is a practical necessity for large-scale content delivery, because the state of the art in content delivery is not yet sufficient to allow for multiplexed content-delivery infrastructures. *See id.*

[55] *See supra* notes 13, 31-32 and accompanying text. A network's performance can be characterized in terms of both capacity (the amount of data it can transmit in a given period of time) and latency (the amount of time it takes to transmit a single bit of data). The project of statistical multiplexing has generally focused on allowing multiple connections to efficiently share the finite capacity resource. But multiplexed connections also share, and impose congestion externalities upon each other's use of, the latency resource. In this sense, technologies such as those mentioned above are part and parcel of the same project as statistical multiplexing.

However, targeted ads are only one example of application-level active intermediation.[56] While this form of intermediation, and the privacy implications implied therein, raise legitimate concerns, it is also undeniable that users benefit from it. Online advertising revenue is the fuel that fires the consumer Internet's engine.[57]

The natural response to these concerns is, and has been, to resist active intermediation. This is seen in the public's response to network neutrality concerns and, in turn, the Federal Communication Commission's Open Internet Order.[58] Similarly, the Federal Trade Commission's privacy reports[59] and investigations into firms like Google and Facebook, along with even stronger proposed regulation in the European Union,[60] and overwhelming opposition to legislative proposals such as the Stop Online Piracy Act (SOPA)[61] and the PROJECT IP Act (PIPA)[62]—meant to streamline information-sharing between firms and the government to implement more effective cybersecurity programs—demonstrate the public's preference for a simpler, more passive network.

This preference is understandable and follows from the trust equation. Users are unwilling to rely on technologies that may be used to harm them unless they are able to seek recourse against those harms. Even if these technologies bring benefits, because they operate transparently to users

[56] Other examples of active application-level active intermediation include location-based services, predictive searching, and remembering implicit preferences. The latter is especially important in a world in which one extra click can be the downfall of a given service.

[57] Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J.L. SCI. & TECH. 281, 283 (2012) ("The value created by online advertising, which fuels the majority of free content and services available online, has been immense.").

[58] *See* FCC Open Internet Order, 47 C.F.R. § 8.1 (2012) (defining the purpose of the Open Internet Order to "preserve the Internet as an open platform enabling consumer choice, freedom of expression, end-user control, competition, and the freedom to innovate without permission").

[59] *See, e.g.*, FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (Mar. 2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf (evaluating potential initiatives to enhance Internet privacy and making recommendations to private companies regarding such initiatives).

[60] *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012), *available at* http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf (revising the European Union's approach to personal data privacy, which already limits how intermediaries can use personal data more strictly than in the United States, to even further limit how user data can be used by intermediaries with requirements such as "privacy by design" and a "right to be forgotten").

[61] H.R. 3261, 112th Cong. (2011).

[62] Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, S. 968, 112th Cong. § 3(d)(2)(D).

there is little, or at best, *limited*, opportunity for recourse. The preference, therefore, is to reject active intermediation in favor of an Internet less capable of causing harm.

Importantly, this preference has two distinct effects: encouraging passive intermediation, and limiting the development of new active intermediation technologies.[63] The inability to trust the Internet architecture, therefore, has the pernicious effect of limiting the development of technologies that might make the architecture more trustworthy.

## II. Living Without Trust

In the previous Part, I argued that the early Internet was built on a foundation of trust, but that this foundation has given way as the Internet has evolved. The primary drivers of this change are the increasing complexity of the network—especially with the rise of active intermediation—and the transition away from a small community of users generally interested in the success of the Internet and toward a large user base, with diverse and often adverse interests, and no particular interest in the Internet as a technology in and of itself.

This transition is problematic because it is unclear what can replace trust—a willingness of users to rely on the Internet architecture without assurances that recourse is available should they be harmed—as a foundation for online interaction. The Internet is not the only institution that needs to operate without trust, however. In fact, many institutions operate in such an environment.

This Section looks to three standard approaches used by institutions to foster interaction in lieu of trust: the law, mechanisms that "establish trust" endogenously, and vertical integration.[64]

### A. *Legal Recourse*

The law offers a simple alternative to trust: remedies. In contrast to trust-based institutions' premise of reliance *without* recourse, legal institutions stand on the promise of reliance *with* recourse. Where parties are unable to rely on one another due to lack of trust, the law steps in as an

[63] *See infra* Part IV.

[64] Analytically, these alternatives comprise a complete set of options. Given a set of intermediaries, $\{I_1 \ldots I_n\}$, recourse can be sought in one of three ways: (1) exogenously, relying on an entity outside of the set of intermediaries; (2) endogenously, by relying on the intermediaries to coordinate recourse amongst themselves; or (3) by integrating the set of intermediaries into a single entity $I_{1-n}$ to internalize harm.

external institution to enforce parties' expectations, thereby allowing them to rely on one another without jeopardizing their security.

The clearest example of this phenomenon is contract law, which can be understood precisely as the law of enforcing mutual expectations between individuals. But the law's role in fostering a willingness among individuals to rely on one another is not limited to contract law; most private legal institutions benefit this goal. Tort law, for instance, establishes duties that individuals have to each other independent of any mutual agreement. These duties create expectations regarding how parties will treat one another, on which they can rely, and upon which they can seek recourse. And property law establishes domains in which parties know they need not (or must) defer to other parties' expectations, and provides remedies when those domains are encroached upon.

These different areas of the law serve a common purpose: facilitating interactions between individuals. The menu of different mechanisms exists due to the underlying characteristics of various sorts of interactions.[65] But each faces the same basic set of issues: What is the duty placed upon each party? What is the mechanism for enforcement when that duty is breached? What are the damages for that breach?[66]

Contract law, for instance, gives parties great flexibility in determining their mutual duties, including specifying their preferred consequences for breach of duty, but imposes various requirements upon the parties to ensure that courts understand (and will enforce) their agreement.[67] Tort law, on the other hand, often operates in situations where parties are unable to negotiate ex ante, and therefore relies on generalized duties and indicia of harm to determine a party's responsibility.[68] In comparison, property law

[65] As Coase famously made clear, absent transaction costs, the legal rule would not matter. R.H. Coase, *The Nature of the Firm*, 4 ECONOMICA 386 (1937).

[66] For examples of work relating areas of law to one another, see Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1106-10 (1972) (relating property and liability rules); Thomas W. Merrill & Henry E. Smith, *The Property/Contract Interface*, 101 COLUM. L. REV. 773, 809-48 (2001) (relating contract and property law depending on whether the property right is in rem or in personam).

[67] Think, for instance, of offer and acceptance. *See generally* Curtis Bridgeman, *Why Contracts Scholars Should Read Legal Philosophy: Positivism, Formalism, and the Specification of Rules in Contract Law*, 29 CARDOZO L. REV. 1443, 1444 (2008) (explaining realism's view of offer and acceptance in contract theory); Mark L. Movsesian, *Formalism in American Contract Law: Classical and Contemporary*, 12 IUS GENTIUM 115, 119 (2006) (discussing the "mailbox rule," in which "acceptance of an offer made by correspondence is effective immediately upon dispatch . . . even if the offeror has not yet received it").

[68] As a result, damages in tort are more limited. For instance, purely economic harms are generally not recoverable under a tort claim. *See generally* Jay M. Feinman, *The Economic Loss Rule*

assigns the clearest duties between parties, allowing owners to rely on the quiet enjoyment of their property and prohibiting nonowners from any reliance on that property without the permission of the owner.

The basic feature of the law as a mechanism for establishing trust is that it is an *external institution* that imposes rules upon private, interacting parties. The different mechanisms of contract, tort, and property law are structured to facilitate different types of interactions. However, these doctrines are simultaneously structured to facilitate the operation of the law in its own right. Contract law disfavors oral agreements, for instance, because they are more difficult—and sometimes impossible—for courts to interpret and enforce. Tort law places the burden to prove harm on the injured party because the injured party is best situated to provide both the court and the defendant with information needed to proceed. Property law, meanwhile, operates where parties can easily negotiate over clearly defined boundaries. This requires property owners to establish boundaries and requires courts to impose strict penalties on parties who violate properly maintained boundaries, in order to foster private negotiation.

As an external institution, the law relies on parties to an interaction to provide sufficient information for legal mechanisms to operate. This is, in part, why the law has historically recognized a closed number of forms of property, contracts, and other mechanisms for interaction.[69] The advent of general causes of action and the ability to freely negotiate novel contracts are still relatively recent innovations in the law. The problem of observable but nonverifiable information (information available to parties to an interaction but information that cannot be demonstrated to a court or another third party) is a central problem in contract theory, with corresponding problems in other areas of the law.[70]

Recourse to legal institutions therefore offers one mechanism for facilitating interactions between untrusting parties—subject to important constraints. One set of constraints is that specific legal institutions must be contoured to the characteristics of specific interactions. What this means in the context of online interactions will be considered in Part III. A more

*and Private Ordering*, 48 ARIZ. L. REV. 813 (2006) (grounding economic loss in the law of contract rather than tort law because of the law's respect for private ordering between parties).

[69] For meaningful commentary on the limited variations of property law, see generally Juan Javier Del Granado, *The Genius of Roman Law from a Law and Economics Perspective*, 13 SAN DIEGO INT'L L.J. 301 (2011); Thomas W. Merrill & Henry E. Smith, *Optimal Standardization in the Law of Property: The* Numerus Clausus *Principle*, 110 YALE L.J. 1 (2000).

[70] *See* Oliver Hart & John Moore, *Foundations of Incomplete Contracts*, 66 REV. ECON. STUDS. 115, 124 (1999) (describing the sufficiency of the "observable but non-verifiable" assumption to a theory of incomplete contracts).

fundamental constraint is that legal institutions can only operate where sufficient information is available to individuals and to courts. In the context of online interactions, where a design goal of the Internet is to seamlessly facilitate myriad transparent and transient interactions, this may prove a fundamental limitation on effectuating the law online. Part III will also consider the tradeoffs this might require between the operation of legal institutions online and the design choices underlying the Internet architecture.

### B. *Vertical Integration*

Legal institutions are costly. The cost, for instance, of negotiating and entering into a formal contract is substantial, as is the cost of enforcing the contract in court following a breach and collecting damages. In his seminal 1937 article, Ronald Coase identified these costs as the reason that firms exist—why, in other words, independent actors agree to coordinate their efforts into integrated economic units called "firms."[71]

Coase asked why firms exist at all: Why do entrepreneurs have employees, when instead they could coordinate all factors of input (both labor and material) through contracts for labor and materials negotiated on the open market?[72] Famously, Coase's answer is that organizing into firms avoids many of the transaction costs inherent in the price mechanism—chief among these are the costs of contracting.[73] Transaction costs can make firm-like organizations less costly than relying on price mechanisms. Indeed, these costs may be high enough that it would be unprofitable to rely on the price mechanism, but still profitable to rely on firm-like organizations.

Coase's explanation for why firms exist in the first instance gave rise to decades of debate over the converse question: Given that firms avoid

[71] Coase, *supra* note 65.

[72] *Id.* at 392-93 ("One entrepreneur may sell his services to another for a certain sum of money, while the payment to his employees may be mainly or wholly a share in profits. The significant question would appear to be why the allocation of resources is not done directly by the price mechanism.").

[73] According to Coase,

> The main reason why it is profitable to establish a firm would seem to be that there is a cost of using the price mechanism. The most obvious cost of "organising" production through the price mechanism is that of discovering what the relevant prices are. This cost may be reduced but it will not be eliminated by the emergence of specialists who will sell this information. The costs of negotiating and concluding a separate contract for each exchange transaction which takes place on a market must also be taken into account.

*Id.* at 390.

transaction costs, why does any market have more than a single firm? The general answer is that, just as contracts and the price mechanism incur transaction costs, so too does the operation of the firm.[74] There is, therefore, an optimal size to any given firm.

Michael Jensen and William Meckling built on this framework to develop an agency cost model to understand the optimal size of a firm.[75] According to their vision,

> If both parties to the relationship are utility maximizers there is good reason to believe that the agent will not always act in the best interests of the principal. The principal can limit divergences from his interest by establishing appropriate incentives for the agent and by incurring monitoring costs designed to limit the aberrant activities of the agent.[76]

Framing their analysis as a principal–agent problem also frames it as a trust problem. If an agent may have incentives that conflict with those of the principal, the agent cannot be trusted. It is possible that the principal could respond by structuring the relationship to offer recourse to legal institutions.[77]

Rather than rely on legal institutions, Jensen and Meckling argue that firms may structure the principal–agent relationship so as to avoid (or reduce) the need for recourse.[78] One such approach is to give the agent a stake in the outcome of the principal's business.[79] Another approach, which is generally understood as the greatest cost facing most firms, is for the principal to direct and monitor the work of her agent.

The monitoring approach is similar to relying on a contract that is enforceable by recourse to a legal institution. Both parties have expectations of their relationship upon which they rely in conducting their interactions. But in the context of the firm, the principal is able to structure her agent's conduct to ensure the availability of information sufficient to confirm the

[74] *Id.* at 394-98 (asking, "Why is not all production carried on by one big firm?" and suggesting several possibilities); *see also* OLIVER E. WILLIAMSON, MARKETS AND HIERARCHIES: ANALYSIS AND ANTITRUST IMPLICATIONS 126-29 (1975) (discussing limitations on the size of the firm).

[75] Michael C. Jensen & William H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure*, 3 J. FIN. ECON. 305 (1976); *see also* Armen A. Alchian & Harold Demsetz, *Production, Information Costs, and Economic Organization*, 62 AM. ECON. REV. 777 (1972) (using an agency model to understand the institutional design of a firm); Eugene F. Fama, *Agency Problems and the Theory of the Firm*, 88 J. POL. ECON. 288 (1980) (same).

[76] Jensen & Meckling, *supra* note 75, at 308 (emphasis omitted).

[77] Indeed, most principal–agent relationships do occur in the context of a contractual relationship. *Id.* at 310 (arguing that "[c]ontractual relations are the essence of the firm" and that "most organizations are simply legal fictions which serve as a nexus for a set of contracting relationships among individuals" (emphasis omitted)).

[78] *Id.* at 308.

[79] For example, stock options or, conversely, bonding the agent to the principal. *Id.* at 308.

performance of these expectations, and the remedy for breach of these expectations is termination of the relationship, at the principal's discretion.

This yields a second mechanism for operating outside of trusted relationships: integration between parties to the interaction. This approach is effective where the parties can structure their interactions such that they face aligned incentives, or where monitoring is sufficient to dissuade an agent's breach of the principal's trust. The great advantage of this approach is that it does not require costly or uncertain recourse to an exogenous institution (such as a court). It is, however, limited to contexts where such integration is possible, where incentives can be aligned, and where discontinuation of the relationship is sufficient should recourse become necessary.[80]

### C. *"Establishing Trust"*

Communities often develop endogenous mechanisms to facilitate interactions between their members and to preserve the autonomy of their members without need for recourse to exogenous institutions like the law. This can be thought of as establishing trust between otherwise untrusting parties based on the circumstances of their interaction.

Examples familiar to legal and economics scholars include the seminal works of Robert Ellickson and of Elinor Ostrom.[81] Both consider how communities form rules between their members that are enforced internally. Indeed, when Ellickson examined Shasta County, he found that such rules can even form in the presence of working legal institutions, thereby demonstrating that they can be preferred to legal recourse.[82]

[80] More substantial recourse could be available via legal mechanisms, subject to the limitations discussed above. One would expect, for instance, that an employer could both fire and sue an employee caught stealing from the company.

[81] ROBERT ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (1991); ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION (1990).

[82] Ellickson notes that

> [i]n rural Shasta County, where transaction costs are assuredly not zero, trespass conflicts are generally resolved not in "the shadow of the law" but, rather, beyond that shadow. Most rural residents are consciously committed to an overarching norm of cooperation among neighbors. In trespass situations, their applicable particularized norm, adhered to by all but a few deviants, is that an owner of livestock is responsible for the acts of his animals. Allegiance to this norm seems wholly independent of formal legal entitlements.

ELLICKSON, *supra* note 81, at 52-53.

Such approaches are probably the best-known responses to concerns about online trust today. Examples of this approach include reputation and encryption.

Reputational models are among the most successful responses to concerns about trust online. One of the early pioneers of these models was eBay, which relied on parties to leave publicly viewable feedback about their interactions on its auction website. Users could rely on buyers and sellers with established histories of satisfactory dealings as more trustworthy than those without established histories (or, worse, with less-than-satisfactory histories).

Similarly, parties that want to interact online but do not trust their data to be handled by untrusted intermediaries have long turned to encryption to protect against those intermediaries. To use encryption, the parties need to first coordinate the use of an encryption algorithm. This is done by relying on a trusted third party, called a certificate authority.[83]

Both of these mechanisms (indeed, all mechanisms that rely on actors within a system to establish trust) are built upon the fundamental assumption that parties being relied upon to establish trust are independent from the party for whom trust is being established.[84] This has been a reasonable assumption for most of the Internet's history. Of course, online trust has not been a problem for most of the Internet's history. Where it may be possible for members of a community to co-opt that community's trust-establishing mechanisms, however, those mechanisms necessarily fail.

The continuing viability of this assumption is suspect. Reputation mechanisms have proved to be effective in many cases, but these are typically cases where reputation is established by a relatively small or homogeneous community.[85] These mechanisms have also fallen prey to manipulations meant precisely to breach trust—typically where those

[83] NETWORK ASSOCS., INC., AN INTRODUCTION TO CRYPTOGRAPHY 23 (1999), *available at* ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf (defining a certification authority, or CA, as "a human entity—a person, group, department, company, or other association—that an organization has authorized to issue certificates to its computer users").

[84] *See generally* ELLICKSON, *supra* note 81; OSTROM, *supra* note 81.

[85] Even eBay falls into this category, because its reputation mechanisms (which have required several modifications to prevent gaming) were initialized in the early days of the Internet. Indeed, most new online communities are born from a surprisingly small community of users. *See* Benjamin Jackson, *How White is the New Internet?*, BUZZFEED (Aug. 29, 2012), http://www.buzzfeed.com/benjaminj4/how-white-is-the-new-internet (illustrating the lack of gender and racial diversity among early adopters and emphasizing that "the earliest adopters are often influential . . . tech leaders based in and around New York and the Bay Area").

seeking to establish trust, or their affiliates, attempt to manipulate the reputation system.[86]

Endogenous systems have been subject to more serious problems. For instance, in 2011, a firm named DigiNotar was breached by hackers. DigiNotar is one of a small number of Certificate Authorities. As a result of this breach, false (but authentic) certificates were issued for a number of high-profile Internet entities.[87] In effect, the mechanism for establishing trust upon which online encryption is based requires users to ask themselves a more complicated question: to be effective, Internet browsers must ask, "Do we trust the person vouching for party *A*?" instead of, "Do we trust party *A*?"[88]

[86] "Astroturfing" is the best-known example of such efforts. *See, e.g.*, George Monbiot, *Robot Wars*, MONBIOT (Feb. 23, 2011), http://www.monbiot.com/2011/02/23/robot-wars ("The anonymity of the web gives companies and governments golden opportunities to run astroturf operations: fake grassroots campaigns, which create the impression that large numbers of people are demanding or opposing particular policies."). There are many specific examples of the significance of reputation in the Internet economy. *See, e.g.*, Rachel Botsman, *Welcome to the New Reputation Economy*, WIRED UK (Aug. 20, 2012), http://www.wired.co.uk/magazine/archive/2012/09/features/welcome-to-the-new-reputation-economy (announcing an Internet "reputation economy, where [one's] online history becomes more powerful than [one's] credit history"); Ray Fisman, *Should You Trust Online Reviews? Economists Weigh In*, SLATE (Aug. 14, 2012), http://www.slate.com/articles/business/the_dismal_science/2012/08/tripadvisor_expedia_yelp_amazon_are_online_reviews_trustworthy_economists_weigh_in_.html (exploring the ease with which companies may invent positive reviews for themselves); Helen A.S. Popkin, *Facebook: More Than 83 Million Users Are Fake*, NBC NEWS, http://www.nbcnews.com/technology/technolog/facebook-more-83-million-users-are-fake-919873 (highlighting the increase in the creation of Facebook accounts for "fake" users); *The Underground Economy of Social Networks*, NET SECURITY (Aug. 7, 2012), http://www.net-security.org/secworld.php?id=13380 (reporting that the "underground economy" of fake online profiles "consists of dealers who create and sell the use of thousands of fake social accounts, and Abusers who buy follows or likes from these fake accounts to boost their perceived popularity, sell advertising based on their now large social audience or conduct other malicious activity").

[87] *See supra* note 47.

[88] "Multifactor authentication" is a related trust-establishing mechanism. Multifactor authentication requires a user to provide multiple independent pieces of information (instead of simply a password) in order to establish her identity. Since 2005, financial institutions have been encouraged to adopt multifactor authentication for online transactions. *See* FED. FIN. INSTS. EXAMINATION COUNCIL, AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT 1-2 (2005), *available at* http://www.ffiec.gov/pdf/authentication_guidance.pdf ("Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks."). As with encryption, where the question becomes whether we trust the speaking party as well as the party vouching for it, multifactor authentication begs the question whether we trust both pieces of information. However, as with other mechanisms for establishing trust, malicious users have been able to bypass multifactor authentication. *See, e.g.*, ERAN KALIGE, & DARRELL BURKEY, A CASE STUDY OF EUROGRABBER: HOW 36 MILLION EUROS WAS STOLEN VIA MALWARE (Dec. 2012), *available at* http://www.checkpoint.com/products/downloads/whitepapers/Eurograbber_White_Paper.pdf (detailing a criminal effort to steal more than 36 million Euros from over 30,000 European banking customers by compromising

## III. PROBLEMS WITH STANDARD SOLUTIONS TO LIVING WITHOUT TRUST

The mechanisms considered in the previous Part work to facilitate interactions between parties that may not trust each other. None, however, is sufficient to address the basic problem of online trust—that one of the design purposes of the Internet is to allow myriad users and intermediaries to interconnect in a transparent manner and independently of each other. Each mechanism also faces specific problems in the context of online interactions. This Part considers the reasons that each of these mechanisms is insufficient to address the lack of trust online.

### A. *Limitations of Legal Institutions*

Legal institutions face two general problems when applied to online intermediaries. First, at a technical level, the operation of these intermediaries is meant to be transparent to the user. As a result, the basic information needed for the legal system to operate is unavailable. Second, even if sufficient information were available, it is unclear which legal rules a user could use to secure satisfactory recourse against intermediaries.

As a design principle, users are not supposed to need—or even necessarily have access to—information about the operation of intermediaries. In fact, this principle, called layering, applies even more generally: just as users ought not to need information about the operation of intermediaries, intermediaries at one layer of the Internet ought not to need access to information about those deeper intermediaries.[89] For instance, users should not need to know how their web browsers work; the web browser need not know how the computer is connected to the Internet but only that it *is* connected; and the protocols establishing the computer's connection to the Internet need not know how the network is configured.

But this means that users have very little visibility into the operation of the network. They may not even be able to recognize that harm is occurring in real time, and even then, they may only be able to make such a determination by inference or proxy.[90] When users can identify that some harm is

both customers' computers and mobile phones in order to bypass their banks' multifactor authentication).

[89] *See* Solum & Chung, *supra* note 3, at 829-31.

[90] *See, e.g.*, PETER ECKERSLEY, FRED VON LOHMANN & SETH SCHOEN, ELECTRONIC FRONTIER FOUND., PACKET FORGERY BY ISPS: A REPORT ON THE COMCAST AFFAIR 1-2 (2007), *available at* https://www.eff.org/files/eff_comcast_report.pdf (detailing the discovery of Comcast's handling of BitTorrent connections by a Comcast subscriber and the Electronic Frontier Foundation); *see also* Jim Gettys & Kathleen Nichols, *Bufferbloat: Dark Buffers in the*

occurring, they may not be able to localize its source to a single intermediary.[91] And even when they are able to locate the source, it is unlikely that they will be able to document the problem in a way cognizable to a court.

The converse of this concern is equally problematic: users do not want to be exposed to the majority of information about the operation of intermediaries. Most users lack the sophistication, or interest, to make use of such information. And, even in the early days of the Internet, simple online interactions could involve dozens of intermediaries. But it is a false choice to think that users must choose, or the technology must support, either a drought or a flood of information. The challenging questions are *how much*, and *what*, information is needed and relevant to support recourse to legal institutions—a topic discussed in this Section.

The second general challenge facing the use of legal institutions to provide recourse is understanding what causes of action may apply to interactions between users and intermediaries. Even if users have perfect information about how intermediaries (mis)handle their data, recourse will only be available subject to some cognizable legal claim. There are a number of possible causes of action that may apply, none of which fits the problem particularly well.

A first possible cause of action may lie under contract law. If a user has reasonable expectations for how an intermediary will handle her data, and the intermediary fails to act in accordance with this expectation, liability might attach. This would clearly be the best approach if the user had an express contractual relationship with the intermediaries—that is, if the user had negotiated terms of service with a service-level agreement, monitoring guidelines, some consideration paid, and contractually defined damages.

In the majority of online interactions, however, users generally never have any direct interactions with any given intermediary. In fact, users may never know about the intermediary's involvement. Regardless, we might argue that a user who relies upon intermediaries to behave in a certain way—e.g., as defined by Internet standards organizations—might hold a reliance interest. Given the best-effort nature of the Internet, this nonetheless may prove challenging.[92] A better argument might be that by conforming

*Internet*, COMM. ACM, Jan. 2012, at 57, 57-65 (demonstrating the difficulty of diagnosing protocol problems).

[91] *See supra* note 90.

[92] The Internet provides "best-effort" service, meaning that intermediaries make no assurances for how or whether data will be delivered. *See* Eric Crawley et al., *A Framework for QoS-based Routing in the Internet* 4 (IETF Network Working Grp. RFC No. 2386, 1998), *available at* http://tools.ietf.org/pdf/draft-ietf-qosr-framework-05.pdf ("Routing deployed in today's Internet . . . typically supports only one type of datagram service called 'best effort.'"); Christopher Lefelhocz et al.,

the information she sends over the Internet to standardized specifications, the user is expressing an understanding that the data will be handled in accordance with those expectations. The expectations, in turn, would be such that any intermediary that accepts the data, accepts it subject to those standards. In other words, offering data in conformance with standards, and accepting that data, could equate to an offer and acceptance in an agreement that the data will be handled in accordance with relevant standards.[93]

This approach still presents difficulties. For instance, where is the consideration supporting the agreement? The operator of the intermediary may receive compensation from some third party, but intermediaries rarely receive anything directly from the user. This setup presents a traditional privity of contract problem.[94] Even if we iron out this wrinkle, there is still the question of damages, which are likely de minimis for any interaction. Unless the user can show consequential damages, any recovery is likely insufficient to justify bringing a claim.

Tort law offers an alternative to the law of contract that overcomes privity of contract limitations. As the New York Court of Appeals held in *MacPherson v. Buick Motor Co.*, the negligence of an upstream supplier is sufficient to establish liability between that supplier and a purchaser of the ultimate product, even in the absence of any relationship between the two.[95] If an intermediary unreasonably handles a user's data—for instance, by not properly implementing standards, misconfiguring those systems, or failing to monitor or secure its systems against hackers—in a way that causes harm to the user, an action might lie in tort. But here the fundamental limitation is the harm itself. Any harm is likely to be purely economic, and therefore generally unrecoverable under a negligence theory.[96]

We might also consider theories under property law or intentional torts. For instance, a user might argue that she is the bailor of her data and the intermediaries her bailees. Or the user might claim that the intermediary has converted her data. The virtue of these approaches is that they offer

*Congestion Control for Best-Effort Service: Why We Need a New Paradigm*, IEEE NETWORK, Jan.-Feb. 1996, at 10, 10 ("[I]n best-effort service, the network tries to forward all packets as soon as possible, but cannot make any quantitative assurances about the quality of service delivered.").

[93] At a technical level, this would likely require more express specification of the standards a user expects will govern the treatment of her data. For example, a user might expect a header option indicating that Internet Protocol (IP) traffic will only be accepted by routers implanting specific AQM technologies.

[94] *See, e.g.*, Sisson v. Jankowski, 809 A.2d 1265, 1267 (N.H. 2002) ("While a contract may supply the relationship, ordinarily the scope of the duty is limited to those in privity of contract with one another." (citation omitted)).

[95] 111 N.E. 1050, 1053 (N.Y. 1916).

[96] *See supra* note 68.

more flexible damages, including punitive damages.[97] That said, a user seeking to rely on these causes of action faces substantial hurdles. Bailor–bailee claims, for instance, typically only lie where the property is damaged, not where the bailor is harmed by how the bailment is handled. And conversion would require some legally cognizable right violated by the intermediary by its very handling of data contrary to expectations.

This leaves the user with the possibility of statutory causes of action to establish intermediary liability. Given the difficulty of establishing harm, and the limitations under existing common law causes of action, it may be appropriate to rely on statutory damages for specific classes of intermediary (mis)conduct. The details of any statutory approach would be complicated and controversial—indeed, the current statutory approach, as exemplified by section 230 of the Communications Decency Act, is one of immunity for intermediaries.[98] More importantly, as discussed in the next Part, it is premature to put in place a specific statutory scheme. But it is important to recognize that, depending on how the technology continues to evolve, statutory damages should be part of the discussion here. Engineers working to implement next-generation technologies should be aware that design decisions they make today will affect the legal rules adopted tomorrow. Awareness of a possible need for statutory damages, and the appurtenant controversies and difficulties, will encourage the development of next-generation technologies that provide better access to the information necessary for legal institutions to work well. Alternatively, if the technology is incapable of supporting recourse to legal institutions, we should be wary of relying upon it to an extent that unduly exposes users to harm.

### B. *Limitations of Vertical Integration*

Vertical integration is an incomplete response to trust-related concerns for a few reasons. First, it is incoherent as an approach, because broad integration between users and intermediaries is not possible. Second, it also runs afoul of a design principle of the Internet: the interconnection of independent actors. Third, there already is a great deal of vertical integration online—greater integration may be as much a poison as a cure. The challenging question is how much integration we want and between which

[97] *See, e.g.*, Feld v. Feld, 783 F. Supp. 2d 76, 77-78 (D.D.C. 2011) (mem. opinion) (awarding punitive damages supported only by nominal harms in the case of an intentional trespass and discussing cases reaching this conclusion in other jurisdictions).

[98] *See infra* notes 131-33 and accompanying paragraph.

actors—an idea that leads to an important legal problem: whether and how to rely on joint and several liability to address trust concerns.

The first and second of these concerns are fundamental but relatively straightforward. It is misleading to say that users can resolve their inability to trust intermediaries through vertical integration. This would require users to establish a management or ownership relationship with every intermediary with which they interact. Establishing such a relationship with even a few intermediaries would be difficult—each relationship would require overcoming the same informational and contractual issues that present challenges to legal institutions. And because most users do not derive revenue from their use of the Internet, joint ownership does not offer a solution, either: principals establish trust with their agents by offering the agents an ownership interest in the venture. This concept does not apply to the relationship between users and intermediaries.[99]

Similarly, the very concept of the Internet is that it is a network of independent networks. Each of those networks may be integrated internally. But the relationship between networks is modular—each network is supposed to operate independently. Indeed, the greater concern about integration today is, if anything, that there is too much of it: there is substantial debate about media consolidation and whether the Internet is becoming a network of walled gardens.[100]

Vertical integration will never prove a complete solution to trust concerns. However, it does play an important role. Traditionally, the Internet has separated various functions between intermediaries based upon technical considerations. The resulting boundaries segregate different functions into separate modules.[101] The basic idea of modularity is that related functions

[99] To the extent that it might apply, it would be through competition, with intermediaries constrained by the concern that users might move away from them.

[100] *See, e.g.*, Jonathan Zittrain, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT (2008) (discussing the Internet's transition from an open, *generative* platform that supports applications independent of any service-provider involvement to an increasingly locked-down, *appliancized* network, that can be used only for applications expressly facilitated by service providers); *see also* Bruce Schneier, *When It Comes to Security, We're Back to Feudalism*, WIRED (Nov. 26, 2012), http://www.wired.com/opinion/2012/11/feudal-security (likening certain vendors to feudal lords to whom internet users must "pledge allegiance" as "vassals").

[101] Engineers design systems using modular functions. *See* 1 CARLISS Y. BALDWIN & KIM B. CLARK, DESIGN RULES: THE POWER OF MODULARITY 63-92, 149-220 (2000) (exploring the need for modularity in the creation of complex systems, such as computers); Clark et al., *supra* note 5, at 466 ("Systems designers know to break complex systems into modular parts."); *see also* CARPENTER, *supra* note 3, at 4 ("Modularity is good. If you can keep things separate, do so."). *But see* David D. Clark, *Modularity and Efficiency in Protocol Implementation* 1 (IETF RFC No. 817, 1982), *available at* http://www.rfc-editor.org/rfc/pdfrfc/rfc817.txt.pdf (arguing "that modularity is one of the chief villains in attempting to obtain good performance"). Each "module" implements a

that need to share information in order to operate efficiently should be grouped together. The information needed by those functions is kept internally and not shared with functions in other modules. This is an important design principle that should be embraced because the Internet would not be possible without it.

The lesson to take from modularity, and that should be applied to future modular design decisions, is that modular boundaries should be drawn on boundaries designed to support both the technical and the nontechnical institutions that comprise the Internet ecosystem. This, in fact, runs directly counter to the approach put forth by David Clark, who has advocated designing modular boundaries to isolate nontechnical issues so as to protect the technical architecture from legal controversy.[102] Although this is an eminently reasonable way to design an architecture that is technically robust, it is an approach that is simultaneously all but designed to starve nontechnical institutions of the information needed to facilitate recourse.

Indeed, the idea of modularity has a legal analog in joint and several liability. Where legal institutions are unable to assess or apportion liability between a group of defendants—typically because those defendants have private information needed for the legal institution to do so—the law will assess liability upon them as a whole.[103] This is a modular approach. If a plaintiff targets one defendant out of a modular group of defendants, that defendant can implead other members to join the module.

This analysis suggests that there may be separate legal and technical modular boundaries. The interesting, and challenging, question is whether these boundaries can or should be aligned. Where harm occurs, the law will seek to define the relevant modular boundaries needed to offer recourse (assuming there is a viable cause of action). Conforming the technology to these legal boundaries requires tradeoffs, such that it may or may not make sense to respect them.[104] The critical issue is that those designing and

specific function or set of functions upon data that is passed to it, and the module then passes the result on to some next module for further processing (or to an output device once processing is complete). When designing a modular system, engineers need to consider both where to draw the boundary between different modules and what information needs to be passed between modules. These decisions are typically based on technical considerations.

[102] *See* Clark et al., *supra* note 5, at 466-68 (using the domain name system (DNS) design as an example to demonstrate the modularity principle).

[103] RESTATEMENT (THIRD) OF TORTS: APPORTIONMENT OF LIABILITY, § C18 cmt. a & reporters' note to cmt. a (2000) ("Liability of Multiple Tortfeasors for Indivisible Harm").

[104] To give a nontechnical example, a general contractor could face liability for the poor work of a subcontractor, whom she may then implead if a suit results. This does not mean that she must, or even should, hire that subcontractor as an employee. There are reasons she may choose

implementing the technology understand that their design choices have legal implications—and that those legal implications are clear.

### C. *Limitations of Endogenous Institutions*

The final institution considered in the previous Part was the use of endogenous institutions to "establish" trust between users. While unquestionably the most relied-upon mechanism today—especially in the cases of reputation and encryption—this approach has substantial limitations.

Most fundamentally, relying upon third parties to a transaction to establish trust assumes the trustworthiness of those third parties. This makes the question of trust more complicated by involving more parties. Moreover, the greatest requirement for endogenous institutions is that they require the interacting parties to have no affiliation with the third parties. In a network in which a user cannot trust those third parties, this is a suspect assumption. Indeed, instances of parties influencing third-party reputational mechanisms, either directly or through enlisting confederates, are common.[105] As the Internet continues to become a prominent forum for economic and social interactions, the incentives for third parties to manipulate endogenous mechanisms will increase.[106]

At their core, endogenous systems have worked because the Internet community, as a whole, has been trustworthy. But as this trust continues to dissipate, the efficacy of these endogenous mechanisms almost certainly must fail—a conclusion supported by both Ellickson and Ostrom.[107] Small communities are able to function as commons, with norm-based rules, almost precisely because they are small and have shared incentives or values. As they grow, they develop exogenous institutions—such as courts—to provide redress for harms.

Moreover, endogenous institutions may also restrict the range of uses that the network can support. The best example is encryption. Encryption relies upon a number of actors to coordinate an information exchange to make that information unintelligible to unauthorized intermediaries.[108] This has the advantage of limiting the range of harm that intermediaries can

such an arrangement, and reasons she may not. The critical concern is that she understand these tradeoffs.

[105] *See supra* note 86 and accompanying text.

[106] *See supra* notes 35-37 and accompanying text.

[107] *See* ELLICKSON, *supra* note 81; OSTROM, *supra* note 81.

[108] *See generally* NETWORK ASSOCS., INC., *supra* note 83, at 30-33 (discussing various trust models); Gerck, *supra* note 4, at 24 ("Trust, as qualified reliance on information, needs multiple, independent channels to be communicated.").

inflict upon users. The technical goal of encryption is to make any two pieces of data indistinguishable from each other; this, in turn, means that intermediaries have no basis for treating any two pieces of data differently. Therefore, if users are concerned about disparate treatment of their data or being treated disparately based upon the content of their data, encryption offers strong protection.

But users may value disparate treatment of their data, both vis-à-vis their own data and that of other users. There is a great deal of value to be had, for instance, in prioritization of certain types of traffic[109]—indeed, prioritization might be necessary to make certain applications viable online, or it might allow them to operate far more efficiently.[110] At a more basic level, a core value proposition of the Internet is "statistical multiplexing," which allows connections to be shared among multiple users and applications.[111] But firms and users will only be willing to share their connections if doing so does not jeopardize their own uses. A firm, for instance, might be willing to invest $1 billion in a network that would generate $3 billion in social welfare spillovers, provided that at least a third of that social benefit accrued to its own private interest. If this is only possible with prioritization, then we ought to prefer such prioritization.

Finally, recent work in economics suggests that liability is more effective than endogenous mechanisms such as reputation in facilitating interactions between untrusting parties. This follows from economic studies of credence goods.[112] Recent empirical work shows that liability plays a crucial role in ensuring that parties in trust-based interactions behave in a trustworthy

[109] *See* Christopher S. Yoo, *Network Neutrality and the Economics of Congestion*, 94 Geo. L.J. 1847, 1879-83 (2006) (discussing the benefits of prioritizing traffic based on the particular application or content in question); Shigang Chen & Klara Nahrstedt, *An Overview of Quality of Service Routing for Next-Generation High-Speed Networks: Problems and Solutions*, IEEE NETWORK, Nov.-Dec. 1998, 64, 64-70 (describing data flow management approaches in the context of high-quality audio-visual information); Bob Briscoe & Steve Rudkin, Commercial Models for IP Quality of Service Interconnect, 9-11 (June 2, 2005) (unpublished manuscript), *available at* http://bobbriscoe.net/projects/ipe2eqos/gqs/papers/ixqos_bttj05.pdf (analyzing data flow management in a scenario with multiple applications, each having a minimum usable rate).

[110] For example, efficient multiplexing of jitter- or delay-sensitive applications may require scheduled-transport, bandwidth or route reservation, or other forms of temporal multiplexing. *See generally* Wischik et al., *supra* note 53. Without such options, applications might rely instead on protocol-unfriendly alternatives. *See supra* note 54.

[111] *See* Wischik et al., *supra* note 53, at 48 (describing the goals and mechanisms of "statistical multiplexing").

[112] Credence goods are goods whose quality is difficult to ascertain both before and after a consumer purchases or consumes them. For a description of credence goods, see Michael R. Darby & Edi Karni, *Free Competition and the Optimal Amount of Fraud*, 16 J. L. & ECON. 67, 68-72 (1973).

manner.[113] Reputation, on the other hand, is a relatively ineffective constraint on the behavior of untrustworthy parties—its primary effect is rather to encourage greater strategic behavior on the part of deceptive parties.[114]

## IV. TOWARD A POST-TRUST LAW OF INTERMEDIARIES

The limitations seen in the mechanisms considered above provide guidance for moving forward. This Part offers a general framework for thinking about the post-trust law of intermediaries.

Generally, it is premature to develop comprehensive legal rules to impose liability on intermediaries for harm they may cause—the technology is still evolving and the potential range of harms is ill-defined. Rather, the focus should be on developing a framework to understand the rules that will apply to the Internet architecture, however that architecture may evolve. This will provide engineers with a menu of legal implications that may follow from technical design decisions, and also helps us understand what any rules should look like today. The general approach is modeled after Calabresi and Melamed's work on property and liability rules. It suggests that we should initially rely on liability rules, with burdens placed on intermediaries, but as technology develops, we may move towards property rules that place burdens on users to exercise control over their data.[115] Hopefully, these rules will help ensure that such a transition occurs.

### A. *Moving Forward: The Approach and the Stakes*

Understanding what it means to move forward is challenging because of the limitations inherent in the network considered throughout this Article. It is also difficult because those limitations continue to change as the Internet and our uses of it evolve.

As a starting point, it is clear that we are moving in *a* direction regardless of the availability of legal recourse against intermediaries. The status quo, in which intermediaries are increasingly able to use or handle user data in ways unsatisfactory to those users, is not a stable equilibrium. We see this with network neutrality and online privacy—both uses of active-intermediation

[113] *See* Uwe Dulleck, Rudolf Kerschbamer & Matthias Sutter, *The Economics of Credence Goods: An Experiment on the Role of Liability, Verifiability, Reputation, and Competition*, 101 AM. ECON. REV. 526, 528 (2011) ("[O]ur results suggest that legal liability clauses are most suitable to cure many of the inefficiencies associated with the provision of credence goods.").

[114] *See id.* at 549 (analyzing the limitation of reputational effects to control behavior).

[115] *See* Calabresi & Melamed, *supra* note 66, at 1106-10 (describing the difference between property and liability rules).

technology that users intuitively resist, but both developed as ways to fund the Internet architecture. The path that has led to these concerns can be understood in terms of trust: humans have a natural predisposition to trust machines,[116] and this propensity naturally leads to acceptance of technologies regardless of whether they are trustworthy. But as users learn to question the trustworthiness of that technology, they will either move away from the technology or demand accountability.

At the same time, there is ongoing concern about vertical integration and the turn toward appliance-like models of Internet-based devices and services. Jonathan Zittrain and Tim Wu both express concern about the loss of generativity and increasing consolidation of control over key Internet infrastructure—trends that push the network toward so-called "walled gardens."[117] Other authors, however, argue for a walled garden–like online experience, with walls defined by trusted relationships.[118] Beyond academic discourse, and as shown by Zittrain and Wu, walled gardens are an increasing reality. For those who believe in the value of generativity, or those who have concerns about consolidation and insufficient competition, this suggests a bleak future.

Today's Internet is therefore poised between two equilibria: one characterized by a return to a simpler Internet of passive intermediation; the other characterized by a future of more powerful but less generative walled gardens. Against this backdrop, developing mechanisms that allow users to seek recourse against intermediaries adds an appealing third option—one that would allow for the continued development of these technologies without having to forego generativity or cede control of the architecture to a walled-garden experience.

Any framework for a law of intermediaries therefore has parallel goals. First, recourse must be available for users to accept active intermediation. But that legal remedy cannot be static—the Internet architecture is changing,

[116] *See* Camp et al., *supra* note 6, at 97 ("Previous research has supported the hypothesis that people are more trusting of computers than of other people.").

[117] *See* TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES 260-64 (2010) (discussing the use of "walled gardens" to consolidate dominance in the Internet as has happened in the past with other competitive new technologies); ZITTRAIN, *supra* note 100, at 29 (describing "walled gardens" using the examples of AOL and CompuServe); *see also* Schneier, *supra* note 100 (discussing consumers' increased reliance on external applications, hardware, and Internet resources to provide security).

[118] *See* Johnson et al., *supra* note 4, at 11 (noting that "it may be possible and advisable to shift" to a "'connect only with whom you trust' model" of the Internet); *see also* David D. Clark & Marjory S. Blumenthal, *The End-to-End Argument and Application Design: The Role of Trust*, 63 FED. COMM. L.J. 357, 380-83 (2010) (proposing modularization in application design to promote trust in networks). Fundamentally, walled gardens are a form of vertical integration.

and will change in response to the law. The better approach is to provide a framework: a menu of legal rules that will apply as the architecture changes. Such a framework will provide guidance both to legal institutions to which users might turn when they feel they have been harmed, and also to technologists and engineers as they develop and implement next-generation architectures.

### B. *A Framework for Intermediary Liability*

In 1972, Calabresi and Melamed synthesized approaches from various areas of law into a coherent framework of remedies.[119] Their approach considered two factors: which party should bear the benefit of a given entitlement, and what mechanism should protect that benefit.[120] They identified two common mechanisms[121]: property rules and liability rules, which are distinguished by how clearly the entitlement can be delineated and valued between the parties.[122] This approach provides a basic framework for considering intermediary liability.

Intuitively, it seems that a user's data—as suggested by the very term "user's data"—is property-like. This understanding is too simplistic. The primary characteristic of property-like rights is the right to exclude, or to seek an injunction precluding others from encroaching upon that right. It is certainly the case that users can exclude intermediaries from causing any harm to them by simply not engaging in online interactions. But at the time of the relevant interaction, the user has necessarily relinquished control of her data to the intermediary. We must therefore focus the inquiry on the rights available to that subset of individuals who have elected to subject their data to an architecture that does not support a property-like delineation of rights.

The characteristics of the current Internet architecture—transparency and independence of intermediaries—militate in favor of assigning the benefit of the entitlement to the user but treating it under a liability rule. Liability rules are useful where "the cost of establishing the value . . . by negotiation is so great that even though a transfer of the entitlement would

[119] *See* Calabresi & Melamed, *supra* note 66, at 1089-93 (summarizing their framework of legal entitlements and remedies).

[120] *Id.* at 1093.

[121] They also identify a third mechanism: inalienability rules. *See id.* at 1092-93 ("[R]ules of inalienability not only 'protect' the entitlement; they may also be viewed as limiting or regulating the grant of the entitlement itself."). These rules, however, do not apply well in the present context. *See generally* Lee Anne Fennell, *Adjusting Alienability*, 122 HARV. L. REV. 1403, 1409-27 (2009) (offering a detailed exploration of inalienability rules).

[122] Calabresi & Melamed, *supra* note 66, at 1105.

benefit all concerned, such a transfer will not occur."[123] This is precisely the situation presented online. Due to the transparency and independence of intermediaries in the current architecture, it is implausible that either side could seek out the other to negotiate the terms of an intermediary's handling of a user's data.

It is reasonable, however, to assign the benefit of the entitlement to the user, for two reasons. First, as a matter of traditional application of the Calabresi and Melamed framework, the informational asymmetries resulting from the transparency and independence of intermediaries suggest that the burden of ensuring the entitlement be put to its highest-value use falls upon the intermediary. Since the benefit of the use of individuals' data must accrue to those individuals, this requires the intermediaries to use this data to the benefit of the users.[124] Second, this information asymmetry exists as a result of design decisions in implementing the Internet architecture—that is, in developing and implementing the intermediaries that comprise the Internet's core. The burden to protect those whom these decisions harm should fall upon those making such decisions.

Importantly, this set of rules can change as the capabilities of the Internet architecture changes: Further, if the current set of rules is suboptimal (e.g., it unduly burdens intermediaries), this framework creates incentives for engineers to develop new technologies that increase the efficiency of the rules.

For instance, these rules may encourage the development of technologies that give users greater control over their data; both to specify how it can or cannot be handled and to monitor that it is, in fact, handled in accord with those specifications. In such a case, the clearer delineation of rights would suggest placing the burden on users to ensure that their data was being handled in accordance with their expectations, and to refuse to deal with intermediaries that would not adhere to those expectations. This would mark a transition toward property rules; accordingly, the burden of ensuring the efficient use of the entitlement would be placed on the users.[125]

We can see how this framework would play out as new technologies develop. For instance, users today cannot specify whether their data is handled by routers and switches implementing deep packet inspection or quality-of-service technologies, let alone monitor whether such preferences

[123] *Id.* at 1106.

[124] This is true of even the subset of users who have given control over their data to intermediaries; they would not have done so unless it was beneficial to them.

[125] That is, in the event of a lawsuit, the entitlement would favor the intermediary, unless the user could prove harm.

are respected.[126] Under the framework's approach, users concerned about whether their data is being unduly deprioritized by any of a group of intermediaries should be able to bring a lawsuit against that group as a whole.[127] The burden would be on the intermediaries to demonstrate that that they handled the user's data in a manner consistent with the user's interests, as best as the intermediary could discern them to be.

In response, mechanisms foreseeably could be developed to allow users to specify whether they want, or are willing to allow, their data to be subject to prioritization. In fact, technical mechanisms allowing this specification are already being developed.[128] As such mechanisms become available and robust, we should expect the burden to shift: once users can express expectations for how their data will be handled, they should use that capability. Failure to do so would give rise to a reasonable inference that those users are not sufficiently concerned about how their data is handled to justify damages.

Another example can be found in the evolving "do not track" standard,[129] the purpose of which is to allow users to specify whether they want web intermediaries to track their online activity. In a world without this technology—that is, as the world exists today—we should expect liability rules with burdens placed upon intermediaries to protect, and to prove that they have protected, the entitlement.[130] But as web browsers implement "do not track," allowing for a clearer delineation of rights, we should transition

[126] They have limited ability to specify a QoS preference, the meaning of which is ambiguous and not consistently used.

[127] For an example of such a lawsuit, see generally First Amended Class Action Complaint, *Hart v. Comcast*, No. 07-6350 (N.D. Cal. June 25, 2008), 2008 WL 5185811. In that instance, because there was privity and express terms of service, users were able to file a suit (which resulted in a class action settlement), including under California consumer protection laws. Such a suit, however, would not have been possible against any intermediaries other than the consumers' ISP, due to lack of a contractual relationship.

[128] Such mechanisms could be incorporated into the network layer via the IP header, or at the transport layer, perhaps as part of the RSVP protocol. *See generally* R. Braden et al., *Resource ReSerVation Protocol (RSVP)* (IETF Network Working Grp. RFC No. 2205, 1997), *available at* http://www.rfc-editor.org/rfc/pdfrfc/rfc2205.txt.pdf (outlining the specifications for RSVP, a protocol that allows users to request specific resources for, or handling of, their data as it traverses the Internet).

[129] *See Do Not Track-Universal Web Tracking Opt Out*, DO NOT TRACK, http://donottrack.us (last visited Mar. 15, 2013) (describing the "do not track" proposal, which would provide users with "a single, simple, persistent choice to opt out of third-party web tracking" via an HTTP header).

[130] Thus, we might expect to find no liability if an intermediary shares information needed to generate advertising revenue commensurate with the price it would charge the user for access to the site; however, we would find liability if the intermediary indiscriminately shared this information or shared more information than was needed to generate sufficient advertising revenue.

to a property-like rule with burdens placed on the user to make use of "do not track" technology.

Calabresi and Melamed present an argument that, at first blush, can be understood as *opposing* the treatment of "do not track" headers under a property rule. They use hold-out and free-riding problems as examples of situations in which liability rules are preferable to property rules. Under an advertisement-supported model, "do not track" can support free-riding behaviors: users could refuse to share their information with targeted advertisers while benefiting from the services funded by others who have shared such information. But so long as web sites are able to treat users differently based upon the content of the users' "do not track" preferences, there is no free-riding problem. To the contrary, a website confronted with a "do not track" user confronts the perfect opportunity to engage in the voluntary transactions that define property rules. The site needs only to present "do not track" users with a blank page explaining that the site is funded by either advertising or subscription revenue, and present the user with a set of choices: allow tracking, make a direct payment to the website, or take her web-browsing business elsewhere.

### C. *Some Specifics*

This framework presents specific recommendations to facilitate online interactions on today's Internet. But it is unwise to develop comprehensive rules only for the current architecture—the Internet's architecture is still evolving and does not yet present a stable institutional equilibrium. Any rules we adopt today will likely be obsolete all too soon. Indeed, the greater purpose of these recommendations is to hasten the architecture's movement toward a stable institutional equilibrium.

The most important task might be to establish the *possibility* of intermediary liability on today's Internet. Unfortunately, a number of obstacles stand in the way. First, section 230 of the Communications Decency Act of 1996 has long stood for a broad proposition of immunity for intermediaries.[131] It is unclear—and hopefully unlikely—that courts would apply the statute so broadly as to encompass the broad class of intermediaries considered in this Article.[132] Regardless, an important justification for this statute—the

[131] *See* Pub. L. No. 104-104, sec. 509, § 230(c)(1), 110 Stat. 133, 138 (codified as amended at 47 U.S.C. § 230(c)(1) (2006)) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

[132] Courts have consistently interpreted the Communications Decency Act broadly, almost certainly beyond the boundaries contemplated by Congress. *See* David Lukmire, *Can the Courts*

need to provide for the Internet to develop unfettered by investment-stifling regulation—is no longer relevant in the current architecture. This section is as outdated as its justification, so it should (at minimum) be updated.

Indeed, where intermediaries once needed immunity to encourage development, today the prospect of liability may more effectively encourage development. We are beyond the point where the goal is simply to make the Internet work; today, our goal should be to make it work *well*. Too often, we have been slow to deploy well-designed technologies, instead allowing ourselves to be satisfied with *good-enough* technologies until the system breaks. Engineers have recognized the benefits of AQM for twenty years, but today only the simplest forms of this technology have been implemented to any significant extent.[133] The same can be said of IPv6: first developed in the late 1990s, it is only just now beginning to be deployed seriously. Similarly, security has too often been an afterthought, even in the face of known dangers.[134] Immunity-based approaches, if anything, encourage the development of technologies whose value accrues to the intermediaries and discourage the development of technologies whose benefits accrue primarily to users. Liability rules reverse the effects of these incentives.

These considerations suggest a second recommendation: the statutory immunity regime should give way to statutory liability rules. The difficulty of establishing and measuring harm and the limitations of existing causes of action suggest a need for statutorily cognizable damages. The precise target or level of damages is less important than their mere existence. Perhaps the solution is as simple as allowing statutory cost-shifting in favor of plaintiffs who bring reasonable claims. The primary goal of this approach is to encourage the development and use of technologies that give users control of their online interactions.

Third, courts should recognize broad joint and several liability, both as part of a liability rule and as an information-forcing mechanism to ensure that intermediaries handle information to the benefit of users.

*Tame the Communications Decency Act?: The Reverberations of* Zeran v. America Online, 66 N.Y.U. ANN. SURV. AM. L. 371, 372 (2010) ("Over the years, state and federal courts have interpreted section 230 expansively, conferring a broad immunity upon website operators that host third-party content.").

[133] *See, e.g.*, B. Braden et al., *Recommendations on Queue Management and Congestion Avoidance in the Internet* (IETF Network Working Grp. RFC No. 2309, 1998), *available at* http://tools.ietf.org/pdf/rfc2309.pdf (describing AQM as providing "[t]he solution to the full-queues problem . . . [because it allows] routers to drop packets before a queue becomes full, so that end nodes can respond to congestion before buffers overflow").

[134] *See supra* note 9.

Finally, regulatory intervention should be sought only as a backstop when private causes of action fail. Regulation likely has a role to play in many types of online interaction, but it is a heavy hand upon a delicate technology. Regulation lacks the nuance of voluntary negotiations between parties—it is the ultimate liability rule. As demonstrated by "do not track," technology can facilitate voluntary interactions between parties subject to property-like rules. Regulation should be careful to encourage, not stifle, such innovation.

## CONCLUSION

The early model of the Internet—a relatively simple network that was designed, constructed, and used by a relatively small community of research and governmental institutions, with broadly aligned incentives—is a thing of the past. In that early iteration, trust was a sufficient mechanism to order online interactions. But as the range of uses and users has grown, and as incentives have diversified, there is and will continue to be an increasing need for more sophisticated mechanisms to mediate these conflicting incentives.

This Article has looked at one set of conflicting incentives—that between users and intermediaries—and has considered users' need to hold intermediaries accountable for any harm that they may cause to users. Historically, this has not been a relevant consideration, both because the technology has been simple enough (i.e., passive) that intermediaries have had limited ability to cause individualized harm, and because intermediaries and users had aligned incentives. But this is no longer the case.

The challenge moving forward is that the technological design principles of the Internet—the very things that give the Internet its character and have allowed it to thrive—also make establishing liability for intermediaries difficult. By design, intermediaries are supposed to operate transparently and independently. Users are not supposed to, or even be able to, directly observe how intermediaries operate, control which intermediaries are used in their online interactions, or even know which intermediaries these are. These technological principles make establishing liability difficult, if not impossible.

This is worrisome because the Internet is still evolving, and it is unclear how it will continue to develop. Three possibilities present themselves. First, the Internet could return to its earlier passive-intermediary model. This is largely the world advanced by advocates of network neutrality and broad privacy protections. Though a move backward in technological time, and one that would limit value created by active intermediation, this option may be preferable to the second alternative: increased vertical integration between intermediaries. This approach would reduce the number of intermediaries, thereby making intermediary liability easier to establish. But it would also reduce the range of uses available to Internet users. In Zittrain's language, it would limit the generative nature of the Internet, moving us further toward a walled-garden model.[135] While integrated intermediaries would likely maximize specific, highest-value uses of the Internet, they would do so at the expense of the myriad low- and uncertain-value uses that have made the Internet such a fertile platform for innovation.

Intermediary liability presents, and is a necessary condition for, a third option: a network of active intermediaries accountable to users. This approach allows for value-creating active intermediation, but constrains intermediaries from using active technologies contrary to users' interests.

The challenge lies in establishing intermediary liability, especially given the technological limitations created by transparency and independence. This Article has suggested a framework for establishing such liability, modeled on Calebresi and Melamed's model of liability and property rules. Under this framework, today's intermediaries would be governed by broad liability rules with burdens placed on the intermediaries themselves to prove that they have not harmed users. But, as technology develops, it may give users greater control over how their data is used, a shift that this framework hopefully encourages. In the case that technological advances do provide such increased control, intermediaries would be better governed by property rules with burdens placed on users to exercise control over their data. Such an approach would present engineers with a menu of options, so that they may understand the legal consequences that follow from technical design decisions.

Fundamentally, this menu approach helps to align the incentives of engineers and those of the law. Historically, the Internet was developed to accomplish technical objectives, with little consideration of the legal ramifications of technological decisions. Given the uncertainty of the underlying technology, this was a reasonable approach. But the Internet is now an established social and economic infrastructure, and legal concerns need to be incorporated into its ongoing development. By adopting a framework rather than trying to develop specific legal rules, this Article hopefully provides guidance to technologists for understanding the legal consequences of their technological decisions, so that they can balance technical and legal considerations.

[135] *See* ZITTRAIN, *supra* note 100.

On the legal side of the equation, this Article raises the prospect of imposing liability on intermediaries. Establishing such liability is difficult under current law: neither common law nor statutory law is well-suited to the task. Nonetheless, such liability is important to the continued vitality of the evolving Internet. It is important that we understand how the law may apply vis-à-vis users and intermediaries. This Article therefore makes a number of discrete proposals, with the overarching purpose of channeling the ongoing technological development of the Internet along a path that will normalize the availability of legal recourse for online interactions with that of other legal institutions. As particular examples, this Article argues that section 230 should be revised to clarify (and narrow) the extent of intermediary immunity provisions; statutory liability rules should be used to augment existing rules where the Internet's architecture may limit the viability of civil recourse; and civil courts should broadly embrace joint and several liability, and similar rules, both to ensure the availability of civil recourse to individuals harmed by intermediaries and to encourage the development of future technologies that better facilitate intermediary liability.