RESPONSE

WHAT'S "ACTIVE INTERMEDIARIES" GOT TO DO WITH IT?

JERRY KANG†

In response to Justin Hurwitz, *Trust and Online Interaction*, 161 U. PA. L. REV. 1579 (2013).

I. CAGE MATCHES, THE INTERNET, AND TRUST

Suppose that I am about to engage in potentially risky activity. It might be bungee jumping, shopping on eBay, or sparring. Suppose further that I am "rational" in the standard rational choice theory sense.[1] In other words, I always try to ensure that Benefits exceed Costs ($B > C$). Let's focus on Costs. How might I estimate the potential Costs of my behavior?

I certainly would consider the potential Harm of the activity. In other words, I would consider my subjectively determined ex ante expectation value[2] of the Harm resulting from engaging in the activity (H). But suppose further that even if Harm takes place, there may be some possibility of recourse. If so, I would also consider the ex post expectation value of

† Professor of Law, Korea Times-*Hankook Ilbo* Chair in Korean American Studies and Law, UCLA School of Law.

1 By "rational," I mean very loosely that natural persons try to maximize something called "utility;" analogously, firms try to maximize "profit." In invoking this model, I'm agreeing to have the conversation on the conceptual terrain that Professor Hurwitz implicitly stakes out, as evidenced by his favorable citations to works by Coase, Jensen and Meckling, Ellickson, and Calabresi and Melamed. *See* Justin Hurwitz, *Trust and Online Interaction*, 161 U. PA. L. REV. 1579, 1600-01, 1602, 1615-18 (2013).

2 By "expectation value," I mean the product of the probability of the event taking place and its magnitude.

receiving Recourse (R).[3] In this simple model, my estimation of the Costs of engaging in the risky activity is Harm minus Recourse, ($C = H - R$). Let's run through some concrete examples.

Example 1: Light Sparring. Suppose that I am trying to decide whether to spar with my young daughter who's studying taekwondo. Given my relative advantage in size, strength, and experience, H is extremely low. Our interests are also aligned since we don't want to hurt each other. For me, there is almost no chance of significant injury. In such cases, I do not even consider what Recourse might be available—for instance, whether I could sue my daughter for medical bills or shame her publicly—because Harm is so low.

Example 2: Cage Match. By contrast, suppose that I'm trying to decide whether to enter an amateur mixed martial arts competition. Given my relative disadvantage in age, size, strength, and viciousness, H is extremely high. Some sort of injury is very likely; even catastrophic injury is possible. Indeed, some of the competitors might not obey the rules. They might take steroids, strike to the back of the head, or not release a strangle or joint lock promptly upon surrender. My groin cup could fail. Or maybe the referee could be slow to respond and take too long to call a TKO. For all these reasons, Harm is very high, in which case I must consider more seriously my ex post expectation value of Recourse. Are there any "deep pockets" to go after, and could money actually make me whole if I'm paralyzed? The size of R suddenly matters.

What do a rational choice model of cage matches and Professor Hurwitz's analysis of the Internet have to do with one another? Not much, really, except for *trust*. Specifically, my model clarifies the relationship between harm and recourse in Hurwitz's understanding of "trust," which he defines as "reliance without recourse."[4] If we are rational, why would we ever trust in the sense of relying without recourse? One reason could be that we think Harm is minimal. Recall *Example 1: Light Sparring*. If Harm is de minimis, who cares whether any Recourse is available? By contrast, when H is high—as in *Example 2: Cage Match*—a rational person would try to figure out what Recourse is available.

According to Hurwitz's narrative, a long, long time ago, in the era of the "Early Internet," using the Internet was safe.[5] People were nice and agreeable; networks were simple and well understood; not much was at stake.[6] This

---

[3] Let's fold the transaction costs of obtaining relief into R itself. These costs would reduce R.

[4] *See* Hurwitz, *supra* note 1, at 1584 ("[O]ne 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.").

[5] *Id.* at 1585-88.

[6] *Id.*

description sounds a lot like *Example 1: Light Sparring*. In other words, there was "trust" on the Internet because *H* was low. This characterization of the "Early Internet" sounds somewhat nostalgic, but let's suppose that, once upon a time, the Internet was as Hurwitz describes.

But now, Hurwitz claims the "brave new Internet"[7] has become much more dangerous.[8] Harm is rising, and rising fast. Interestingly, Hurwitz attributes this change to the rise of "active intermediaries."[9] Since *H* has risen, we, as rational beings, presumably should be much more concerned about *R*.[10] And by definition, being so concerned means we no longer blindly trust. Using the Internet has become much more like *Example 2: Cage Match*.

In this post-trust era of the Internet, Hurwitz predicts that users will try to contain overall Costs by reducing Harm.[11] How? By opting out of active intermediation, which Hurwitz believes will pose its own problems.[12] Hurwitz suggests an alternative strategy. Rather than *reducing H*, he would try to *increase R*—not through any method as ham-fisted as comprehensive regulation, but by creating some sort of dynamic legal "framework" for private causes of action.[13]

II. Active Intermediaries

Hurwitz's central diagnosis is that Harm is increasing because of the rise of active intermediaries. To evaluate this claim, we must know what he means by "active intermediary."

---

7 *Id.* at 1592.

8 *Id.* at 1592-97.

9 *Id.* at 1581; *see also id.* at 1590-92 (describing how the character of the Internet changed in the 1990s and characterizing the rise of active intermediaries as the "greatest technological change to the Internet architecture" during that period).

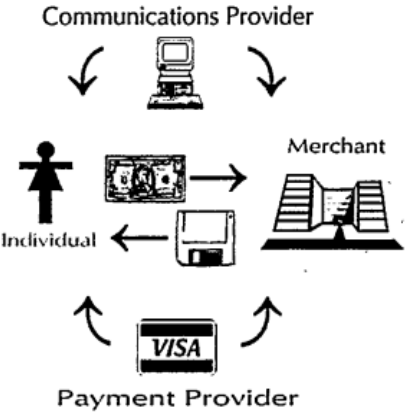
10 *See id.* at 1585 ("As harm has become a concern, so too has the need for protection from that harm. Absent the availability of recourse against such harms, users must alter their behavior to protect against them.").

11 *Id.*

12 *See id.* at 1595 (arguing that "active intermediation has the potential to add substantial value to the Internet value chain").

13 *Id.* at 1615.

Intermediary. Way back in 1998, in modeling the privacy implications of Internet transactions, I offered the following schematic[14]:



In this diagram, the "transacting parties" (or counterparties) are the *Individual* and the *Merchant*; the "transaction facilitators" are divided into two categories, *Communications Provider* and *Payment Provider*.[15] In my view, these transaction facilitators are the "intermediaries" to the counterparties' interaction. I offer this schematic in the hope that it will help to clarify Hurwitz's use of the term "intermediary."

Unfortunately, Hurwitz does not provide a clean, precise definition of "intermediary." We can, however, glean some clues from the following passages. According to Hurwitz:

> 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* . . . —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. 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.[16]

---

14 Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1223 (1998).

15 *Id.* at 1224, 1232.

16 Hurwitz, *supra* note 1, at 1590 (emphasis added) (footnote omitted).

This passage suggests that "intermediaries" encompass hardware, including off-the-shelf networking components, such as switches and routers. They also apparently include software, such as applications and services. Interestingly, intermediaries—as Hurwitz uses the term—needn't be legal persons. An intermediary could be the WiFi router you just bought from Best Buy, or some huge piece of machinery, sitting in some air-conditioned building downtown, that is part of the Internet's guts.[17] Hurwitz doesn't, however, expressly exclude legal persons, such as Internet Service Providers, from his definition.[18] Thus, "intermediary" seems quite broad in scope.

Two further observations: First, I'm not sure whether Hurwitz considers Visa—which I call a Payment Provider—an "intermediary." Surely credit card firms intermediate Internet transactions, but Hurwitz might be interested only in those persons and things that intermediate electronic communications, not finances. Second, I presume that Hurwitz wishes to maintain a distinction between *counterparties* (the transacting parties) and *intermediaries*, who merely facilitate an interaction between the counterparties.

Active. The above passage also sheds light on what it means to be "active," which is to be complex (rather than stupidly and passively forwarding datagrams as received)[19] and responsive to various environmental conditions (rather than exhibiting slave-like obedience to user requests).[20] Hurwitz continues:

> [T]he 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.[21]

This suggests that being "active" also means using and manipulating user data, behavior that is consistent with being dynamically responsive to environmental conditions. We are further told that "active intermediaries" may have incentives that differ from individual users. We normally don't think of hardware as having "incentives," but it is designed to accomplish certain goals, which could conflict with a user's preferences.

---

17 *See id.* at 1580-81 ("All online interactions are conducted through intermediaries—the routers, servers, applications, services, and switches that make up the Internet's 'core.'").

18 *See, e.g.*, *id.* at 1593 n.46, 1603 n.83 (classifying certificate authorities, which are "human entit[ies]," as "intermediaries").

19 *Id.* at 1590.

20 *Id.*

21 *Id.* at 1592 (emphasis added).

Finally, Hurwitz writes:

> 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. . . . Similarly, active intermediaries can *collect and manipulate user information* in ways that are entirely transparent to users.[22]

This cements a particular understanding of Hurwitz's conception of "active."

To summarize, Hurwitz seems to use "intermediaries" to describe things (software and hardware) and legal persons that somehow facilitate Internet communications—roughly what I call "Communications Providers." They express their "active" nature by prioritizing data traffic[23] (think "net neutrality"[24]) or processing user information[25] (think "privacy"). Put in slightly tendentious terms, Hurwitz's "active intermediary" is a thing or person that facilitates Internet communication by responding dynamically to the environment in ways that (arguably) violate net neutrality and privacy.

Having teased out what Hurwitz means by "active intermediaries," we confront the next basic question: Are active intermediaries the principal reason that Harm is rising on the Internet? I'm not sure.

Consider the various salient sources of increased Harm on the Internet. First, think of *hackers*, who steal personal information and wreck websites for economic and political gain. They can't be viewed as "intermediaries" under Hurwitz's definition because facilitating Internet interactions is neither their goal nor function.

Second, think of *cyberbullying*, which periodically prompts hopeless teenagers to commit suicide and may disproportionately impact women's physical and emotional well-being.[26] Are mean and taunting anonymous posts on unmoderated bulletin boards primarily attributable to the actions of any "intermediary," active or otherwise? Or are they the cruel and malicious deeds of posters who do not intermediate anything?[27]

---

22 *Id.* at 1593 (emphasis added).

23 *Id.*

24 It might seem odd to bring net neutrality into the conversation, but Hurwitz does just that. *See id.* at 1581 ("[U]sers 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.").

25 *See id.* at 1593 ("[A]ctive intermediaries can collect and manipulate user information in ways that are entirely transparent to users."). By "transparent," Hurwitz means invisible or without notice to users.

26 *See* Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373, 384-90 (2009).

27 The same logic applies for cyberstalking.

Third, think of exposure to *inappropriate content*, be it sexual or violent. Sometimes such material is accessed intentionally by a curious kid in defiance of parental wishes; other times it is stumbled upon accidentally. In either case, is the easy accessibility of hardcore pornography or crush films really a problem caused by being "active," in the sense of prioritizing delivery of certain types of Internet protocol packets or mining user data?

Fourth, think of *oversharing personal information* on social media sites, where TMI ("Too Much Information") is SOP ("Standard Operating Procedure"). If I share my drunken, naked pictures with my vast network of so-called "friends" and a prospective employer rejects my application because of these photos, was my Harm induced by active intermediaries? Or was it caused by Facebook—which, though part intermediary, is also at least as much a *counterparty* to the transaction—and governed by its Terms of Service, which I gladly (and blindly) clicked through?

I don't mean to strawman Hurwitz's argument. He specifically concedes that harm on the Internet comes from multiple sources, including other users.[28] But he repeatedly insists on emphasizing that active intermediaries "have become a vector for harming end users."[29] On the one hand, Hurwitz is certainly right. Of course things and persons that facilitate Internet communications by prioritizing user data (thereby arguably violating net neutrality) and mining personal data (thereby arguably violating privacy) can cause Harm. This claim—that net neutrality violations can cause net neutrality–related harms and privacy violations can cause privacy-based harms—is almost tautological. On the other hand, this sets far too low a bar. Almost anything, even a butter knife, can cause *some* harm. Hurwitz's proposition must be that active intermediaries cause so much harm—or such distinctive harm relative to the harm created by all other Internet sources—that users will notice these intermediaries and incrementally change their behavior, either by opting out of active intermediation specifically or out of the Internet altogether. To me, that result doesn't seem likely.

III. USER DROP OUT

In Part II, I contested Hurwitz's claim that active intermediaries were the dominant—or an especially salient—source of increasing Harm on the Internet. Although intermediaries no doubt contribute to this increased

---

[28] *See* Hurwitz, *supra* note 1, at 1592 ("Users can be harmed online through many vectors. The best-known concern is harm from other users.").

[29] *Id.* at 1593.

Harm, they are not its principal drivers. Hurwitz and I do agree, however, that *H* is on the rise on the Internet.

How will users respond? Hurwitz suggests that users eventually will realize that *H* is rising, attribute that increase to active intermediaries, and stop using these intermediaries[30] or maybe even the Internet as a whole.[31] This decrease in demand for intermediaries' services will, in turn, reduce the supply of active intermediation technologies,[32] which is not entirely a good thing because Hurwitz sees value in intermediation's data prioritization and data mining.[33] In other words, violating net neutrality and privacy is not all bad. After all, one person's net neutrality is another person's ineffective network management; one's privacy violation is another's efficient targeted marketing.[34] Notice the potential inconsistency, or tradeoff, that Hurwitz's analysis presents: Harm on the Internet—at least from an individual user's perspective—is rising because of active intermediaries, but active intermediation also produces societal Benefits.

Consider all the links in Hurwitz's proposed causal chain. I agree that users may vaguely sense that *H* is increasing, even though the Internet is also becoming more ubiquitous and routine, which decreases the perceived threat. Even so, do users view the danger as coming from active intermediaries? When a parent thinks about making sure that his pre-teen is safe on the Internet, what threat preoccupies him? Is it the threat of Quality of Service packet prioritization that keeps him up at night and off the Internet? For reasons explained in Part II, I doubt that typical users will attribute their vague sense of rising *H* to "active intermediaries."

More importantly, regardless of users' views toward active intermediaries, there is little reason to think that users actually will stop using the Internet, which would likely be the only way to opt out of using active intermediaries that are embedded invisibly (as opposed to transparently)

---

30 *See, e.g.*, *id.* at 1581 ("First, users lacking the ability to seek recourse may demand that active intermediation *not* be used. . . . 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 . . . ."); *id.* at 1592 ("Absent a mechanism to prevent such use—or, in the language of trust, 'recourse'—we can expect users to resist active intermediation."); *id.* at 1596 ("The natural response to these concerns is, and has been, to resist active intermediation.").

31 *See id.* at 1590-91 ("[I]t is possible, even likely, that the post-trust Internet will disabuse users of this predisposition [to trust impersonal interactions] over time. When the curtain is pulled back, so to speak, it is unclear what will replace trust in allowing users to feel confident in the network.").

32 *Id.* at 1581.

33 *See id.* at 1595-96 (arguing that active intermediation technologies, such as statistical multiplexing and targeted advertising, benefit users).

34 *See* Kang, *supra* note 14, at 1217-18 (noting that "privacy applies friction to the flow of information," which can hurt commerce because, presumably, "better information leads to better markets").

into the communications architecture. Consider how many hacking scandals and Facebook and Google privacy disasters there have been in recent years. And yet, users generally have not opted out.

Perhaps users continue to use the Internet because of information asymmetry—that is, because they don't know what is really going on. Or, it might be that Benefits still outweigh Costs, even as Costs have been increasing.[35] Hurwitz's Article focuses only on the cost side of the equation, where $C = H - R$. But even if Harm is increasing, the Benefits of using the Internet may be so great that most people simply won't opt out. Consider the value of Facebook to a sociable teenager: For her, B seems infinite. No matter how high H (and thus C) becomes, my guess is that $B > C$ for that teenager. She won't opt out.

Hurwitz might respond that one can stay on the Internet and still opt out of active intermediation. According to Hurwitz, the way to do so would be to protest loudly in favor of net neutrality and against privacy-invading communications technologies.[36] On the one hand, I guess this is true, but on the other, this response betrays a certain oddness in the problem's framing. Somehow, both net neutrality and privacy have been reincorporated as a problem of "active intermediaries." But privacy anxiety is hardly limited to intermediaries. Amazon knows what you buy; Google knows what you email and search for; Facebook knows your life. Are these all "intermediaries" according to Hurwitz's use of the term? No, they are counterparties.

In addition, active intermediation is only loosely related to the problem of net neutrality. Suppose, for example, that the FCC had classified Internet access as a "telecommunications service" under Title II of the Communications Act.[37] This would have satisfied the strongest proponents of net neutrality. Yet this legal classification would not have forced any radical change to or dumbing down of currently deployed routers, switches, applications, or services, which Hurwitz describes as already being "active." Or consider the FCC's recently adopted Open Internet rules, which explicitly permit reasonable network management practices.[38] Certainly those practices

---

35 Recall the basic analytics from the opening of my Response. If we assume that people are rational, Benefits of using the Internet must exceed Costs.

36 *See* Hurwitz, *supra* note 1, at 1596-97 (citing the public's response to network neutrality and online privacy concerns as examples of users resisting active intermediation).

37 Instead, the FCC classified broadband cable Internet service as a Title I "information service," a category not subject to common-carrier regulations. *See* Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 973-76, 1003 (2005) (affirming the FCC's classification).

38 See 47 C.F.R. § 8.11(d) (2012) ("*Reasonable network management*. A network management practice is reasonable if it is appropriate and tailored to achieving a legitimate network management

would leverage the fact that intermediaries are in some sense "active," but doing so would be entirely consistent with a neutral or "open" Internet.

IV. UNDERSPECIFIED SOLUTION

In Part II, I suggested that Hurwitz's diagnosis is suspect (rising *H* is not driven substantially by active intermediaries). In Part III, I questioned whether users would defend themselves by opting out of the Internet generally, or active intermediation specifically. In particular, Hurwitz never demonstrated that, even with active intermediaries, Benefits will be subjectively estimated to be lower than Costs ($B < C$) for most users. But suppose I'm mistaken on both matters. Assuming that *H* is rising principally or saliently because of active intermediaries, and assuming that users will respond by opting out of using either the Internet or active intermediaries, what's Hurwitz's solution?

Recall that Cost = Harm – Recourse ($C = H - R$). Instead of trying to decrease *H* (by killing off active intermediation), Hurwitz wants to increase *R*. Because Hurwitz explains that vertical integration and "endogenous" mechanisms, such as reputation and encryption, are deeply limited,[39] he reluctantly considers potential legal reforms to achieve this end. To be clear, he is no fan of comprehensive regulation. Rather, he seeks a softer, more dynamic "framework."

That framework draws on the famous work of Guido Calabresi and Douglas Melamed, which requires answering at least two questions: (1) Who should receive the initial legal entitlement, and (2) Should that entitlement be protected by a liability or a property rule?[40] Hurwitz concludes that the entitlement should be granted initially to the user, and should be protected by a liability rule.[41]

But it's unclear how this framework applies to active intermediation in the form of, say, data prioritization. Suppose that I'm Verizon, which provides last-mile broadband Internet service to an end user. Suppose that I become more "active" by speeding up certain content provider video packets

---

purpose, taking into account the particular network architecture and technology of the broadband Internet access service.").

[39] *See* Hurwitz, *supra* note 1, at 1608-13 (discussing the limitations of vertical integration and endogenous institutions).

[40] *Id.* at 1613-20; *see also* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1090-92 (1972) (describing their model).

[41] Hurwitz, *supra* note 1, at 1615-16. Liability rule protection permits the involuntary transfer of the entitlement if the buyer is willing to pay an objectively determined value for it. Calabresi & Melamed, *supra* note 40, at 1092.

because I've cut a deal to favor Hulu over Netflix. Applying Hurwitz's framework, we have to give the initial entitlement over "user data" to the user. But in my hypothetical, what counts as "user data"? Does it include the bits that constitute the movie I'm trying to stream from Netflix? Given preexisting intellectual property rights, in what sense does the user hold this entitlement? Are we talking about some legal entitlement to packet delivery without prioritization? If so, why should the individual user be granted that entitlement initially, considering extant background law (that Internet service is not common carriage)[42] and the contractual Terms of Service the user assented to?

Also, what does it mean to say that this entitlement should be protected by a liability rule? This suggests that Verizon must compensate me after it "takes" my entitlement without prior, explicit permission. Does Hurwitz's framework provide me with a tort action I can launch against Verizon? Would Hurwitz want me to have such a tort action, considering his suggestion that active intermediation of this sort provides societal benefits? It's all quite intriguing but frustratingly murky.

The "entitlement-to-user and liability rule" framework makes more sense as applied to privacy violations by intermediaries. However, this framework would have essentially no impact on counterparties, such as Facebook, which, by definition, aren't intermediaries. And even if Facebook were an intermediary, unless the entitlement is inalienable, a clickwrap license embedded in Facebook's Terms of Service would allow it to do whatever it wants to.

Finally, even with respect to intermediaries, Hurwitz's justification for initial entitlement and liability rule protection is a bit thin. As for initial entitlement to the user, Hurwitz smartly points out that we shouldn't take it for granted that the initial entitlement must go to the user because "the user has necessarily relinquished control of her data to the intermediary."[43] However, deeper analyses of and justifications for this initial entitlement have appeared elsewhere in the literature.[44] For example, I have demonstrated why initial entitlement to the user makes sense on both efficiency (applying an Ian Ayres–Robert Gertner default rule analysis)[45] and dignity grounds.[46]

---

42 *See supra* note 37 and accompanying text.

43 Hurwitz, *supra* note 1, at 1615.

44 *See, e.g.*, Jerry Kang & Benedikt Buchner, *Privacy in Atlantis*, 18 HARV. J.L. & TECH. 229, 237-40 (2004) (exploring the initial grant of entitlement problem).

45 *See* Kang, *supra* note 14, at 1249-59 (concluding, based on an efficiency analysis, that an information collector should be permitted to process personal data "only in functionally necessary ways," as opposed to processing it any way it likes); Kang & Buchner, *supra* note 44, at 238-40

As for liability rule protection (versus property rule protection), I'm left uncertain. There is extensive literature describing the rise of new sorts of markets for personal information—with matchmaking technologies that decrease transaction costs between buyers and sellers[47]—in ways that could justify applying a property rule requiring ex ante negotiations for taking personal information instead of providing ex post liability protection. Hurwitz specifically points out that one consequence of adopting the liability rule might be to encourage technologies that "allow users to specify whether they want, or are willing to allow, their data to be subject to prioritization."[48] If this is so, why wouldn't a property rule—which explicitly requires prior user authorization—encourage even more strongly the production of such technologies?

In addition to the Calabresi–Melamed framework, Hurwitz provides other specifics, suggesting, for example, that 47 U.S.C. § 230[49] might have to be modified. Section 230 immunizes a "provider or user of an interactive computer service" from being deemed a "publisher or speaker" of content provided by "another information content provider."[50] It has been interpreted by courts to provide a breathtakingly broad immunity,[51] and Hurwitz gestures toward a new regime with greater potential liability.[52] But it's not clear how this immunity has any application to the threat model that preoccupies Hurwitz.[53] First, there is no one-to-one mapping between the statute's "provider or user of an interactive computer service" and Hurwitz's "active intermediary." Second, according to Hurwitz, Harm on the Internet is increasing because of data prioritization and personal data mining, but neither process would tend to render the active intermediary the publisher

(suggesting that "it would be most efficient to give citizens [as opposed to merchants] the property right in the first place").

46 *See* Kang, *supra* note 14, at 1259-65 (arguing that cyberspace surveillance frequently infringes upon the dignity of the individual user); Kang & Buchner, *supra* note 44, at 234-36 (suggesting that privacy generally, and *information* privacy more specifically, can be viewed as a "fundamental human right").

47 *See, e.g.*, Jerry Kang et al., *Self-Surveillance Privacy*, 97 IOWA L. REV. 809, 836-37 (2012) (discussing "infomediaries" (information intermediaries) that reduce the costs of matchmaking).

48 Hurwitz, *supra* note 1, at 1617.

49 47 U.S.C. § 230 (2006).

50 47 U.S.C. § 230(c)(1).

51 *See, e.g.*, JERRY KANG, COMMUNICATIONS LAW AND POLICY: CASES AND MATERIALS 319-30 (Robert C. Clark et al. eds., 4th ed. 2012) (discussing cases that interpret 47 U.S.C. § 230, and noting that "[t]he immunity provided by § 230 has been stunning in its scope and strength").

52 *See* Hurwitz, *supra* note 1, at 1618 ("The most important task might be to establish the *possibility* of intermediary liability on today's Internet.").

53 Hurwitz briefly acknowledges this point. *See id.* ("It is unclear—and hopefully unlikely—that courts would apply [§ 230] so broadly as to encompass the broad class of intermediaries considered in this Article.").

or speaker of content provided by someone else, in which case the immunity offered by § 230 would remain irrelevant.

CONCLUSION

Hurwitz should be credited for focusing our attention on the importance of trust on the Internet, and on what might happen as trust erodes. But his construct of "active intermediaries"—which entangles hard questions about net neutrality and privacy—fails to diagnose precisely or solve concretely the problem. We should care and fight about net neutrality. We should care and fight about privacy. What I'm less sure about is whether we should do so under the rubric of "active intermediaries."

Preferred Citation: Jerry Kang, Response, *What's "Active Intermediaries" Got to Do With It?*, 161 U. PA. L. REV. ONLINE 303 (2013), http://www.pennlawreview.com/responses/5-2013/Kang.pdf.