University of Chicago Legal Forum

Volume 1996 | Issue 1 Article 22

Regulating Cyberactivity Disclosures: A Contractarian Approach

Keith Sharfman
Keith.Sharfman@chicagounbound.edu

Regulating Cyberactivity Disclosures: A Contractarian Approach

Keith Sharfman†

Users of an online service or operating system[1] providing access to the Internet often can monitor each other:[2] fellow users can discover each other's identities and can, at least to some extent, observe each other's 'cyberactivity.'[3] This 'disclosure environment' is beneficial insofar as the prospect of outside observation deters those who would otherwise engage in socially undesirable conduct[4] from so engaging.[5] The capacity for monitoring, however, is harmful in that it chills some socially useful activities as well.[6] Another ill effect of monitoring is that it ex-

---

† B.A. 1993, Johns Hopkins University; J.D. Candidate 1997, University of Chicago.

[1] The best example of this is "UNIX," the computer operating system most commonly used at universities to provide access to the Internet. The claim I make concerning monitoring is true for UNIX and is often true for other operating systems as well.

[2] For a description of this monitoring potential in the UNIX context, see Lawrence Lessig, *The Path of Cyberlaw*, 104 Yale L J 1743, 1748 (1995). In addition to being monitored by their peers, users can, of course, be monitored by system operators. Necessary monitoring by a single system operator whose identity is known (or can readily be discovered) by the user is, however, less surprising to the user and therefore less troubling than potential monitoring by a myriad of fellow users. For this reason, monitoring by system operators is not a concern of this Comment.

[3] 'Cyberactivity' is my own term and is meant to connote the various reading, browsing, and communications activities in which a system user might engage.

[4] Harassment, slander, blackmail, and (verbal) assault are examples of undesirable activities that are facilitated when the perpetrator is cloaked in anonymity. Several commentators have pointed to these and other potential abuses that would be facilitated by an anonymity environment. See George P. Long, III, *Who Are You?: Identity and Anonymity in Cyberspace*, 55 U Pitt L Rev 1177, 1184 (1994). Lamentably, such abuses have actually occurred. See *United States v Baker*, 890 F Supp 1375 (ED Mich 1995) (dismissing charges against college student who allegedly made anonymous, electronically transmitted threats to injure, kidnap, and rape a female classmate).

[5] Other possible benefits of a disclosure environment include: (1) the potential for businesses to identify likely consumers of their products at a low cost; (2) the potential for individuals to identify others with similar backgrounds, situations, predicaments, habits, or interests; and (3) the potential for individuals and businesses to learn from (either by copying or by avoiding the mistakes of) the "netsurfing" techniques of others.

[6] Such activities include the free exchange of controversial or unpopular ideas and freedom to associate with groups that espouse politically unpopular views. America's founders so highly valued these freedoms that their exercise is protected by the First Amendment to the U.S. Constitution. The Supreme Court has zealously enforced this protection, reviewing all government efforts to curtail these freedoms under a "strict scrutiny" standard. See *NAACP v Alabama*, 357 US 449, 461 (1958); *Gibson v Florida*

poses users who are unaware of a system's monitoring capabilities to potential invasions of their privacy.[7]

Against this backdrop of competing policy considerations, a debate now rages among academics and policymakers over how best to regulate cyberactivity disclosures. There are those who favor a governmentally imposed regime of mandatory disclosure,[8] arguing that the social gains from disclosure outweigh its attendant costs. Others, however, take the opposite view, arguing that anonymity ought to be guaranteed to protect the user's privacy notwithstanding the attendant social cost of this protection.[9] A third view[10] is that government—both legislatures and the courts—should neither guarantee nor ban anonymity but should instead adopt a 'wait and see' approach to give both society and governmental institutions sufficient time to arrive at a common

---

Legislative Investigation Committee, 372 US 539, 545 (1963).

[7] The cost here is the shame system users might feel upon finding out that their ostensibly private activities in fact were—or could have been—observed by others. The privacy concern raised by cyberspace is similar to the fear that telephone companies could disclose information about their customers' calling habits to third parties or the fear that video store proprietors could share information about their customers' viewing habits with third parties. In the telephone and video contexts, however, courts and legislatures have somewhat alleviated these privacy concerns. For an example of courts protecting customer privacy in the telephone context, see *Barasch v Bell Telephone Co.*, 529 Pa 523, 605 A2d 1198 (1992) (holding telephone company's "Caller ID" service violated state Wiretap Act because it nonconsensually deprived callers of their anonymity). For an example of protective legislation in the telephone context, see Cal Pub Util Code § 2891 (West 1994) (prohibiting telephone companies from disclosing what services their customers purchase). For legislation in the video context, see The Video and Library Protection Act of 1988, 18 USC § 2710(b) (1994) (prohibiting video providers from knowingly disclosing personal information about their customers, such as titles of movies rented, without first obtaining written consent). As yet, there are no similar analogous mandated privacy protections in cyberspace.

[8] Consider the proposal of Connecticut State Representative Pat Dillon "that would virtually eliminate anonymity on-line." Lessig, 104 Yale L J at 1750 n 20 (cited in note 2) (citing Beverly Galge, *The Babe File*, New Haven Advocate 7 (Feb 9, 1995)). See also Walter S. Mossberg, *Accountability Is Key to Democracy in the On-Line World*, Wall St J B1 (Jan 26, 1995) (arguing that "[o]ur democracy and society require accountability, not anonymity . . . ."). Some universities, including Harvard, have already forbidden anonymous postings. See Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 Yale L J 1639, 1643 n 11 (1995).

[9] Consider the vigorous defense of privacy and anonymity protections in response to the government's recent "Clipper Chip" proposal. Lessig, 104 Yale L J at 1751 n 23 (cited in note 2) (citing National Research Council, *Rights and Responsibilities of Participants in Networked Communities* 25 (Dorothy E. Denning & Herbert S. Lin, eds, National Academy Press, 1994)). Similar defenses of online anonymity abound on the Internet itself. For instance, see Raph Levien, *Chaos and Anonymity Keep the Internet Vital*, draft of editorial to be sent to San Francisco Chronicle posted on the Internet (Jan 14, 1995) (on file with the author).

[10] This view is espoused, principally, by Professor Lessig. See Lessig, 104 Yale L J at 1752-53 (cited in note 2). See also Branscomb, 104 Yale L J at 1678-79 (cited in note 8).

understanding of this new frontier called cyberspace.[11] A fourth view is that cyberactivity disclosure ought to be governed by contract.[12]

Proponents of the 'contract' approach to the regulation of cyberactivity disclosure have not suggested, however, what default rule[13] courts should adopt in the absence of an express contract.[14] Possible approaches include adopting either a

---

[11] Lessig, 104 Yale L J at 1754 n 32 (cited in note 2).

[12] The Clinton Administration has argued in favor of a contractarian approach in a recent Commerce Department White Paper. See Ronald H. Brown, et al, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information*, US Department of Commerce (1995) (arguing that system operators should be required to "provide notice" and to obtain "customer consent" before collecting and using "sensitive personal information" concerning their users, and to "provide notice" and to receive "tacit consent" before collecting and using any other nonsensitive, personal information). The 'contract' approach to cyberspace was first suggested in David R. Johnson and Kevin A. Marks, *Mapping Electronic Data Communications onto Existing Legal Metaphors: Should We Let Our Conscience (and Our Contracts) Be Our Guide?*, 38 Vill L Rev 487 (1993).

[13] Default rules determine the legal status of parties in the absence of express contractual provisions to the contrary. That is, they "fill the gaps" left open by incompletely specified agreements. On default rules generally, see Charles J. Goetz and Robert E. Scott, *The Limits of Expanded Choice: An Analysis of the Interactions Between Express and Implied Contract Terms*, 73 Cal L Rev 261 (1985); Ian Ayres and Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 Yale L J 87 (1989); Richard Craswell, *Contract Law, Default Rules, and the Philosophy of Promising*, 88 Mich L Rev 489 (1989); Jules L. Coleman, Douglas D. Heckathorn, and Steven M. Maser, *A Bargaining Theory Approach to Default Provisions and Disclosure Rules in Contract Law*, 12 Harv J L & Pub Pol 639 (1989); Randy E. Barnett, *The Sound of Silence: Default Rules and Contractual Consent*, 78 Va L Rev 821 (1992); Ian Ayres and Robert Gertner, *Strategic Contractual Inefficiency and the Optimal Choice of Legal Rules*, 101 Yale L J 729 (1992); *Symposium on Default Rules and Contractual Consent*, 3 S Cal Interdisciplinary L J 1 (1993). In the context of cyberactivity monitoring, statutes or common law doctrine could set the default rule in favor of either anonymity or disclosure. By definition, a default rule is "waivable" rather than "immutable." The party against whom the default rule is set can, with the other party's express agreement, have the rule waived in favor of an alternative rule. Ayres & Gertner, 99 Yale L J at 87.

[14] True, the Clinton Administration has argued that the customer's "consent" ought to be obtained, which is in effect an anonymity default rule. Notably absent from the government's White Paper, however, is a statement of how the proposed contract regime would be enforced. See Brown, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (cited in note 12). The paper leaves open the questions of injunctive relief and damage remedies for consumers whose privacy rights have been violated as well as the institutional issue of who should promulgate and enforce the rule—the legislature, the common law courts, or an administrative agency?

'market-mimicking'[15] or a 'penalty'[16] default rule around which the parties—system users and operators—can expressly contract.

Building on the default rule approach found in the academic literature on contracts, this Comment argues for the adoption of a default rule—either by statute or at common law—permitting system operators to disclose (or to facilitate disclosure of) their users' 'cyberactivities' to third parties, so long as users are warned ex ante that they will be operating in a disclosure environment and are offered an opportunity to 'opt out' if they choose. The Comment argues against both anonymity default and immutable, mandatory disclosure rules, as well as against Professor Lessig's 'wait and see' suggestion. The Comment rejects an anonymity default rule, because anonymity is probably not the preferred choice of most system users.[17] Likewise, the Comment rejects the mandatory disclosure approach because such a rule would deny privacy protection across the board—even to those who place an especially high value on privacy.[18] The Comment

---

[15] The phrase, coined by Charles Goetz and Robert Scott, suggests that "[i]deally, the preformulated rules supplied by the state should mimic the agreements contracting parties would reach were they costlessly to bargain out each detail of the transaction." Charles J. Goetz and Robert E. Scott, *The Mitigation Principle: Toward a General Theory of Contractual Obligation*, 69 Va L Rev 967, 971 (1983). The best expression of this 'market-mimicking' idea in an actual case is *Market Street Associates Ltd. v Frey*, 941 F2d 588, 596 (7th Cir 1991) (declaring the "overriding purpose of contract law" to be "to give the parties what they would have stipulated for expressly if at the time of making the contract they had had complete knowledge of the future and the costs of negotiating and adding provisions to the contract had been zero."). Market-mimicking default rules are sometimes referred to as 'majoritarian' because they mimic only what most people would have wanted to do in a given situation, not what everyone would have done. See Ayres & Gertner, 99 Yale L J at 90-91 (cited in note 13); Craswell, 88 Mich L Rev at 504 (cited in note 13). For a more recent treatment of majoritarian, market-mimicking default rules, see Ian Ayres and Eric Talley, *Solomonic Bargaining: Dividing a Legal Entitlement to Facilitate Coasean Trade*, 104 Yale L J 1027 (1995).

[16] Rather than being determined on the basis of what most similarly situated parties "would have wanted" had they known all the facts in advance and been able to bargain costlessly, a penalty default rule is deliberately slanted against a particular party, usually the more sophisticated party and thus the party more likely to know the rule and best equipped to contract around the rule ex ante. Often referred to as "information forcing," a penalty default rule induces the party more likely to know the background legal rule to share that information with its counterpart (in the course of contracting around the rule) by penalizing parties that force courts to adjudicate issues arising ex post that the parties themselves could have resolved more cheaply in advance. On penalty default rules generally, see Ayres & Gertner, 99 Yale L J at 93-94 (cited in note 13).

[17] This is an empirical claim based on the observation that the current legal regime does not protect anonymity and yet most users do not seem to mind. See note 30 for a discussion and defense of this claim.

[18] Moreover, the rule would be impracticable given the now widespread use of "anonymous remailers," which allow message senders to conceal—impenetrably—their identities. See A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip,*

similarly rejects 'wait and see' because this approach does not tell a court what to do when an actual dispute arises, and waiting and seeing is no longer an option.[19] This Comment argues instead in favor of disclosure as the default environment. This waivable disclosure rule should be slanted in the direction that most of the people the rule affects would prefer—disclosure—and yet should be flexible enough to meet the idiosyncratic privacy concerns of the small number of sensitive users that every system inevitably has.

Part I of this Comment explores the anonymity default rule, the mandatory disclosure rule, and the 'wait and see' approaches, rejecting all three. Part II of this Comment develops, and argues in favor of, the waivable disclosure rule approach.

I. ALTERNATIVE APPROACHES TO THE PROBLEM

A. An Anonymity Default Rule

Some scholars and politicians[20] argue that because the policy concerns in favor of protecting the right to anonymity are so strong, anonymity should be adopted as a default rule.[21] In an anonymity default environment, a system operator wishing to create a disclosure environment would have to receive affirmative contractual consent from the user to avoid the liability rule[22] a court would otherwise impose.

---

and the Constitution, 143 U Pa L Rev 709 (1995).

[19] Were a court to deny a system user any remedy against a system operator that had made nonconsensual disclosures of the user's activities, the court would, in effect, be choosing a default rule in favor of disclosure. 'Waiting and seeing' is thus itself a choice.

[20] See Ronald H. Brown, et al, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information*, US Department of Commerce (1995) (cited in note 12) (arguing for a requirement that "consent" be obtained from system users before information concerning them can be collected and used); David R. Johnson and Kevin A. Marks, *Mapping Electronic Data Communications onto Existing Legal Metaphors: Should We Let Our Conscience (and Our Contracts) Be Our Guide?*, 38 Vill L Rev 487 (1993) (cited in note 12); Lawrence Lessig, *The Path of Cyberlaw*, 104 Yale L J 1743, 1751 n 23 (1995) (cited in note 2) (citing National Research Council, *Rights and Responsibilities of Participants in Networked Communities* 25 (Dorothy E. Denning & Herbert S. Lin, eds, National Academy Press, 1994)).

[21] It should be noted that these commentators argue for adoption only as a default rule and nothing more. Neither a legislature nor a court could make this rule inalienable because doing so would obviously violate the First Amendment. System users cannot be stopped from revealing their own identities should they choose to do so.

[22] As it is determined by legislative enactment or common law doctrine. Setting a damage amount would be difficult, but not more difficult than any other instance where a plaintiff needs compensation for a nonpecuniary loss.

There are indeed some strong policy arguments in favor of protecting anonymity in cyberspace, though anonymity is by no means constitutionally guaranteed.[23] Included among these policy arguments are the notions that anonymity: (1) promotes the free exchange of ideas;[24] (2) ensures the protection of a group's ability to associate freely;[25] and (3) protects the user from annoying business solicitations and embarrassing personal revelations.

There are, however, other policy arguments which point in the opposite direction. Benefits of a disclosure environment include: (1) the ability of businesses to identify likely customers at a low cost; (2) the ability of individuals to identify others with similar backgrounds or interests; (3) the potential for individuals and businesses to learn 'netsurfing' techniques from each other; and (4) the deterring effect of disclosure on the commission of crimes and torts in cyberspace.

Moreover, many of the policy justifications for protecting anonymity could just as easily be addressed in other legal regimes. Consider, for instance, a flexible disclosure environment that allows users affirmatively to "opt" for anonymity.[26] Consider too that users who value their privacy especially highly can always protect themselves unilaterally, regardless of the underlying legal rule, by resorting to "anonymous remailer" technolo-

---

[23] This claim needs to be qualified somewhat. The Supreme Court has recognized "the right of an individual not to have his private affairs made public by the government." *Whalen v Roe*, 429 US 589, 599 n 24 (1977) (upholding a New York statute requiring state officials to keep computerized records of New York citizens who use certain drugs). Disclosure is permitted, however, when the public interest in disclosure outweighs the individual privacy interest at stake. Id at 598-604. Therefore it is constitutionally permissible for the government to compel disclosure when there is a sufficiently strong public interest in disclosure. Moreover, private system operators have even more latitude in this area than the government. Because the Constitution does not guarantee anonymity, an anonymity rule must therefore be justified on policy grounds. For an excellent discussion of this issue, see A. Michael Froomkin, *Anonymity and its Enmities*, 1995 J Online L art 4 (1995) (arguing that a narrowly drawn statutory ban on anonymity would likely be upheld by the courts).

[24] This idea is recognized in *Hynes v Mayor and Council of Oradell*, 425 US 610, 628 (1976) (Brennan concurring in part).

[25] See *Bates v City of Little Rock*, 361 US 516, 522-24 (1960) (holding that the NAACP could not be required to disclose the names of its members).

[26] This approach will be examined at greater length in Part II.

gy.[27] Both of these points show how privacy concerns can be accomodated outside of an anonymity default environment.

To be sure, the benefits from disclosure could also be obtained under an anonymity default rule by the clever system operator that can induce system users to agree to disclosure. Here, however, we run into the classic 'collective action' or 'free rider' problem.[28] The value of a disclosure environment to individual users is that with disclosure they can obtain more information and be better protected against crimes and torts. Users thus benefit from having other users agree to disclosure. They have little incentive, however, to agree to disclosure themselves. In an anonymity default environment, therefore, it is likely that a suboptimal number of users will waive their anonymity.

By contrast, in a disclosure default environment, the users who benefit the most from anonymity—that is, the users who place the highest value on their privacy—have exactly the right incentive to opt for anonymity because all of the gains from doing so accrue to the users who opt for it. That is, there is no external benefit (or harm) associated with opting for anonymity over disclosure. Assuming the informational and transactional costs[29] with respect to the "opt out" provision are sufficiently low, a close to optimal number of "opt outs" will occur. Moreover, since most users would probably prefer a disclosure environment,[30] fewer

---

[27] An anonymous remailer allows system users to send untraceable messages, thereby guaranteeing their anonymity. Froomkin observes that very little can be done to prevent users from availing themselves of this technology. See Froomkin, 1995 J Online L art 4 at ¶ 30 (cited in note 23).

[28] These terms have been borrowed from economics and have many applications in the law. For a more detailed explanation of these ideas and their application to law, see Richard A. Posner, *Economic Analysis of Law* 63 (Little, Brown, 4th ed 1992).

[29] Users need to be informed of their status under the background legal rule and then need to be given a means to contract around the rule if they choose. One of the nice features about cyberspace is that the cost of informational exchange and communication is almost nil. Hence, strong anonymity interests are not likely to be compromised by a disclosure default rule. For a discussion of low transaction costs in the cyberspace context, see Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U Chi Legal F 217.

[30] This is an empirical claim. It is based on the facts that: (a) most system users currently operate in a disclosure environment; (b) only a small minority use anonymous remailers; and (c) anonymous remailers are relatively easy to obtain. Possible objections to this claim are: (a) perhaps most users are unaware that they in fact are operating in a disclosure environment; (b) even if they are aware of this, perhaps they are either unaware of the possibility of using anonymous remailers or else unable to obtain (or learn how to use) anonymous remailers at a sufficiently low cost to make it worthwhile; and (c) perhaps there are some people who do not conduct activities in cyberspace precisely because it currently is a disclosure environment. My response to these objections is simply to look at the costs and benefits of disclosure: for most people, the benefits—low cost advertising, social possibilities, protection from anonymous harrassers and criminals, and

corrective opt out transactions[31] would be required under a waivable disclosure rule. An anonymity default rule is more costly—in terms of both transaction costs and allocative effect—than a disclosure default rule. And an anonymity rule would also be antimajoritarian.[32]

B. An Immutable Mandatory Disclosure Rule

Some politicians and pundits are so concerned about the harms that anonymous actors in cyberspace may cause they advocate banning anonymity from the Internet entirely and nonnegotiably.[33] This argument is foolish for two reasons. First, it ignores the fact that anonymous remailers (which the government, by its own admission, cannot stop)[34] can facilitate these criminal and tortious actors in any event. Second, the argument ignores the enormous benefits that anonymity can sometimes provide individual users.[35] This inflexible rule thus yields few benefits beyond what a waivable disclosure rule would yield while at the same time imposes significant costs on system users who deeply value their privacy. The rule is therefore exceedingly unwise on its face and merits no further discussion.

C. The 'Wait and See' Approach

Professor Lawrence Lessig acknowledges the policy tension

'netsurfing' information sharing—seem quite large, while the costs—loss of the ability to conceal one's actions in cyberspace—seem almost nil. This suggests that people operate in a disclosure environment because it is in their interest to do so rather than because they are uninformed in some way.

[31] By "corrective" transactions I mean instances of users contracting around a default rule that does not suit their tastes.

[32] On majoritarian default rules, see Ian Ayres and Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 Yale L J 87 (1989) (cited in note 13).

[33] See, for instance, the proposal of Connecticut State Representative Pat Dillon. Beverly Galge, *The Babe File*, New Haven Advocate 7 (Feb 9, 1995); Walter S. Mossberg, *Accountability Is Key to Democracy in the On-Line World*, Wall St J B1 (Jan 26, 1995) (cited in note 8).

[34] See A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U Pa L Rev 709, 717 n 21 (1995) (cited in note 18) (suggesting that if the government had the capacity to stop cryptography, it would be such a "vital national secret . . . the government would never use that capability in a manner that would risk revealing its existence.").

[35] For the idiosyncratically private, anonymity has extremely high benefits that would be entirely lost in a mandatory disclosure environment. Even if this loss would only affect a small number of users, the stakes in this debate are high at least for them.

between anonymity and disclosure in a recent article.[36] Instead of arguing for one or the other, however, he suggests that "we follow the meandering development of the common law" and "stand back from deciding these conflicts until the nature of these conflicts is well mapped, well constructed, [and] well understood."[37] This view is qualified by the assertion that lower courts should "wrestle with these questions . . . . But no court should purport to decide these questions finally or even firmly."[38] At bottom, Lessig believes that cyberspace is somehow different from other things over which law exercises control. Hence he concludes that "[i]t will require that individuals gain an experience with this new space" before we can "expect law to understand enough to resolve these questions rightly."[39]

Lessig's romantic vision of cyberspace as a completely new entity that cannot be analyzed like other areas of law is fundamentally flawed.[40] New technology arrives on store shelves every day, yet its patenting, licensing, packaging, distribution, and sale are successfully governed by standard doctrines of patent, copyright, trademark, agency, and contract that substantially predate the technology in question. Law is well equipped to adjust to changing technology.

Moreover, the 'wait and see' approach does not help a court faced with an actual case.[41] The court must pick a rule in any event, so it might as well pick the one it thinks is best, notwithstanding our perhaps limited knowledge of this new entity called cyberspace. Even a bad rule will have the salutary effect of letting the parties—system users and operators—know where they stand in relation to one another and thus will help them structure their future activities in a more informed way. Professor Lessig's wait and see suggestion is thus at odds with the "rule of law" values fundamental to our system of justice.[42]

---

[36] Lessig, 104 Yale L J at 1749-52 (1995) (cited in note 2).

[37] Id at 1752.

[38] Id at 1752-53.

[39] Id at 1752.

[40] For a lively criticism of this type of thinking, see Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U Chi Legal F 207.

[41] Were a system user to bring suit against a system operator for making nonconsensual disclosures of the user's cyberactivity to third parties, the court could hardly tell the litigants to come back in a few years when the court will have a better understanding of what cyberspace is. Even a no liability ruling is effectively a particular type of default rule. Whatever the court does, therefore, will in some sense "decide" the case today. Why is Professor Lessig against deciding it "finally and firmly?"

[42] Friedrich A. von Hayek, *The Road to Serfdom* 72 (University of Chicago, 1944) (explaining the "rule of law" ideal). See also Antonin Scalia, *The Rule of Law as a Law of*

II. A DISCLOSURE DEFAULT RULE APPROACH

A disclosure default rule, without any duty on the system operator to inform users that they are operating in a disclosure environment, would fail to protect system users from having their privacy invaded without their knowledge or consent. The likelihood that users will not know the background legal rule is high, and thus the chance of market failure due to informational asymmetries is also high. It is no surprise, therefore, that no commentator has advocated insulating from liability system operators who, without warning, expose their users to a disclosure environment. Yet, this in fact is the state of the law today.

One possible response to this problem of asymmetric information is to have the court adopt a 'penalty'[43] default rule slanted against the more sophisticated of the two parties. The anonymity default rule[44] is an example of the penalty default approach. Some policy makers and commentators, no doubt motivated by the problems inherent in a disclosure default rule, in effect argue for a penalty default rule of this type—a rule, that is, slanted against system operators.[45]

Waivable anonymity rules have problems of their own, however.[46] I believe it is possible to address the information problem that a disclosure default rule presents without necessarily switching over to an anonymity rule. This could be done by adding two additional features to the disclosure default rule: namely, a warning requirement and an "opt out" provision.

Rules, 56 U Chi L Rev 1175 (1989).

[43] On penalty default rules, see Ian Ayres and Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 Yale L J at 93-94 (1989) (cited in note 13). Often referred to as an "information forcing" rule, the penalty default rule is typically slanted against the more sophisticated party—in this case probably the system operator—who is more likely to know the legal rule and hence is in a better position to propose contracting around the rule should it be in the mutual interest of the parties to do so.

[44] See notes 20-32 and accompanying text.

[45] See Ronald H. Brown, et al, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information*, US Department of Commerce (1995) (cited in note 12) (arguing for a requirement that "consent" be obtained from system users before information concerning them can be collected and used). See also the statutory proposal in David R. Johnson and Kevin A. Marks, *Mapping Electronic Data Communications onto Existing Legal Metaphors: Should We Let Our Conscience (and Our Contracts) Be Our Guide?*, 38 Vill L Rev 487 (1993) (cited in note 12) (advocating a statute requiring system operators affirmatively to obtain consent from their users prior to making disclosures to third parties); George P. Long, III, *Who Are You?: Identity and Anonymity in Cyberspace*, 55 U Pitt L Rev 1177 (1994) (cited in note 4).

[46] See, for instance, the above discussion of the free rider and collective action issues raised in connection with an anonymity default rule in the text accompanying notes 28-32.

First, system operators could be required affirmatively to warn their users that they operate in a disclosure environment. This would put users on notice that their privacy potentially could be invaded.

Second, system operators could also be required to offer users the choice of opting out from participation in the disclosure environment. A user wishing to opt out would have to do something affirmatively to indicate that preference. System operators would be free to make disclosures (without liability) of the cyberactivity of any user who has not opted out. In this way, users who value their privacy particularly highly will be put on notice that their private actions potentially could be monitored. These users could then go through the relatively painless procedure of opting out.

Both the warning and the opt out choice could be communicated electronically at a very low cost. With transaction costs as low as they are in cyberspace, placing additional communicative burdens on transacting parties is not prohibitive. At the same time, these additional communications yield an end result more closely in line with the parties' preferences than the result produced by any other rule here considered.

Another nice effect of this disclosure default rule with warning and opt out provisions is that the rule is simultaneously majoritarian and information forcing.[47] A disclosure environment is majoritarian since most users would contract for it on their own ex ante with knowledge of all the facts.[48] The warning requirement is information forcing in that the more sophisticated party—here, the system operator—must tell the less sophisticated party—here, the user—about the background legal rule in order for that rule to go into effect.[49]

What about the problem of the anonymous harrasser, who will surely choose to opt out? As argued above,[50] anonymous

---

[47] Normally, the whole justification for adopting a penalty default rule is that a majoritarian rule hurts the minority who would contract around the background rule if only they knew what it was. See Ayres & Gertner, 99 Yale L J 87 (cited in note 13). Here, the majoritarian rule itself is information forcing, given the warning requirement.

[48] I concede this is an empirical claim. For a discussion and defense of this claim, see note 30. Also remember that if this assumption turns out to be wrong, all that will happen is that a majority of users will "opt out." Should this happen, the system operator will in effect be back in a waivable anonymity environment and will be free to contract around the rule with its users if it wishes.

[49] In effect, this regime employs a penalty default, anonymity rule slanted against all system operators who create a disclosure environment without warning their users.

[50] See note 34 and accompanying text.

remailers will in any event be the avenues of choice for "cybercriminals" and "cybertortfeasors." The risk of coming into contact with people like these is a fixed cost of interacting in cyberspace regardless of the legal rule chosen. No one would say, however, that this cost is so high it justifies shutting down cyberspace.[51] Moreover, this cost will not vary much in response to the selection of alternative legal regimes to govern cyberspace. So this cost has no effect on the analysis here as it bears no relation to the background legal rule.

Finally, the free rider/collective action problem discussed above[52] is avoided with the adoption of the disclosure/warning rule suggested here. Only the user who values privacy idiosyncratically highly has an incentive to opt out.

Why will everyone not opt out? Because there is a cost (albeit a small one) to opting out. The user will be required to fill out an electronic "opt out request form," which requires a small amount of time and effort. This exertion of time and effort is not worthwhile for the typical user who does not care in the least about disclosure. The typical user gains nothing from opting out. Moreover, note that the potential for everyone to opt out will give the system operator an incentive to design a disclosure environment in which most people will prefer to participate.[53]

CONCLUSION

This Comment has considered several alternative approaches to the regulation of cyberactivity disclosures. The current legal regime of disclosure as the default rule[54] is recommended as the correct policy with two small modifications: in the future, system operators ought to be required (1) to warn their users of the prevailing background legal rule and (2) to offer their users an option not to participate in a disclosure environment. This approach is superior to the anonymity default and mandatory disclosure

---

[51] Just as no one would say we should ban free speech just because some people can yell racial slurs at us when we walk through the park. Even with a legal ban on hate speech, the racist will continue to yell. We therefore do not ban speech. Nor do we ban walking in the park. Both the racist and the cybercriminal will be with us irrespective of the rules we choose.

[52] See notes 28-32 and accompanying text.

[53] We see a phenomenon similar to that suggested here in the telephone industry, where companies compete along the dimension of privacy assurance as well as on price and quality. See Brown, et al, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* n 35, US Department of Commerce (1995) (cited in note 12).

[54] No liability now attaches to system operators who expose their users to a disclosure environment, the Clinton Administration's policy suggestions notwithstanding.

rules advocated by some and also is more useful in practice than Professor Lessig's 'wait and see' approach. This is so, principally, because none of the other legal rules considered is at once majoritarian, information forcing, and bereft of free riding and collective action concerns.