Hardware-Based ID, Rights Management, and Trusted Systems

Jonathan Weinberg*

Networked digital technology enables the easy and inexpensive movement of speech and information among persons who are strangers to one another. People may not always find unfettered movement desirable, though. A content producer may want to disseminate information to some recipients, such as those who have paid, but not others. A parent may wish that the computers in her home not display certain sexually explicit content offered by a willing speaker. A government might wish that certain speech be available to some recipients but not others, for example, that gambling solicitations be inaccessible in specific geographic jurisdictions.

In order to determine whether particular content should be disseminated to a particular recipient, the decisionmaker must have information about both the content and the recipient. To block content requiring payment to persons who have not paid, one needs to know both whether the requested document requires payment and whether the requester has paid; to block sexually explicit content to minors whose parents wish to shield them from such material, one needs to know both whether the particular document contains proscribed content and whether the requester is such a minor; to block gambling solicitations to persons in certain geographic jurisdictions, one needs to know both whether the particular document is a gambling solicitation and the geographic location of the requester. As Larry Lessig and Paul Resnick point out, this can present a difficulty: No one actor, at the outset, may possess all of that information.[1]

Various techniques are available to overcome that difficulty. One approach is filtering. A parent concerned about her child's access to sexually explicit speech knows something about her child's characteristics, but little

---

* Professor of Law, Wayne State University. I owe thanks to Phil Agre, Karl Auerbach, Lorrie Cranor, Jessica Litman, Neil Netanel, Paul Resnick, and Joel Reidenberg. Earlier versions of this paper were presented at a Haifa University Conference on the Commodification of Information and at the Telecommunications Policy Research Conference.

1. *See generally* Lawrence Lessig & Paul Resnick, *Zoning Speech on the Internet: A Legal and Technical Model*, 98 MICH. L. REV. 395 (1999). Lessig and Resnick present a model including three categories of information: the content of the speech, the characteristics of the recipient, and the jurisdiction of the recipient (which they assume determines the law describing whether it is permissible to send speech with that content to a recipient with those characteristics).

about the contents of each of the Web sites her child might visit. Filtering systems attempt to solve that problem by generating information about those Web sites, so that the parent, armed with both the characteristics of the speech and those of her child, can make blocking decisions based on her own policy preferences. However, the filtering enterprise turns out to be problematic in several respects. One problem lies in the difficulty of collecting accurate and nuanced information about myriad Internet speech resources; another lies in the difficulty of vindicating users' individual policy preferences via off-the-shelf software. Entry barriers and informational costs mean that only a few firms can manage to tag huge numbers of Web resources; consumers, in turn, do not know and have difficulty evaluating the evaluators' substantive criteria.[2] As a result, although filtering in theory diffuses power among hosts of information recipients, to some extent it concentrates power in the third-party ratings providers.[3]

Filtering, though, is not the only possible response to this sort of difficulty. Another approach, as Lessig and Resnick point out, is to set up Internet architecture to require the would-be recipient of speech to transmit information about *her* characteristics back to the *content provider*, so that the provider can then make content dissemination choices according to *its* policy preferences or binding legal rules.[4] Increasingly, firms interested in commerce in information goods are designing structures to enable that process.

This paper examines the implications of different choices for managing the information flow from consumers to content providers. In particular, it focuses on the implications of an Internet architecture that identifies each consumer by a single unique identifier that can be tied to the consumer's real-world identity and that is available to a wide range of applications and content providers. Such a system can be implemented through hardware-based identification like Intel's Processor Serial Number (PSN). It allows the content provider easily to identify the consumer originating any given

---

2. Because filtering software companies protect their evaluation processes and algorithms as trade secrets, consumers only have access to the descriptions of the guidelines in the companies' promotional materials. These have often proved inaccurate. For example, companies' claims that a human employee reviews each blocked site are routinely belied by an examination of the sites that end up being blocked. *See, e.g.*, MICHAEL SIMS, BENNETT HASELTON, JAMIE MCCARTHY, JAMES S. TYRE, JONATHAN WALLACE, DAVID SMITH & GABRIEL WACHOB, THE CENSORWARE PROJECT, CENSORED INTERNET ACCESS IN UTAH PUBLIC SCHOOLS AND LIBRARIES 10 (1999), *available at* <http://www.censorware.org/reports/utah> (noting that although Secure Computing states that "[a]s a rule, sites are not [blocked] without first being viewed and approved by our staff," its filtering product blocks in its "Drugs" category the Iowa State Division of Narcotics Enforcement Web page).

3. *See generally* Jonathan Weinberg, *Rating the Net*, 19 HASTINGS COMM. & ENT. L.J. 453 (1997) (discussing filtering technology's limitations and drawbacks).

4. *See* Lessig & Resnick, *supra* note 1, at 406-09, 416-17.

packet stream and to correlate incoming payment and other information to the outgoing information and entertainment that the content provider releases to that consumer: All of the data is simply filed under the consumer's unique ID. That architecture stands in contrast to one in which content providers use more sophisticated cryptographic techniques to assign consumers identifiers that cannot be linked to their real-world identities or their activities in other contexts. Those techniques would protect consumers' choices from disclosure and would preclude the assembly of dossiers on particular individuals.

Technologies involving the assignment of user or platform identifiers, enforced through hardware-based user identification such as the PSN, can give providers of information goods extensive new capabilities. Such technologies provide an easy and straightforward way for publishers to verify the authenticity of messages claiming authorization to receive digital works, giving them greater ability to limit availability of their works to folks who meet certain criteria. The technology dovetails with the use of trusted systems, allowing content providers to prevent recipients from passing usable copies of the work to anyone who has not paid the content provider, and giving content providers flexibility in specifying the nature of the event that will trigger a payment obligation.

These technologies, though, have other consequences as well. The most obvious relate to privacy: Trusted systems relying on transparent unique identifiers, and in particular systems built around the PSN, threaten to sharply diminish anonymity and informational privacy on the Internet. They raise the prospect that a much larger proportion of ordinary transactions will require consumers to present unique identification numbers digitally linked to a wide range of personally identifiable information. They are well-suited to across-the-board use by a large number of unrelated information collectors, increasing the ease with which a wide range of information about a person can be aggregated into a single overall dossier.

Moreover, the combination of trusted-systems technology that enables publishers to ensure that speech released to one consumer does not make its way via sharing or secondary markets to another, and the privacy effects of allowing publishers to collect extensive individualized information on consumers, will likely affect the economics and politics of speech markets. It will sharply enhance producers' ability to discriminate among individual consumers, on price and other grounds, in connection with the sale and marketing of information goods. Some commentators suggest that this concentration of control is a good thing because the price discrimination it enables

will broaden distribution of information goods.[5] Yet the benefits of such a system are clouded; any increase in distribution due to price discrimination comes at the cost of shutting down the distribution that comes, in today's less-controlled system, through sharing or secondary markets. It will likely be accompanied by increased media concentration and a self-reinforcing cycle of commercial pressure on individual privacy.

Publishers can get the benefits of trusted systems without these socially undesirable consequences by relying on identification techniques that assure consumers a greater degree of privacy. Building trusted systems around hardware-based consumer identifiers therefore not only carries with it a dystopian future of universal personal monitoring and identification, but also is unnecessary to meet publishers' legitimate needs.

In Part I of this paper, I explore the market incentives for the widespread deployment of systems under which information flows from consumers to content providers. In Part II, I discuss the blend of anonymity and identifiability presented by current Internet architecture, and in Part III, I focus on a particular technology—the Processor Serial Number built into the Intel chips powering most computing devices today. In Part IV, I discuss the implications of such technology for privacy and the economics and politics of communications markets. Unique identifiers, and their associated technology, promise to give content providers vastly expanded powers to discriminate among consumers by setting prices on an individual basis and by picking and choosing who will be allowed to view or read particular works. Although some argue that these would be positive developments, I submit that they are, on balance, unfortunate. In Part V, I note that the negative consequences of this technology are avoidable: Content providers could rely on more sophisticated cryptographic techniques to manage access to their information goods. Such systems would allow content owners to exploit their intellectual property, but would avoid the consequences described in this paper.

I. RIGHTS MANAGEMENT AND TRUSTED SYSTEMS

The most important concern driving the information flow from consumers to content providers relates to rights management. The term "rights management" is commonly associated with the protection of intellectual property rights, but it need not be so limited. One can think of rights management as covering any technological means of controlling public access to, and ma-

5. *See, e.g.*, William W. Fisher III, *Property and Contract on the Internet*, 73 CHI-KENT L. REV. 1203, 1239 (1998) (arguing that concentration of control and the price discrimination it enables are desirable because they will broaden the distribution of goods).

nipulation of, digital resources. That sort of control is basic to any system of networked computing. At the heart of Unix, for example, is the concept of permissions, that define *which* users on a network can take *what* actions (read, write, execute) on *which* files and directories.[6] Networking would not be very practical without a way of defining and limiting the set of people who can have access to particular documents and other network resources. Rights management techniques, in that sense, are simply a form of network security.

Those techniques demand a reliable way to match usernames with real-world individuals. After all, it is the individual, not the username, whose access to files is at issue. In the old days, when mainframe computers ruled the world, system administrators had little difficulty associating the individuals using their systems with unique usernames, and thus using permissions or similar file access rights to enforce that aspect of system security. The systems administrators themselves had assigned those usernames to the individuals in question.[7] The situation was not much different for a self-contained local area network.

But the Internet changed things: It has no system administrator. There is no reliable automated way, under current technology, to tell which individual is associated with any given username on an Internet-connected network.[8] Indeed, even your own computer does not know who you are; if you tell your PC that you are Napoleon or Joan of Arc, it has no reason to disbelieve you.[9] For this reason, the ordinary Internet architecture stymies attempts at rights management beyond a given network. It provides no convenient set of options in the middle ground between blocking access by anyone outside one's own network and granting access to everyone in the world.

How can one extend sophisticated file access rights beyond the controlled network environment into the Internet universe at large? Put another way, how can a local server extend secure control over the many intercon-

---

6. *See* JOHN R. LEVINE & MARGARET LEVINE YOUNG, UNIX FOR DUMMIES 313-18 (1993); MATT WELSH & LAR KAUFMAN, RUNNING LINUX 104-09 (2d ed. 1996).

7. *See* Philip E. Agre, *The Architecture of Identity: Embedding Privacy in Market Institutions*, 2 INFO., COMM. AND SOC'Y 1, ¶ 25 (Spring 1999) <http://www.infosoc.co.uk/00105/feature.htm>.

8. *See generally* S. Bradner, *Source Directed Access Control on the Internet* (Nov. 1996) <ftp://ftp.isi.edu/in-notes/rfc2057.txt> (Network Working Group RFC 2057) (stating that no one has control and oversight over the Internet, and that there is no central database of computer addresses and user identities). While Unix systems may supply such information in response to the "finger" command, there is nothing in the Internet architecture that requires them to do so, or to do so accurately. *See* ED KROL, THE WHOLE INTERNET USER'S GUIDE & CATALOG 171-74 (1992) (explaining finger queries).

9. *See* Agre, *supra* note 7, at 11.

nected networks that make up the Internet? To do that, it must be able to reliably identify everybody out there seeking access to its files, or at least, everybody to whom it is willing to grant access, and then be able to sort those persons by whichever of their characteristics it deems relevant. That is to say, it must have some way of reliably associating incoming packet streams with identified real-world individuals, and it must have—or be able to collect—enough information about each of those individuals to implement a set of rules determining whether to grant access.[10]

One way for a content provider to accomplish these tasks is to allow access only if the recipient's computer (or other device) incorporates hardware and software, meeting security specifications approved by the content provider, enforcing rules under which individuals can access and use particular digital content. In such a case, technologists refer to the server and recipient as being part of a "trusted system."[11] The server can rely on "trusted" elements of the recipients' device to identify the recipient, to transmit only accurate information about the recipient, and to limit the recipient's ability to manipulate any content it receives from the server in ways that exceed its authorization.

Trusted systems enable the sophisticated network security I discussed above, because they give the content provider a way to verify the authenticity of any message it receives that claims authorization to read a digital work. But their implications are broader. They allow the content provider to make the works available only to persons the content provider knows have paid for access. They allow the content provider to prevent the recipient from passing usable copies of the works to unauthorized persons. And they allow the content provider great flexibility in specifying the nature of the event that will trigger a payment obligation. For example, a content provider could allow a consumer to download a work for free, but require payment each time she reads or listens to it. In short, trusted systems have the capability to be an extraordinarily effective and profitable means of controlling, and rationing, access to works of information and entertainment.[12]

---

10. This criterion is oversimplified, as Part V of the paper demonstrates, but it will do for now.

11. *See* Mark Stefik, *Trusted Systems*, SCI. AMER., Mar. 1997, at 78, *available at* <http://www.sciam.com/0397issue/0397stefik.html>; *see also* XEROX CORP., THE DIGITAL PROPERTY RIGHTS LANGUAGE: MANUAL AND TUTORIAL – XML EDITION 5 (ver. 2.00 1998) ("A trusted system is a system that can hold digital works and which can be trusted to honor the rights, conditions, and fees specified for a work.").

12. *See generally* XEROX CORP., *supra* note 11 (describing the use of trusted systems to control access to, transfer of, and usage of digital works); Mark Gimbel, *Some Thoughts on the Implications of Trusted Systems for Intellectual Property Law*, 50 STAN. L. REV. 1671 (1998) (arguing that trusted systems enable an unprecedented degree of control over protected works). Xerox's

If trusted systems could be extended to the ordinary home computer, they would provide content owners with an important tool in the economic exploitation of their works. This would not be entirely straightforward, though. First, there is the issue of market acceptance: If the home PC is to take its place as part of a trusted system, then it will have to include hardware and/or software that disables, to some extent, the PC's ability to interact anonymously with other machines and to manipulate data stored on its own hard disk. As Mark Stefik puts it: "What's in all this for consumers? Why should they welcome an arrangement in which they have less than absolute control over the equipment and data in their possession?"[13] Stefik, a proponent of trusted systems, answers that participation in trusted systems will benefit consumers in the long run because content providers will make desirable digital content available over the Internet only if trusted systems are available to them.[14]

This is contested ground. Although major record labels and Hollywood studios have worked hard to ensure that their products are available over the Internet only in secured form,[15] the music industry, at least, appears to have reconciled itself to the fact that music is increasingly available over the Net in other formats.[16] It seems plausible that the industry might reconcile itself to releasing its own product in a less-than-secure format if it believed that, on

---

ContentGuard is an example of sophisticated trusted-system technology. ContentGuard uses Java applets to control Self Protecting Documents (SPD), which are sent to particular users customized according to the user's credentials, the rights purchased for a given document, and the environment in which the document is to be viewed or printed. The SPD interacts with a back-office server to allow only authorized viewing or printing. *See* ContentGuard, *Self-Protecting Document*™ (visited Dec. 6, 1999) <www.contentguard.com/overview/tech_spd.htm>; Arun Ramanujapuram & Prasad Ram, *Digital Content & Intellectual Property Rights*, DR. DOBB'S J., Dec. 1998, at 20-26 (Dec. 1998).

13. Stefik, *supra* note 11, at 81.

14. *See id.*

15. *See, e.g.*, Beth Lipton Krigel, *Music Industry Blames MP3 for Sagging Sales*, CNET NEWS.COM (Mar. 25, 1999) <http://www.news.cnet.com/news/0-1005-200-340395.html> (reporting on the Recording Industry Association of America's concern about free downloading of music from the Internet).

16. The Recording Industry Association of America (RIAA) initially attempted to block the manufacture and sale of any consumer electronics devices that could play music in the MP3 file format. MP3 allows the transmission of high quality music recordings over the Internet, and does not encorporate copy-protection technology. After failing to suppress MP3 entirely, the RIAA entered into an agreement under which consumer electronics manufacturers are free to sell devices that play MP3 files, but will later on offer consumers a voluntary software upgrade allowing them to play music in an encrypted format, while disabling them from playing a confusingly defined category of other music. The music industry is in the process of developing this more secure, SDMI format, which will allow publishers to sell music in a more trusted environment. *See* Jessica Litman, *Electronic Commerce and Free Speech*, 1 J. ETHICS & INFO. TECH. 213 (1999), *available at* 15-18 (visited Feb. 19, 2000) <http://www.law.wayne.edu/litman/papers/freespeech.pdf>.

balance, there was money to be made that way. Even absent the legal and technological protections sought by content owners, the Web now provides both extensive professionally created and formatted commercial content, and extensive valuable content that is not professionally formatted and created.[17] And the trend, even absent such protections, has been towards making more and more content available. But the proponents of trusted systems, at least, argue that the most commercially valuable content will not become available without robust technological (and backup legal) protections.

Next, there is the issue of technological feasibility. In order to implement large-scale trusted systems, the computer industry must develop technology well-suited to feeding reliable identifying information about consumers' home PCs back to content providers. Such technology is hardly imaginary; indeed, it is at the center of a growth industry. In the next section of this paper, I will start by discussing the degree to which identifiability is inherent in Internet architecture. I will then discuss new identification technology that companies have sought to put in place.

II. ANONYMITY AND IDENTIFIABILITY ON THE INTERNET

In the physical, face-to-face world, we encounter an imperfect blend of anonymity and identifiability. We do not all know everything about each other, nor are we are all completely anonymous. In some respects, we are easily identifiable (a four-year-old cannot walk into a 7-11 and buy a copy of *Playboy*); in others, we are not (an adult can, without showing identification). We know some things about each other but not others; we negotiate boundaries through social interaction.[18]

Internet architecture presents a different blend of anonymity and identifiability.[19] On one level, it provides for a higher degree of anonymity. "On the Internet," as the old saw has Rover explain while sitting at his computer, "nobody knows you're a dog."[20] In ordinary social and commercial transactions, it is easy to conceal one's identity, or to adopt a new one. Further, that anonymity is for the most part socially acceptable. This has important ad-

---

17. *See* Jessica Litman, *Copyright Noncompliance (Or Why We Can't "Just Say Yes" to Licensing)*, 29 N.Y.U. J. INT'L L. & POL. 237, 246-51 (1996-97); *see also* Jessica Litman, *The Exclusive Right to Read*, 13 CARDOZO ARTS & ENT. L.J. 29, 43-46 (1994) (pointing out that copyright protection is not necessary for a flourishing of creativity).

18. *See* Agre, *supra* note 7, ¶ 16.

19. I am indebted to Lorrie Cranor for emphasizing the points in the next two paragraphs.

20. This joke has sunk into the public consciousness; it was originally penned by Peter Steiner, in a *New Yorker* cartoon. I owe the citation to Joseph M. Reagle Jr., *Why the Internet is Good: Community Governance That Works Well* (Mar. 26, 1999) <http://cyber.law.harvard.edu/people/reagle/regulation-19990326.html>.

vantages: It means, as Larry Lessig has explained, that one can explore the Internet without an internal passport, without having to present credentials.[21]

On another level, this apparent anonymity is deceptive. The Internet monitors the origin and destination of the packets that traverse it. It is therefore, in fact, extremely difficult to conceal one's identity while engaging in Internet activities from a truly determined adversary (such as a law-enforcement agency armed with subpoena power). And once one's identity is revealed, extensive information about one's online activities may come with it.

The most important reason for the absence of profound anonymity lies in the Internet's reliance on "IP addresses" to get packets to their destinations. IP addresses are the unique numbers that identify each computer connected to the Internet. Just as it would be impractical for a person to receive postal mail without a unique name-and-postal-address combination, a computer cannot receive or send information over the global Internet without a unique IP address.[22] Further, every packet of information transmitted over the Internet contains its origin and destination addresses in plain sight in its packet headers.[23] Thus, when I undertake any transaction over the Internet, I transmit to the recipient (and anybody else listening in) the IP address of my home computer.

For most residential Internet users, this is only a limited concern. Most of us get IP addresses on a dynamic basis from our Internet service providers, using DHCP (Dynamic Host Configuration Protocol), so that we get different IP addresses each time we log on.[24] While a law enforcement agency armed with Internet service provider records would be able to trace the IP addresses we used during different logons, and thus track our online activity, we are not at the mercy of the casual commercial or social observer.[25]

---

21. *See* Lawrence Lessig, The Laws of Cyberspace 7 (Apr. 3, 1998) (unpublished draft), *available at* <http://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf>.

22. This is oversimplified: Network address translation can allow a computer to function using an address, assigned by the local network, that is not globally unique. More simply, a user can piggyback on the IP address of a remote computer by logging into a shell account on that computer. The extent to which such a user's traffic can be traced to him individually (as opposed to the remote server generally) depends on the information retained by that server. Finally, a particular computer's IP address may change over time. *See* notes 24-25 *infra* and accompanying text.

23. *See* Thomas Narten, *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*, at 2-3 (Oct. 1999) <http://search.ietf.org/Internet-drafts/draft-ietf-ipngwg-addrconf-privacy-01.txt>.

24. This is somewhat oversimplified. A DHCP server will sometimes return to an Internet user the same address that it had used previously, if that address is still available. In certain contexts, a client could use the same address for months at a time. *See id.*

25. The situation is different if a computer's IP address is "static" as opposed to dynamic. In that case, the address will be associated with that computer for an extended period of time. Users with broadband, "always on" Internet connections are more likely to have persistent IP addresses.

This concern may become somewhat more important with the introduction of a new Internet addressing structure known as IPv6.[26] As currently planned, IPv6 will incorporate an address configuration procedure under which, if a computer is connected to the Internet via an Ethernet card or certain other classes of hardware, and the IP address is not unilateraly set by a DHCP or PPP server, then the computer's IP address will automatically include the unique identifier associated with that Ethernet card or other hardware.[27] This will make it easier to match IP addresses to individual computers,[28] and will make it possible for observers to pull together a given device's Internet traffic even though the device, for instance a laptop, is connected at different times to different networks at different physical locations.[29] On the other hand, it should not affect the identifiability of the Internet traffic of an ordinary user with a dial-up connection and no Ethernet card.[30]

In sum, it is inherent in Internet architecture that Internet traffic carries identifying information along with it. At the same time, though, this information is not cheaply and immediately useful on a commercial level. In particular, a mass-market content provider cannot rely solely on IP addresses to identify residential users.[31] Content providers want—and are beginning to develop—cheaper and more precise tools better suited to their needs.

Once a particular IP address is firmly associated with a user, it is easy to match that IP address with the entity (an Internet service provider, corporation, government agency, etc.) to which the relevant block of IP addresses was assigned. However, one cannot further match the IP address to the identity of an individual user without information supplied either by the intermediate entity or by the user himself (as in a registration database). *See* Electronic Privacy Information Center, *Request for Participation and Comment from the Electronic Privacy Information Center* (visited Dec. 6, 1999) <http://www.ftc.gov/bcp/profiling/comments/shen.pdf>.

26. *See* R. Hinden Nokia & S. Deering, Cisco Systems, *IP Version 6 Addressing Architecture* (July 1998) <ftp://ftp.isi.edu/in-notes/rfc2373.txt> (Network Working Group RFC 2373); Steve King, Ruth Fax, Dimitry Haskin, Wenken Ling, Tom Meehan, Robert Fink & Charles E. Perkins, *The Case for IPv6* (Oct. 22, 1999) <http://search.ietf.org/Internet-drafts/draft-ietf-iab-case-for-ipv6-05.txt>.

27. *See* King et al., *supra* note 26, at 10; Narten, *supra* note 23, at 4.

28. That will especially be the case if business information-exchange standards encourage the matching of a person's name and address with the identifier of the Ethernet card preinstalled in the computer he buys. *See* note 78 *infra*.

29. *See* Narten, *supra* note 23, at 4-5. One of the developers of IPv6 has suggested changes in the IPv6 addressing architecture to ameliorate this concern. *Id.* at 5-11.

30. *See generally* J. Bound & C. Perkins, *Dynamic Host Configuration Protocol for IPv6* (Feb. 25, 1999) <http://search.ietf.org/Internet-drafts/draft-ietf-dhc-dhcpv6-14.txt> (discussing DHCP as it relates to IPv6).

31. Instead, online advertisers tend to rely on cookies accepted by users and stored on their hard disks. Firms use a technique called cookie synchronization to share cookies and their associated information across multiple sites. *See* Junkbusters, *Profiling: Comments to the Dept. of Commerce and Federal Trade Commission* § 2.2 (Oct. 18, 1999) <http://www.junkbusters.com/

As of this writing, the most notorious system for feeding consumer information back to content providers is one quietly put in place by RealNetworks, makers of the leading multimedia software. It became public some time ago that each copy of RealPlayer, like Windows Media Player, contained a globally unique identifier (GUID) that was transmitted to the provider when the user accessed streaming media.[32] It only recently became known that the same company's RealJukebox player transmitted information back to its makers including the names of all the CDs the user played, the number of songs recorded on her hard disk, the brand of portable MP3 player she owned, and the music genre she listened to most.[33] The information was tied to a unique identification number that could be mapped to the user's email address via the registration database. In short, RealNetworks had the capability to collect, in personally identifiable format, information regarding the listening activities of each user of its software. Responding to negative publicity, RealNetworks made available a software patch to disable RealJukebox's data collection function,[34] and announced a new version of RealPlayer software that would not transmit a GUID unless the user affirmatively turned that feature on.[35] The company noted, though, that some content providers might require that consumers enable the GUID in order to access their content.[36]

Nor was this the first time a software-generated GUID gained public attention. Users discovered not too long ago that various Microsoft applications label each of the documents they create with a unique identifier. If the computer running the applications contains an Ethernet card, the document identifier incorporates that Ethernet card's unique identifier, and thus definitively identifies the computer in question.[37] As a result, documents created

---

profiling.html>. *But see* text accompanying note 82 *infra* (reporting Doubleclick's statement that it relies on IP addresses to target advertisements). The use and abuse of cookies is beyond the scope of this paper, but their importance in online privacy issues cannot be overstated. *See* Deborah Kong, *Online Profiling on the Rise*, SAN JOSE MERCURY NEWS, Jan. 3, 2000, at C1.

32. *See* Mark D. Fefer, *Media Player and Privacy*, SEATTLE WKLY., Apr. 8-14, 1999, *available at* <http://www.seattleweekly.com/features/9914/tech-fefer.shtml>; *see also* Peter H. Lewis, *Peekaboo! Anonymity Is Not Always Secure*, N.Y. TIMES, Apr. 15, 1999, at G1 (repeating the conclusions of the *Seattle Weekly* report).

33. *See* Richard M. Smith, *The RealJukeBox Monitoring System* (Oct. 31, 1999) <http://www.tiac.net/users/smiths/privacy/realjb.htm>; Sara Robinson, *CD Software Said to Gather Data on Users: RealNetworks Receives Variety of Information*, N.Y. TIMES, Nov. 1, 1999, at C1.

34. *See* Sara Robinson, *RealNetworks to Stop Collecting User Data: Music Software Will No Longer Transmit Personal Information*, N.Y. TIMES, Nov. 2, 1999, at C2.

35. *See* RealNetworks, *RealNetworks Consumer Software Privacy Statement* (visited Dec. 6, 1999) <http://www.realnetworks.com/company/privacy/software-privacy.html>.

36. *See id.*

37. *See* Junkbusters, *Privacy Advisory on Microsoft Hardware IDs* (visited Dec. 6, 1999) <http://www.junkbusters.com/ht/en/microsoft.html#advisory>.

in Microsoft Word and Excel, and perhaps other Microsoft programs, can be traced back to the originating computer.[38] Until recently, Microsoft's Windows 98 Registration Wizard transmitted the Ethernet card identifier to Microsoft upon software registration, along with the identification information (name, address, phone number, etc.) entered by the user.[39] Microsoft too has backpedaled somewhat in response to publicity: It announced that it would make a software patch available to prevent the insertion of the GUID into Microsoft Office documents, and would stop collecting the information during registration.[40] Office 2000, it added, would not insert the GUID at all.[41]

Each of these systems has powerful identification capabilities, but is limited in certain respects. Microsoft's is limited in scope, because the GUID identifies an individual's computer only if that computer contains an Ethernet card.[42] The RealNetworks system is limited in a different respect: The GUIDs it assigns are not used by anyone other than RealNetworks.[43] Although RealNetworks was in a position to use the GUID to catalog an individual's listening information, the system was not designed to be used by a variety of content providers in multiple contexts.

III. INTEL AND THE PROCESSOR SERIAL NUMBER

Intel, which manufactures the vast majority of the chips powering personal computers today, introduced a technology in early 1999 that it described as the foundation for a whole new world of trusted systems: the Processor Serial Number, or PSN. The PSN is a unique identification number burned into each computer's central processing unit as part of the normal manufacturing process.[44] Intel announced plans to incorporate the PSN into all of its products, including not only its Pentium III chips for personal com-

---

38. *See id*.; Chris Oakes, *Sniffing Out MS Security Glitch*, WIRED NEWS, Mar. 8, 1999, ¶ 3 <http://wired.lycos.com/news/news/technology/story/18331.html>. At least Microsoft's own Web site embedded the GUID in cookies. *See* Chris Oakes, *Is Microsoft Tracking Visitors?*, WIRED NEWS, Mar. 12, 1999, ¶ 2 <http://wired.lycos.com/news/news/technology/story/18405.html>.

39. *See* John Markoff, *Microsoft Will Alter Its Software in Response to Privacy Concerns*, N.Y. TIMES, Mar. 7, 1999, §1, at 1.

40. *See Microsoft Addresses Customers' Privacy Concerns*, ¶ 14 (visited Dec. 6, 1999) <http://www.microsoft.com/presspass/features/1999/03-08custletter2.htm>.

41. *See id.*

42. *See* Junkbusters, *supra* note 37; *Advanced Streaming Format – Specification – Appendix: GUIDs and UUIDs*, ¶ 6 (visited Feb. 2, 2000) <http://www.microsoft.com/asf/spec3/c.htm>.

43. Each RealNetwork GUID is randomly generated by a RealNetworks consumer application during installation. *See* Smith, *supra* note 33.

44. *See* Patrick Gelsinger, A Billion Trusted Computers, Speech at the RSA Data Security Conference and Expo '99, ¶ 96 (Jan. 20, 1999) (transcript), *available at* <http://www.intel.com/pressroom/archive/speeches/pg012099.htm>.

puters, but also the microprocessors embedded in devices such as television set-top boxes, telephones, and "Internet appliances."[45] Applications running on any device equipped with a PSN can read the unique identification number and transmit it to any requesting remote server. Such a system could provide a foundation for the reliable flow of identification information from *every* consumer to Internet-based content providers.[46]

In introducing the PSN, Intel vice-president Patrick Gelsinger explained that the company was shifting its vision from "a world of a billion connected computers" to "a billion *trusted* computers."[47] A vision of a world fully populated with myriad personal computers, each communicating with the rest, he explained, is insufficient unless those connected computers are trusted, and the first step on "the road to . . . trusted connected PCs" is the PSN.[48] Because each computer's PSN is unique, he continued, the PSN pro-

---

45. *See* Robert Lemos, *The Biggest Security Threat: You*, ZDNET NEWS (Feb. 25, 1999) <http://www.zdnet.com/zdnn/stories/news/0,4586,2216772,00.html> (referring to Intel's StrongARM embedded processor, and quoting Michael Glancy, general manager of Intel's platform security division). Intel purchased the StrongARM line of embedded processors in 1998; StrongARM processors are currently used in cellular phones and handheld computers, and are suitable for use in set-top boxes and other Internet-aware consumer electronics. *See* Lisa DiCarlo, *Intel Seals StrongARM Deal*, PC WEEK ONLINE (Feb. 27, 1998) <http://www.zdnet.com/pcweek/stories/news/0,4153,288760,00.html>.

Intel also included a PSN, apparently inadvertently, in some Pentium II and Celeron chips. *See* Robert Lemos, *Intel Admits PII Serial Snafu*, PC WEEK ONLINE (Mar. 11, 1999) <http://www.zdnet.com/pcweek/stories/news/0,4153,2224186,00.html>; Ephraim Schwartz & Dan Briody, *Intel's Pentium Security Woes Continue*, INFOWORLD ELECTRIC (Mar. 10, 1999) <http://www.infoworld.com/cgi-bin/displayStory.pl?990310.wcpsn.htm>. *But see* Juan Carlos Perez, *Some Intel Mobile Chips Dispense IDs*, COMPUTERWORLD (Mar. 11, 1999) <http://www.computerworld.com/home/news.nsf/all/9903113mobile> (quoting Howard High, Intel spokesman, that the value returned by the PII and Celeron chips may not be unique).

46. *See* text accompanying notes 47-58 *infra*. The PSN is not the only form of hardware-based ID. Indeed, smart cards and biometrics provide more secure ways to uniquely identify a user across a network. Windows NT 5.0 can be set to require smart cards for network authentication on login. *See* MicroSoft Windows CE, *Smart Cards* (last modified Dec. 6, 1999) <http://www.microsoft.com/windowsce/smartcard/info/default.asp>. Smart cards can also be used with Windows 95/98 and Windows NT 4.0 to authenticate secure connections. *See id*. Intel is engaged in active research on biometrics (fingerprints, facial images, voiceprints, retinal or iris images, thermal images, or signature) for authentication and acquisition of network privileges. *See* INTEL CORP., USER AUTHENTICATION SERVICES (UAS) SPECIFICATION: EXTENSION TO THE CSSM FRAMEWORK, at 6 (ver. 1.0 Sept. 1998) (draft), *available at* <http://developer.intel.com/ial/security/docs/r2_0/license.htm> [hereinafter UAS SPECIFICATION]; *see also* RICHARD SARGENT, CDSA EXPLAINED: A SOURCE BOOK FROM THE OPEN GROUP 59-60 (1998) (noting that Intel is working with Veridicom to incorporate interfaces for biometrics into its software security architecture). These technologies are primarily designed to enhance the security of a particular network, rather than to identify a user to the Internet at large. But as with the Intel PSN, once a user is uniquely identified, that information can be used to grant or deny him access to resources across a wide variety of Internet-connected systems.

47. Gelsinger, *supra* note 44, ¶¶ 3-4 (emphasis added).

48. *Id*. ¶¶ 66, 93.

vides a hardware framework for treating the home PC as part of a trusted system[49]—that is, to allow servers on distant networks to authenticate the identity of a home PC user, and administer authenticated permissioning and rights management.[50] It could thus create a "trusted virtual world" for secure virtual enterprises, business-to-consumer electronic commerce, and secure delivery of high-value digital media content like movies and music.[51]

Gelsinger explained that the PSN, "enabl[ing] platforms and the users that are on those platforms to be better identified,"[52] was Intel's first building block in constructing this system. "You think about this maybe as a chat room, where unless you're able to deliver the processor serial number, you're not able to enter that protected chat room . . . providing a level of access control."[53]

Atop that hardware framework, Intel was constructing the Common Data Security Architecture (CDSA), a cross-platform software framework embodying a common security architecture.[54] The CDSA framework, initiated by Intel and developed in an open standards process, contemplates that independent software and hardware vendors will provide "add-in modules" that perform specific security functions for applications.[55] Applications can thus more easily be written to require that third parties establish their identity or authentication before gaining access to intellectual property.[56] Identity and authorization, in such a trusted environment, are verified on the basis of digital credentials; the Common Security Services Manager, part of CDSA, facilitates linking digital certificates to trust protocols.[57]

---

49. *See id.* ¶¶ 61, 66, 99.

50. *See id.* ¶¶ 66-67.

51. *Id.* ¶ 17. On the other hand, the PSN was unlikely to achieve that result effectively. As noted cryptographer Bruce Schneier urged, PSN-based authentication is inherently insecure because a remote site cannot know whether a home PC's software is accurately reporting the hardware PSN. *See* Bruce Schneier, *Why Intel's ID Tracker Won't Work*, ZDNET NEWS (Jan. 26, 1999) <http://www.zdnet.com/zdnn/stories/comment/0,5859,2194863,00.html>.

52. Gelsinger, *supra* note 44, ¶ 66. Intel, indeed, worked with content providers to develop Web sites that restrict access based on the user's PSN. The sites, though, used the PSN only to determine whether the user's computer was a Pentium III. The idea was to develop processor-intensive Web sites limited to Pentium III users, and thus sell the proposition that Pentium III-equipped computers could show Web content that other computers could not. *See* David Flynn, *Pentium III-Only Sites Coming*, SYDNEY MORNING HERALD, Mar. 2, 1999, at 8.

53. Gelsinger, *supra* note 44, ¶ 99.

54. *See* Intel Architecture Labs, *Common Data Security Architecture: Frequently Asked Questions* (visited Dec. 6, 1999) <http://developer.intel.com/ial/security/faq.htm> (Question 1).

55. *See id.* (Question 2); UAS SPECIFICATION, *supra* note 46 § 1.1.

56. *See* Intel Architecture Labs, *Intel Common Data Security Architecture: Overview* (visited Dec. 6, 1999) <http://developer.intel.com/ial/security>.

57. *See* INTEL CORP., INTEL SECURITY PROGRAM 3, 6 (1998), *available at* <ftp://download.intel.com/ial/security/intelsp.pdf>.

Gelsinger announced plans to add significantly to the PSN and the CDSA's capabilities the following year, "allowing . . . trusted access, adding authenticated permissioning to PCs, [and] increasing levels of capability" in the security architecture.[58] He announced plans to add capability in 2001 relating to "platform and peripheral integrity," thus "accomplishing the trusted transactions [and providing] a platform strong enough to bring all forms of valuable content to the PC."[59] It is easy to imagine that with an architecture incorporating all of these capabilities, the hardware and software of the home PC might enable a remote server to query that PC for its unique PSN, determine whether the machine associated with that PSN has received rights to play a movie, and (if so) deliver the movie in a form such that the PC could play it a set number of times, but could not make a digital copy outside the control of trusted systems.[60]

The PSN excited considerable controversy. Privacy advocates requested that the Federal Trade Commission initiate an inquiry,[61] and followed that up with a complaint formally asking the Commission to halt distribution of the Pentium III as a violation of individual privacy.[62] The Electronic Privacy Information Center announced a boycott of Intel.[63] Large PC makers responded by announcing that, when shipping Pentium III machines for the consumer market, they would set the BIOS (the first software instructions a computer loads when it boots) to make the PSN invisible to most programs.[64]

---

58. Gelsinger, *supra* note 44, at 7.

59. *Id.*

60. This discussion to some extent elides the distinction between identification of *computer platforms* and identification of *consumers*. The distinction comes into play to the extent that (a) more than one consumer uses a single computer; or (b) a single consumer uses more than one computer. The latter case is most important in connection with consumer acceptance of trusted systems; consumers may be reluctant to accept systems that limit them to a single computer in viewing the works they purchase.

61. *See* Letter from Jeffrey Chester *et al.* to R. Pitofsky, Chairman, Federal Trade Commission (Feb. 22, 1999) *available at* <http://www.bigbrotherinside.com/ftc-letter.html> (letter from eight consumer and privacy groups including the Electronic Privacy Information Center) [hereinafter Letter to FTC].

62. *See* Center for Democracy & Tech., *Press Release: Privacy and Consumer Groups File Complaint Against Intel at Federal Trade Commission* (visited Dec. 6., 1999) <http://www.cdt.org/press/022699press.shtml>.

63. *See* Big Brother Inside, *Protect Your PC's Privacy* ¶ 35 (visited Dec. 6, 1999) <http://www.bigbrotherinside.com/#who> (describing the efforts and reasoning behind the boycott).

64. *See* Robert Lemos, *Big PC Makers Decide to Disable Chip ID: IBM, Dell, Gateway and Compaq Shipping PCs with the Technology Off, Letting Users Decide*, ZDNET NEWS (Feb. 26, 1999) <http://www.zdnet.com/zdnn/stories/news/0,4586,2217252,00.html>. I write "most programs" because it appears that even a seemingly invisible PSN may be vulnerable to hacking. *See New Pentium III Security Flaw?*, WIRED NEWS (Mar. 11, 1999) <http://wired.lycos.com/news/news/technology/story/18395.html>; Andy Riga, *Zero-Knowledge Runs at Intel, Again*, MONTREAL GAZETTE, May 5, 1999, at D1.

Intel announced plans to release software patches that consumers could use to do the same thing.[65] These developments, though, have not entirely quieted the controversy over the PSN: A unit of the European Parliament, for example, recently published a working paper urging that the relevant committees of the Parliament call upon the NSA and FBI to provide information on their role in the PSN's creation, and suggesting that the Parliament "consider legal measures to prevent PSN-equipped (or PSN-equivalent) chips from being installed in the computers of European citizens, firms and organi[z]ations."[66]

That manufacturers are shipping computers to consumers with the PSN disabled does not completely dispose of this issue. One can imagine PC owners finding themselves under significant pressure to turn PSN accessibility back on. Web sites can require a PSN as a condition of access. Software applications—including personal finance software, word processing applications, email clients, browsers, and even the operating system—can be written so as not to run unless the PSN is enabled. The markets for PC processors, operating systems, and major classes of applications in the PC environment, after all, are highly concentrated.[67] Information and entertainment resources on the Net are similarly characterized by a small number of powerful publishers existing alongside a huge number of weak ones.[68] To the extent that powerful publishers control attractive intellectual property, they have market power that they can use to influence consumers' choices, and to push the en-

---

65. *See* Robert O'Harrow Jr. & Elizabeth Corcoran, *Intel Drops Plans to Activate Chip IDs*, WASH. POST, Jan. 26, 1999, at E1, *available at* <http://www.washingtonpost.com/wp-srv/washtech/daily/jan99/intel26.htm>.

66. DR. FRANCK LEPREVOST, DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION: ENCRYPTION AND CRYPTOSYSTEMS IN ELECTRONIC SURVEILLANCE § 8(D) (European Parliament Scientific and Technical Options Assessment Panel Working Paper No. PE 168.184 / Part 3/4, 1999), *available at* <http://www.europarl.eu.int/dg4/stoa/en/publi/pdf/98-14-01-3en.pdf>.

67. On the PC processor market, see, for example, *National Semi Quits the Field*, WIRED NEWS (May 5, 1999) <http://wired.lycos.com/news/news/business/story/19508.html>. Eighteen months after buying PC processor manufacturer Cyrix, National Semiconductor announced it would exit the market, stating "we cannot afford to fight Intel." *Id.* National sold Cyrix to Via Technologies and agreed to manufacture chipsets for Via; Intel has taken the position that that deal is illegal. *See* Michael Kanellos, *How Via, National May Skirt Intel Restrictions*, CNET NEWS.COM (July 7, 1999) <http://news.cnet.com/news/0-1003-200-344532.html?st.ne.lh..ni>.

68. Today, one-tenth of 1% of all Web sites capture approximately 32% of user volume. *See* LADA A. ADAMIC & BERNARDO A. HUBERMAN, XEROX PALO ALTO RESEARCH CENTER, THE NATURE OF MARKETS IN THE WORLD WIDE WEB 4 (1999), *available at* <http://www.parc.xerox.com/istl/groups/iea/www/webmarkets.html>. The study suggests that the market for Internet users' attention will be characterized by winner-take-all dynamics.

vironment toward one in which consumers consent to become part of a trusted architecture.[69]

This advantage, further, would not flow merely to those individual publishers with the best market position. It seems unlikely that consumers, even if they have the tools to do so, would routinely toggle the PSN on every time they wish to run a protected program or access a protected Web site, and then immediately toggle it off. It has been reported that once a PSN is enabled, it will be quite difficult for the ordinary consumer, with the tools typically available to such a consumer today, to turn it off.[70] But without regard to the ease or difficulty of that step, inertia is a powerful force. It seems most likely that a typical consumer seeking access to protected software or Web sites would simply turn the PSN on and keep it on, available to anyone to whom his software had the capability to display it.

Chastened by the public reaction to the PSN, Intel retreated and regrouped. It has not mentioned the PSN in any public statement in recent months; instead, it has sought to focus attention on its new Trusted Computing Platform Alliance (TCPA) initiative.[71] Like the trusted computing program Intel had earlier announced, the TCPA is seeking to deliver an "enhanced HW [hardware] and OS [operating system] based trusted computing platform" to ensure, among other things, "[p]latform [a]uthentication"—to provide a standard way for outsiders to query a computer and establish its owner's identity, thus establishing "confidence in interacting with [that] platform."[72] This time, however, TCPA statements emphasize that computer owners must control their personal information and the system's authentication capabilities.[73] The TCPA has not yet released a specification with details to the public.

---

69. *See* Gimbel, *supra* note 12, at 1683-85; Letter to FTC, *supra* note 61.

70. *See* Niall McKay, *Pentium III Serial Numbers Hacked*, SALON 3, ¶ 7 (Feb. 24, 1999) <http://www.salon.com/21st/log/1999/02/22log.html>.

71. *See* Trusted Computing Platform Alliance, *Background* (visited Dec. 6, 1999) <www.trustedpc.org/home/home.htm>. The TCPA was formed by Compaq, Hewlett-Packard, IBM, and Microsoft as well as Intel, *id.*, but Intel appears to be providing at least the administrative infrastructure. *See, e.g.*, Register.com, *Whois Results for Trustedpc.com* (visited Dec. 6, 1999) <http://www.register.com/whois-results.cgi?domain=trustedpc.com> (illustrating that Intel registered the domain name for the TCPA's Web site).

72. TRUSTED COMPUTING PLATFORM ALLIANCE, TCPA OVERVIEW PRESENTATION 3, 9, 10 (1999), *available at* <http://www.trustedpc.org/press.html> (emphasis omitted) (slide presentation).

73. *See id.* at 5, 12.

IV. TRUSTED SYSTEMS AND COMMON IDENTIFIERS

A. *Introduction*

I want to explore some of the social implications of implementing, on a widespread basis, trusted systems based on identifiers such as the PSN. In that connection, it seems to me that two characteristics of the PSN are notable. First, the PSN is keyed to the holder's *identity*, rather than his characteristics. It enforces a particular model of trust, in which to learn the characteristics of a particular would-be information recipient, a publisher first ascertains that person's identity and then looks up the characteristics associated with that identity.

This model stands in contrast to a more privacy-protective approach, in which a person can present credentials verifying certain characteristics, such as country of residence, without necessarily disclosing his identity at all.[74] For an example, consider an idea floated by Ira Magaziner in 1988.[75] Magaziner was looking for an answer to one problem presented by Internet anonymity: It undercuts the ability of geographic jurisdictions to tax, because it may not be clear to the merchant and interested governments whether taxes are due and to whom. Magaziner suggested that consumers could make purchases online through the use of "electronic 'resident cards'" encoding their country of residence, so that escrow agents could collect taxes associated with that jurisdiction.[76] The proposal was unworkable, but was in one respect privacy-friendly: It contemplated that people would reveal, and carry with them online, a single personal characteristic (their country of residence), without having to reveal any other characteristics. The merchant could learn a buyer's residence, but that information transaction would not reveal his name. The PSN, by contrast, eschews this approach. For the PSN to be used as the basis for a trusted system, the content provider must correlate the PSN with its other data relating to the individual owning that computer, by tying all of that data to the single identifier that the PSN represents.

The second notable characteristic of the PSN is that it is a *common* identifier. That is, it is well-suited to use by different information collectors in unrelated transactions, increasing the ease with which a wide range of infor-

---

74. *See* Agre, *supra* note 7, ¶¶ 18, 35; David Chaum, *Security Without Identification: Transaction Systems to Make Big Brother Obsolete*, 28 COMM. OF THE ACM 1030, 1030 (1985); Lessig & Resnick, *supra* note 1, at 412-13. Part V *infra* discusses this in greater detail.

75. Ira Magaziner, at the time, was the President's Senior Internet Advisor.

76. *See Internet Taxation System is Mulled by White House*, WALL ST. J., Sept. 11, 1998, at B4.

mation about a person can be aggregated into a single overall dossier.[77] The greatest obstacle to efficient aggregation and manipulation of data today is the need to reconcile inconsistent formats and identifiers;[78] a standard, common GUID can eliminate that obstacle.[79] To the extent that a variety of content providers and other merchants have each collected information tied to individual PSNs, it is a simple matter to compile those files into larger databases.

B. *Privacy*

Widespread deployment of trusted systems based on such global identifiers will have social consequences. Such systems—in which the user's computer identifies itself during every transaction, to anybody who asks—are pernicious from a privacy perspective. They allow the user to be tracked through cyberspace more easily and thoroughly than is possible under current technology. They have the potential to make the Internet a forum in which database proprietors have what Phil Agre has referred to as a "God's-eye view of the world"—a perspective in which all things have their true names and our Internet representations can straightforwardly be traced back to our real-world identities.[80] Under such an architecture, a much greater

---

77. *See* David Chaum, *Achieving Electronic Privacy*, SCI. AM., Aug. 1992, at 96, *available at* <http://ganges.cs.tcd.ie/mepeirce/Project/Chaum/sciam.html>.

78. For an example of an attempt to gain the benefits of such standardization, consider the RosettaNet specification, under development by a consortium of information technology companies. *See* RosettaNet, *Executive Overview* (visited Jan. 2, 2000) <www.rosettanet.org/general/overview.html>. The point of the RosettaNet project is to build an XML-based language of common data descriptors and business processes to streamline electronic business-to-business transactions. *See, e.g.*, Ellis Booker, *XML Greases Supply Chain*, INTERNET WEEK, Aug. 23, 1999, at 1, *available at* <http://www.techweb.com/se/directlink.cgi?INW19990823S0001> (describing the current status of XML-driven supply chains). Yet an initial draft of the RosettaNet specification raised controversy in part because of the ease with which such standardization allows the sharing of personally identifiable information: The specification directed vendors to provide the purchaser's name and address to every company involved in the item's production. *See* James Glave, *RosettaNet: Nothing Personal?*, WIRED NEWS (Sept. 10, 1999) <http://wired.lycos.com/news/news/technology/story/21699.html>; James Glave, *The Killer Consumer Gossip App*, WIRED NEWS (Sept. 10, 1999) <http://wired.lycos.com/news/news/technology/story/21668.html>.

79. *See* Graham Greenleaf, "IP, Phone Home": ECMS, (c)-tech, and Protecting Privacy Against Surveillance by Digital Works 7-8 (1999) (paper presented to the 21st International Conference on Privacy and Personal Data Protection held September 13-15, 1999, in Hong Kong), *available at* <http://www2.austlii.edu.au/~graham/publications/ip_privacy> ("The success, importance and danger of ECMS [electronic copyright management systems] is likely to depend in large part on the extent to which they achieve interoperability between multiple publishers (within one ECMS), and ultimately, between different ECMS and different media types.").

80. Agre, *supra* note 7, ¶¶ 23, 26. Agre, I should note, disclaims authorship. *See* Email from Phil Agre to the author (May 10, 1999) (on file with the author). He cites Donna Haraway's reference to the "god-trick" in connection with the postulated ability to see like a God from a position

proportion of ordinary transactions would require consumers to present unique identification numbers that would in turn be digitally linked to a much wider range of personal information. To the extent that collecting identification and assembling dossiers is easy, content providers may do so even when they have no compelling use for the information.

Advertisers and others already see great value in compiling dossiers of personally identifiable information for each of us. Consider, in this regard, the recent Abacus-Doubleclick merger. The combined company announced plans to cross-reference Abacus's database of consumer buying habits, containing real names and addresses and detailed buying information, with Doubleclick's database of consumer Internet surfing and buying habits.[81] Doubleclick targets ads to users, based on "dozens of characteristics, including geographic[al] region, language, and business."[82] It backed off plans to associate its online information about individual consumers with Abacus's personally identifiable offline information only in the face of Federal Trade Commission and state investigations, private lawsuits, and a consumer boycott.[83] The adoption of common identifiers would facilitate the correlation of individual data profiles across databases without public relations headaches.

Systems facilitating the close tracking of content—of what people read, view, or listen to—seem particularly problematic. All of these are the constitutents of human thought. In the analog world, information or entertainment goods are commonly sold on a cash basis, leaving no paper or electronic trail. The copies themselves have no surveillance capabilities, and cannot report back to their makers. The copyright owner, indeed, collects no

---

transcendent and outside of lived experience, *see* DONNA J. HARAWAY, *Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective, in* SIMIANS, CYBORGS, AND WOMEN: THE REINVENTION OF NATURE, 183, 193 (1991), and Edwin Burtt's much earlier reference to a similar perspective in THE METAPHYSICAL FOUNDATIONS OF MODERN PHYSICAL SCIENCE: A HISTORICAL AND CRITICAL ESSAY (1925). Neither author developed the idea, though, in relation to computer representations of identity, much less privacy policy.

81. *See* Courtney Macavinta, *DoubleClick, Abacus Merge in $1.7 Billion Deal*, CNET NEWS.COM (Nov. 24, 1999) <http://news.cnet.com/news/0-1005-200-1463444.html>; Courtney Macavinta, *Privacy Advocates Target Abacus Shareholders*, CNET NEWS.COM (June 29, 1999) <http://www.news.cnet.com/news/0.1005-200-344244.html>; Courtney Macavinta, *Privacy Fears Raised by Doubleclick Database Plans*, CNET NEWS.COM (Jan. 25, 2000) <http://news.cnet.com/news/0-1005-200-1531929.html>.

82. *See* Doubleclick, *Annual Report–Overview: Making Internet Advertising Work* (visited Dec. 6, 1999) <http://www.doubleclick.net/annualreport/overview.htm>.

83. *See* Diane Anderson & Keith Perine, *Privacy Issue Makes Doubleclick a Target*, STANDARD (Feb. 3, 2000) <http://www.thestandard.com/article/display/0,1151,9480,00.html>; Jeri Clausing, *Michigan Moves Against Doubleclick*, CYBERTIMES (Feb. 19, 2000) <http://www.nytimes.com/library/tech/00/02/cyber/articles/18doubleclick.html>; Bob Tedeschi, *In a Shift, Doubleclick Puts Off Its Plan for Wider Use of the Personal Data of Internet Consumers*, N.Y. TIMES, Mar. 3, 2000, at C5.

information about the user at all.[84] Trusted systems threaten to abandon those rules, facilitating the monitoring of individual thought. They raise the specter of the Panopticon, and of subtle and not-so-subtle pressures on individuals to eschew socially or governmentally disfavored information goods.[85]

C. *Communications Policy*

A second set of consequences relates to the effects of this technology on the economics and politics of content markets. To begin with, all technological measures protecting digital content (of which trusted systems are a subset) raise an important set of issues typically associated with intellectual property law. Such measures allow sellers of entertainment or information to assert effective control over uses that are privileged by intellectual property law, and over subject-matter that is assigned by intellectual property law to the public domain. That is, they enable sellers to exercise control notwithstanding intellectual property law's judgment that society in those circumstances is best served by free use of the material by the public at large.[86] Others have written cogently about these points, and I will not linger long on them here.[87] Instead, I want to raise broader concerns, which I believe reso-

---

84. *See* Greenleaf, *supra* note 79, ¶ 8.

85. *See* Julie E. Cohen, *Some Reflections on Copyright Management Systems and Laws Designed to Protect Them*, 12 BERKELEY TECH. L.J. 161, 184-85 (1997).

86. Given its enactment of the Digital Copyright Millennium Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860 (1998), which criminalizes the act of "circumventing" such technological protections, Congress appears not to share that concern. *See generally* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anticircumvention Regulations Need to be Revised* (visited Jan. 2, 2000) <http://www.sims.berkeley.edu/~pam/papers/Samuelson_IP_dig_eco_htm.htm> (criticizing the anticircumvention rules).

87. *See generally, e.g.*, Symposium, *Intellectual Property and Contract Law in the Information Age: The Impact of Article 2B of the Uniform Commercial Code on the Future of Transactions in Information and Electronic Commerce*, 13 BERKELEY TECH. L.J. 809 (1998) (collection of articles critically examining proposed Article 2B of the Uniform Commercial Code); James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177 (1997) (explaining that legal rules barring circumvention of technological protection measures clothe both the state and content providers with power they would not otherwise have); Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1089 (1998) (arguing that self-enforcing digital contracts grant publishers absolute control inconsistent with copyright and First Amendment principles); Mark A. Lemley, *Dealing with Overlapping Copyrights on the Internet*, 22 U. DAYTON L. REV. 547 (1997) (emphasizing the broad scope of rights granted to copyright holders by a rote application of the existing statute to Internet technology); Lawrence Lessig, *Intellectual Property and Code*, 11 ST. JOHN'S J. LEGAL COMMENT. 635 (1996) (suggesting that technological protection of intellectual property can make legal protections irrelevant, and thus privatize law); Jessica Litman, *Reforming Information Law in Copyright's Image*, 22 U. DAYTON. L. REV. 587 (1997) (pointing out the dangers to important information-policy concerns presented by the intersection of copyright law and Internet technology); Greenleaf, *supra* note 79 (observing

nate less with those of intellectual property law, and more with those of communications policy generally.[88]

It is useful here to review two capabilities that trusted systems based on common identifiers give to sellers of entertainment or information. First, the reliable identification of the would-be consumer, together with any other information the seller can collect describing that would-be consumer, helps give the seller individualized information about each member of its target audience. Second, the access and copy protection capabilities of the system mean that the seller has much stronger control over which consumers get access to the work; the seller therefore can sharply limit any secondary market in the work.

In the Old Way of Doing Things, technical inefficiencies made it difficult to disseminate speech to a dispersed but tightly controlled group of folks. There was always some leakage: If you wanted to disseminate speech, you had to give up some control over its dissemination. For example, once a content owner distributed a copy of a work, it had no technological means of preventing the owner of that copy from selling, loaning, privately displaying, or giving away the copy as he chose.[89] And the copyright law's "first sale doctrine" denied content owners the ability to impose such restrictions within the four corners of the copyright law.[90] These limitations on content owners' effective rights helped democratize access to content. They allowed gratis redistribution of, and secondary markets in, copies of the works. Though content owners have complained that the Internet threatens to divest them of any control over the distribution of their works, trusted systems threaten to eliminate even the small avenues for royalty-free redistribution that exist in the nondigital world.[91]

It is worth lingering on the role of sharing, and other forms of redistribution, in the nontrusted system world. "Small-scale, decentralized reproduction of intellectual property" has long been a fact of life in markets for information, entertainment, and computer software.[92] People copy music

---

that technical protections of intellectual property may obviate public interest protections in intellectual property law).

88. *Cf.* Kenneth W. Dam, *Self-Help in the Digital Jungle*, 28 J. LEGAL STUD. 393, 395-97 (1999) (suggesting that copyright scholars, precisely because they tend to approach technological protection systems from an intellectual property standpoint, have been insufficiently appreciative of the virtues of technological protections).

89. *See* Litman, *supra* note 87, at 600-01.

90. *See id.*

91. *See* note 12 *supra* and accompanying text.

92. Stanley M. Besen & Sheila Nataraj Kirby, *Private Copying, Appropriability, and Optimal Copying Royalties*, 32 J.L. & ECON. 255, 255 (1989); *see also* Yannis Bakos, Erik Brynjolfsson & Douglas Lichtman, *Shared Information Goods*, 42 J.L. & ECON. 117 (1999) (investigating how

tapes and CDs for themselves, family, and friends; they photocopy magazine articles; they allow family and friends to use, and copy, their computer software. They persist in doing so, notwithstanding the best efforts of the copyright industries to convince them that it is illegal, largely because they find it hard to believe that this is something the law does or should proscribe.[93] And that system seems to work—at least, it has not obviously injured in any palpable way producer incentives to create intellectual property.

The nontrusted-system world is also characterized by a lot of sharing, in the vernacular sense, that does not implicate copyright law. As I noted above, people *lend* each other analog copies of protected works, and read, watch, or listen to works they have borrowed, all without implicating the copyright laws at all. At least in a static analysis,[94] both of these sorts of sharing are good, since they increase the distribution of information and thus social benefit without any social cost.[95] Put another way, sharing allows the distribution of information at the optimal demand price, because that price is equal to the marginal cost of distribution, which in this case is close to zero.[96] The most successful institutions in American life today that are based on such sharing are public libraries, which were established precisely to enable large-scale sharing of analog works.

The trusted-system world could involve a number of changes to this status quo. The content provider's enhanced control over access to the work could constrain both types of sharing I have described above. It would allow content providers to sharply limit the small-scale copying of intellectual property that has become both accepted and commonplace among consumers today, but that producers contend violates their copyrights. It could also greatly limit the small- and large-scale lending and borrowing of intellectual property that takes place today and is unimpeachably consistent with the copyright laws. After all, as noted above, the control given content providers by trusted systems does not rest on whether the content provider can assert

---

consumer sharing of information goods affects seller profits); Litman, *Copyright Noncompliance (Or Why We Can't "Just Say Yes" to Licensing)*, *supra* note 17; Michael J. Meurer, *Price Discrimination, Personal Use and Piracy: Copyright Protection of Digital Works*, 45 BUFF. L. REV. 845, 852-56 (1997) (discussing the economic impacts of unauthorized sharing).

93. *See* Litman, *Copyright Noncompliance (Or Why We Can't "Just Say Yes" to Licensing)*, *supra* note 17, at 252-53; Jessica Litman, *Revising Copyright Law for the Information Age*, 75 OR. L. REV. 19, 40-41 (1996).

94. *But see* text following note 108 *infra* (discussing the dynamic impact of sharing).

95. *See* Kenneth J. Arrow, *Economic Welfare and the Allocation of Resources for Invention*, *in* THE RATE AND DIRECTION OF INVENTIVE ACTIVITY: ECONOMIC AND SOCIAL FACTORS 609 (1962); Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354, 424 (1999).

96. *See* Benkler, *supra* note 95, at 424 & n.273.

intellectual property rights in the work, or whether a particular use of the work by a consumer would violate those rights.

The trusted-system world also seems well-suited to facilitate discrimination on the part of the content provider, a change with more ambiguous results. Most obviously, trusted systems will facilitate price discrimination—that is, the content provider can ask different consumers to pay different prices, unrelated to the provider's own costs. That is not the way markets typically work: Most commonly, a producer sets a uniform price, which each consumer chooses to pay or not pay. Sellers cannot effectively engage in price discrimination unless three conditions are met.[97] First, the seller must be able to prevent (or limit) arbitrage—it must ensure that buyers who paid a low price do not turn around and resell the information or entertainment to someone who would otherwise be willing to pay the content provider the higher price. Otherwise, any attempt by the producer to partition the market would be unavailing. Trusted systems make this possible by greatly enhancing the content provider's ability to control any redistribution of the work.

Second, the seller must have market power. All copyright owners have some degree of market power because of the legal control that intellectual property law gives them; that is one reason they are able to charge prices in excess of marginal cost. Some, naturally, have more market power than others, based on the demand for the work and the availability of near-substitutes.

Finally, the seller must be able to set prices in a way that in fact reflects consumers' willingness to pay. Trusted-system technology can make this possible in two ways. First, as noted above, a trusted online architecture based on global user or platform identifiers will allow content providers to tie each consumer to a wide range of personally identifiable information. For example, when the consumer presents her PSN to gain access to a digital work, the content provider will be able to pull up other information associated with that PSN in order to make a judgment about the particular consumer's willingness to pay.[98] Alternatively, the content provider can shift its payment model from the "sale" model prevalent today, in which the consumer buys a copy of the work and can then read, listen to, or watch that copy an unlimited number of times without further payment, to a "pay-per-read" system in which the customer pays a smaller amount on each occasion

---

97. *See* Meurer, *supra* note 92, at 870.

98. Economists refer to this as third-degree price discrimination. *See* W. KIP VISCUSI, JOHN M. VERNON & JOSEPH E. HARRINGTON, JR., ECONOMICS OF REGULATION AND ANTITRUST 290-91 (2d ed. 1995).

that she reads, listens to, or watches the work. This allows the content provider to collect more money from those customers who want to use the work many times and presumably are willing to pay more for that ability, and less from those who want to view the work only once. The difference between those prices is largely unrelated to the content provider's own costs.[99]

Is this price discrimination a good thing or a bad one? Some have argued that it is beneficial.[100] Price discrimination in information goods is socially useful, the argument runs, because it increases the distribution of information. Without price discrimination, the content provider must charge a single market price, and people unwilling to pay that price will be shut out of the market entirely. If the content provider can engage in price discrimination, by contrast, it can charge every consumer the exact price that she is willing to pay, thus simultaneously maximizing profits and maximizing the number of people who will be exposed to the information and entertainment in question. "[W]e can say with confidence that many more consumers [will benefit] from the author's creation."[101]

The matter, though, is not nearly so straightforward. Price discrimination is unquestionably good for producers since it converts consumer surplus into producer profits. But whether, as a general matter, price discrimination increases overall welfare is a more difficult question, resting on the facts of each case.[102] An increase in the distribution of the good is a necessary, but not a sufficient, condition for increasing total welfare.[103]

More to the point, in thinking about whether the price discrimination enabled by trusted systems would be a good thing, we need to ask the question, "Compared to what"? One of the key reasons that trusted systems enable price discrimination is that they sharply decrease sharing; they are designed to eliminate any redistribution of the information good beyond the control of the content provider. That is, price discrimination allows the sale of information to consumers willing to pay less, but at the expense of cutting off *existing* means, through sharing and secondary markets, of getting the information or entertainment at low or no cost to some of those same consumers. Indeed, from a static perspective sharing is a more efficient way of

---

99. This falls within a category that economists refer to as second-degree price discrimination. *See id*. at 249-55, 290-91.

100. *See, e.g.*, Fisher, *supra* note 5 (arguing that price discrimination makes information products available to a wider range of consumers). *But see* Wendy J. Gordon, *Intellectual Property as Price Discrimination: Implications for Contract*, 73 CHI.-KENT L. REV. 1367 (1998) (querying Fisher's premises).

101. Fisher, *supra* note 5, at 1239.

102. *See* VISCUSI ET AL., *supra* note 98, at 290-95; Meurer, *supra* note 92, at 896-98.

103. *See* VISCUSI ET AL., *supra* note 98, at 293-95; Meurer, *supra* note 92, at 898.

allowing the market to reach those consumers, since it makes the good available to them at a price more nearly approaching the zero marginal cost of supplying it to them.

Secondary markets, involving redistribution of information goods after their first sale and outside the control of the initial seller, can do the same job as price discrimination of getting information goods at lower prices to lower-valuation users. That is what used bookstores are all about. The price discrimination that trusted systems may facilitate therefore may not increase the number of consumers getting the good at all; it may simply ensure that the low-valuation consumers receive the good from the initial seller rather than someone else.[104] Further, it does so at the distributional cost of shifting all surplus away from consumers.

The points I have made so far are open to a variety of counterarguments. First, it might be argued that price discrimination will do a better job of getting the information or entertainment to low-valuation users, many of whom may not have the opportunity to gain access to the work through resale or sharing. The copyright-law implications of issues surrounding small-scale redistribution, even when no new copies are created (aside from the RAM copies that are associated with any invocation of a digital work), are hotly debated within the legal community. Large-scale copying and redistribution of digital works is illegal even when no price is charged.[105] Yet public libraries, at least, are set up precisely for the purpose of getting free information works to users unwilling to pay the price set by the market. Consumers interested in viewing a work only once and willing to wait until it is available can borrow from the library; those interested in viewing the work multiple times are more inclined to buy it. This is precisely the sort of result price discrimination is supposed to achieve.

By contrast, it is unclear to what extent price discrimination in practice can achieve the advantages theory promises for it. It is difficult to gauge consumer preferences precisely, and publishers are unlikely to drop prices too far based on guesses about a particular class of consumers' willingness to pay. While theoretical perfect price discrimination promises perfectly efficient markets, real-world third-degree discrimination will fall short of that ideal, as publishers group consumers by second-best proxy characteristics and attempt to set prices for each group. Nor will consumers easily accept

---

104. *See* Gordon, *supra* note 100, at 1378-89.

105. *See* No Electronic Theft (NET) Act of 1997, Pub. L. No. 105-147, 111 Stat. 2678 (codified at, inter alia, 17 U.S.C. §§ 506-07 & 18 U.S.C. §§ 2319-2320); William McCall, *College Student Convicted of Piracy*, AP ONLINE, Aug. 21, 1999, *available in* WESTLAW, WL 22036202 (describing the first conviction under the 1997 law).

second-degree discrimination: The splashy failure of DIVX, a pay-per-view movie format, should give rise to some doubt about the enthusiasm with which ordinary folks will embrace usage-based prices for digital works.[106]

Next, one might argue that if sharing were technologically disallowed then market prices would fall. Without the possibility of sharing, the argument runs, information goods are not as valuable to purchasers. Yet when the content provider must set a single market price, it cannot easily raise that price to take into account the benefits of sharing, because different buyers will place significantly different values on the ability to share (and will in fact share with markedly different numbers of people).[107] Moreover, the existence of leakage also acts to constrain prices, by providing a near-substitute for the purchased good.[108]

Finally and most obviously, one might argue that this analysis overlooks the dynamic impact of sharing and the nature of secondary markets in digital works: Sharing and resale do not generate revenues to the content provider, so they do not provide incentives to stimulate production. More baldly, one might argue that my discussion is in essence an argument for piracy—which will certainly lower prices to the consumer, but at the cost of diminishing incentives to produce. Secondary markets in the digital world, the argument runs, may involve large numbers of illegal perfect copies. Sale of those copies cuts directly into the profits, and thus the incentives, of the initial producer.

I do not contest that producer incentives are necessary. Publishers must be able to sell information goods at a price sufficiently above marginal cost, and for a sufficiently long period of time, to recover their fixed (first-copy) costs. Otherwise, they would lose money. To that end, there must be suffi-

---

106. The DIVX plan was that a user would purchase a videodisk for $4-5, and have free access for 48 hours after the first play. After that time, the user would pay a fee for every subsequent viewing; those viewings would be purchased through a central server connected to the DIVX player by telephone line. *See* DAVID DRANOVE & NEIL GANDEL, THE DVD VS. DIVX STANDARD WAR: NETWORK EFFECTS AND EMPIRICAL EVIDENCE OF VAPORWARE 8 (Tel Aviv Univ. Eltan Berlgas School of Economics Working Paper No. 14-99, 1999). DIVX was discontinued, for lack of consumer interest, in June 1999. *See* Carl Laron, *Of Edsels and DIVX*, ELECTRONICS NOW, Sept. 1, 1999, at 2.

107. Bakos et al., *supra* note 92, engage in a much more sophisticated analysis of this phenomenon. The authors conclude that sharing decreases producer profit when the diversity in team size, defined as the number of consumers sharing any particular copy of the good, exceeds the diversity in individual consumer valuations. They note that seller profit is enhanced if high-valuing consumers tend to share with low-valuing consumers rather than with each other, and if low-valuing consumers tend to share with a greater number of people than do high-valuing consumers. Both of these contingencies will tend to "even out" the value that each team places on the good, and thus will allow the producer to reflect that value more nearly in its selling price. *Id.* at 122-27.

108. *See* Benkler, *supra* note 95, at 433 n.302.

cient entry barriers limiting other folks' ability to sell those works as cheaply. We do not know, though, how much in the way of incentives producers need.[109] Ordinary economic theory suggests that publishers will invest so long as they expect profits, taking into account normal rates of return. If publishers have adequate incentives even without the extra rents that price discrimination gives them, then we *may* get a better social result by reaching lower-valuation users through secondary markets, sharing, or even some degree of piracy than through the increased control that trusted systems bring.[110]

Further, there is a connection between media concentration and the power of information providers to identify consumers and to thus discriminate. To the extent that sellers' ability to price discriminate will rest on their access to personally identifiable information about buyers, publishers with access to those databases will have a competitive advantage over those who do not. This may have two negative effects. First, it will tend to concentrate media markets—and, to the extent those markets are characterized by winner-take-all dynamics,[111] will help determine who those winners are. Second, it will increase the value of the dossiers, and thus increase the commercial pressure on privacy.

The control facilitated by trusted systems and common identifiers may allow other sorts of discrimination as well. Most generally, it will increase producers' ability to pick and choose who will be allowed to view or read particular works. Given the power of a common identifier such as Intel's PSN to facilitate the association of a wide range of information with a given personal identifier, producers could in theory use these tools to allow access to a speech work only by persons who live in preferred zip codes, have certain levels of family income, or are white. There may be only limited circumstances in which a mass marketer of entertainment and information would have an incentive to do so: Most obviously, perhaps, a publisher might discriminate because of ideological motivations, or if particular content gained cachet from only limited distribution. From a free speech and communications policy standpoint, though, it seems disturbing to see extensive social investment in a technology built around the ability to *prevent* the movement of speech and information to the public at large.

---

109. *See* Litman, *The Exclusive Right to Read*, *supra* note 17, at 44-46.

110. *See* Bakos et. al., *supra* note 92, at 148 ("[P]rofitability and social efficiency need not go hand in hand: sharing can be profitable [for content providers] in situations where it is not efficient, and efficient in situations where it is not profitable.").

111. *See* note 68 *supra*.

For the most part, today, content producers and consumers share control over the uses and dissemination of speech works. Content producers have extensive control by virtue of their ability to produce and license the technological artifacts (such as film reels) embodying those works, reinforced by the rights granted them by the copyright law. Consumers have some control as well, by virtue of their own abilities to use, copy, and manipulate such works in ways that the copyright law either does not forbid or expressly privileges,[112] or in ways that have been effectively immune from copyright enforcement. And because these are speech works, that distribution of control has political consequences. It shapes the overall movement of information and expression within society. The rise of trusted systems based on common identifiers would shift that control.[113]

V. IDENTIFICATION AND CREDENTIALS

In short, trusted systems based on common identifiers that are tied to consumers' real-world identities have plainly undesirable privacy consequences. Their consequences for the structure of content markets appear to be negative on balance. And yet, one might think, they are unavoidable if we are to allow content providers control over exploitation of their works in the networked digital environment. That statement, though, is not correct. In fact, the Internet's architecture can support trusted systems, and the concomitant control by content providers over works of information and entertainment, without any need for common identifiers.

Recall the original concern driving industry plans for unique identification of Internet-connected computers and consumers: Content providers wish to be sure that a packet stream requesting access comes from a person who has paid or is otherwise entitled to access. One way to accomplish that result is to tag every computer/consumer with a single identifier that shows up in the packet stream requesting access and allows the provider to reference a database of consumers' characteristics. But that approach conveys much more information to the content provider than the provider actually needs.

---

112. *See, e.g.*, 17 U.S.C. § 1008 (privileging consumers' noncommercial use of digital audio recording devices, digital audio recording media, analog recording devices, and analog recording media for making musical recordings); Recording Indus. Ass'n v. Diamond Multimedia Sys., 180 F.3d 1072 (9th Cir. 1999) (declining to enjoin the manufacture and sale of the Rio portable music player, which plays downloaded MP3 files).

113. *See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 154-56 (1999) (raising equity-based concerns).

What the content provider needs is a way to verify that the user has specific credentials: that the user has paid, or that he has some other characteristic that the content provider desires in its readers. Establishing the user's identity is an instrumental step towards verifying his credentials. Yet it is well-established in the cryptography literature that one can prove credentials without proving identity: That is the basis for anonymous digital cash.[114] A person, for example, can interact with other entities through a "pseudonym"—a name that is reliably associated with that individual in a particular context through cryptographic techniques, but cannot be associated with other names the person uses in other contexts.[115]

The word "pseudonym" sounds vaguely disreputable, but the goal is simple and usually honorable: It is to allow the user to enter into transactions and relationships in which they can be held accountable, without allowing data miners to collect into a single global profile the universe of transactions that the user enters into. It is consistent with current rights-management technology[116] to build structures under which consumers interact with content providers anonymously or pseudonymously, without sacrificing content owners' ability to enforce contractual restrictions.[117]

This approach would address the privacy issues raised earlier in this article, by making the aggregation of a user's information across unrelated transactions impossible. It would not make it impossible for a content provider to discriminate among users, but it would make that process more open and public. Because the content provider would not know any information about the user that the user did not provide, it could discriminate on the basis of a particular characteristic only after expressly asking the user to provide

---

114. *See* Agre, *supra* note 7, at ¶¶ 6, 35; Chaum, *supra* note 77; Chaum, *supra* note 74; Roger Clarke, Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice (1999) (unpublished paper), *available at* <http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html>; *see also* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY, SECOND EDITION: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C 112-14 (2d ed. 1996) (blind signatures); *id.* at 125-27 (secure voting); *id*. at 139-45 (digital cash).

115. *See* Chaum, *supra* note 74.

116. *See, e.g.*, note 12 *supra* (citing sources that discuss trusted systems); R. MARTIN RÖSCHEISEN, A NETWORK-CENTRIC DESIGN FOR RELATIONSHIP-BASED RIGHTS MANAGEMENT (1997) (Ph.D. dissertation), *available at* <http://pcd.stanford.edu/~roscheis/dissertation.pdf> (examining techniques for articulating and enforcing boundaries of control on the Internet, while enabling collaboration and sharing in a peer-to-peer environment).

117. Indeed, technologists are now building a variety of services that could offer such pseudonymity. *See* Declan McCullagh, *A New ID-Less ID System*, WIRED NEWS (Feb. 22, 2000) <http://www.wired.com/news/politics/0,1283,34477,00.html>; Chris Oakes, *Pseudonymity Now*, WIRED NEWS (Jan. 21, 2000) <http://www.wired.com/news/technology/0,1282,33805,00.html>; David Pescovitz, *Undercover Agents*, STANDARD (Jan. 3, 2000) <http://www.thestandard.com/article/display/0,1151,8482,00.html>.

credentials relating to that characteristic. Content providers would be reluctant to seek information where such requests would be unpopular in the marketplace or the forum of public opinion.

I do not mean to suggest that verification systems protecting user privacy would be the first choice of content providers. For the reasons set out earlier in this paper, content providers may find such systems significantly less profitable, and hence less desirable, than those that give them access to a greater range of user information. However, the feasibility of privacy-friendly systems means that from the perspective of social policy, building trusted systems around common identifiers is not merely undesirable; it is unnecessary.

VI. CONCLUSION

Technologies involving the assignment and use of global user IDs, enforced through hardware-based user identification such as Intel's Processor Serial Number, could give providers of information goods extensive new capabilities. Such technologies provide an easy and straightforward way for publishers to verify the authenticity of messages claiming authorization to receive digital works, giving them greater ability to limit availability of their works to folks who meet certain criteria. These technologies, though, will have other consequences as well. The most obvious relate to privacy: Trusted systems relying on common identifiers, and in particular systems built around the PSN, threaten to sharply lessen anonymity and informational privacy on the Internet. They raise the prospect that a much larger proportion of ordinary transactions will require consumers to present unique identification numbers digitally linked to a wide range of personally identifiable information. They are well-suited to being used across the board by a large number of unrelated information collectors, increasing the ease with which a wide range of information about a person can be aggregated into a single overall dossier.

Moreover, the combination of trusted-systems technology, which allows publishers to ensure that speech released to Bob does not make its way via sharing or secondary markets to Alice, and the privacy impacts of allowing publishers to collect extensive individualized information on consumers will likely affect the economics and politics of speech markets. It may sharply enhance producers' ability to discriminate among individual consumers, on price and other grounds, in connection with the sale and marketing of information goods. Some commentators suggest that this concentration of control is a good thing; the price discrimination it enables, they argue, will broaden distribution of information goods. Yet the benefits of such a system are

clouded; any increase in distribution due to price discrimination comes at the cost of shutting down distribution that comes, in today's less-controlled system, through sharing or secondary markets. It will likely be accompanied by increased media concentration and a self-reinforcing cycle of commercial pressure on individual privacy.

It is important to remember, finally, that publishers can get the benefits of trusted systems without these socially undesirable. Building trusted systems around common identifiers, in other words, is gratuitous.