DRAFTv5

Anonymity in the Balance

A. Michael Froomkin

The right to anonymity in the USA and elsewhere is in an odd state of paradox and flux. Despite a few small clouds on the jurisprudential horizon, in the US (although perhaps, all of a sudden, not in the EU[1]) the formal legal protection of the right to anonymous speech is at an all-time high. Yet, while the law in the books creates a strong right to anonymous speech, it is reasonable to question how long the effective exercise of that right will remain a practical possibility. If doctrinally the right to anonymous speech is better enshrined in law today than ever before, at the same time there are efforts by both public and private parties to use pre-existing legal and especially technical means to undermine anonymity (and pseudonymity). These efforts are at an all-time high -- and are still growing.

The Patriot Act,[2] the law-enforcement investigatory power legislation passed in the wake of the 2001 terrorist attack on the World Trade Center, had only a very limited effect on the right to anonymity. Congress did not attempt to impose any new limits on the legal right to possess and use the cryptographic tools that make Internet anonymity possible. But the Patriot Act was probably only a first step, and it is difficult to predict what a changed political climate may produce; for example, there are calls from various quarters for a national ID card system. Meanwhile, the U.S. government is widely reported to have stepped up its communicative surveillance efforts, including the much-touted, perhaps even over-hyped, Carnivore system. And, even before all this, the exercise of the right to the anonymous exchange of information was under substantial pressure, primarily from commercial interests who seek to know exactly who is accessing digital content in order to be able to charge for it.

---

[1] Sadly, the EU seems to be about to set in motion a full regime of telecommunications monitoring and logging. *See* Wendy Grossman, *A New Blow To Our Privacy*, THE GUARDIAN (June 6, 2002), http://www.guardian.co.uk/online/story/0,3605,727644,00.html; Statewatch, *European Parliament caves in on data retention* (May 30, 2002), http://www.statewatch.org/news/2002/may/10epcavein.htm; *see also* Cryptome.org, *Draft Agenda: Expert meeting on cyber crime: Data retention*, http://cryptome.org/europol-rape.htm (reprinting required draft data retention wishlish of European law enforcement agencies). For a survey of worldwide developments, see ELECTRONIC PRIVACY INFORMATION CENTER, AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS (2002), http://www.privacyinternational.org/survey/phr2002/.

[2] Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56 (2001). On the Patriot Act see generally Orrin Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U.L. REV. (forthcoming 2003).

This chapter concentrates on legal norms and developments in the US because I am a US-trained lawyer. The Internet, however, is a world-wide network, and anonymity-enhancing policies in the US may assist persons elsewhere seeking to evade restrictions imposed by local dictators and totalitarians, and even democrats.[3] Although sufficiently motivated governments can deploy technical counter-measures, such as the 'Great Firewall of China,' these come at a cost and are not certain to be effective. Conversely, anonymity-blocking policies in the US may make it easier for other governments to prevent their citizens from organizing opposition movements or practising their religions, since dissidents and others would be denied the use of anonymity-enhancing Internet service providers, remailers, and anonymous digital cash providers based in the U.S. Furthermore, U.S. computer policies and technologies often set world-wide standards; if nothing else the use of a standard in the large U.S. market tends to drive down its price. Of course, what happens outside the U.S. also has effects on it: citizens of the US can take advantage of more anonymity-friendly policies elsewhere; furthermore anti-anonymity policies originating abroad may affect US rules, as they may be cited as models, or even as legal standards to which the US has a moral obligation to conform.

If the legal analysis is every bit as parochial as it seems, the discussion of technical developments is considerably more international than it may appear. Although the examples are drawn almost entirely from US sources, both the technology in question and the profit motive know few boundaries; the push for complete content control in the US is either symptomatic, or at best only a slight precursor, of similar developments elsewhere.

I. Underlying Issues

It remains as true today as ever[4] that there is no consensus in the United States as to whether, on balance, anonymity is a good. Anonymity has both valuable and harmful consequences, and different persons weigh these differently. Some, focusing on anonymity's contribution to many freedoms, argue that anonymity's benefits outweigh any likely harms it may cause, or that the harms (e.g. censorship, lack of privacy) associated with trying to ban anonymity are not worth any benefits that could ensue. Others, perhaps focusing on the victims of harmful actions that can be accomplished anonymously (libel, spamming, massive copyright violations), look at anonymity and see dangerous license. Their conclusion is that at least some forms of anonymity should be banned.

The case against anonymity is simple. Anonymity is generally dishonorable because it "facilitates wrong by eliminating accountability, which is ordinarily the very purpose of the anonymity." To create

---

[3] See note 1.

[4] Parts of this chapter are a revised and updated version of A. Michael Froomkin, *Legal Issues in Anonymity and Pseudonymity*, 15 THE INFORMATION SOCIETY 113 (1999).

legal protection for anonymous communication absent a reason to expect "threats, harassment, or reprisals," is to allow "a coarsening of the future" in which people act without the necessary fear of consequences.[5] Anonymous communication poses particularly stark enforcement problems for libel law and intellectual property law. While it may be true that a signed defamatory message carries more credibility and thus is more damaging than an anonymous one, it does not necessarily follow that an unsigned message is harmless. Most people would probably be upset to discover a series of unsigned posters accusing them of pedophilia tacked to trees or lampposts in their neighborhood. Perhaps aware that some people believe that where there is smoke there must be fire, the victim of such a libel is unlikely to be soothed by the suggestion that anonymous attacks lack credibility.[6] An Internet libel can be spread world-wide, and may be effectively indelible since it may be reproduced, and stored, in countless and untraceable numbers of computers. Anonymity can also be used to cloak the identity of someone revealing a trade secret, or distributing pirated copies of copyrighted intellectual property such as software and digitized photographs.

Anonymous communication is a great tool for evading detection of many varieties of illegal and immoral activity. Not just libel and disclosure of trade secrets and other valuable intellectual property, but conspiracy, electronic hate-mail and hate-speech, electronic stalking and "spamming," general nastiness, all become lower-risk activities if conducted via anonymous communications. These activities are merely low-risk rather than no-risk because it always remains possible to infer the identity of the author of some messages from clues intrinsic to the message itself.

The case for anonymity is more complicated. Communicative anonymity encourages people to post requests for information to public bulletin boards about matters they may find too personal to discuss if there were any chance that the message might be traced back to its origin. In addition to the obvious psychological benefits to people who thus find themselves enabled to communicate, there may be external benefits to the entire community. To pick just one example, public health is enhanced by the provision of information regarding communicable diseases, but many people would feel uncomfortable asking signed questions about sexually transmitted diseases, and might be especially cautious about being identified as a potential sufferer of AIDS. This caution may be particularly reasonable as data-collection technology improves: any post to a public newsgroup or bulletin board is liable to be archived and searchable, perhaps for all eternity.

Anonymous communication, whether traceable or not, fosters the development of digital personae, which may be experienced as liberating by some.[7] The option of creating such personae is

---

[5] McIntyre, v. Ohio Elections Commission, 514 U.S. 334, 385 (Scalia, J., dissenting).

[6] *See, e.g.*, New York v. Duryea, 351 N.Y.S.2d 978, 996 (N.Y. Sup. Ct.) , *aff'd* 354 N.Y.S.2d 129 (1st Dep't 1974) (arguing that people tend to apply an appropriate discount to anonymous writing).

[7] For a celebration of such "digital personalities" see Curtis E.A. Karnow, *The Encrypted Self:*

likely to increase and enhance the quantity, if not inevitably the quality, of speech. In addition to increasing the quantity of speech, anonymous communication might also enhance the quality of speech and debate. Communications that give no hint of the age, sex, race, or national origin of the writer must be judged solely on their content as there is literally nothing else to go by. This makes bigotry and stereotyping very difficult, and also should tend to encourage discussions that concentrate on the merits of the speech rather than the presumed qualities of the speakers. (On the other hand, it may be that "disclosure advances the search for truth," because when propaganda is anonymous it "makes it more difficult to identify the self interest or bias underlying an argument."[8])

Given this uncertain background, two factors make the current situation particularly volatile. First, the Supreme Court has in recent years weighed in heavily in favor of a right to take part anonymously in political activities, and indeed has done so in terms that suggests a willingness to find broad rights of anonymity in the Constitution. The Supreme Court's most recent decision upheld a claim of a right to proselytize anonymously from door to door against a community's assertion of the right to require persons planning solicitations to register.[9] The decision thus confirms the trend, and does so in the face of the political, law enforcement, and social mobilization following the terrorist attack on the World Trade Center.

What's at stake in debates over the right to anonymity, and how the legal system will weigh the interests, varies with the circumstances. Three sets of variables seem particularly important: whether the speaker is anonymous or using a 'nym; how secure the communication is; and the substance and circumstances of the communication. If one somewhat artificially treats the first two categories as binary, one can identify four types of communication in which the sender's physical (or "real") identity is at least partly hidden: (1) *traceable anonymity*, (2) *untraceable anonymity*, (3) *untraceable pseudonymity*, and (4) *traceable pseudonymity*. These categories highlight the separation between whether and how an author identifies herself as opposed to whether and how the real identity of the author can be determined by others. The last variable, the substance and circumstances of the communication may determine to what extent the state will seek to regulate the communication, but it's important to note that whatever the state seeks to do, it may lack the ability to effectuate its commands if the sender's identity is 'untraceable'.

A. Pseudonymity or Anonymity

Whether the communication is anonymous or pseudonymous is perhaps the least important issue

---

Fleshing Out the Rights of Electronic Personalities, 13 J. COMPUTER & INFORMATION L. 1 (1994).

[8] Note, *The Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil*, 70 YALE L.J. 1084, 1109, 1111 (1961).

[9] *See* Watchtower Bible and Tract Soc. of New York, Inc. v. Village of Stratton, 122 S. Ct. 2080 (2002).

to the legal analysis, although it may matter greatly to the participants in the communication. Pseudonymity differs from anonymity in a number of ways. Perhaps the most important difference is that pseudonymity allows for the creation and continuity of a "nym" -- an alternate identity. An example of a (very insecure) nym would be the creation of a free internet email account at popular services such as Yahoo or Hotmail; the service knows something about the user's identity if only his IP number, but correspondents do not.

Suppose Alice is a repeat participant in chat room or a mailing list. Alice might decide to sign her messages as "Andrea". Alice could, however, have chosen to sign her messages as "Frank", on the theory that this might allow her to avoid anti-female discrimination. Indeed, either sex can masquerade as the other; children as adults (and vice-versa). If nothing else, this creates some potential for embarrassment, and concerns some parents. And, as Prof. Jerry Kang has suggested, the ability to masquerade as others might perpetuate stereotypes: If many members of a dominant culture (say, white males) present themselves as members of other groups (say, women or minorities) and do so on the basis of widely shared stereotyped ideas of what members of those groups are like, then persons interacting with them who do not guess that the 'self' presented as authentic is actually a case of bad acting will instead take that presentation as the vindication of the cultural stereotypes.[10]

B. Security

While the presentation of self matters greatly to the experience of the communication, it is separate from whether the communication can be traced back to its sender -- whether the anonymizing or pseudonymizing technique is secure. Security tends to be a continuum, but for analytical purposes security can usefully be treated as binary: Some *traceable* communications are insecure because there is a known (or knowable) intermediary who can identify the speaker. For other, more secure, *'untraceable'* communications, there is no such person. To make the examples that follow clearer, in each case Alice will be the person sending an e-mail message to Bob. Ted, Ursula, and Victor will be remailer operators, and Carol a judge with subpoena power.

The traditional anonymous leaflet required a printing and distribution strategy that avoided linking the leaflet with the author. If the leaflet risked attracting the attention of someone armed with modern forensic techniques, great pains were required to avoid identifying marks such as distinctive paper or fingerprints. In contrast, on the Internet communications are all digital; the only identifying marks they carry are information inserted by the sender, the sender's software, or by any intermediaries who may have relayed the message while it was in transit. Ordinarily, an e-mail message, for example, arrives with the sender's return address and routing information describing the path it took to get from sender to receiver; were it not for that information, or perhaps for internal clues in the message itself ("hi mom!"), there would be nothing about the message to disclose the sender's identity.

[10] Jerry Kang, *Cyber-race*, 113 Harv. L. Rev. 1130 (2000).

Traceable pseudonymity is communication with a *nom de plume* attached which can be traced back to the author (by someone), although not necessarily by the recipient. While a traceable pseudonymous system makes it much easier for someone to discover Alice's identity, it usually offers one large compensating advantage: the recipients of Alice's message can usually reply to it by sending e-mail directly to the pseudonymous e-mail address in the "From:" field of the message. The message will then either go to Ted, the remailer operator or bulletin board operator, who keeps an index of the addresses that link Andrea to Alice, or in the case of commercial service providers who allow subscribers to use pseudonymous IDs, directly to Alice's account.

Before it was closed down, Anon.penet.fi, probably the best-known "anonymous" remailer, was in fact merely a very user-friendly traceable pseudonymous remailer. It allocated each user an id which it used for all subsequent newsgroup posts and emails from that user. Mail messages sent to that-person's-id@anon.penet.fi were redirected to the person's original, real address.[11]

The anon.penet.fi system kept a record of each user's e-mail address. The security of the approximately 8,000 messages that pass through anon.penet.fi daily[12] thus depended critically on the willingness of the operator, Johan Helsingius, a Finnish computer scientist, to refuse to disclose the contents of his index which maps each anonymous ID to an e-mail address. In February 1995, the Church of Scientology successfully enlisted the aid of the Finnish police, via Interpol, to demand the identity of a person who had, the Church of Scientology claimed, used anon.penet.fi to post the contents of a file allegedly stolen from a Scientology computer to a USENET group called "alt.religion.scientology." Helsingius surrendered the information, believing that the only alternative under Finnish law would have been to have the entire database seized by the police.[13] Ultimately Helsingius later closed down the service primarily because it was being flooded with "spam" messages.

Today, many commercial ISPs and on-line service providers, such as America Online (AOL) and e-Bay, allow users to use any unique name they like as their "user ID," their on-line identifier. As we shall see, when people think they have been defamed or otherwise injured by the actions of a user who employs a pseudonym, the party claiming injury is likely to ask courts to require the disclosure of the identity of the subscriber, at least when the ISP or service provider is in an accessible jurisdiction.

Traceable anonymity in its simplest case is very similar to traceable pseudonymity, except that two-way communication is harder. By participating in discussions under a consistent pseudonym-often

---

[11] *See* Sabine Helmers, *A Brief History of anon.penet.fi - The Legendary Anonymous Remailer*, CMC MAGAZINE (Sept. 1997), http://www.december.com/cmc/mag/1997/sep/helmers.html.

[12] Douglas Lavin, *Finnish Internet Fan Runs Service Allowing Anonymous Transmissions*, WALL ST. J. July 17, 1995 at A7 (reporting 8,000/day figure).

[13] *See* Helmers, *supra* note 12.

abbreviated to "nym" on the Internet-Alice can establish Andrea as a digital persona. If Alice is worried that someone else may try to masquerade as Andrea, her 'nym, Alice can sign her message with a digital signature[14] generated specially for "Andrea," which will uniquely and unforgeably distinguish an authentic signed message from any counterfeit.

Remailers vary, but all serious remailing programs share the common feature that they delete all the identifying information about incoming e-mails, and substitute a predefined header identifying the remailer as the sender. Even so, using a single remailer does not make a communication untraceable, as the user of the system cannot know whether the remailer actually deletes identifying information, or whether, perhaps, he keeps them. If Alice sends Bob a message using only Ted's anonymous remailer, she is effectively putting her fate in Ted's hands.

In the simplest example, Alice sends an unencrypted e-mail to a remailer operated by Ted, with instructions to forward the e-mail to Bob. Ted's remailer deletes Alice's identifying return address and sends the message on to Bob purporting to be from "nobody@remailer.com". Alice has no way of knowing whether Ted has logged the message, keeping a record of Alice and Bob's e-mail addresses, or indeed the entire text of the message. If Ted has done this, then Bob can find out who sent him the message by persuading Ted to tell him -- or, in some cases, if the message appears to violate a law, by enlisting the aid of Carol, a judge with subpoena power. Of course, if Ted lives in another country, outside Carol's jurisdiction, there may be little that Carol can do to assist Bob in his quest to persuade Ted to reveal Alice's identity. Many countries do have agreements for judicial assistance, but these can be costly, difficult, and in many cases require that the act complained of be illegal in both nations.

Although traceable anonymity offers the lowest security, it suffices for many purposes. Some messages do not require any more security than a new header. There have been occasions when I have posted messages to newsgroups and received a great deal of unwanted e-mail in reply because my e-mail signature identifies me as a law professor. One way to avoid getting requests for free legal advice, or long and vicious notes attempting to re-educate me about gun control, is to delete the signature and route comments through a remailer. That simple expedient suffices because the consequences of my being discovered as the author of my posts on legal topics are not terribly severe.

To make communications more or less 'untraceable' requires the help of *multiple*

---

[14] Public-key systems allow users to append a digital signature to an unencrypted message. A digital signature uniquely identifies the sender and connects the sender to the message. Because the signature uses the plaintext as an input to the encryption algorithm, if the message is altered in even the slightest way, the signature will not decrypt properly, showing that the message was altered in transit or that the signature was forged by copying it from a different message. A properly implemented digital signature copied from one message has only an infinitesimal chance of successfully authenticating any other message. *See* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 35 (2nd ed. 1996).

intermediaries. By employing easily automated cryptographic precautions widely available on the Internet, and routing a message through a series of remailers, a user can ensure three things conducive to high-security anonymity: (1) none of the remailer operators will be able to read the text of the message because it has been multiply encrypted in a fashion that requires the participation of each operator in turn before the message can be read.; (2) neither the recipient nor any remailer operators in the chain (other than the first in line) can identify the sender of the text without the cooperation of every prior remailer's operator; (3) therefore it is impossible for the recipient of the message to connect the sender to the text unless every single remailer in the chain both keeps a log of its message traffic and is willing to share this information with the recipient (or is compelled to do so by a court or other authority). Since some remailer operators refuse to keep logs as a matter of principle, there is a good chance that the necessary information does not exist. Even if logs exist, it would be prohibitively expensive to compel all the operators to divulge their logs because remailers are located in different countries. The expense of hiring foreign legal counsel, and possible language difficulties are only some of the problems. Many legal systems require that an act be an offense in both jurisdictions before allowing a prosecution, or in some cases even discovery, to proceed.

Current Internet technology enables the strongest anonymity via the routing of messages through multiple anonymous remailers. The technique is called "chained remailing" and is about as anonymous as directed communication can get. Nothing is foolproof, however: as explained below, if Alice has the bad luck to use only compromised remailers whose operators are willing to club together to reveal her identity, she is just out of luck. Assuming the good faith of even one member of the chain, however, Alice can ensure that no single remailer operator can connect her to the message Bob receives so long as she uses both encryption and chaining. Even these two techniques together may not be enough to foil a determined eavesdropper who is able to track messages going in and out of multiple remailers over a period of time. To foil this level of surveillance, which has nothing to do with the bad faith of the remailer operators, requires even more exotic techniques including having the remailers alter the size of messages and ensuring that they are not remailed in the order they are received.

Encryption ensures that the first remailer operator cannot read the message and effortlessly connect Alice to Bob and/or the contents. But encryption also has a far more important and subtle role to play. Suppose that Alice decides to route her anonymous message via Ted, Ursula, and Victor, each of whom operates a remailer and each of whom has published a public key in a public-key encryption system such as PGP. In a public-key system, each user creates a public key, which is published, and a private key, which is secret. Messages encrypted with one key can be decrypted only with the other key, and vice-versa.[15] A strong public-key system is one in which possession of both the algorithm and

[15] For a fuller description see Whitfield Diffie & Martin E. Hellman, *New Directions in Cryptography*, IT-22 IEEE TRANSACTIONS INFO. THEORY 644 (1976), and Ralph C. Merkle, *Secure Communication over Insecure Channels*, COMM. ACM, Apr. 1978, at 294; BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 29 (1994); Whitfield Diffie, *The First Ten Years of Public-Key Cryptography*, 76 PROC. IEEE 560 (1988) (discussing the history of public key cryptography).

one key gives no useful information about the other key. The system gets its name from the idea that the user will publish one key, but keep the other one secret. The world can use the public key to send messages that only the private key owner can read; the private key can be used to send messages that could only have been sent by the key owner.

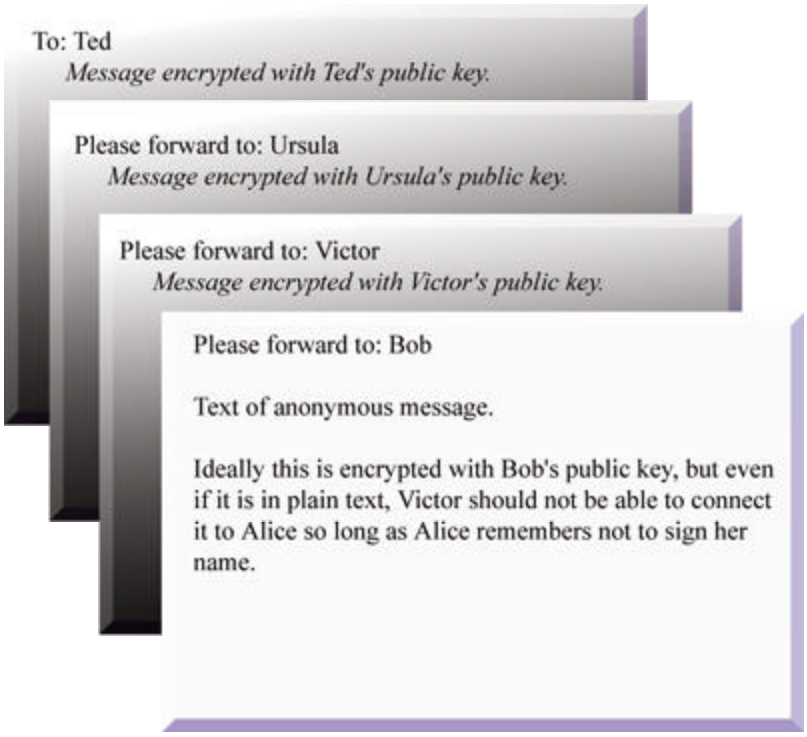
Thus, if Alice wants to send a secure e-mail message to Bob, and they both use compatible public-key cryptographic software, Alice and Bob can exchange public keys on an insecure line. If Alice has Bob's public key *and knows that it is really Bob's* then Alice can use it to ensure that only Bob, and no one pretending to be Bob, can decode the message. A strong public key system makes it possible to establish a secure line of communication with anyone who is capable of implementing the algorithm. (In practice, this is anyone with a compatible decryption program or other device.) Sender and receiver no longer need a secure way to agree on a shared key. If Alice wishes to communicate with Bob, a stranger with whom she has never communicated before, Alice and Bob can exchange the plaintext of their public keys. Then, Alice and Bob can each encrypt their outgoing messages with the other's public key and decrypt their received messages with their own secret, private key. The security of the system evaporates if either party's private key is compromised, that is, transmitted to anyone else.

Alice wants to ensure that no member of the chain knows the full path of the other remailers handling the message; anyone who knew the full path would be able to identify Alice from the message Bob will receive. On the other hand, each member of the chain will necessarily know the identity of the immediately previous remailer from which the message came, and of course the identity of the next remailer to which the message will be sent.

Alice thus wants Ted, the first member of the chain, to remove all the information linking her to the message; she is particularly anxious that Ted not be able to read her message since he is the one party in the chain who will know that Alice sent it. Alice also wants Ted to know only that the message should go to Ursula, and to remain ignorant of the message's route thereafter. Alice wants Ursula, the second member of the chain, to know only that the message came from Ted and should go to Victor; Victor should know only that it came from Ursula and should go to Bob, although by the time the message reaches Victor, Alice may not care as much whether Victor can read the message since her identity has been well camouflaged.

Alice achieves these objectives by multiply encrypting her message, in layers, using Ted, Ursula and Victor's public keys. As each remailer receives the message, it discards the headers identifying the e-mail's origins and then decrypts the message with its private key, revealing the next address, but no more. If one thinks of each layer of encryption as an envelope, with an unencrypted address on it, one can visualize the process as the successive opening of envelopes, as follows:

Alice sends a message to Ted as follows:



Chaining the message through Ted, Ursula, and Victor means that no remailer operator alone can connect Alice to either the text of the message or Bob. Of course, if Ted, Ursula and Victor are in a cabal, or all in Carol's jurisdiction and keep logs that could be the subject of a subpoena, Alice may find that Bob is able to learn her identity. All it takes to preserve Alice's anonymity, however, is a single remailer in the chain that is both honest and either erases her logs or is outside Carol's jurisdiction. In theory, there is no limit to the number of remailers in the chain, and Alice can, if she wishes, loop the message through some remailers more than once to throw off anyone attempting traffic analysis.

C. Nature of the Communication

Although US law does not currently differentiate the right to anonymous communication according to the nature of the communication at issue, that may only be a matter of time. The leading cases on a right to anonymous communication are set in the context of political or religious speech, which receive the highest protection in US law. The language of the cases is broad, and it is certainly possible that they would be followed in other, more commercial or more criminal, contexts. But it is not inevitable. It is important therefore, to keep in mind the many different purposes for which anonymity might be used: a person may be communicating or receiving a communication, or may be aiding and abetting anonymous communication by providing services such as network access or anonymous remailing. Furthermore, a "communication" can be any of a large number of things such as a diary entry, a love note, a political tract, or an order to purchase; under US law, not all of these necessarily enjoy the same constitutional protection. Or, the communication could be a thing of value itself such as software or electronic cash, which raises additional issues.

Two special circumstances, one involving digital cash, the other content rights management systems, seem especially likely to invite government intervention and regulation. These are discussed in section III.

II. Legal Doctrine

The US Constitution does not guarantee a right to be anonymous in so many words. The First Amendment's guarantees of free speech and freedom of assembly (and whatever right to privacy exists in the Constitution) have, however, been understood for many years to provide protections for at least some, and possibly a great deal of, anonymous speech and secret association. While most of the important decisions pre-date the Internet, more recent decisions establish the Supreme Court's willingness to apply the constitutional standards used for print to this new medium, at least as an initial matter.

Anonymous speech also benefits from its association with well-remembered incidents in which political actors holding unpopular views that many now accept benefited from the ability to hide their identity. The *Federalist Papers*, the nation's most influential political tracts, were published pseudonymously under the name "Publius". More recently, the Supreme Court held the guarantee of free speech in the Constitution protects a right of anonymous association and that a state therefore lacked the power to compel a local chapter of the NAACP to disclose the names of its members.[16] In so doing, the Court protected the NAACP members from danger at the hands of bigots who would have had access to their identities if the state had prevailed. Anonymity basks in the glow of association with good causes.

Despite all this, quite a number of statutes, primarily at the state level, require disclosure of identity in particular circumstances. To the extent that these rules regulate commercial interactions, they benefit from the significantly lower protections afforded to commercial speech and the tradition of allowing government to regulate the marketplace.

A. Constitutional Background

The Supreme Court has repeatedly noted the existence of a "profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open."[17] Political speech receives the highest constitutional protection because it, like religious speech, "occupies the core of the protection afforded by the First Amendment".[18] Other types of speech, notably "commercial

[16] NAACP v. Alabama ex rel. Patterson, 357 U.S. 449 (1958).

[17] New York Times Co. v. Sullivan, 376 U.S. 254, 270 (1964).

[18] McIntyre v. Ohio Elections Commission, 514 U.S. 334, 346 (1995).

speech," sometimes receive a reduced level of First Amendment protection. Core political speech need not center on a candidate for office, but can affect any matter of public interest - especially if it is an issue in an election.[19]

The leading case on anonymous political speech is *McIntyre v. Ohio Elections Commission*.[20] The facts in *McIntyre* were simple: In 1988, Margaret McIntyre distributed some leaflets outside the Blendon Middle School in Westerville, Ohio. Indoors, the superintendent of schools was discussing raising the school tax, which would require approval in a referendum; Ms. McIntyre opposed it. Some of the leaflets had her name; others were signed "Concerned Parents and Taxpayers." The unsigned leaflets violated a section of the Ohio Code that required any general publication designed to affect an election or promote the adoption or defeat of any issue or to influence voters in any election to contain the name and address of the person responsible for the leaflet. After a complaint by school officials lodged five months later, Ms. McIntyre was fined $100 by the Ohio Elections commission, and this fine provided the occasion for all that followed. Ms. McIntyre died while the case was wending its way through three levels of Ohio state courts, but her husband, as executor of her estate, appealed the adverse decision of the Ohio Supreme Court to the U.S. Supreme Court, which issued its decision in 1995, some seven years after the imposition of the fine.

In tone, the *McIntyre* opinion is a ringing affirmation of the right to anonymous political speech; arguably the defense of anonymity might stretch broader still. "Under our Constitution," Justice Stevens wrote for seven members of the Court, "anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent."[21] Thus, "an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment" and "the anonymity of an author is not ordinarily a sufficient reason to exclude her work product from the protections of the First Amendment."[22] To those, like Justice Scalia in dissent, who worried that anonymous speech might be abused, Justice Stevens replied that "political speech by its nature will sometimes have unpalatable consequences" but "our society accords greater weight to the value of free speech than to the dangers of its misuses."[23]

Despite these ringing words, how broad a right one has to be anonymous in the US remains

---

[19] *See* First Nat. Bank of Boston v. Bellotti, 435 U.S. 765, 776-777 (1978).

[20] 514 U.S. 334 (1995).

[21] 514 U.S. at 357.

[22] *McIntyre*, 514 U.S. at 341.

[23] *Id.* at 357.

unclear, since difficult cases are precisely those in which exceptions are made to fit facts that sit uncomfortably within the rules that apply "ordinarily."[24] To date, the Supreme Court has addressed the easy cases such as broad prohibitions of anonymous political or religious speech. As a result, it is now clear that ordinances prohibiting all anonymous leafletting, like the one in *McIntyre*, are an unconstitutional abridgment of free speech.[25] Thus, in *McIntyre* Justice Stevens found the state's "interest in preventing fraudulent and libelous statements and its interest in providing the electorate with relevant information" was insufficiently compelling to justify a ban on anonymous speech that was not narrowly tailored.[26] The Supreme Court has also tended to be highly solicitous of the need of dissidents and others to speak anonymously when they have a credible fear of retaliation for what they say. Thus, the Supreme Court has struck down several statutes requiring public disclosure of the names of members of dissident groups.[27] If the facts were less clear-cut, the Court might find a compelling state interest which would justify overcoming the right to privacy in one's political associations and beliefs. Nothing in *McIntyre* really changes this. Justice Stevens carefully distinguished earlier cases upholding statutes that sought to preserve the integrity of the voting process.[28] And indeed, in earlier cases the Supreme Court sometimes upheld more targeted restrictions on anonymous political speech and association, such as the Federal Regulation of Lobbying Act, which requires those engaged in lobbying to divulge their identities.[29] As a constitutional matter, therefore, the anonymity issue remains far from resolved even for the most highly protected category of speech.

If maximal protection of anonymity is not yet compelled, the doctrinal preconditions for it definitely exist, as can be seen from a recent decision of the Colorado Supreme Court. In *Tattered Cover, Inc. v. City of Thornton* that court interpreted both the state and federal constitutions to "protect an individual's fundamental right to purchase books anonymously, free from governmental

---

[24] For a contrary view that "*McIntyre* will prove to be dispositive" in providing First Amendment protections to anonymous political speech, see Richard K. Norton, Note, McIntyre v. Ohio Elections Commission*: Defining the Right to Engage in Anonymous Political Speech*, 74 N. CAL. L. REV. 553 (1996).

[25] *Id*.; Talley v. California, 362 U.S. 60 (1960).

[26] 514 U.S. at 348-49.

[27] *See, e.g.*, Brown v. Socialist Workers' 74 Campaign Comm., 459 U.S. 87, 91 (1982) (holding that the "Constitution protects against the compelled disclosure of political associations"); Shelton v. Tucker, 364 U.S. 479, 485-87 (1960) (holding invalid a statute that compelled teachers to disclose associational ties because it deprived them of their right of free association).

[28] McIntyre, 514 U.S. at 344.

[29] United States v. Harriss, 347 U.S. 612, 625 (1954) (discussing Federal Regulation of Lobbying Act, codified at 2 U.S.C. § 267).

interference."[30] It thus required a "heightened showing" by law enforcement officers before they would be allowed to execute a search warrant seeking customer purchase data from an innocent bookstore. As the Court explained,

> When a person buys a book at a bookstore, he engages in activity protected by the First Amendment because he is exercising his right to read and receive ideas and information. Any governmental action that interferes with the willingness of customers to purchase books, or booksellers to sell books, thus implicates First Amendment concerns. Anonymity is often essential to the successful and uninhibited exercise of First Amendment rights, precisely because of the chilling effects that can result from disclosure of identity."[31]

Given that the book in question was a "how to" book on operating a methamphetamine lab, and that drug cases are notorious for their tendency to bend constitutional rights to the breaking point,[32] this demonstrates the extent of judicial solicitude for the right to remain anonymous.

In practice, however, many state interests are routinely found to be sufficiently compelling to justify restrictions on First Amendment rights, and it is from the First Amendment that the right to anonymity derives. For example, the state interest in applying sufficiently targeted measures to forbidding discrimination in places of public accommodation has been held to be sufficiently compelling to overcome the First Amendment associational privacy rights of property owners and club members.[33] Similarly, in *Buckley v. Valeo*,[34] the Supreme Court upheld a statute forbidding donations of more than $1,000 to a candidate for federal office, and compelling disclosure to the Federal Election Commission of the names of those making virtually all cash donations.[35] Since the Court in the same decision

---

[30] Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044, 1047 (Col., 2002).

[31] Id. at 1052.

[32] *See, e.g.*, Steven Wisotsky, *Crackdown: The Emerging "Drug Exception" to the Bill of Rights*, 38 HASTINGS L.J. 889 (1987).

[33] *See* Board of Directors of Rotary Int'l v. Rotary Club of Duarte, 481 U.S. 537, 544 (1987); *see also* New York State Club Ass'n v. City of New York, 487 U.S. 1, 13 (1988) (stating that freedom of expression is a powerful tool used in the exercise of First Amendment rights); Roberts v. United States Jaycees, 468 U.S. 609, 617-19 (1984) (recognizing that an individual's First Amendment rights are not secure unless those rights may be exercised in the group context as well).

[34] 424 U.S. 1, 143 (1976).

[35] *Id*. at 23-29, 60-84.

essentially equated the expenditure of money in campaigns with the ability to amplify political speech,[36] the decision appears to say that given a sufficiently weighty objective, and a statute carefully written to minimize the chilling or otherwise harmful effects on speech, even political speech can be regulated.[37] (The Supreme Court will undoubtedly have occasion to revisit the issue of the First Amendment as applied to campaign finance, since lawsuits challenging the constitutionality of the recent campaign finance act have already been filed.[38]) And again, in *First Nat. Bank of Boston v. Bellotti*,[39] the Supreme Court struck down a state requirement forbidding corporations from making political contributions except for ballot measures directly affecting its business, but it contrasted the unconstitutional state law with others that it suggested would surely be acceptable: "Identification of the source of advertising may be required as a means of disclosure, so that the people will be able to evaluate the arguments to which they are being subjected."[40]

In sum, no form of speech, not even political speech, is completely immune from regulation. Despite its privileged position, political speech can be regulated given sufficient cause, especially if the regulation is content-neutral, as a regulation on anonymous speech would likely be.

A taste of the likely effect of this opening on the regulation of anonymous political speech can be seen in a decision of the Supreme Court of California, *Griset v. Fair Political Practices Comm'n*. The California court upheld a state statute forbidding anonymous mass political mailings by political candidates.[41] The facts involved a political dirty trick: Griset had sent a mass mailing attacking his opponent and pseudonymously purporting to be from a neighborhood association. The court concluded

---

[36] *Id*. at 19.

[37] *Cf*. Los Angeles v. Taxpayers for Vincent, 466 U.S. 789 (1984) (upholding ban on posting any signs, including political ones, on utility poles). Justice Stevens held, however, that the utility poles were not public fora, *id.* suggesting that the court might not extended this idea to public fora and that *Vincent* may be come to be seen as simply a decision upholding a particular time, place, and manner restriction.

[38] See Helen Dewar, *Lawsuits Challenge New Campaign Law*, WASHINGTON POST, May 8, 2002, at A6 .

[39] 435 U.S. 765 (1978).

[40] *Id*. at 792 n.32. The Supreme Court again noted the communicative importance of the identity of a speaker, albeit in a different context, in *City of Ladue v. Gilleo*. 114 S. Ct. 2038, 2046 (1994) (noting that a poster in front of a house associates speech with the identity of the speaker).

[41] Griset v. Fair Political Practices Comm'n, 884 P.2d 116, 126 (Cal. 1994) (upholding Cal. Government Code sec. 84305), *cert. denied* 514 U.S. 1083 (1995).

that prospective voters could have been deceived into thinking that Griset had "grass roots" support.[42] Deception was the evil that the statute was designed to cure, the ban was necessary to further the state's interest in "well-informed electorate" at election time, and the statute was "narrowly drawn to meet that goal."[43] The Court therefore distinguished *Griset* from federal Supreme Court decisions, such as *Talley v. California*,[44] *Bates v. City of Little Rock*,[45] and *NAACP v. Alabama*,[46] which had held that the First Amendment freedom of association limited the state's ability to pierce an organization's anonymity. One could perhaps read *Griset* as concerning the mis-use of pseudonymity rather than anonymity. The argument would be that there is a greater harm to the political process from a *false* statement of support by a non-existent "citizen's group" than from an anonymous source, since the latter's secrecy puts readers on notice that the author could be anyone. While this approach is attractive, and probably constitutional, neither the opinion nor the statute makes a distinction between a false statement and one that fails to identify the author.

The Supreme Court denied certiorari in the *Griset* case, a refusal to hear which has no precedential value. Nevertheless, when one considers the contexts in which the Supreme Court has already sustained limitations on the privacy of individuals engaged in the political process, particularly the *Buckley* decision,[47] it seems quite possible that despite the language of *McIntyre* the Court would uphold a narrowly tailored statute prohibiting anonymity even in the context of political speech if the statute had clear and palatable objectives. Once down this slippery slope of regulation it is notoriously difficult to find a logical place to stop. A particularly difficult case might be a statute that sought to ban all anonymity in political campaigns on the theory that if the message is not signed with the actual name of the author, it is impossible to know whether it originated in a political campaign and thus violates campaign finance expenditure limits. This would juxtapose the *Talley-McIntyre* line of cases with the *Buckley-Griset* line of cases. Without forcing everyone to sign their messages there may, it could be argued, be no way to monitor what campaigns spend, and thus no way to ensure they do not seek to get an edge by spending beyond the legal limits.

---

[42] *Id*. at 125.

[43] *Id*. at 123.

[44] 362 U.S. 60 (1960).

[45] 361 U.S. 516 (1960).

[46] 357 U.S. 449 (1958).

[47] *See supra* text accompanying note 34; *see also* Citizens Against Rent Control v. Berkeley, 454 U.S. 290, 298 (1991); *id* at 299-303 (Blackmun, J. concurring); *id.* at 308-09 (White, J., dissenting). All Justices agreed that identification requirements in political campaigns could be appropriate.

The Supreme Court's hostility to the regulation of anonymity -- at least when it impinges on 'core' First Amendment speech -- is manifest in *Watchtower Bible and Tract Soc. of New York, Inc. v. Village of Stratton*,[48] decided in June, 2002. The case concerned a village ordinance requiring all door-to-door solicitors and canvassers to register with the village, and disclose their identities and the reason for which they were going door-to-door. Upon provision of this information, the Mayor was required to issue a permit, without fee, unless he found that the applicant had "(1) failed to complete the Registration Form, (2) provided fraudulent information on the form, (3) made false or fraudulent statements or misrepresentations while canvassing, (4) violated any other local, state, or federal laws, (5) trespassed while canvassing, or (6) ceased to possess the qualifications required to obtain a Solicitation Permit."[49] The rule applied to commercial and non-commercial speakers alike. The Watchtower Bible and Tract Society (known also as Jehovah's Witnesses), a religious group based in a neighboring village that wished to go door-to-door in Stratton in order to proselytize, challenged the ordinance as unconstitutional. The Sixth Circuit Court of Appeal upheld the statute as a reasonable and proportionate exercise of government power,[50] a somewhat surprising result in light of the *McIntyre* case which this case so closely resembles. The Supreme Court reversed, a result remarkable only because it took place after the terrorist attacks of 9/11, and thus at a time one might expect to find the Supreme Court becoming more solicitous of the police power in the face of privacy-based challenges.

B. Application to the Internet

The Internet carries a high volume of every type of speech. Some of it is undoubtedly pornography, but much of it is non-eroticized, and indeed political, speech. As a practical matter, therefore, it would be exceedingly difficult, and probably impossible, to craft a ban on anonymous speech on the Internet that distinguished between political and non-political speech and yet was enforceable. Remailer operators, for example, will ordinarily be unable to decrypt the encrypted messages that they are forwarding. Neither the operators nor the regulators will be unable to tell whether the message is core First Amendment speech or unprotected obscenities. A ban on anonymous speech cannot therefore meaningfully distinguish by subject matter, nor can it necessarily even distinguish between visual depictions and mere words. Thus, to a surprisingly great extent, the US government's ability to subject non-political anonymous speech turns on the vexed and disputed question of the legality of limitations on encryption.

---

[48] Watchtower Bible and Tract Soc. of New York, Inc. v. Village of Stratton, Ohio, 122 S. Ct. 2080 (2002).

[49] Watchtower Bible and Tract Soc. of New York, Inc. v. Village of Stratton, Ohio, 240 F.3d 553, 558 (6th Cir.2001), *rev'd* 122 S. Ct. 2080 (2002).

[50] Id.

In the absence of a ban on encrypted messages, any meaningful attempt to ban anonymous Internet speech must either attempt to ban it all, or craft some more limited rule that has the same result. Under current First Amendment doctrine, a ban on all anonymous speech is unlikely to survive even cursory review: it is too far from being narrowly tailored to prevent harmful messages from being forwarded or to help legitimate law enforcement attempts to trace threatening messages.

On the other hand, there might be an ostensibly neutral means to achieve the same end in a different way. If, for example, operators of anonymous remailers were made strictly liable for carrying messages that are used to conduct terrorist operations, perhaps on the theory that some categories of speech have harmful secondary effects, the result would be to force all remailers in the jurisdiction to close since the operators would have no other way to protect themselves from the liability. This hypothetical strict liability statute could be vulnerable to the accusation that it discriminated against points of view that are not openly stated,[51] and its constitutionality is far from certain, but it is more likely to be found constitutional than a straight ban on anonymous messages. I return to this issue below.

C. Statutory Examples

The *Talley* and *McIntyre* cases suggest the outer limit of tolerance for anonymous speech that is *not* "political speech" and also not one of the areas of general public concern such as religion, art, or literature, areas that commentators usually include within the rubric of so-called "core" First Amendment speech. Indeed, one might reasonably expect that anonymity involving less favored categories of speech, such as "commercial speech" might be more subject to regulation. As we have seen, the Supreme Court has carefully left open the question whether a statute regulating (or prohibiting) anonymous political speech would survive review if the statute were narrowly tailored, e.g. to "provid[e] a way to identify those responsible for fraud, false advertising and libel."[52]

Statutes designed to attack the enforcement problems caused by laundering of anonymous digital cash or electronic violations of intellectual property rights therefore might be in a particularly good position to survive judicial review. Although in *McIntyre* the Court found that the state's "interest in preventing fraudulent and libelous statements and its interest in providing the electorate with relevant information" was insufficiently compelling to justify a ban on anonymous political speech, the weighing might produce a different result if there were some way to tailor it to types of speech that ordinarily receive less protection, such as commercial speech.

---

[51] "The wildest possible dissemination of information from diverse and antagonistic sources is essential to the welfare of the public." Associated Press v. United States, 326 U.S. 1, 20 (1945) (upholding application of Sherman Act to newsgathering agency), *quoted with approval* in Metro Broadcasting v. FCC, 497 U.S. 547, 567 (1990).

[52] *See* Talley, 362 U. S. at 64, also discussed in McIntyre, 514 U.S. at 343 n.7.

Despite some scholarly suggestions that the First Amendment should apply with undiluted force, "commercial speech" tends to be easier to regulate.[53] Restrictions are more likely to be upheld if they appear plausibly tailored to strike at illegal non-political non-speech "conduct" particularly when the speech "incidentally" burdened is non-political. And restrictions are most likely to be upheld when the speech burdened falls into the ill-defined, and predominately salacious, category of speech that is for all practical purposes disfavored. Thus, for example, the D.C. Circuit rejected a First Amendment challenge to the Child Protection and Obscenity Enforcement Act. It reasoned that although neither actors nor producers of "visual depictions" of "actually sexually explicit conduct" made after November 1, 1990, could remain anonymous, the statute was consistent with the First Amendment because it imposed a "content-neutral" burden on speech designed to achieve the significant legislative goal of controlling the harmful "secondary effects" on children of their participation in the production of child pornography.[54] In other words, as the statute ostensibly aimed to control a social ill rather than speech itself, the purportedly incidental burden on anonymous non-political speech was tolerable. In theory, therefore, if the government's interest in combating the effects of child pornography is sufficient to justify the Act's effects on adult performers and those who produce materials containing their visual images, it might be equally constitutional to require that at least non-political messages on the Internet include information sufficient to allow a libel victim to trace the source of the defamation.

Indeed, there are already a number of specific statutory or regulatory restrictions on anonymous or pseudonymous speech and commerce in the U.S. today. The contexts are diverse, and they make summary difficult. Generally, restrictions on anonymous non-commercial speech are more likely to run into constitutional difficulties in the courts. The First Amendment, states that "Congress shall make no law . . . abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble."[55] As anonymity may help realize the freedom of speech and the freedom of association, the First Amendment imposes substantial constraints on the regulation of anonymity. Nevertheless, the sheer number of long-standing limits on anonymity makes it clear that these restrictions are not in and of themselves considered repugnant to our law.

Lower courts have sustained private identification requirements in various regulatory settings

---

[53] *See* Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 771 n.24 (1976). The Court has also stated that the overbreadth doctrine is inapplicable in various commercial speech contexts. *See* Village of Schaumburg v. Citizens for a Better Env't, 444 U.S. 620, 638-39 (1980).

[54] American Library Association v. Reno, 33 F.3d 78, 81, 84-85 (D.C. Cir. 1994), *reh'g en banc den.*, 47 F.3d 1215 (D.C. Cir. 1995), *cert. den.* 515 U.S. 1158 (1995).

[55] U.S. CONST. Amend. I.

involving the workplace.[56] And, service providers in certain regulated industries are required to identify themselves to potential customers, e.g. to allow customers to establish their *bona fides* or the validity of their licenses. Contractors in Florida, for example, cannot operate anonymously because clients are entitled to inspect their licenses and to contact regulatory officials to check that they are still current. Similarly, taxi drivers in many jurisdictions must display their hack licenses where patrons can see them, although there is no requirement that the passenger identify herself to the driver. In contrast, a smaller number of industries, primarily financial, are required to "know your customer" before conducting certain types of transactions, thus making it illegal for businesses to facilitate client money laundering.

Not all restrictions on anonymity are limited to purely commercial contexts. Pennsylvania[57] and Georgia have passed statutes restricting anonymous communications. Georgia's statue made it an offense

> to transmit any data through a computer network . . . for the purpose of setting up, maintaining, operating, or exchanging data with an electronic mailbox, home page, or any other electronic information storage bank or point of access to electronic information if such data uses any individual name . . . to falsely identify the person[58]

The Georgia statute did not last long. A federal district court enjoined the anti-anonymity portion of the Georgia statute, on the grounds that it appeared to impose an unconstitutional content restriction on Internet speech. The court reasoned that the name of the author was content that the author had a First Amendment right to choose to include or omit.[59] The state chose not to appeal.

---

[56] See, e.g. Big Bear Super Market No. 3 v. I.N.S., 913 F.2d 754 (9th Cir. 1990) (upholding worker identification provisions of Immigration Control Act, 8 U.S.C.A. § 1324a against void for vagueness challenge).

In *Viereck v. United States*, 318 U.S. 236 (1943), the Supreme Court upheld a pre-WW I statute requiring foreign agents to register with the Secretary of States, but several subsequent decisions, culminating in *NAACP v. Alabama* ex rel *Patterson*, 357 U.S. 449 (1958), suggested that the Supreme Court had turned away from the analysis in *Viereck*, *see Anonymous Note, supra* note 8, at 1093-1102. In *Lewis Publishing Co. v. Morgan*, 229 U.S. 288 (1913), the Court upheld a requirement that mailers wishing 2nd class mailing status publish a list of editors and proprietors twice annually, but it is somewhat unlikely that this decision would be upheld today.

[57] Pennsylvania's statute makes it a crime to possess, program, or use a device which can be used to "conceal or to assist another to conceal ... the origin or destination of any telecommunication." 1995 PA S.B. 655 (June 13, 1995) (amending 18 PA. Consl. Stat. § 910(a)(1)), *codified at* 18 Consolidated Statutes Ann. § 910 (Purdon's Supp 1997).

[58] Act No. 1029, Ga. Laws 1996, p. 1505, codified at O.C.G.A. § 16-9-93.1.

[59] American Civil Liberties Union of Georgia v. Miller, 977 F.Supp. 1228 (N.D.Ga. 1997).

Several federal laws reach non-commercial contexts. In 1983, the D.C. Circuit upheld the constitutionality of a Communications Act requirement that paid political radio and television broadcasts include the name of the sponsor, and the Supreme Court denied certiorari.[60] In order to protect consumers from junk faxes, in 1991 Congress required the FCC to make rules requiring that fax machines mark the name and telephone number of a business or individual sending the fax on the first page of every transmission.[61] The FCC's regulation makes it unlawful

> for any person within the United States to use a computer or other electronic device to send any message via a telephone facsimile unless such message clearly contains, in a margin at the top or bottom of each transmitted page or on the first page of the transmission, the date and time it is sent and an identification of the business, other entity, or individual sending the message and the telephone number of the sending machine or of such business, other entity, or individual.[62]

The Child Protection and Obscenity Enforcement Act requires that producers of certain kinds of sexually explicit speech ascertain and record information about performers' age and identities and that producers of such speech affix a notice to each copy disclosing their own identity and address.[63] In addition to ascertaining the performer's real name and age, the producer must also ascertain all aliases "ever used" by the performer including "maiden name, alias, nickname, stage, or professional name", and maintain records of all affected performers cross-indexed by their aliases.[64]

Some states forbid demonstrations and travel by masked persons. Antimask laws have been justified as a means of helping to prevent violence, but this justification has met with a mixed reception

---

[60] Loveday v. FCC, 707 F.2d 1443 (upholding 47 U.S.C. § 227(d)(2) against constitutional challenge), *cert. denied* 464 U.S. 1008 (1983). The *Loveday* rule cannot be explained as relying on a special feature of radio and television such as shortage of spectrum, *cf*. Turner Broadcasting, 512 U.S. 622 (1994), because the rule has been extended to cable television. *See* 47 C.F.R. § 68.318(c)(3).

The continuing validity of the *Loveday* rule may be questioned in the wake of the *McIntyre* decision.

[61] The Telephone Consumer Protection Act of 1991 (TCPA), Pub. L. No. 102-243, 105 Stat. 2394, *codified at* 47 USC § 317(a).

[62] 47 C.F.R. § 68.318(d).

[63] Child Protection and Obscenity Enforcement Act of 1988, Pub. L. No. 100-690, 102 Stat. 4181, 4485-4503 (1988), *amended by* the Child Protection Restoration and Penalties Enhancement Act of 1990 Pub. L. No. 101-647, 104 Stat. 4789, 4816-17 (1990), *codified at* 18 U.S.C. § 2257(b)(1).

[64] 18 U.S.C. § 2257(b)(2)-(3).

by courts and commentators, and the constitutionality of antimask laws remains largely unsettled.[65]

D. Civil Subpoenas

The use of the Internet as a means of making anonymous and pseudonymous derogatory comments has lead to a rash of lawsuits in which firms, and more rarely individuals, seek to learn the identity of those attacking them. Since 1988, U.S. firms have filed at least 150 suits against anonymous "cybersmear" defendants.[66] Suggestions that not all of these cases were filed with pure motives, and that retaliation of some sort might follow disclosure of the poster's identity, has lead some to call these "cybersslapp" lawsuits, after the "strategic litigation against public participation (SLAPP) suit.[67]

Firms sue for any number of reasons, not least the ability of online anonymous comments in investment chatrooms to move stock prices. Firms may wish to know if they are dealing with short sellers, disgruntled employees (whom they might wish to fire, or whose comments might cause liability for the firm), possible predators, or members of the public. If a person or firm feels it is entitled to judicial redress from economic or reputational harms caused an online comment, it will need to learn the identity of the poster because, unlike in the case of, say, libel in a newspaper, redress cannot be had from any publishing intermediary. Section 230 of the Communications Decency Act provides that no ISP "shall be treated as the publisher or speaker of any information provided by another information content provider."[68] This is an all but absolute shield to an Internet Service Provider (ISP) or bulletin board that acts as an innocent conduit for speech -- and even extends this protection to material that the ISP purchases from a writer. Although not considered common carriers like the telephone company, the intermediaries have an essentially equivalent protection from liability for their customers' speech.[69]

---

[65] *See generally* Oskar E. Rey, Note, *Antimask Laws: Exploring the Outer Bounds of Protected Speech Under the First Amendment*—State v. Miller, *260 Ga. 669, 398 S.E.2d 547 (1990)*, 66 WASH. L. REV. 1139, 1145-46 (1991) (arguing antimask laws are unconstitutional).

[66] David C. Scileppi, Note, *Anonymous Corporate Defamation Plaintiffs: Trampling the First Amendment or Protecting the Rights of Litigants?*, 54 FLA. L. REV. 333, 333 (2002).

[67] *See* George W. Pring & Penelope Canan, *SLAPPs: Getting Sued for Speaking Out* 8 (1996).

[68] CDA § 230(c)(1), codified at 47 U.S.C. § 230(c)(1). *Cf*. Zeran v. America Online, Inc., 129 F.3d 327, 334 (4th Cir.1997) (stating that Congress enacted § 230 "to promote unfettered speech" and thus it "must supersede conflicting common law causes of action"); Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998) (dismissing libel action); Doe v. America Online, Inc., 783 So.2d 1010 (Fla. 2001) (upholding dismissal of charges stemming from user's offer of sale of child pornography in a chat room due to § 230 pre-emption of state law).

[69] There are some exceptions, especially for copyright and trademark violations.

Ordinarily, a party aggrieved by an unknown, but potentially knowable, person can seek redress by filing a "John Doe" lawsuit against the unknown person. In so doing the plaintiff not only avoids any statute of limitations but secures access to judicial process to help obtain the information necessary to identify the person who should be named in the lawsuit.[70] In most cases implicating anonymous internet speech, that means a subpoena directed against the ISP or bulletin board operator, or a related discovery request aimed at someone presumed to know the speaker's identity. Sometimes the recipient of the subpoena just gives in, but sometimes it files for a protective order or notifies its customer, who then can move to quash the subpoena. The outcome of these quashing actions have varied. The earlier cases tended to uphold the subpoenas, leading to cries of outrage about the chilling effect on First Amendment activities. More recent cases have tended to be more solicitous of the speakers' rights,[71] but it remains to be seen how the higher courts will balance "the right of the plaintiff to protect its proprietary interests and reputation through the assertion of recognizable claims based on the actionable conduct of the anonymous, fictitiously-named defendants"[72] against the First Amendment rights of speakers.

Thus, for example, in *Dendrite International, Inc. v. John Doe, No. 3* a New Jersey state court of appeals ruled that online posters can keep their identities secret in most cases, and crafted rules to protect their interests.[73] Dendrite, a maker of sales-force technology, sued to reveal the identities of several message-board posters, claiming they posted false statements about the company. In affirming the denial of the discovery request, the *Dendrite* court set guidelines for New Jersey trial courts to follow when companies sued to determine the names of anonymous posters, although it emphasized that each case should be decided individually:

> when such an application is made, the trial court should first require the plaintiff to undertake efforts to notify the anonymous posters that they are the subject of a subpoena or application for an order of disclosure, and withhold action to afford the fictitiously-named defendants a reasonable opportunity to file and serve opposition to the application. These notification efforts should include posting a message of

---

[70] *See generally* Roger M. Rosen & Charles B. Rosenberg, *Suing Anonymous Defendants for Internet Defamation*, 19 NO.2 COMP. & INTERNET L. 9 (2002).

[71] See, e.g., Anderson v. Hale, 49 Fed.R.Serv.3d 364 (N.D. Ill.) (holding that disclosing information about publicly known members of a white supremacist organization would not chill their First Amendment rights to freedom of association because it is not directed at the heart of the organization's protected activities, but disclosure that aims to reveal the identity of the organization's anonymous members directly chills associational rights.)

[72] Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756, 760 (N.J. Super. 2001).

[73] *Id*.

> notification of the identity discovery request to the anonymous user on the ISP's pertinent message board.
> The court shall also require the plaintiff to identify and set forth the exact statements purportedly made by each anonymous poster that plaintiff alleges constitutes actionable speech.
> The complaint and all information provided to the court should be carefully reviewed to determine whether plaintiff has set forth a prima facie cause of action against the fictitiously-named anonymous defendants. ... the plaintiff must produce sufficient evidence supporting each element of its cause of action, on a prima facie basis, prior to a court ordering the disclosure of the identity of the unnamed defendant.
> Finally, assuming the court concludes that the plaintiff has presented a prima facie cause of action, the court must balance the defendant's First Amendment right of anonymous free speech against the strength of the prima facie case presented and the necessity for the disclosure of the anonymous defendant's identity to allow the plaintiff to properly proceed.[74]

The court, however, immediately demonstrated that this is far from an absolute protection for anonymous speakers. The same day that the New Jersey appellate court decided *Dendrite*, it also decided *Immunomedics, Inc. v. Jean Doe*.[75] Here, applying the *Dendrite* test, the court determined that a biopharmaceutical corporation was entitled to disclosure from Yahoo! regarding the true identity of Jean Doe, an anonymous poster to a Yahoo! message board, because the corporation had presented sufficient evidence that the user was an employee of the corporation who had breached a confidentiality agreement by posting to the message board.[76] The court stated that the employee had "contracted away her right to free speech," and that by "choos[ing] to . . . violate an agreement through speech on the Internet [she] cannot hope to shield [her] identity and avoid punishment through invocation of the First Amendment."[77]

Similarly, in *John Doe v. 2TheMart.com Inc.*,[78] 2TheMart.com sought a subpoena to force InfoSpace, an ISP, to reveal the identities of 23 posters who used pseudonyms on InfoSpace's investment-related message boards. 2TheMart.com was defending itself against a class-action lawsuit alleging the company engaged in securities fraud, but the anonymous posters were not parties to the

---

[74] *Id.* at 760-761.

[75] 775 A.2d 773 (N.J. Super. 2001).

[76] *Id*.

[77] *Id.* at 775, 777-78.

[78] 140 F.Supp.2d 1088 (W.D. Wash. 2001).

case. In the course of refusing to order InfoSpace to disclose the names, the court fashioned a four-pronged test that also sought to balance the interests while giving due but clearly not overwhelming weight to the writers' interest in remaining anonymous,

> Whether (1) the subpoena seeking disclosure was brought in good faith; (2) the information sought relates to a core claim or defense; (3) the identifying information is directly and materially relevant to a core claim or defense; and (4) the information sufficient to establish or disprove the claim or defense is unavailable from any other source.[79]

Once again, the balance is considerable solicitude towards the citizen's interest in remaining anonymous, but not to the point that it inevitably trumps competing values.

III. 9/11 and Beyond

The terrorist attack on the United States now known as "9/11" together with the subsequent fear of further attacks, inevitably led to calls for strengthened law enforcement and surveillance. Surprisingly, however, the first wave of legislation resulting from the US government's concerted anti-terrorism efforts in the wake of the attack on the World Trade Center (the Patriot Act), had only a limited effect on the right to anonymity. The statute does not attempt to limit the freedom to possess and use the cryptographic tools that make Internet anonymity possible. A large number of additional legislative changes that might make communicative anonymity difficult have been proposed, but it is unclear which, if any, will actually become law.

The initial reactions to 9/11 that impact the exercise of the right to anonymity seem primarily to involve not legislation but changes in police and intelligence behavior. In particular, the U.S. government is reputed to have stepped up its communicative surveillance efforts, including much-touted technologies such as the Carnivore system. Additionally, calls are heard from various quarters for a national ID card system, but there is also substantial opposition and the outcome is far from certain.

Thus, for now, it appears that the greatest clear threats to anonymity remain technological developments and commercial pressures that began before 9/11 and continue unabated. The privacy commons continues to erode in the face of surveillance technologies such as cameras in public places and electronic point-of-sale record keeping. And, a particularly notable trend is pressure on the right to the anonymous reception of information - and especially digitized and Internet-based information - being exerted by intellectual property rights holders who seek to know exactly who is accessing digital content in order to be able to charge for it.

---

[79] *See id.* at 1095.

A. The Patriot Act and Law Enforcement

Although the Patriot Act did substantially expand the access of law enforcement to electronic data, and eliminate some state privacy protections, the changes were mostly of degree rather than in kind.[80] The Act overrides existing state and federal privacy laws, allowing law enforcement to compel disclosure of any kind of records, including sensitive medical, educational and library borrowing records, upon the unsupported claim that they are connected with an intelligence investigation. These records were previously shielded from disclosure without a higher showing -- but they were not anonymous. Also, the statute broadened the definition of what constitutes "dialing, routing, addressing, and signaling information," so that law enforcement can access it with a mere "pen register" order as opposed to the full-blown warrant required for the contents of a communication. This change, while greatly increasing the ease with which large amounts of personal information can be gathered, is a difference in degree not in kind. It lessens the process required to acquire information that was always available to the government upon a proper showing of need.

Many other provisions of the act broaden the reasons why law enforcement can request various information, or alter the standards applied to those requests, but the Act does not prohibit anonymous communications, nor does it alter the regulation of cryptographic tools, which remain subject to some export controls, but have no restrictions at all on importation or domestic use.

In contrast to the absence of legislative changes, there have been a plethora of journalistic reports of vastly more aggressive uses of existing investigatory powers.[81] Many of these reports played up the role of the Carnivore e-mail tracking device. These reports may, however, have been both over- and under-alarmist. FBI documents recently acquired by the Electronic Privacy Information Center under the Freedom of Information Act suggest that the FBI may have lied about Carnivore's ability to discriminate between messages the FBI is entitled to read and other traffic--and that, at least before 9/11, awareness of this violation of federal wiretap law may have made the FBI reluctant to use Carnivore even in terrorism investigation.[82] Whether this reluctance continues is a matter of speculation.

---

[80] *See* Kerr, *supra* note 2. A very useful tabular summary of the changes appears at American Library Association, Matrix of USA Patriot Act Provisions, http://www.ala.org/washoff/matrix.pdf.

[81] E.g. Dan Verton, Computerworld, *FBI Investigating Internet's Role in Attacks* (Sept. 14, 2001).

[82] *See* EPIC, *FBI's Carnivore System Disrupted Anti-Terror Investigation*, http://www.epic.org/privacy/carnivore/5_02_release.html (May 28, 2002). For a useful technical description of Carnivore (albeit one that takes FBI statements as true), and a discussion of some of the issues, see E. Judson Jennings, *Carnivore: US Government Surveillance Of Internet Transmissions*, 6 VA. J.L. & TECH. 10 (2001).

B. Shrinkage of the Privacy Commons

Moving about in public is not truly anonymous: Someone you know may recognize you, and anyone can write down the license plate number of your car. Nevertheless, at least in large cities, one enjoys the illusion, and to a large extent the reality, of being able to move about with anonymity. That freedom is soon to be a thing of the past, as the "privacy commons" of public spaces becomes subject to the enclosure of privacy-destroying technology.[83]

Fear of crime, and now of terrorism, and the rapidly declining cost of hardware, bandwidth, and storage, are combining to foster the rapid spread of technology for routinely monitoring public spaces and identifying individuals. Monitoring technologies include cameras, facial recognition software, and various types of vehicle identification systems. Related technologies, some of which have the effect of allowing real-time monitoring and tracking of individuals, include cell-phone location technology and various types of biometric identifiers.

Closed Circuit Television ("CCTV") cameras and video recorders are increasingly ubiquitous in both public and private spaces. Attempts -- not always successful[84] -- are under way to replace human observers with machines using facial recognition technology. Combined with a database full of driver's license photos, images from a series of ubiquitous cameras could be indexed by name and stored for an indefinite period of time. Indeed, the United States Secret Service and other agencies have expressed interest in a national database of drivers licence photos, and the government has spent at least $1.5 million helping a private corporation amass the data.[85]

C. Privacy Enhancing Technologies Remain Legal -- For Now

While privacy-destroying technology spreads, privacy-enhancing technologies (PETs) remain legal, cumbersome to use, and with the exception of marginal items such as Internet cookie blockers, not widely used. Despite a little saber-rattling from some legislators, the federal government has made no move to block access to cryptography or to otherwise burden anonymous communication. And, as

---

[83] *See generally* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461 (2000), http://www.law.miami.edu/~froomkin/articles/privacy-deathof.pdf.

[84] *See*, *e.g.*, P. Jonathon Phillips, Alvin Martin, C.L. Watson & Mark Przybocki, NIST, *An Introduction to Evaluating Biometric Systems*, http://www.dodcounterdrug.com/facialrecognition/DLs/Feret7.pdf (reporting high error rates even under optimum conditions).

[85] *See* Image Data, LLC, *Application of Identity Verification and Privacy Enhancement to Treasury Transactions: A Multiple Use Identity Crime Prevention Pilot Project* 3 (1997) http://www.epic.org/privacy/imagedata/image_ data.html.

noted above, clumsy state-level attempts to limit anonymity have met with a hostile reception in the courts.

The availability of PETs is critical to effective online anonymity, but technology alone is not sufficient. Currently, the most effective, least traceable, Internet anonymity requires cryptographic tools and several willing remailer operators who volunteer to provide the identity masking services that make anonymous communication possible. The cryptographic tools are in ready supply. As outlined in Part I, if the user deploys the cryptographic tools properly it does not matter whether she trusts the remailer operators as long as there are enough of them. In the worst case some messages will not be delivered, but so long as any single operator in a chain of remailers carries out the promise to re-mail the message anonymously and keep no log of the action, the user is safe from anything but surveillance approaching complete recording of all traffic passing through the network. This level of dataveillance may exist already in some countries; worse, it may be coming to the EU: In May, 2002, the EU Parliament endorsed plans to allow member states to require ISPs to keep complete records of the traffic they carry.[86] This, when combined with national legislation such as the UK's Anti-Terrorism, Crime and Security Act (ATCS), could produce the sort of "dataveillance" that Roger Clarke presciently described almost fifteen years ago.[87]

Although it's possible that the European example will be used to encourage the U.S. Congress to embark on a similar regime of dataveillance, there are substantial legal obstacles. In any case, even under a national regime of total logging, it is still possible to use remailers to send anonymous messages so long as at least some participants in the remailing chain are based in foreign jurisdictions that either do not require logging or do not share information with the sender's government. The more remailers in the chain, however, the longer it may take the message to get to its destination, and the greater the chance that an operator in the chain will fail to pass the message on down the line.

Since even in the absence of mandatory logging it takes several remailers to guard against the danger of a remailer who keeps voluntary logs, the supply of remailer operators in non-logging jurisdictions emerges as the major factor determining the availability of Internet anonymity. Anonymous remailer programs are currently operated by a relatively small number of volunteers located in a few countries; they receive no compensation for this service, and in the absence of anonymous electronic

---

[86] *See supra* note 1.

[87] Roger Clarke, *Information Technology and Dataveillance*, 31 COMM. ACM 498 (May 1988) (defining dataveillance as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons"), http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html. *See gener*ally Roger Clarke, *Roger Clarke's Dataveillance and Information Privacy Pages*, http://www.anu.edu.au/people/Roger.Clarke/DV/.

cash or the equivalent it is difficult to see how an electronic payment system could be constructed that would not risk undermining the very anonymity the remailers are designed to protect.

Remailers are not, however, invulnerable. No remailer operator can control the content of the messages that flow through a remailer. Furthermore, the last remailer operator in a chain has no reliable way of concealing the identity of the sending machine from the message's ultimate recipient. Suppose, Alice wants to send an anonymous death threat to Bob via remailers operated by Ted, Ursula, and Victor. If Victor does nothing to mask his email address, Bob will know he was the last to remail the message. Victor can make any attempt to identify him more difficult by forging his email address in the message to Bob, but Victor cannot be certain that this will work. Indeed, Victor can be almost certain that if a sufficient number of messages pass through his remailer, in time Victor's identity will be detected by a motivated Internet sleuth.[88]

The last remailer in a chain thus risks being identified by an unhappy recipient. An identifiable person is a potential target for regulation. If the remailer operators were made strictly liable for the content of messages that passed through their hands, even though they were unable to learn the content of those encrypted messages, most reasonable people probably would find running a remailer to be an unacceptable risk if they resided in a jurisdiction capable of enforcing such a rule.

At some point, if the number of remailers becomes small, it becomes technically feasible for the authorities to conduct traffic analysis[89] on all the remailers and make deductions about who sent what to

---

[88] To understand why this is so requires some background in how an ordinary e-mail message is transmitted from Alice's machine to Bob's via the Internet. Ordinarily the two computers do not communicate directly. Instead Alice's machine sends the message to a machine that it hopes is in Bob's general direction, and the message passes from machine to machine until it finds one that is in regular communication with Bob's. Each machine that handles the message appends "path" information to the email that identifies it as having taken part in the communication. The final recipient receives the entire path data along with the text of the message, but most commercial email packages are designed to avoid displaying this path information to the reader unless she asks for it.

Victor can instruct his computer to lie about its identity, and indeed can forge information suggesting that the message originated elsewhere far away, but he has no way to persuade the machine to which he sends the message to cooperate. As a result, it is possible for a sufficiently motivated internet detective to identify the first machine to which Victor sent the message, especially if she has several messages to work with. *See* The Spam-L FAQ § 3 (Apr. 24, 2002), http://www.claws-and-paws.com/spam-l/. If the machine that communicated with Victor keeps records of its email handling, or if its operator can be persuaded to do start doing so, the Internet detective can identify Victor's machine, and perhaps even Victor, as the source of the remailed message.

[89] Traffic analysis is the study of the sources and recipients of messages, including messages that the eavesdropper cannot understand. *See* A. Michael Froomkin, *The Metaphor is the Key:*

whom. In the absence of a compensation mechanism, or a jurisdiction capable of offering a safe haven for remailers, the cornerstone of Internet anonymity currently relies entirely on the charity of strangers.

In at least the medium term, the existence of anonymous remailers and jurisdictions willing to host them means that communicative anonymity is an inevitable consequence of allowing citizens access to the Internet. Given the international nature of the Internet, even a clever attempt to ban anonymous remailers in one jurisdiction at a time may be ineffectual. Even if every remailer in the U.S stops operating, there is nothing to stop U.S. citizens from sending and receiving messages via foreign-based remailers -- at least not yet. The continuous and conspicuous use of remailers and the equivalent might even be seen to create a reasonable expectation of privacy for Fourth Amendment purposes, thus reinvigorating a part of the Constitution which otherwise appears to be heading towards desuetude.

Remailer operators already have come under various forms of attack, e.g. lawsuits and subpoenas instigated by officials of the Church of Scientology who sought to identify the person they allege used remailers to disseminate copyrighted and secret Church teachings.[90] As a result, operating a remailer is not a risk-free activity today. Indeed, one can imagine a number of creative lawsuits that might reasonably be launched at the operator of a remailer. Examples include a new tort of concealment of identity, a claim of conspiracy with the wrong-doer, and a RICO claim. A remailer operator whose remailer was used to harass someone might face a common law tort claim of harassment. A conspiracy charge would be difficult since it would be difficult the prove the element of agreement that is a necessary part of a conspiracy. It is difficult to say that Bob conspires with a stranger, even if he leaves a tool lying in plain sight, knowing that criminals are likely but not certain to come by and use it. If Bob is really ignorant of the identity, content, and purposes of the messages he retransmits, he can plausibly say that there is no agreement between him and the conspirator, and that he should be no more liable for the misuse of his remailer than the rental car company that leases a car to a terrorist. Although it is far from obvious that any of these legal theories would or should succeed, some raise non-frivolous issues and thus would be expensive to defend.[91]

Cryptography, the Clipper Chip and the Constitution, 143 U. PENN. L. REV. 709, 747 (1995), available online http://www.law.miami.edu/~froomkin/articles/clipper.htm.

[90] *See* Helmers, *supra* note 12.

[91] Academic papers addressing these and related issues include Michael M. Mostyn, *The Need For Regulating Anonymous Remailers* (March 30, 1999), http://www.bileta.ac.uk/99papers/mostyn.html; Noah Levine, *Establishing Legal Accountability for Anonymous Communication in Cyberspace*, 96 COLUM. L. REV. 1526 (1996); Marie M. Stockton, Comment, *Protecting Copyrights in Cyberspace: Holding Anonymous Remailer Services Contributorily Liable for Infringement*, 14 T.M. COOLEY L. REV. 317 (1997); George F. du Pont, Comment, *The Criminalization of True Anonymity in Cyberspace*, 7 MICH. TELECOMM. & TECH. L. REV. 191 (2000-2001).

D. Control of Anonymous E-Cash as the Enemy of Anonymity

Digital cash can be fully traceable, can anonymize the identity of the payer only, or can (with some extra effort required to ensure that no one attempts to cheat the system by copying the digital money) leave no record at all of either party to the transaction.[92] Were anonymous digital cash to become widespread, it would pose a substantial obstacle to current law enforcement practices. The fight against money laundering has increasingly become a linchpin of modern law enforcement, which relies more and more on tracing the proceeds of criminal activity in order to identify suspects. As a result, the specter of anonymous digital cash would seem to be a development particularly threatening to law enforcement interests. Similarly, the widespread acceptance and use of anonymous digital cash would threaten to undermine regulatory schemes based on making financial records accessible to investigators. It would also promote limited forms of "regulatory arbitrage" in which persons choose to transact for anything that can be digitized in jurisdictions with congenial regulations.[93] Yet despite confident predictions to the contrary,[94] digital cash of any kind has yet to take off in any commercially significant manner, so this danger continues to be more theoretical than real. It remains possible that in the long run, anonymous networked communications moving sums of anonymous digital cash will pose a greater threat to the detection of money laundering than could any anonymous account. That day, however, remains on what appears to be a continually receding horizon as United States tax authorities wage a persistent campaign against anonymous bank accounts and funds transfers. As the IRS Commissioner's recently boasted, "the guarantee of secrecy associated with offshore banking is evaporating."[95]

If the campaign against secret funds transfers is not especially controversial, this may in part be due to insufficient understanding of the inevitable side-effects of any serious regulatory campaign to control money laundering via anonymous digital cash. The issue remains somewhat hypothetical today because true digital cash is a failure in the marketplace, and thus whether its users are traceable is almost a non-issue. But if digital cash ever does take off, there will be great pressure to ban anonymous digital

---

[92] See generally, A. Michael Froomkin, *Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases*, 15 U. PITT. J. L. & COM. 395 (1996), http://www.law.miami.edu/~froomkin/articles/ocean.htm.

[93] *See generally* A. Michael Froomkin, *The Internet as a Source of Regulatory Arbitrage*, (book chapter) in BORDERS IN CYBERSPACE (Brian Kahin and Charles Nesson, eds. 1997), http://www.law.miami.edu/~froomkin/articles/arbitr.htm.

[94] I am at least as guilty of these incorrect predictions as anyone. See Froomkin, *supra* note 92.

[95] Mike Godfrey, *IRS Offshore Credit Card Tax Evasion Investigation Extended*, Tax-News.com (27 March 2002), http://www.tax-news.com/asp/story/story_print.asp?storyname=7724.

cash for fear that it would enable widespread, untraceable, money laundering,[96] and these issues will rush to the fore.

Imagine a future where one must pay for access to reading materials on many web pages, one in which the web or its successors has become the major source of information for many citizens. Will those payments be in traceable cash? If so, will the traceablity of that cash mean that all for-pay reading will become part of the user's profile? Depending on precisely what types of digital cash were banned, a prohibition on anonymous digital cash could make it effectively impossible to speak and/or read web pages anonymously whenever any "marked" funds changed hands. Because the loss of anonymity occurs when digital money that identifies its owner changes hands, the anonymity of the author and reader would not be preserved by using either an anonymous web browser or a web page that could not be traced back to its author. This seems all too likely, for the legal restraints that protect anonymity in the political arena largely are absent in the marketplace. A legal ban on the use of anonymous digital cash for ordinary tangible, i.e. non-electronic, commerce faces as few constitutional or practical obstacles as does any regulation that might be applied to the sale of ordinary goods. Yet, as applied to the sale of reading matter, or information more generally, the ban potentially is problematic. If every visit to a fee-based web page leaves a data trail behind it, the reading habits of some persons are certain to be chilled.[97]

A ban on purely anonymous digital cash only, one which did not affect payer-anonymous schemes, would raise few if any constitutional issues. The privacy of readers would be unaffected and the author of the web page would give up only a very limited degree of anonymity when she turned the coins in to the bank because nothing about the coin redemption transaction, absent fraudulent attempts at double-spending, necessarily tells the bank where the cash came from or how the author came to acquire it.

On the other hand, a ban on anonymous digital cash that extended to payer-anonymous schemes could have First Amendment implications for its effect on both authors and readers. A ban on payer-anonymous schemes means that the reader must disclose her identity at least to the issuing bank, and probably to the author as well. It also means that the issuing bank is able to link the author to the

---

[96] See, for example, discussions in Jonathan I. Edelstein, Note, *Anonymity And International Law Enforcement In Cyberspace*, 7 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 231 (1996); Andres Rueda, *The Implications of Strong Encryption Technology on Money Laundering*, 12 ALB. L.J. SCI. & TECH. 1 (2001).

[97] *See, e.g.*, Fabulous Associates Inc. v. Pennsylvania Public Utility Comm'n, 896 F.2d 780, 786 (3rd Cir. 1990) (noting testimony before FCC that telephone sex lines suffer enormous loss in calling volume if customers are required to identify themselves); Frederick Schauer, *Fear, Risk and the First Amendment: Unravelling the "Chilling Effect"*, 58 B.U.L. REV. 685, 693 (1978).

reader if not inevitably to the precise reading matter being exchanged. Furthermore, in some schemes the reader may be able to learn the identity of the author.

This last effect, the loss of anonymity of the author, is the effect most clearly at odds with current First Amendment law.[98] Furthermore, the author also loses if readers are deterred from purchasing the material because they cannot do so anonymously. It is well-established that authors and publishers do not lose their First Amendment rights by charging for their work.[99] The Supreme Court has recognized that a regulatory scheme that denies authors the incentive of compensation "imposes a significant burden on expressive activity"[100] and that "[s]ome of our most valued forms of fully protected speech are uttered for a profit."[101]

The First Amendment protects the rights of readers up to a point. We have seen that in the U.S. the right to speak anonymously derives from the First Amendment's protection of speech and association. The Supreme Court also has repeatedly stated that the First Amendment protects the right to read (sometimes called the right to receive information),[102] most recently striking down a ban on

---

[98] *See generally* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look At "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996).

[99] *See* Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Bd., 502 U.S. 105 (1991); Arkansas Writers' Project, Inc. v. Ragland, 481 U.S. 221, 227-231 (1987); Minneapolis Star & Tribune Co. v. Minnesota Commissioner of Revenue, 460 U.S. 575 (1983).

[100] United States v. National Employees Treasury Union, 513 U.S. 454, 467-72 (1995); *see also* Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Bd., 502 U.S. 105, 115 (1991) (stating that the imposition of financial burdens may have a direct effect on incentives to speak); Minneapolis Star & Tribune Co. v. Minnesota Comm'r of Revenue, 460 U.S. 575, 585 (1983) (observing that the threat of burdensome taxes "can operate as effectively as a censor to check critical comment").

[101] Board of Trustees v. Fox, 492 U.S. 469, 482 (1989); *see also* New York Times Co. v. Sullivan, 376 U.S. 254 (1964); Buckley v. Valeo, 424 U.S. 1 (1976) (per curiam).

[102] *See* United States v. National Employees Treasury Union, 513 U.S. 454, 467-72 (1995) (declaring statute violates First Amendment in part because it "imposes a significant burden on the public's right to read"); Board of Educ. v. Pico, 457 U.S. 853, 867 (1981) ("[T]he right to receive ideas is a necessary predicate to the recipient's meaningful exercise of his own rights of speech, press and political freedom."); Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 756-757 (1976); Red Lion Broadcasting v. FCC, 395 U.S, 367, 390 (1969) (noting "right of the public to receive suitable access to social, political, esthetic, moral, and other ideas and experiences"); Stanley v. Georgia, 394 U.S. 557, 564 (1969) ("[i]t is now well established that the Constitution protects the right to receive information and ideas"); Griswold v. Connecticut, 381 U.S.

honoraria to mid- and low-level government employees in part because of the "significant burden on the public's right to read and hear what the employees would otherwise have written and said."[103]

The First Amendment right to read is bound up with a variety of understandings of the place of the First Amendment in a system of ordered liberty. It can be said to derive from the right to speak; it can also be viewed as an independent right without which speech would be meaningless. The right to receive information can be seen as an integral part of the individual's right to self-definition and self-actualization.[104] Alternatively, the right to receive information can be understood as an essential part of the republican vision in which an informed citizenry takes part in a continuing national political and moral debate; if citizens do not have access to information the debate is impoverished to the point of pointlessness. In any of these senses, the right to read undisturbed is indeed a right that "is fundamental to our free society".[105]

In light of the First Amendment's protection of anonymous speech, and of the importance of the right to read, logic suggests that the First Amendment could be read to protect a right to read

---

479, 482 (1965) (holding that "the right to receive, the right to read" are protected by the First Amendment); Martin v. City of Struthers, 319 U.S. 141, 143 (1943) (First Amendment "necessarily protects the right to receive" information); *see also* Ginsberg v. New York, 390 U.S. 629, 649 (1968) (Stewart, J., concurring) ("[t]he Constitution protects more than just a man's freedom to say or write or publish what he wants. It secures as well the liberty of each man to decide for himself what he will read and to what he will listen."); Lamont v. Postmaster General, 381 U.S. 301, 307-08 (1965) (Brennan, J., concurring).

A somewhat contrary decision is Rust v. Sullivan, 500 U.S. 173 (1991), which held that when subsidizing medical care, the government can attach conditions preventing the money from being used to provide counseling, i.e. information, about abortion.

[103] United States v. National Employees Treasury Union, 513 U.S. 454, 467-72 (1995) (declaring statute violates First Amendment in part because it "imposes a significant burden on the public's right to read").

[104] "The First Amendment serves not only the needs of the polity but also those of the human spirit--a spirit that demands self-expression. Such expression is an integral part of the development of ideas and a sense of identity. To suppress expression is to reject the basic human desire for recognition and affront the individual's worth and dignity." Procunier v. Martinez, 416 U.S. 396, 427 (1974) (Marshall, J. concurring).

[105] Stanley v. Georgia, 394 U.S. 557, 564 (1969) (holding that First Amendment protects possession of obscene materials in the home)

anonymously.[106] Indeed, the Colorado Supreme Court said as much in the *Tattered Cover* decision.[107] There is, however, no directly relevant decision of the U.S. Supreme Court to support this assertion. The closest thing is *Lamont v. Postmaster General*, in which the Court struck down a statute requiring post offices to refuse to deliver foreign-mailed communist propaganda unless the addressee specifically requested the material. The Court accepted that this requirement would very likely deter addressees from requesting mail that might be categorized as communist propaganda, and held that the statute therefore was "at war with the `uninhibited, robust and wide-open' debate and discussion that are contemplated by the First Amendment."[108] Justice Brennan's concurrence underlined the idea that the right to speak means little unless the right of the reader is protected also.[109]

Federal courts of appeal have recognized right to read in terms that suggest anonymous reading may be protected by the First Amendment. "When the effect of banning a form of speech is to prevent receipt of the message by the intended audience, it cannot seriously be argued that the ban is innocuous because it applies only to the mode of speech."[110] Indeed, the Third Circuit held that "[a]n identification requirement exerts an inhibitory effect" which "raises First Amendment issues comparable to those raised by direct state imposed burdens or restrictions."[111] Thus, after concluding that strict scrutiny was the appropriate standard, the Third Circuit struck down a state statute imposing an identification requirement for the use of phone sex services because there was a less restrictive alternative.[112]

---

[106] See Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044, 1047 (Col., 2002).; Cohen, *supra* note 97.

[107] Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044, 1047 (Col. 2002).

[108] Lamont v. Postmaster General, 381 U.S. 301, 302, 307 (1965) (quoting New York Times Co. v. Sullivan, 376 U.S. 254, 270 (1964)).

[109] 381 U.S. at 308 (Brennan, J., concurring) ("the dissemination of ideas can accomplish nothing if otherwise willing addressees are not free to receive and consider them").

[110] Yniguez v. Arizona, 69 F.3d 920, 936 (9th Cir. 1995) (enjoining "English only" amendment to state constitution), *vacated as moot sub nom* Arizonans for Official English v. Arizona, 520 U.S. 43 (1997).

[111] Fabulous Associates v. Pennsylvania Public Utility Com'n, 896 F.2d 780, 785 (3d Cir. 1990) (citing Talley, 362 U.S. at 64-65).

[112] *Fabulous*, 896 F.2d at 787-88. The Third Circuit distinguished F.C.C. v. Pacifica Foundation, 438 U.S. 726 (1978), on the grounds that the telephone was far less pervasive than broadcast media and required the active choice of the listener to receive it. *Fabulous* at 783. It is debatable whether that distinction applies to the Internet.

The counter-argument to all this remains that the right to read and receive information is a derivative right, as is the right to speak anonymously. The "right" to read anonymously could be described as doubly derivative from the First Amendment; if so, perhaps it need not be derived at all. One also might argue that negative and positive rights should not be confused. Even if there may be a right to be free of government-created registration rules, such as *Lamont*, it does not follow that the government is foreclosed from taking actions that happen to make it more difficult for people to read anonymously.[113]

A ban on anonymous digital cash would affect all transactions equally, not just speech for pay. As such, the ban would be a content-neutral burden on the right to speak anonymously and/or read fee-based digital materials anonymously. The ban would therefore be subject only to intermediate scrutiny on the theory that speech was incidentally burdened by a more general, legitimate, regulatory scheme.[114] The general rule would be examined to see whether it burdened "substantially more speech than is necessary to further the government's legitimate interests."[115] The legitimate interests put forward in

---

[113] Recognition of a right to read anonymously might pose difficulties for the regulation of reading material that must be denied to particular classes of readers, e.g. material that cannot be furnished to minors. There is, however, a partial technical solution to this problem if a trusted third party can be found to issue digitally signed anonymous age credentials. Alas, the system is not foolproof. If Alice, age 17, can persuade Bob, age 21, to give her the private key associated with the public key in Bob's certificate, Alice can impersonate Bob and no one on the Internet will be the wiser. It is possible to imagine versions of a digital signature infrastructure in which possession of another person's digital signature created such a risk for the original owner that signature sharing became rare, but this is not inevitable.

[114] *See* Turner Broadcasting Sys., Inc. v. FCC, 114 S. Ct. 2445, 2459-62 (1994) (applying intermediate scrutiny after deciding that must-carry provision that distinguished between speakers solely by the technical means used to carry speech is not a content-based restriction); Geoffrey R. Stone, *Content-Neutral Restrictions*, 54 U. CHI. L. REV. 46 (1987) (exploring the nature of content-neutral review).

[115] Turner Broadcasting, 114 S. Ct. at 2469 (quoting Ward v. Rock Against Racism, 491 U.S. 781, 799 (1989)).

Intermediate scrutiny explains why public libraries can keep records of who checks out their books even if the First Amendment does protect a right to read anonymously. The library's record-keeping is a content-neutral rule that burdens no more speech than is necessary to further the government's legitimate interests in getting the books back from bibliophillic and larcenous patrons. Whether libraries can keep the information about the reading habits of their patrons once the books have been returned is a different question. It is difficult to see what interest the government has in this information; book usage statistics, for example, do not require that the identity of the patron be

favor of the ban are likely to be compelling, including the need to control money laundering, and to trace illicit transactions, particularly illegal narcotics but perhaps other crimes also. Against such weighty interests, the only claims that would have any reasonable hope of prevailing in traditional intermediate scrutiny balancing would be that the same objectives could be realized with a lesser burden on speech, or that the cost to free speech was too enormous to be tolerated.

There are at least two schemes less restrictive than an outright ban on all forms of anonymous digital cash that might meet the felt needs of law enforcement. The first scheme is simply to ban only fully anonymous digital cash, and to allow payer-anonymous digital cash to circulate. While knowledge of the recipients of large amounts of cash is of value to identifying possible money launderers, this is not a perfect solution from the point of view of maintaining the status quo. Under current rules the recipient of a large amount of cash must report the transaction and identify the payer.[116] With payer-anonymous digital cash this is no longer possible. Thus, although a world of merely payer-anonymous digital cash may be acceptable to many privacy advocates, it is unlikely to satisfy law enforcement especially if they were able to persuade legislators of the need for the broader ban. In any event, since this scheme does not fully realize the objectives of a ban on all forms of anonymous digital cash, it is not evidence that the general ban failed to be narrowly tailored for First Amendment intermediate scrutiny purposes.

The second scheme relies on a technical solution. Rather than encode the identity of the owner into the cash in a form that the recipient and/or the digital cash issuer can read, the owner's identity could be encoded in a fashion that only the government, or other trusted third parties, could read. The government's right to access the information in this `Clipperized cash' could be hedged with procedural safeguards, or it could be triggered automatically whenever a Clipperized digital cash transaction exceeded current reporting limits. This scheme would meet any of the needs of law enforcement that could reasonably be asserted for an outright ban on anonymous cash -- and it would protect the privacy of users against profiling by private parties -- but it would do so at a cost that privacy advocates are likely to find very hard to accept. Whether this scheme would protect against government profiling of the reading and spending patterns of citizens would depend on the safeguards regulating the government's access to the identifying data.

---

maintained. It may be that the First Amendment, like the American Library Association's cannons of ethics, requires that the library at least refuse to release this information, and perhaps requires that it be routinely erased.

In this connection it is interesting to note that one of the first uses of the Patriot Act was to acquire library records relating to use of a library internet terminal. See John Holland, Paula McMahon, Fred Schulte & Jonathon King, *Library Computers Targeted in Terrorism Investigation*, SUN-SENTINEL (Sept. 18, 2001).

[116] Federal law requires a U.S. bank involved in a cash transaction exceeding $ 10,000 to file a report with the Secretary of the Treasury. *See* 31 U.S.C. § 5313(a); 31 C.F.R. § 103.22(a).

Because intermediate scrutiny often seems to involve a balancing test, whether a ban on anonymous digital cash "`unduly constrict[s] the opportunities for free expression.'" is likely to be a critical issue.[117] These decisions are frankly contextual: "Each method of communicating ideas is `a law unto itself' and that law must reflect the 'differing natures, values, abuses and dangers' of each method."[118]

In dissent Justice Holmes described the mails as "almost as much a part of free speech as the right to use our tongues."[119] Anonymous reading may yet come to be viewed as almost as much a part of free speech as the right to use our eyes. As Justice Thomas noted in his concurrence in *McIntyre*, "It is only an innovation of modern times that has permitted the regulation of anonymous speech."[120] Reading has not been a traditional subject of regulation; and if fee-based Internet speech comes to displace television or newspapers as a prime information medium, we may yet find the possibility of this monitoring, even if only by private parties, to be sufficiently intolerable to justify placing restraints on the government's power to deny readers the ability to remain anonymous.

The regulation of e-cash interacts with the regulation of anonymity in two ways. The less threatening relates to direct regulation of e-cash itself. Fully anonymous e-cash enables both anonymous authorship and anonymous reading. But the same technology also enables money laundering. If e-cash looks likely to become popular, attempts to ban it on the ground that it facilitates crime are likely. It may be that the First Amendment will be interpreted to prevent such legislation, but there are many reasons to think that constitutional regulations can be crafted. Money laundering control, after all, is a compelling government interest. The *Tattered Covers* decision discussed above[121] breaks new ground in emphasizing the importance of the reader's rights to hide their identity, and did so on both state and federal constitutional grounds -- and yet even it did no more than instruct the lower court to re-think the

---

[117] City of Ladue v. Gilleo, 512 U.S. 43, 55 n.13 (1994) (quoting Geoffrey R. Stone, *Content-Neutral Restrictions*, 54 U. CHI. L. REV. 46, 58 (1987)); *see also* Wayte v. United States, 470 U.S. 598, 611 (1985) (noting that part of the test is whether an "incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest" (quoting United States v. O'Brien, 391 U.S. 367, 377 (1968))).

[118] Metromedia v. City of San Diego, 453 U.S. 490, 501 (1981) (quoting Kovacs v. Cooper, 336 U.S. 77, 97 (1949) (Jackson, J., concurring)).

[119] Milwaukee Social Democratic Publishing Co. v. Burleson, 255 U.S. 407, 437 (1921) (dissenting opinion); *cf.* Blount v. Rizzi, 400 U.S. 410, 416 (1971) (quoting Holmes's description with approval).

[120] 514 U.S. at 367.

[121] See *supra* text accompanying note 30.

issue of police access to bookstore records, giving the privacy right due weight. Even if there is a First Amendment right to read anonymously, that right will not necessarily outweigh a content-neutral restriction justified by a compelling government interest, especially if there appears to be no alternative regulation that could accomplish the legitimate and important goal.

The more worrying intersection between e-cash regulation and anonymity arises from a basic property of encrypted information: Once encrypted, all messages look alike. Other than intercepting them and decrypting them, there is no way to tell which messages are protected political speech, which are economic transactions due a lower level of protection, and which are criminal conspiracies. If the government interest in preventing money laundering is sufficiently great to overcome First Amendment concerns about the effects on anonymous writing and reading, it might also be great enough to justify more far-reaching controls on anonymous communication. The First Amendment requires that the government use the narrowest effective means to accomplish legitimate goals that impinge on speech rights. In a world of encrypted messages, e-cash regulation must either be able to find and regulate a chokepoint in the financial system through which e-cash must pass[122] or it will require regulation of all anonymous speech. It may be that banks and other financial intermediaries will suffice as the targets of regulation; but if they don't then any regulation designed to place effective controls on anonymous digital cash will almost inevitably end up trying to catch all anonymous communications within its sweep.

E. Content Management as the Enemy of Anonymity

Today, the greatest threat in the United States to the exercise of the right to be anonymous comes not from anti-terrorism initiatives nor from the possible anti-money laundering proposals. Instead, the greatest threat to communicative anonymity arises from the campaign against digital "piracy" being mounted by intellectual property (IP) rights holders. Animated by a fear that movies, song and other digitizable content will lose value in a world of cheap copying and internet file sharing, IP rights holders are mounting a four-pronged campaign to control the reproduction and distribution of information. A key part of this strategy is to preserve and extend IP rights owners' ability to track content copiers and distributors-- which means making it as difficult as possible to exchange information anonymously.

The IP rights holders' "digital rights management" (DRM) campaign is well-funded and comprehensive. At the standards level it impacts both hardware and software. In the legal and political realm it involves legal attacks on content-sharing services as contributory copyright violators; makers of non-compliant hardware or software face liability under the 1998 Digital Millennium Copyright Act.[123]

---

[122] *See* Peter P. Swire, *Financial Privacy And The Theory Of High-Tech Government Surveillance*, 77 WASH. U. L.Q. 461 (1999).

[123] The DMCA, codified at 17 U.S.C. §§ 1201-1205, imposes civil and criminal penalties for the creation or distribution of DRM circumvention tools.

Last, but not least, the DRM movement seeks additional legal changes to further protect intellectual property rights; some of these changes would require content intermediaries to keep records of the information accessed by their customers.

Hardware. The DRM campaign involves several proposals for modifying hardware standards to ensure that material encoded on hard drives, DVDs, CDs, and other media cannot be played or copied without the permission of the rights holder. For example, in 2000, IBM, Intel, Matsushita, and Toshiba jointly proposed a "Content Protection for Removable Media" standard that would have imposed DRM on all computer hard drives, cd-rom and cd-rw drives, flash memory, and other media storage devices. A consumer backlash forced them to scale back the proposal[124] More recently, one record company is experimenting with CDs that cannot be played in personal computers for fear they may be copied.[125]

Software. Similar projects involve placing DRM into software used for writing or playing digitized content. Other software assigns an identifier to content or to the content player, and attaches personal information to the identifier. Many programs including Microsoft's Windows Media Player[126] and older versions of Microsoft Word[127] use globally-unique identifiers (GUID) to link a computer or user to content. While the specific technologies vary, many of them involve having devices 'phone home' in order to enforce licensing conditions including pay-per-view. While designed primarily to enforce payment, these systems have obvious implications for anonymity (and privacy more generally): every access to the digital work is logged, and transmitted to the rights holder. Anonymous reading and viewing of content becomes impossible.

Attacks on File Sharing. Numerous peer-to-peer file-sharing systems have been deployed on the Internet, among them Napster, KaZaA, Morpheus, Freenet, and Gnutella.[128] The Recording

---

[124] *See* EPIC, Digital Rights Management and Privacy, http://www.epic.org/privacy/drm/ .

[125] The CD had the unfortunate side-effect of locking iMacs. See *Celine Dion kills iMacs!*, MacUser (May 10, 2002), http://www.macuser.co.uk/macsurfer/php3/openframe.php3?page=/newnews/newsarticle.php3?id=1990

[126] *See* Richard M. Smith, *Serious Privacy Problems in Windows Media Player for Windows XP*, COMPUTERBYTESMAN (Feb. 20, 2002), http://www.computerbytesman.com/privacy/wmp8dvd.htm.

[127] *See* Yusef Mehdi, *Microsoft Addresses Customers' Privacy Concerns*, PressPass, Mar. 8, 1999, http://www.microsoft.com/presspass/features/1999/03- 08custletter2.htm.

[128] For a thoughtful look at the underlying issues see Raymond Shih Ray Ku, *The Creative Destruction Of Copyright: Napster And The New Economics Of Digital Technology*, 69 U. CHI.

Industry Association (RIIA) of America and the Motion Picture Association of America (MPAA) have spearheaded a counter-effort to eradicate online file-sharing systems on the grounds that they are little more than organized copyright infringement enabling mechanisms. These efforts have borne fruit. KaZaA went out of business, citing its inability to defend itself against "Rambo-style" litigation.[129] Napster lost a lawsuit filed by record companies and music publishers charging it with contributory and vicarious copyright infringement and was ordered to shut down until it could remove every file from its music index if Napster has reasonable knowledge that the file contains the plaintiffs' copyrighted work.[130] Napster subsequently filed for Chapter 11 bankruptcy.[131]

In the eyes of the MPAA and RIIA, if file-sharing is bad, *anonymous* file sharing is worse, since it makes it much more difficult to track down copyright violators.[132] Edgar Bronfman, the CEO of the parent company of Universal Studios, expressed the MPAA's view of these services when he said,

> Anonymity, disguised as privacy, is still anonymity, and it must not be used to strip others of their rights, including their right to privacy or their property rights. We need to create a standard that balances one's right to privacy with the need to restrict anonymity, which shelters illegal activity.
>
> ...
>
> In the appropriation of intellectual property, myMP3.com, Napster, and Gnutella (which has stolen from the breakfasts of 100 million European children even its name) are, in my opinion, the ringleaders, the exemplars of theft, of piracy, of the illegal and willful appropriation of someone else's property.[133]

L. REV. 263 (2002).

[129] AP, Music swapping firm to fold under weight of lawsuits (May 22, 2002), http://sfgate.com/cgi-bin/article.cgi?file=/news/archive/2002/05/22/financial1929EDT0213.DTL.

[130] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir.2001); *see also* A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002).

[131] cnnMoney, *Napster files bankruptcy* (June 3, 2002), http://money.cnn.com/2002/06/03/technology/napster.reut/index.htm.

[132] If the content is tagged or watermarked in some way, it may still be possible to identify the owner of the original copy.

[133] Edgar Bronfman, Jr., Remarks As Prepared For Delivery by Edgar Bronfman, Jr. (May 26, 2000), http://www.mpaa.org/copyright/EBronfman.htm.

The anonymous file-sharing networks are still more experimental, or at least smaller, than the first round of MPAA/RIIA targets, but given this depth of feeling it is likely to be only a matter of time before they are targets too.

Lobbying for Additional Protection.

Private lawsuits against file-sharing networks may become unnecessary if the DRM movement is able to enlist the government to do the work of its technology-shaping agenda. The 1998 passage of the DMCA demonstrated the IP lobby's clout: the DMCA includes sui generis protection for intellectual property protection devices in the form of penalties for the "circumvention" of any copy-protection device. Further new legislation may not be needed, however, if the anti-anonymity portion of the DRM agenda can be achieved through administrative regulation.

As an example of how this may work, consider the somewhat obscure debate over the license fees that internet radio stations should be required to pay for their webcasts of copyrighted music. RIIA petitioned the Copyright office, asking for rules that set a fee schedule for Internet radio stations. It also proposed that the federal government require webcasters to keep and submit for inspection a "Listener's Log" that would, "identify the name of the Service, the channel or program accessed, information on the user, such as date and time the user logged in and out, the time zone of the place at which the user received the transmission, the user identifier, and the country in which the user received the transmission."[134] In its initial decision, the Copyright Office agreed that listeners should be tracked in this manner, as "the request for the Intended Playlists, Listener's Log, and Ephemeral Phonorecord Log seems reasonably based on the premise that the copyright owners need certain specific information to monitor compliance and use by the Services."[135] (Subsequently, however, the Librarian of Congress, issued an Order rejecting the Panel's determination and promising to issue a revised order no later than June 20, 2002.)

IV. Anonymity in the Balance?

We live in an age of sense-enhanced searching via satellite, infrared, and other high-tech methods;[136] tomorrow may see much greater capabilities for identifying people and linking personal data to that identification. Larger and faster database processing techniques combined with the ever-increasing quantity of personal data available on individuals makes it possible for both governments and private organizations to construct personal profiles based on transactions, demographics, and even

[134] Library Of Congress, Copyright Office, Proposed Rules, Notice and Recordkeeping for Use of Sound Recordings Under Statutory License, 67 FR 5761, 5763 (Feb. 7, 2002).

[135] *Id*.

[136] *See generally*, Froomkin, *supra* note 83.

reading habits of most citizens. If merchants know your demographic information, income, credit rating and buying history when you walk in the store, or log into the cyber-mall, they may be tempted to engage in price discrimination[137] or even more invidious forms of discrimination.

Anonymity may turn out to be the only tool available to ordinary people that can provide even a partial defense against tracking and profiling. The degree of anonymity afforded to communications and transactions is a critical question because of the continuing growth of personal data profiles. Consumers may have to resort to strong forms of anonymity if they wish to restrict the spread of information about their tastes and activities. This is especially true in countries such as the U.S. that have limited data protection laws, but it applies with diminished force even to nations with more regulation because no system of regulation can control all of the ways in which personal data can be stored, disseminated, searched, and used.

Commercial considerations aside, anonymous communication may be particularly deserving of protection for its own sake. Not everyone is so courageous as to wish to be known for everything they say, and some timorous speech deserves encouragement. Corporate whistle-blowers, even junior professors, may fear losing their jobs. People criticizing a religious cult or other movement from which they might fear retaliation may fear losing their lives. In some other countries, even in the United States in some times and places, it is unsafe to be heard to criticize the government. Persons who wish to criticize a repressive government or foment a revolution against it may find anonymity invaluable. Indeed, given the ability to broadcast messages widely using the Internet, anonymous e-mail may become the modern replacement of the anonymous handbill.

The ongoing debate over the legality and morality of anonymous communication can most usefully be viewed as one part of a more general debate over the extent to which individuals should control the dissemination of information about themselves, a debate reflected on the one hand in occasional legislative calls for stronger data protection and/or privacy laws and on the other hand in market demands for credit bureaus and data mining and the ever-increasing government use of databases, profiling, and security clearance techniques.

At this moment United States law offers clear protection to anonymous political and religious speech. While it is unclear to how much this principle will necessarily be extended to speech generally, so far the trend is greater, not lesser protection in the courts. At least so far, the chief counter-pressure to date is not, as one might expect, anti-terrorism initiatives ostensibly responding to the 9/11 attacks, but rather commercial pressures from intellectual property rights holders that have been building for

---

[137] *See* J. Bradford DeLong & A. Michael Froomkin, *Speculative Microeconomics for Tomorrow's Economy* in INTERNET PUBLISHING AND BEYOND: THE ECONOMICS OF DIGITAL INFORMATION AND INTELLECTUAL PROPERTY 6 (Brian Kahin &Hal Varian, eds., 2000), http://www.law.miami.edu/~froomkin/ articles/spec.htm.

several years.

Expect a collision.