PART III

ANONYMITY

Building on our investigation of the various concepts and technologies pertaining to identity and identification in Part II, Part III offers a snapshot of the laws governing our ability or inability to be anonymous. Scholars from five North American and European jurisdictions—Michael Froomkin from the United States; Carole Lucock and Katie Black from Canada; Ian Lloyd from the United Kingdom; Simone van der Hof, Bert-Jaap Koops, and Ronald Leenes from the Netherlands; and Giusella Finocchiaro from Italy—survey the place of anonymity across the legal domain and assess the law as it currently stands in each country. Although each survey can be read in isolation, it is interesting to consider some of the similarities and differences among and between them.

No "right to anonymity" is explicitly protected by any of the five jurisdictions' constitutions or human rights provisions. However, anonymity may enjoy limited protection as an acknowledged component of another right or freedom, in particular, privacy, freedom of expression, restrictions on state search and seizure, and provisions related to protecting liberty and life. In fact, it would seem that there is no coherent or integrated approach to anonymity in any jurisdiction. Rather, the law has developed piecemeal in a number of disparate public and private law areas. Consequently, the meaning of anonymity is contextually situated and may vary from one area of law to another.

All in all, each jurisdiction reports scant protection of anonymity, a preference for identifiability, and an increasing encroachment on areas of de facto anonymity that the law, to date, has not protected. Each author discusses the law's specific responses to the network society along with descriptions of existing approaches to anonymity in a broad range of areas within their jurisdictions. Despite differences, there is a great deal of similarity to the legal approach in each country, aided perhaps by adherence to or influence of international agreements, treaties, and directives. In addition, legal protections for anonymity in all five jurisdictions appear to be shrinking, as the focus on safety and security has repeatedly trumped the call or justification for anonymity.

For example, each jurisdiction has considered a requirement to carry a national identity card, and this has created prominent debate in most. The introduction of an all-purpose identity card is a significant change that promises to have a chilling effect on anonymity. This has been presaged in some jurisdictions by judicial decisions that have lowered the threshold of the legal grounds necessary for law enforcement personnel to detain persons and to require them to identify themselves. Even when a national identity card has not been introduced, a number of jurisdictions have added biometrics and radio frequency identification chips to "smart" drivers' licenses, in effect turning them into de facto identity cards.

Apart from a general requirement to identify oneself to the state, each jurisdiction reports instances in which identification is statutorily required. Examples include producing a driver's license when using public highways and providing identifying

information in order to conduct banking transactions. Courts and tribunals have similarly upheld requirements that individuals identify themselves for certain commercial purposes such as obtaining a refund or exchanging goods. In all jurisdictions, there has been an increase in these calls for context-specific mandatory identification and a consequent reduction in the ability to transact or enter commercial or noncommercial relations anonymously.

The use of surveillance in public spaces, particularly video surveillance, is clearly increasing in all jurisdictions. The de facto anonymity once enjoyed in these spaces has, as a consequence, diminished, and to date the law seems to be enabling the deployment of technologies of surveillance rather than protecting anonymity.

The appropriate role of and the degree of control over the providers of communications services, especially Internet service providers, is another area in which the law in currently in flux. The combined interests of law enforcement agencies and the private sector in ensuring that identity can be revealed on demand has resulted in significant pressure to require service providers to collect and maintain records for identification purposes and, in some countries, to allow identifying information to be disclosed to authorities without judicial preauthorization or oversight.

Although there are remarkable similarities in approach among the five jurisdictions, there are also some interesting differences. For example, the United States reports that a strong adherence to the open court principle has limited the use of a pseudonym in criminal and private law proceedings. This is in stark contrast to other jurisdictions where the use of a pseudonym is supported both by the courts and by legislation as a means to protect and promote the pursuit of legal claims. Although in these jurisdictions the use of a pseudonym and a publication ban does not usually shield facts or the identity of witnesses from an accused, there are exceptions. In Canada, undercover operatives may have their identity concealed, and in the United Kingdom, recent legislation now permits the granting of witness anonymity orders to protect the witness's anonymity. Interestingly, Canada also reports that permission to use a pseudonym to protect privacy may now be given to those persons who have used an online pseudonym to enable them to continue to use it in court.

Other differences are equally noteworthy. The UK law enforcement DNA database has been particularly controversial, especially given its size and the wide set of circumstances that allow the government to add information to it. Although other jurisdictions have similar databases, the restrictions on information inclusion and use appear far more stringent. The Netherlands reports growing concerns over electronic voting, including the use of the Internet for remote balloting. As other jurisdictions contemplate or implement e-voting, many wonder how the traditional protection of voter secrecy and the assurance of system integrity and accountability will be preserved and protected. Italy reports

a number of interesting provisions that legally protect the right to be anonymous in some circumstances, including entering a detoxification center, seeking help for social problems, and protecting the name of the mother at the time of childbirth.

Each author expresses a general concern as to the direction the law is taking and calls for greater attention to and protection of anonymity as a necessary component of protecting valued human rights such as liberty, dignity, and privacy.

24. ANONYMITY AND THE LAW IN THE UNITED STATES

A. MICHAEL FROOMKIN

INTRODUCTION

Surveys suggest that the public is increasingly concerned about privacy issues, but post-9/11 concerns have motivated the federal government, in particular, to develop a number of initiatives that lessen the scope for anonymous communication and behavior in the United States. Some of the core protections, however, rest on pre-9/11 constitutional foundations, and the courts are only beginning to hear challenges to these new statutes and programs. That there has been a lurch against anonymity since September 2001 is indisputable; how great a lurch and for how long major parts of it will last remains uncertain and is, in fact, deeply contested.

Underlying this contest is the lack of a consensus as to when and whether anonymity is good, at least outside the realm of core political speech. 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 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.

Generalization about U.S. law regulating anonymity is difficult because U.S. law treats it in a patchwork fashion, owing to the nation's constitutional and federal structure. At present, U.S. law enjoys a strong, reasonably well-entrenched core constitutional protection for anonymous political speech, and this seems likely to endure. As one moves away from this core and includes speech that cannot so easily be characterized as political or religious, legal protection for anonymity generally becomes less clearly protected as the law begins to accumulate some uncertainty. The public law regulation of anonymity is mediated through a mix of federal and occasionally state constitutional provisions, and also a growing patchwork of state and federal legislation. The private law regulation of anonymity is even more decentralized, as it shares all the sources of the public law regulation, albeit sometimes in an attenuated fashion, but also frequently involves state statutes and court decisions.

I. BASELINE PROTECTION OF ANONYMITY IN (FEDERAL) CONSTITUTIONAL LAW

The U.S. 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.

A superficial examination of the recent decisions of the U.S. courts might fail to disclose much ambiguity. On the surface, the Supreme Court's recent decisions evince a strong, repeated endorsement of the legitimate role of anonymity in political discourse. The cases are replete with references to the close relationship between the right to anonymous association and the role that anonymous communication legitimately plays in political discourse. Anonymity has basked in its association with good causes, including the civil rights movement[1] and, as described below, both religious liberty and civic activism.

Game, set, match? Not at all.

Balancing—and in time perhaps overbalancing—these legal protections for anonymity are a number of countervailing legal initiatives and even trends, notably a vast increase in the technical and legal capability to monitor electronic communications at home and abroad, and legal developments suggesting that

1. *NAACP v Alabama ex rel. Patterson*, 357 U.S. 449 (1958).

communication intermediaries must assist the governments and others who seek to discover the identity of anonymous authors. The Bush administration has not been shy about suggesting that it needs the broadest access to communications intelligence for national security, and too few have gainsaid that viewpoint. Meanwhile, a number of traditional civil law doctrines, applied in a doctrinally predictable fashion, combine to provide considerable powers for civil litigants to demand, usually upon the showing of good cause, the disclosure of the identity of otherwise anonymous speakers in a variety of legal settings. And the Supreme Court's most recent relevant decision, although somewhat equivocal as to the details, did uphold a state requirement that persons identify themselves to police officers armed with "reasonable suspicion" when asked to do so.

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."[2] Political speech receives the highest constitutional protection because it "occupies the core of the protection afforded by the First Amendment"[3]; other types of speech, notably "commercial 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.[4]

The leading case on anonymous political speech is *McIntyre v. Ohio Elections Commission*.[5] 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 be stretched

2. *New York Times Co. v Sullivan*, 376 U.S. 254, 270 (1964).
3. *McIntyre v Ohio Elections Comm'n*, 514 U.S. 334, 346 (1995).
4. See *First Nat. Bank of Boston v Bellotti*, 435 U.S. 765, 776–777 (1978).
5. *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995).

even further. "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."[6] 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."[7] 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."[8]

Similarly, in *Watchtower Bible and Tract Soc. of New York, Inc. v. Village of Stratton*,[9] the Supreme Court struck down a village ordinance requiring all door-to-door solicitors and canvassers—whether religious or commercial—to register with the village, and to disclose their identities and the reason for which they wished to go door-to-door. The Watchtower Bible and Tract Society (known also as Jehovah's Witnesses), a religious group that wished to go door-to-door in Stratton in order to proselytize, challenged the ordinance as unconstitutional. The Supreme Court agreed, holding that the "breadth and unprecedented nature of this regulation" meant that it violated the First Amendment: "Even if the interest in preventing fraud could adequately support the ordinance insofar as it applies to commercial transactions and the solicitation of funds, that interest provides no support for its application to petitioners, to political campaigns, or to enlisting support for unpopular causes."[10]

Despite these ringing words, how broad a right one has to be anonymous in the United States remains somewhat unclear, as difficult cases are precisely those in which exceptions are made to fit facts that sit uncomfortably within the rules that apply "ordinarily."[11] To date, the Supreme Court has addressed the easy cases such as broad prohibitions of anonymous political speech. As a result, it is now clear that ordinances prohibiting all anonymous leafleting, like the one in *McIntyre*, are an unconstitutional abridgment of free speech.[12] Thus, in

6. *Ibid.*, 357.

7. *Ibid.*, 341.

8. *Ibid.*, 357.

9. *Watchtower Bible and Tract Soc. of New York, Inc. v Village of Stratton*, 536 U.S. 150 (2002).

10. *Ibid.*, 168.

11. 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," *North Carolina Law Review* 74 (1996): 553.

12. *Ibid.*; *Talley v California*, 362 U.S. 60 (1960).

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.[13] And in *Watchtower*, the Court found the village's attempt to justify the ordinance on grounds of "protecting the privacy of the resident and the prevention of crime" to be unconvincing, given the facts.

There is no doubt that the Supreme Court has been solicitous in considering 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.[14] But the Court has consistently left the door open to finding a compelling state interest which would justify overcoming the right to privacy in one's political associations and beliefs—if state interest is evident. Nothing in *McIntyre* or *Watchtower* really changes this. In *McIntrye*, Justice Stevens carefully distinguished earlier cases upholding statutes that sought to preserve the integrity of the voting process.[15]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 2 U.S.C. § 267, which requires those engaged in lobbying to divulge their identities.[16] As a constitutional matter, therefore, the anonymity issue remains far from resolved even for the most highly protected category of speech.

To be sure, there are doctrinal grounds for near-absolutist protection for anonymity. In *Tattered Cover, Inc. v. City of Thornton* the Colorado Supreme Court interpreted both the state and federal constitutions to "protect an individual's fundamental right to purchase books anonymously, free from governmental interference."[17] 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

13. *McIntyre*, 348 (n. 5).

14. See *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, 485–487 (1960) (holding invalid a statute that compelled teachers to disclose associational ties because it deprived them of their right of free association).

15. *McIntyre*, 344 (n. 5).

16. *United States v Harriss*, 347 U.S. 612, 625 (1954).

17. *Tattered Cover, Inc. v City of Thornton*, 44 P.3d 1044, 1047 (Colo. 2002).

successful and uninhibited exercise of First Amendment rights, precisely because of the chilling effects that can result from disclosure of identity."[18]

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,[19] 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.[20] Similarly, in *Buckley v. Valeo*,[21] 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.[22] Because the Court in the same decision essentially equated the expenditure of money in campaigns with the ability to amplify political speech,[23] 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.[24] Similarly, in *First Nat. Bank of Boston v. Bellotti*,[25] 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

18. *Ibid.*, 1052.

19. See Steven Wisotsky, "Crackdown: The Emerging 'Drug Exception"'to the Bill of Rights," Hastings Law Journal 38 (1987): 889.

20. See *Bd. 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 U.S. 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).

21. *Buckley v Valeo*, 424 U.S. 1, 143 (1976).

22. *Ibid.*, 23–29, 60–84.

23. *Ibid.*, 19.

24. *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 extend this idea to public fora and that *Vincent* may come to be seen as simply a decision upholding a particular time, place, and manner restriction.

25. *First Nat. Bank of Boston v Bellotti*, 435 U.S. 765 (1978).

as a means of disclosure, so that the people will be able to evaluate the arguments to which they are being subjected."[26]

In sum, anonymous speech—especially speech about political or religious matters—enjoys a privileged position under the U.S. Constitution. However, no form of speech is completely immune from regulation. Even political speech can be regulated, given sufficient cause, especially if the regulation is content-neutral, as a regulation on anonymous speech would likely be. What the cases demonstrate is that any regulation of anonymous speech, especially any rule that threatens to touch the most protected types of speech, will require a particularly strong justification to survive judicial review.

II. CRIMINAL LAW/NATIONAL SECURITY LAW

The criminal law and national security arenas exhibit a patchwork of anonymity regulation, and, at present, the law in this area is somewhat fluid. By enabling much greater surveillance on a much lower evidentiary basis, post-9/11 enactments have significantly eroded the capability of citizens to remain anonymous. On the other hand, in specific circumstances, the law clearly upholds the right to anonymity. There may be some tension between the Fourth Amendment's prohibition of unreasonable search and seizure—which is understood to require the government to seek advance court approval for most searches and wiretaps in domestic law enforcement—and the 2008 amendments to the Foreign Intelligence Surveillance Act that expands the government authority to intercept U.S. citizens' and residents' telephone and e-mail communications without a warrant.[27]

Exactly how this plays out in identity/anonymity issues is somewhat up for grabs. The most recent relevant Supreme Court decision, the *Hiibel*[28] case, upheld a state statute requiring persons to identify themselves to police when the investigating officer's demand is "based on reasonable suspicion"[29] that the person may have committed a crime. Even so, the Court upheld the self-identification requirement on the understanding that "the statute does not require a suspect to

26. *Ibid.*, 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*. 512 U.S. 43, 56–57 (1994) (noting that a poster in front of a house associates speech with the identity of the speaker).

27. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110–261, 122 Stat. 2436 (2008).

28. *Hiibel v Sixth Judicial Dist. Court of Nevada, Humboldt County*, 542 U.S. 177, 183 (2004).

29. *Ibid.*, 184.

give the officer a driver's license or any other document"[30] and reserved for a future day the Fifth Amendment question of what rule would apply if disclosure was self-incriminatory.[31] *Hiibel* thus stands for the proposition that the state may demand your identity if it has reason to do so, while also signaling some wariness in the Supreme Court about the issue.

That wariness may be tested as post-9/11 cases begin to wind through the courts. The original law-enforcement investigatory power legislation passed in the wake of the 2001 terrorist attack on the World Trade Center, the Patriot Act,[32] had 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 only a first step. More recent enactments, such as the revised Foreign Intelligence Surveillance Act, empower both data mining and wide-spread surveillance of phone calls and e-mails between the United States and a foreign location. The Act allows dragnet surveillance without requiring the government to make any showing to a court and with almost no judicial oversight, removing any obligation to demonstrate whether the communication has anything to do with terrorism or any threat to national security.[33]

Meanwhile, the U.S. government is widely reported to have stepped up its domestic 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. The United States has also begun to amass biometric data banks and related databases for law enforcement purposes that could be used to identify formerly anonymous persons if DNA evidence of their identity can be collected.

Lest this seem fanciful, consider that the Bush administration has suggested that the Espionage Act of 1917 Act might be used against investigative reporters to get them to reveal their sources. The Act makes it a crime to transmit or receive national defense information, and the administration apparently views it as a tool to be used against leakers and whistle-blowers. As it is, courts traditionally have possessed, and have not feared to use, contempt power to get reporters to reveal anonymous sources, and in the past decade a number of journalists have chosen to be jailed rather than disclose them.

Conversely, it is important to note what has *not* changed in the wake of 9/11. There has, for example, been no serious attempt by either Congress or the

30. *Ibid.*, 185.

31. *Ibid.*, 90–191.

32. Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107–156 (2001).

33. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110–261, 122 Stat. 2436 (2008).

administration to impose any new limits on the legal right to possess and use the cryptographic tools that make Internet anonymity possible. And, at least until further notice, the constitutional protections for anonymous discourse remain in force.

It is also important to note that some doctrines that have the effect of making anonymity difficult as a practical matter—notably the so-called third-party doctrine—long predate 9/11. Under the third-party doctrine, any time a person discloses information to a third party, the disclosing party waives all Fourth Amendment rights in the data revealed.[34] In short, there is no reasonable expectation of privacy in any information disclosed to a third party: absent common-law or statutory evidentiary privileges such as attorney-client and priest-penitent, anyone who knows of a speaker's identity can be forced to reveal it if the police know to ask.

Anonymity of Witnesses

The right to hear and see one's accuser in an open courtroom has been a hallmark of American criminal law. For example, the Confrontation Clause of the Sixth Amendment provides that "[i]n all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witness against him."[35] This imposes severe limits on the anonymity of witnesses at trial, as the clause is understood as a safeguard to ensure the reliability of evidence presented at a criminal trial by subjecting it to adversarial testing. As one authority aptly summarizes the situation,

> American courts have rarely allowed even minor exercises of anonymity. In *Alford v. United States*, 282 U.S. 687, 692 (1931), the Supreme Court held that disclosure of a witness' identity and address were unequivocally required in a criminal trial, reasoning that "prejudice ensues from a denial of opportunity to place the witness in his proper setting and put the weight of his testimony and his credibility to a test." Using dicta in *Smith v. Illinois*, some lower courts have loosened this requirement and refined it to allow witness anonymity in situations where the prosecution can show actual threat to the witness exists and fully discloses such threats to the trial judge. In these courts, the trial judge must weigh the value of disclosure with witness safety. Other trial courts remain fastened to the holding of Alford.[36]

Indeed, courts have struggled with the degree of protection owed even to witnesses whose lives might be endangered by testifying. In *Alvarado v. Superior*

34. For a defense of this justly criticized doctrine, see Orin Kerr, "The Case for the Third-Party Doctrine," *Michigan Law Rev* (forthcoming, 2009): 107, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1138128.

35. U.S. CONST. amend. VI.

36. Nicholas W. Smith, "Evidence and Confrontation in the President's Military Commissions," *Hastings Constitutional Law Quarterly* 33 (2005): 83, 96.

Court[37] the Supreme Court of California held that the Confrontation Clause prevents witnesses from testifying anonymously at trial, if their testimony was crucial to the prosecution's case. On occasion, however, judges have allowed undercover and intelligence agents to testify in disguise so as to protect their identities.[38]

The use of hearsay from anonymous witnesses before the status review tribunals held at Guantanamo has been heavily criticized. One federal court, reviewing a decision based entirely on the hearsay testimony of three absent witnesses, contemptuously characterized the government's defense of the military tribunal's reliance on such poor evidence as equivalent to the line in Lewis Carroll's "Hunting of the Snark": "what I tell you three times is true."[39]

In like vein, U.S. law generally requires open trials. In criminal cases other than those dealing with classified material, there are few mechanisms that allow judges to exclude the public (as opposed to sequestering other witnesses whose testimony might be tainted). Although courts may sometimes issue gag orders to participants and their lawyers, it cannot muzzle the press or the general public. Despite the very rare attempt, successful publication bans such as those found in the UK or Canada are unknown in the criminal and civil courts. Closed hearings, however, do occur in the civil courts (especially for family court matters), and it is possible to seal evidence pertaining to trade secrets and other confidential matters. There is a presumption of openness, although actual practice varies by state and sometimes within them.

In *Waller v. Georgia*[40] the Supreme Court stated that to close a proceeding: (1) the party seeking closure must advance an "overriding interest that is likely to be prejudiced"; (2) the closure must be "no broader than necessary to protect that interest"; (3) the court must consider "reasonable alternatives" to closure; and (4) the court must "make findings adequate to support the closure."[41] This rule applies in the main to child witnesses as it does to adults, all of whom ordinarily must testify in open court.[42] In addition, both the press and the public enjoy a qualified First Amendment right of access to criminal trial proceedings.[43]

---

37. *Alvarado v Superior Court*, 5 P.3d 203 (Cal. 2000).

38. E.g., *United States v Martinez*, 2007 WL 2710430 (S.D.N.Y. 2007), in which the court allowed an undercover officer to testify in disguise, "but without dark glasses so that the Defendant and jury can observe his eyes, his facial reactions to questions, and his body language." *Ibid.* at *3.

39. *Parhat v Gates*, 532 F.3d 834, 848–49 (D.C. Cir. 2008).

40. *Waller v Georgia*, 467 U.S. 39 (1984).

41. *Ibid.*, 48.

42. See *United States v Thunder*, 438 F.3d 866 (8th Cir. 2006) (holding that closure of courtroom during testimony of allegedly abused children violated defendant's Sixth Amendment right to public trial).

43. *Globe Newspaper Co. v Superior Court for the County of Norfolk*, 457 U.S. 596, 603 (1982).

Anonymity of Defendants

There are at least as strong restrictions precluding the anonymity of criminal defendants. The trial courts in southern and central Florida, for example, experimented with a system in which some cases involving defendants believed to be particularly dangerous were kept in a secret docket that was not made part of the public record. This practice was severely criticized by the court of appeal, which said that it violated the First Amendment right of the public, a right that extends to the docket sheets themselves.[44]

Anonymity of Jurors

Under the modern rule, a district court may empanel an anonymous jury in any case in which "the interests of justice so require."[45] The first reported use of an anonymous jury in federal court was in a 1977 trial.[46] Courts have warned that anonymous juries are a "drastic" measure.[47] Nevertheless, since 1977, "significant numbers of federal and state courts throughout the country have utilized the procedure to protect jurors, prevent jury tampering and limit media influence."[48] The court must mitigate the potential prejudicial effects of an anonymous jury by conducting a careful voir dire designed to uncover juror bias and provide the jurors with plausible, nonprejudicial reasons for their anonymity.

The traditional rule that criminal trials should be fully public so that justice can be seen to be done turns out to have accumulated some exceptions, but these are still limited. While post-9/11 pressure may spur further growth, at present, anonymity in any part of a criminal case remains a source of discomfort and as a result this growth will likely remain limited.

III. ANONYMITY IN CIVIL ACTIONS

Protection of anonymity is, in principle, significantly less in the context of U.S. private law than public law. Although it is true that a lawsuit invokes the state's power, and thus in some cases can be seen as a form of state action, the private lawsuit is ordinarily seen as something invoked by a private party, and based on private rights. As a result, constitutional protections designed to limit the state's power over the individual often do not apply, or apply in a more attenuated fashion.

---

44. See *United States v Valenti*, 987 F.2d 708, 715 (11th Cir. 1993) (holding that "dual-docketing system" or "sealed docket" violated the press and public's First Amendment right of access to criminal proceedings, and declaring it facially unconstitutional). See also *United States v Ochoa-Vasquez*, 428 F.3d 1015 (11thCir. 2005).

45. 28 U.S.C. § 1863(b) (7) (2008).

46. See *Ochoa-Vasquez*, 428 F.3d 1015, 1033–34 (11th Cir. 2005).

47. *United States v Ross*, 33 F.3d 1507 (11th. Cir. 1994).

48. *Ibid.*

We see this principle in action as regards plaintiffs, defendants, third parties, and also reports of decisions. Like the criminal law, the civil law begins with the presumption that all proceeding, evidence, and decisions will be public. However, in civil cases this presumption can be displaced for good cause somewhat more frequently than in the criminal arena, and nowhere more so than in state family court matters relating to adoption, divorce, or related issues.

Anonymity of Plaintiffs

The Federal Rules of Civil Procedure contain no provision contemplating fictitious or anonymous parties. Federal pleading presumes the disclosure of the names of adult parties, and the courts rarely allow anonymous (or pseudonymous) plaintiffs, except in special circumstances. Nevertheless, both Jane and Robert Doe and Roe appear with some frequency in the casebooks as plaintiffs, and more rarely as defendants. In all cases, however, proceeding without using one's true name requires leave of court.

On an application a court may permit a "John Doe" plaintiff if the party can show a substantial privacy right that outweighs the presumption of openness in judicial proceedings.[49] Among the factors weighing in the balance are the following:

- Whether plaintiff challenges a government activity
- Whether prosecution of the lawsuit would compel the plaintiffs to disclose very intimate information (thus, for example, the most famous pseudonymous U.S. court case, *Roe v. Wade*[50])
- Whether the plaintiff would be compelled to admit his intention to engage in illegal activity and therefore subject himself to criminal liability
- Whether plaintiff would be subjected to physical harm if identified
- What prejudice the defendant would suffer if plaintiff is permitted able to proceed anonymously[51]

A party's age is also a relevant factor. The Federal Rules contemplate a form of pseudonymity, as they permit a party making a filing to replace the name of a person known to be a minor with the minor's initials.[52] Actual anonymity is rarer, but it is possible with leave of court.[53] Countervailing factors against anonymity include whether the plaintiff has illegitimate ulterior motives, the extent of the public interest in knowing the identity given the subject matter,

49. See 5A Charles Alan Wright & Arthur R. Miller, Federal Practice and Procedure § 1321 (3d ed. 2004).

50. 410 U.S. 113 (1973).

51. See 5A Charles Alan Wright & Arthur R. Miller, Federal Practice and Procedure § 1321 (3d ed. 2004).

52. FED. R. CIV. P. 5.2(a) (3).

53. See 5A Charles Alan Wright & Arthur R. Miller, Federal Practice and Procedure § 1321 (3d ed. 2004)

or the status of the plaintiff as a public figure.[54] In addition, some states have legislated against so-called SLAPP (Strategic Lawsuits Against Public Participation) suits that may provide anonymous parties some protections against John-Doe-as-defendant suits that are actually designed to discover their identity.

Using Legal Process to Identify Defendants

Holders of rights in digital intellectual property have been particularly assiduous in seeking to use the U.S. court system to identify persons they believe to have infringed copyrights via online file-sharing. In a large number of recent cases, a rights holder has brought suit seeking to compel an intermediary, usually an ISP, to disclose the name of a customer whom the plaintiffs believe engaged in unlicensed file-sharing.

In the first wave of such cases, plaintiffs sought to invoke the Digital Millennium Copyright Act[55] (DMCA) to subpoena ISPs for the identities of alleged file-sharers. The DMCA offered copyright holders an expedited means of securing subpoenas directed against the information-holder. Subpoena practice under the DMCA is rapid, because the civil order does not require judicial approval. Warrants in a criminal investigation require that affidavits be submitted to a judge who must sign the order; routine civil discovery requires a series of time-consuming steps that give the subject actual notice and an opportunity to block the discovery by seeking a protective order from the court. In contrast, the DMCA allows the plaintiff to file a short-form request with the clerk of court and the subpoena automatically issues.[56] As a practical matter, the third-party subjects of these requests rarely have a chance to object before the information is disclosed. However, in a 2003 decision that has become the leading case, the D.C. Circuit held that this expedited method was only available in cases where the plaintiff alleged that the infringing material was stored on the ISP's own servers.[57]

Thus, when seeking to find the identities of parties sharing files via peer-to-peer networks, rights-holders must now file a lawsuit against "John Doe" defendants, then use ordinary court discovery procedures to learn their names. This is slower, more expensive, and ordinarily means that the third party will receive actual notice before the subpoena is enforced. Armed with this notice, the third parties can and have contested the issuance of the subpoena—although with rather mixed success.

---

54. *Ibid.*

55. Digital Millennium Copyright Act, Pub. L. No. 105–304, 112 Stat. 2860 (1998) (codified in scattered sections of 17 U.S.C.).

56. 17 U.S.C. § 512(h) (2008).

57. *Recording Indus. Ass'n of America, Inc. v Verizon Internet Servs.*, Inc., 351 F.3d 1229 (D.C. Cir. 2003).

Alleged file-sharers have not generally fared that well in their attempts to block court-ordered disclosure of their identities, but other parties in similar procedural postures have tended to fare much better. In particular, courts have tended to be careful to protect the rights of persons engaged in anonymous online First Amendment activities such as criticism of corporations and politicians. Many states now use some version of the so-called *Dendrite* principles:

> . . . when faced with an application by a plaintiff for expedited discovery seeking an order compelling an ISP to honor a subpoena and disclose the identity of anonymous Internet posters who are sued for allegedly violating the rights of individuals, corporations or businesses [, t]he trial court must consider and decide those applications by striking a balance between the well-established First Amendment right to speak anonymously, and 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.
>
> . . . 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 . . .
>
> 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 . . .
>
> 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.[58]

Courts faced with a disclosure request thus demand that plaintiffs provide something more substantial than a form recitation; armed with this

58. *Dendrite Int'l, Inc. v John Doe,* No. 3, et al., 342 N.J. Super. 134, 141–42 (App. Div. 2001).

information they seek to balance the relevant interests. As courts give substantial weight to First Amendment and privacy values, in cases about controversial speech (as opposed to file-sharing) they are proving to be far from a rubber-stamp for identity disclosure requests.

Even though copyright law is federal, California has made extra efforts to protect the interests of rights holders against anonymous file-sharers by, in 2005, making it a misdemeanor for anyone located in California to "knowingly electronically" disseminate all or most of a commercial recording or audiovisual work to more than ten other people "without disclosing his or her email address, and the title of the recording or audiovisual work . . . [while] . . . knowing that a particular recording or audiovisual work is commercial."[59]

Legal Process to Reveal the Identity of Third Parties

The situation regarding disclosures of identity by and about third parties is also complicated. U.S. civil cases begin with a presumption that the parties should be allowed wide-ranging discovery in order to get at the truth. Working against that presumption are a number of evidentiary privileges (e.g., doctor-patient), and some constitutional issues, including the First Amendment right to speak anonymously (discussed above).

The situation in state court is complex, not only because rules vary from state to state but also because the docket of state courts more commonly includes family law, adoption, and other matters where courts traditionally are more willing to view the private interest in privacy as outweighing the public interest in disclosure. Even in Florida, where a state constitutional provision mandates access to most public records[60] (it is indeed the "sunshine state" for matters of public record as well as weather), the family courts in particular are willing to seal records and protect the identity of parties, especially minors. Similarly, in family-related matters it is sometimes possible to get an order that protects the identity of third parties such as other family members from being disclosed.

Compared to courts hearing criminal cases, judicial tribunals hearing civil matters are significantly more willing to consider claims that parties or witnesses may have legitimate reasons to remain anonymous. Nevertheless, with the

59. Cal. Penal Code § 653aa (a) (West 2008).

60. Florida Constitution, Art. I, section 24(a) states that "Every person has the right to inspect or copy any public record made or received in connection with the official business of any public body, officer, or employee of the state, or persons acting on their behalf, except with respect to records exempted pursuant to this section or specifically made confidential by this Constitution. This section specifically includes the legislative, executive, and judicial branches of government and each agency or department created thereunder; counties, municipalities, and districts; and each constitutional officer, board, and commission, or entity created pursuant to law or this Constitution." The state legislature can create exceptions to this rule only by a two-thirds vote. *Ibid.* at sec. 24(c).

possible exception of the family courts, where a greater solicitude for privacy interests sometimes reigns, the presumption remains strong that plaintiffs and witnesses should be identified. As regards attempts to use the court's powers of compulsion to force third parties to reveal the identities of persons whom plaintiffs would make defendants, the law appears to be settling toward treating these discovery requests with significant solicitude for legitimate third-party rights (if, perhaps, not so much solicitude for unlicensed file-sharing). It is perhaps not yet completely clear where the balance will tilt, but it is increasingly clear that courts have no intention of becoming rubber stamps for anonymity-piercing requests.

Data about persons who are neither witnesses nor parties in civil litigation often emerges in responses to civil discovery requests or to government subpoena—and sometimes these groups are huge. Lawsuits against ISPs or search engines in which plaintiffs demand data about the behavior of large groups threaten the privacy and functional anonymity of tens of thousands, even millions, of users. (Users in these cases are not in the main anonymous to the ISPs or search engines, but are commonly functionally anonymous to the rest of the world.) Firms have demonstrated an inability to anonymize data sufficiently to foil reconstruction efforts.[61] Some courts have demonstrated solicitude to third-party privacy interests by limiting discovery requests or insisting on strong anonymization before release,[62] but the initial (and much-criticized) response elsewhere has been to dismiss privacy concerns as unwarranted.[63] At present it is unclear if legislation will be needed to define companies' and courts' duties in this area.

IV. ANONYMITY IN OTHER CITIZEN-GOVERNMENT RELATIONSHIPS

The right to anonymity in public (or lack thereof) becomes even less clear in the context of citizen-government relationships outside the courtroom and the criminal justice system. In spite of the strong constitutional protections for free speech and against unreasonable search and seizure discussed above, there are a number of circumstances in which citizens are required to identify themselves to the State beyond the obvious cases of citizens who seek government permits or government benefits such as pensions, disability benefits, welfare, or medical benefits. For example, all U.S. states other than North Dakota require voters to register in order to vote.[64] States with voting rolls

61. See Anita Ramasastry, FINDLAW, Privacy and Search Engine Data: *A Recent AOL Research Project Has Perilous Consequences for Subscribers*, http://technology.findlaw.com/articles/00006/010208.html.

62. See *Gonazales v Google*, 234 FRD 674 (ND Cal. 2006).

63. See *Viacom Intern. v Youtube*, 2008 WL 2627388 (July 2, 2008).

64. Lillie Coney, *A Call for Election Reform*, 7 J. L. & Soc. Challenges 183, 186 (2005).

treat them as publicly accessible records, usually including the voter's party identification. These records are "routinely shared with political parties, candidates and for non-election related purposes."[65] The anonymity of the vote itself is protected when exercised at a poll, but that guarantee of anonymity becomes less easy to police as voters in many states increasingly vote by mail in advance of election day.

The Lobbying Disclosure Act[66] requires that organizations or firms register their paid employees as lobbyists if they seek to influence most federal executive or legislative branch activities. However, these registration rules do not apply to citizens acting on their own. Many states also have rules requiring paid lobbyists to register, but as the *McIntyre* case holds, citizens retain a right of anonymity when engaged in unpaid political advocacy.

For every donor making (cumulative) donations of $200 or more, the Federal Election Campaign Act[67] (FECA) requires candidates for federal office to make their best efforts to collect and publicly disclose on a financial report the donor's name, address, occupation, and employer, as well as the date and amount of the contributions. Contribution information is reported quarterly to the Federal Election Commission, which publishes it online and makes it widely available. The Supreme Court upheld FECA's public disclosure provisions in *Buckley v. Valeo*,[68] a decision that remains controversial; critics argue that making donations public may chill contributions to potentially unpopular or controversial causes and may even invite retaliation by employers or others.[69]

Most states also require disclosure of political donations, although the details vary widely.[70] Many cities and counties also have their own local rules.[71]

---

65. *Ibid.*,198.

66. Lobbying Disclosure Act of 1995, Pub. L. No. 104–65, 109 Stat. 691 (1995), *codified at* 2 U.S.C. §§ 1601–1612 (2008), as amended by Honest Leadership and Open Government Act, Pub. L. No. 110–81, 121 Stat. 735 (2007).

67. Federal Election Campaign Act, Pub. L. No. 92–225, 86 Stat. 3 (1972) (codified as amended at 2 U.S.C. § 431 (2008)).

68. *Buckley* (n. 21).

69. For a critique, see, e.g., William McGeveran, "McIntyre's Checkbook: Privacy Costs of Political Contribution Disclosure," *U. Pa. J. Const. L.* 6 (2003): 1.

70. "States generally did not adopt legislative conflict of interest or ethics laws until much later than the federal government did. New York, considered an 'early leader' in ethics regulation, adopted its statute in 1909 and did not enact comprehensive state ethics legislation until 1954. Other states began comprehensive ethics reform in the 1970s." Rebecca L. Anderson, "The Rules in the Owners' Box: Lobbying Regulations in State Legislatures," *Urban Lawyer* 40 (2008): 375, 379.

71. A 2002 survey by the National Civic League found that 135 city and county governments in eighteen states and the District of Columbia had adopted their own campaign finance laws. *National Civic League, Local Campaign Finance Reform* (Feb. 2002).

In addition, the U.S. Constitution requires a decennial census.[72] Participation is formally mandatory,[73] although there appear to have been few if any prosecutions for failing to participate since 1976 when Congress reduced the maximum penalty from 60 days imprisonment to a $100 fine. The primary purpose of the census is to enumerate populations for the purpose of congressional apportionment, but the government also uses it to collect demographic and statistical information. These data are supposed to be anonymized before being released, but questions have been raised as to whether census tracts are now so small, and the information collected of such great granularity, that it would be possible to de-anonymize the data.

Law and tradition say that personally identifiable information disclosed in the census should not be used for any other government function. These rules were skirted, and perhaps breached, both during WWII and in the aftermath of 9/11. Amidst allegations that it may have disclosed even more, the Census Bureau admitted that after 9/11 it provided "specially tabulated population statistics" on Arab Americans to the Department of Homeland Security, including ZIP-code-level breakdowns of Arab-American populations, sorted by country of origin. The Census Bureau also admits to providing a similar "compilation" about Japanese Americans during World War II.[74]

The extent to which reported census data is anonymous is in any case open to serious question. One study demonstrated that public so-called anonymous data from the 1990 census permitted 87 percent of the U.S. population to be uniquely identified by just three data: their five-digit ZIP code, their gender, and their date of birth.[75]

Although their right to anonymity is protected in the context of political and religious rights, U.S. citizens are required to identify themselves in a wide range of other encounters with their government. Identification is required for one to receive almost any recurring government benefit, to vote, to make substantial campaign contributions (but not independent expenditures), and to lobby for pay. The decennial census is mandatory, and although the census is supposed to safeguard personal data, there is ground to fear both intentional and unintentional release of personally identifiable information.

---

72. U.S. CONST. art I, sec 2, cl. 3.

73. Failure to participate is grounds for a $100 fine; willfully giving false information can cost $500. 13 U.S.C. § 221 (2008).

74. Lynette Clemetson, "Homeland Security Given Data on Arab-Americans," *New York Times July* 30, 2004, http://query.nytimes.com/gst/fullpage.html?res=9d02e4db113df933a05754c0a9629c8b63.

75. Latanya Sweeney, "Uniqueness of Simple Demographics in the U.S. Population," (2001), http://privacy.cs.cmu.edu/dataprivacy/papers/LIDAP-WP4abstract.html.

V. DISCLOSURE OF IDENTITY REQUIREMENTS IN DAILY LIFE

Beyond the realms of criminal investigations and civil litigation, U.S. law does not at present have a coherent approach to disclosure of identity requirements—which is consistent with its inconsistent and patchwork approach to privacy. Certain regulated industries are required to ascertain and disclose the identity of customers. In general, however, the law imposes few constraints on identity collection and disclosure in either the context of private economic relations or non-economic relations.

Regulated Industries

Certain, primarily financial, regulated industries are subject to rules requiring them to request and in many cases verify their customers' addresses. Many other firms do so by choice, and there is rarely any legal rule preventing it.

Banks and other financial intermediaries are subject to "know your customer" rules designed to deter money laundering and facilitate its prosecution.[76] Any financial transaction involving $10,000 may trigger a reporting requirement in not just the financial industry but also a range of other businesses. Depending on the circumstances, however, the sending of much smaller sums of money by wire—even as low as $250—may trigger reporting requirements. Furthermore, any income-generating activity requires disclosure of a social security number. All active and most passive income-generating activities also trigger tax-reporting requirements on the payer.

Under the Patriot Act, banks and other financial firms are also responsible for ensuring that their customers are not on any lists of suspected terrorists or money launderers maintained by the federal government, such as the Office of Foreign Assets Control's Specially Designated Nationals list.[77] This list contains thousands of entries and is updated at least monthly. In order to perform this check, firms must know the customer's real identity.

Protection of Identity Requirements

A very small number of federal statutes impose limits upon the sharing of private transactional data collected by persons not classed as professionals.

---

76. For example, the Bank Secrecy Act of 1970, Pub. L. No. 91-508 (as amended, codified at 12 U.S.C. §§ 1829(b), 1951–1959 (2000), and 31 U.S.C. §§ 5311–5330 (2002)), requires most financial institutions to report suspicious transactions. See, e.g., 31 U.S.C. § 5318(g). The Bank Secrecy Act and other post-9/11 laws and regulations also require financial institutions to make a "due diligence" effort to identify their customers.

77. The list is available from the U.S. Dept. of Treasury, Office of Foreign Assets Control, SDN List, http://www.ustreas.gov/offices/enforcement/ofac/sdn/index.shtml.

The most important is the Fair Credit Reporting Act.[78] In addition to imposing rules designed to make credit reports more accurate, the statute also contains rules prohibiting credit bureaus from making certain accurate statements about aged peccadilloes, although this restriction does not apply to reports requested for larger transactions.[79]

There are few statutory federal privacy-oriented restrictions on the sale of commercial data. The Cable Communications Policy Act of 1984 forbids cable operators and third parties from monitoring the viewing habits of subscribers. Cable operators must tell subscribers what personal data is collected and, in general, must not disclose it to anyone without the subscriber's consent.[80] The "Bork Bill," formally known as the Video Privacy Protection Act, also prohibits most releases of customers' video rental data.[81]

As noted above, both state and federal law contain a number of evidentiary privileges that protect priests, lawyers, doctors, and some others from having to disclose the identity of penitents or clients, although it should be noted that some evidentiary privileges, and especially those available to psychiatrists and other therapists, vary by state. The federal Health Insurance Portability and Accountability Act (HIPAA)[82] imposes restrictions on data-sharing by health care providers, health care plans, and health care "clearinghouses" (processors of data created by another), but to the extent that a patient's anonymity enjoys protection, the primary protections lie in medical ethics and evidentiary privileges rather than anything in HIPAA.

Anonymous Online Communication

U.S. law imposes no direct bar to the running and use of anonymous remailers. This in effect creates opportunities to enjoy anonymous speech in the online context. Arguments have been advanced that a remailer operator might be subject to some sort of contributory liability for bad acts committed by arms-length users, but at present there is no support in the case law for this assertion.

However, U.S. law does impose significant restrictions on the export of encryption technology and also on the provision of technical assistance relating

78. 15 U.S.C. §§ 1681–1681s. (2008).

79. See *ibid.* § 1681(c).

80. See 15 U.S.C. § 551.

81. 102 Stat. 3195 (1988) (codified as 18 U.S.C. § 2710 (1999)). The act allows videotape rental providers to release customer names and addresses to third parties so long as there is no disclosure of titles purchased or rented. Customers can, however, be grouped into categories according to the type of film they rent. See *ibid.* § 2710(b)(2)(D)(ii).

82. Health Insurance Portability and Accountability Act ("HIPAA") of 1996, Pub. L. No. 104-191, § 261, 110 Stat. 1936 (1996), codified at 42 U.S.C. § 1320d (2000) et seq.

to the use of such technology. The U.S. export regime has become somewhat more liberal than in the past, with DES exports now decontrolled, and the export of substantially stronger encryption allowed for selected industries such as banks. Despite the occasional trial balloon,[83] the United States does not have mandatory key escrow to enable the state to ensure it has the means to unlock encrypted digital communications without great effort.

Anonymous online communication therefore remains legal in most cases, and indeed as noted enjoys substantial legal protection. But the practical obstacles to anonymous communication remain substantial, especially online. The most prevalent obstacle is that most home and office Internet users have IP numbers that are either fixed or, if variable, are almost certainly logged by employers or ISPs. These numbers thus can easily be traced and linked back to the user. In addition, every internet-capable device has a unique and consistent MAC number, which is emitted by machines using the IPv6 protocol unless altered by a technically savvy user.

Moreover, purely anonymous transactions with untraceable e-cash have yet to make it off the drawing board in any meaningful way. As noted above, cash transactions of any size are likely to trigger reporting requirements. There is thus, in practice, little scope for licit anonymous commerce in the United States beyond small cash transactions.

On the other hand, some areas have free publicly accessible wifi. Public libraries in many communities offer free public internet access, although frequently they require patrons to display a library card or other identification in order to use a machine.

National ID Cards

A particularly hot issue in the American context has been the call for national identity cards.[84] The United States does not currently have national ID cards as such. Every state, however, licenses drivers, and because cars are a practical necessity for most adults living outside the largest cities, the state-issued drivers licenses are gradually becoming de facto national ID cards. This status was semi-formalized in the REAL ID Act of 2005,[85] in which the federal government sought to impose standards on states relating to what information they must include on licenses or other ID (and in what format), what documentation states must demand before issuing the credential, and how states should share data. Implementation of REAL ID has been controversial, with some states vowing not to participate. The federal government has delayed the effective date of some

83. See A. Michael Froomkin, "It Came From Planet Clipper," *University of Chicago Legal Forum* 15 (1996).

84. Ian Kerr, *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society* (New York: Oxford University Press, 2009), Chapter 14.

85. REAL ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 231 (2005).

of the most controversial aspects, and repeal or modification of the statute remains possible.

Anonymity in Public

The baseline rule in the United States with regard to anonymity in public is that there is no right to privacy in public places with respect to anything open to public view or voluntarily revealed.[86] With the exception of certain government facilities, anyone may take photographs in public; state laws vary, however, as to the consent required for sound recordings. Thus, for example, a newspaper that published a photo of persons lining up for unemployment benefits was not liable to an identifiable complainant who claimed the photo violated his privacy.[87] There are some limits on the publication of photographs for advertising and publicity purposes, although these do not apply to the reporting of news. Indeed, the only significant constraints on photographic news reporting are (1) some state anti-paparazzi statutes that impose limits on photography from public areas of activities taking place on private property[88] and (2) state law rules restricting intrusion into private areas.

Thus, in *Shulman v. Group W Productions*, the California Supreme Court allowed two people injured in a car accident to sue a TV station for the tort of intrusion based on a cameraman's recording of emergency roadside care given in a rescue helicopter, holding that there was no right of privacy regarding the images at the accident scene prior to being moved to the helicopter, but there was one inside it even if the patients could be overheard.[89] The court also held that there was a triable issue as to whether "by placing a microphone" on one of the victims "amplifying and recording what she said and heard, defendants may have listened in on conversations the parties could reasonably have expected to be private."[90]

---

86. States make an exception to this rule for so-called upskirt photos. To the extent that they even bother to try to explain it, cases suggest that the general rule may not apply to an indecent and vulgar intrusion that would be embarrassing to an ordinary person of reasonable sensitivity. See Restatement (Second) of Torts § 652B (1977); Jeffrey F. Ghent, Annotation, *Waiver or loss of right to privacy; Matters in public view; photographs*, 57 A.L.R. 3d 16 at § 8 (1974 & 2008 supp.).

87. *Cefalu v Globe Newspaper Co.*, 391 N.E.2d 935 (Mass. App. Ct. 1979).

88. Cal. Civ. Code § 1708.8(b), (e) (West 2008), perhaps the model, limits the offense to invasions offensive to a reasonable person, where there was already a reasonable expectation of privacy. See *generally* Andrew D. Morton, "Much Ado About Newsgathering: Personal Privacy, Law Enforcement, and the Law of Unintended Consequences for Anti-Paparazzi Legislation," *U. Pa. L.* Rev. 147 (1999): 1435.

89. 955 P.2d 469, 486–490 (Cal. 1998).

90. *Ibid.*, 491.

SUMMARY AND CONCLUSION

That the U.S. approach to the regulation of anonymity seems patchwork should not surprise anyone prepared to look past the leading Supreme Court cases. Despite the Court's repeated, ringing endorsements of the role of anonymous advocacy and proselytizing, protection of anonymity is of a piece with the overall protection of privacy in the United States, which is to say that there is no fundamental consensus or coherent national policy. The mish-mash is less the result of neglect than the product of a clash between conflicting strongly felt policies and imperatives interwoven with a federal structure. As a result, at present U.S. policy toward anonymity remains primarily situational, largely reactive, and is slowly evolving.

On the one hand, the courts tend to interpret the protections of speech and assembly and other fundamental rights in ways friendly to anonymity as against the government, and friendly to privacy from government more generally. On the other hand, the courts remain open to governmental demands for identification when the grounds seem sufficiently compelling. And compelling demands have come from varied sources: It may be constitutional norms relating to open trials or the legislature seeking to regulate campaign finance or voter registration; it may be the police investigating a possible crime armed with probable cause; it could be the intelligence services (and police) seeking access to communications in the hunt for terrorists and criminals; it may be businesses seeking to use the court's power to compulsion to force others to divulge the identity of file-sharers. In each of these cases the countervailing case lacked sufficient force to carry the day—although the campaign finance issue in particular remains controversial.

In other cases, such as the attempt by private parties to use the courts to get the identities of political and corporate critics, the demands have seemed insufficiently compelling, and anonymity prevailed. Although it can be overcome for sufficiently good cause, the background norm that the government should not be able to compel individuals to reveal their identity without real cause retains real force.

The picture is quite different when two legitimate private interests come into conflict. Then the capitalist presumption of free contract (or open season) tends to be the background norm. Legislatures and regulators seem reluctant to intervene to protect privacy, much less anonymity, from what are seen as market forces. Thus the government imposes few if any legal obstacles to the domestic use of privacy-enhancing technology such as encryption and remailers. Conversely, and excepting a few special cases such as the Video Privacy Protection Act, the law generally requires little more than truth-in-advertising for most privacy-destroying technologies—firms must not lie about what they are doing

because that would violate general consumer protection law. Absent actual lies and misleading statements, even duties to disclose tend to exist only in highly regulated industries such as the financial sector.

But as surveillance cameras proliferate and facial recognition software improves, it is increasingly hard to be lost in a crowd in real life; as virtual tracking tools improve, the same is even more quickly becoming true online. In the future it is likely to matter little who operates the recorders, as data is easily stored and sold to both private and public buyers. This and other technological changes suggest a possible convergence between de facto public and private sector anonymity destruction—a change that will necessitate a policy debate that has hardly yet begun.