DRAFT 1.05a

Forced Sharing of Patient-Controlled Health Records

A. Michael Froomkin[†]
Professor, University of Miami School of Law
Project HealthDesign ELSI Group

1 Introduction & Summary

The creation of any data repository inevitably excites the attention of third parties who believe they have a use for the information. There are, in principle, three methods by which third parties can get access to stored data, and PHR are no exception to the general rule: (1) by consent, either contractual or otherwise; (2) by compulsion, either legal or otherwise; (3) by trickery or theft. Access via trickery and theft are failure conditions of measures to secure data, and are more properly considered in the context of data security methods such as encryption and biometrics. Below we focus on the question of compelled access by third parties.

The focus is on legal compulsion, and on claims of privacy that may defend against the attempt to get access; thus, this section does not discuss the question of access via consent. Access via consent raises issues of competence to consent, and of informed consent, and should be considered in the broader context of those issues.[1] Similarly, this section does not discuss the difficult question of access by first responders for whom there is implicit consent such as the case of emergency medical treatment of an unconscious patient.

Talk to a lawyer about medical privacy, and today her mind turns immediately to the Health Insurance Portability and Accountability Act (HIPAA).[2] But HIPAA covers health

---

[1]Nor does this section consider the problem of contractual consent that is not freely bargained for. Even when the medical ethics checklist is satisfied there remain a number of significant impediments to true consent for disclosures of personal information, issues that the US legal system deals with notoriously poorly. Chief among these is the problem of standard form contracts, also known as "contracts of adhesion," in which consent while legally binding is nonetheless demanded in a take-it-or-leave-it manner that means it is not freely bargained for, and indeed may be little more than a formality.

[2]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.

care providers, health care plans, and health care "clearinghouses" (processors of data created by another).[3] A patient, even one who holds data created by her doctor, is none of these things, and thus HIPAA does not instruct us as to the privacy rules that apply to data held by the patient herself. The relevant rules thus must be sought elsewhere -- and are to be found in a hodgepodge of federal and (varying) state law. In many cases, personal health information is treated no differently from any other data; in a few cases special privileges may apply.

Keeping in mind that much is speculative as there have been few if any cases relating to patient-controlled health data, the following is the likely lay of the land: Three major distinctions shape the extent of third party access to patient-controlled health records: (1) who seeks access to the data, and for what purpose; (2) where the data are located; (3) whether the data are encrypted. In some cases, further distinctions may arise based on (4) the nature of the data, (5) who initially created the data, and (6) whether the data has been shared with anyone.

Demands for disclosure may come from the government directly (police, public health officials) or from private litigants. Where in the past these demands for health information have often been directed at third parties who held the data, the prospect of a centralized data repository -- a 'PHR on a stick' -- controlled by the patient promises to alter the calculus of risks and incentives. The patient's copy of the records are most likely to become targets of compelled disclosure if they are contain data that are unique and authoritative. Indeed, this is true even if many of the data are available elsewhere, so long as some relevant subset exists only in the patient's control. Furthermore, to the extent that the PHR on a stick is not only authoritative but comprehensive, it also becomes a more attractive target, a one-stop-shopping solution to those seeking data about the patient.

Patient-controlled data will not benefit from HIPAA protections, but data located on media in the patient's control (e.g. a USB drive, a PC, a specially created medical device) will in many cases be significantly better protected from compelled disclosure than information entrusted to any intermediary who is not part of the health care system subject to HIPAA. Encryption will provide little (legal) protection to lawful discovery requests in civil suits, but, in those cases in which expectations are relevant, will serve as evidence of a well-founded expectation of privacy. A more complicated set of facts arises when the data are located in a medium controlled by the patient's agent, such as an online data storage, or even a web-based health organizer. In those cases, the initial question is likely to be whether the data are protected from public view; if they are viewable by others who do not have some special duty of confidentiality, or some special relationship of trust and confidence, many courts will treat this as effecting a waiver of the privacy claim.

Seeking data directly from the patient may also alter the demand-response dynamic in more subtle ways. When third parties hold the data, there is almost always an issue as

---

[3]See Definitions of a Covered Entity, 45 C.F.R. 164.501

to whether the patient must be notified, may be notified, or -- in the case of certain official investigations -- may not be notified. In the middle case there is also the question of whether the holder of the data will exercise the option and actually notify the patient. If the patient has the data, then the issue of notice will often answer itself.[4]

Similarly, if the patient's copy of the data is not only authoritative but in some ways unique, then that data will only be accessible to third parties if they can find it, or at least find the patient and compel disclosure. In some cases these data gathering efforts may run up against the desire of the police not to tip off suspects, or the inability of governments and process-servers to locate the patient.

Last, but not least, placing the data in the patient's hands may have implications for the course of litigation. When faced with criminal defendants seeking to exclude evidence in post-search suppression motions, at least as regards patient-created data that have not yet been shared with medical professionals and possibly with other data also, there will be more cases in which the government will not be able to argue that the defendant waived all privacy interests by sharing the data with a third party. Further, to the extent that data were created by the patient's doctor, existing doctor-patient privileges should continue to apply. Similar considerations will come into play in the courts' treatment of suppression motions aimed at quashing civil discovery attempts.

Litigation costs are always an important driver of civil trials. To the limited extent that placing the data in the patient's hands removes deep-pocketed third parties from the litigation, and thus leaves the patient to her own to resources to defend against discovery requests, those patients trying to block disclosures may be limited by their lack of expertise and financial resources.

2 Disclosures Required By Law

Ordinary citizens -- those not covered by special regulatory schemes relating to, for example, employment as a police officer or firefighter -- may encounter demands for their personal medical records from either public officials or from private citizens armed with a court order. The public officials most likely to demand PHRs are law enforcement officials investigating a crime; more unusual cases include first responders to an epidemic or other

---

[4]The exceptions to this rule include: searches conducted in the absence of the subject via warrant or exigent circumstances; 'black bag' jobs in national security cases; and consent given by an authorized agent such as the subject's spouse, or even roommate. See United States v. D'Andrea, 2007 U.S. Dist. LEXIS 52558 (D. Mass. July 20, 2007) (Password-protected website did not create a reasonable expectation of privacy when the information was shared with another). But see Warshak v. United States, 2007 WL 1730094 (6th Cir. June 18, 2007).

emergency; extreme cases might include national security matters. Demands for disclosures from private sources are most likely to be discovery demands arising from lawsuits, e.g. negligence claims, and in various aspects of family-law-related matters in which the health or competence of persons may be called into question.

2.1 Law Enforcement Organizations

Although the issue is not free from doubt, police armed with judicial authority (e.g. a search warrant or a subpoena duces tecum) will in most but not all cases be able to access personal health records held by the patient as easily as if the information were in a doctor's hands, and in some cases considerably more so, since HIPAA will not apply. There are, however, significant exceptions, and some substantial uncertainty because the courts have yet to decide whether data that a patient is collecting for a doctor's use can benefit from the protection offered by laws designed to protect physician-patient relations.

US citizens enjoy a qualified right to privacy. This right has multiple sources and varies enormously with the circumstances. The United States Supreme Court has articulated a right of privacy based on various "penumbras" found in the United States Constitution. A few states also have a state constitutional right to privacy; most root some privacy protections in state statutes or state common law.

The federal constitutional right to privacy limits only the government's power, not that of private litigants to intrude upon an individual's privacy. The same is true of, for example, the Florida State Constitutional right to privacy.[5] In contrast, state law often creates various evidentiary privileges that may apply more broadly. The federal constitutional right to privacy is not absolute; unlike core Fourth and Fifth Amendment rights, the right to privacy yields to sufficiently weighty government interests. Furthermore, both constitutional and state-law based privacy rights are easily waived: in many states disclosure to any third parties who are not covered by legally recognized non-disclosure obligations (e.g. physicians or attorneys) will in almost every case constitute a waiver of a

---

[5]Fl. Const. Art. I, sec. 23 states,

> Right of privacy.--Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law.

There is no similar constitutional protection against private intrusion.

"In modern times, five states--Alaska, California, Florida, Hawaii, and Montana--have amended their constitutions to expressly protect the right of privacy." Jeffrey M. Shaman, *The Right Of Privacy In State Constitutional Law*, 37 RUTGERS L.J. 971, 974-75 (2006).

privacy claim.[6] In addition, records required to be kept for legal or regulatory purposes are outside the privilege.[7]

As a general matter, law enforcement organizations can acquire (and retain) personal records when executing a valid search warrant, or pursuant to a judicial or administrative subpoena. A search warrant is "[a]n order in writing, issued by a justice or other magistrate, in the name of the state, directed to a sheriff, constable, or other officer, authorizing him to search for and seize any property that constitutes evidence of the commission of a crime." No search warrant can be issued, however, until proper evidence is presented to a neutral magistrate specifically stating the place to be searched, the objects to be searched for, and the reason for the search. These requirements stem from the Fourth Amendment, which states that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Fourth Amendment protections apply to medical records just as they do to other papers and effects, but no more -- and thus absent some other legal protection, the subject of the criminal investigation's main protection is the right to challenge the validity of the search or seizure after the fact, or to seek to quash a subpoena if it was improperly issued.

Medical records, like other records, do not need to be turned over to law enforcement if they violate the Fifth Amendment privilege against self-incrimination. Even here, however, the scope of protection is narrower than it used to be, and much narrower than the protection against compelled replies to questions: that the documents are incriminating is no defense against a production order -- that is, after all, why the police want them. Instead, the Fifth Amendment privilege applies to pre-existing documents only if the act of turning them over would "testimonial" -- i.e. itself incriminating in that it would authenticate the records or tie the owner to them in some fashion.[8]

---

[6]See, e.g., Braswell v. United States, 487 U.S. 99, 109-10 (1988) (holding that a custodian of corporate records may not withhold them on the grounds that such production will incriminate him in violation of the Fifth Amendment); Andresen v. Maryland, 427 U.S. 463, 472-73 (1976) (holding that a legal search of the petitioner's office resulting in the seizure of voluntarily recorded business records authenticated by a prosecution witness was not a violation of the Fifth Amendment).

[7]Shapiro v. United States, 335 U.S. 1 (1948).

[8]See United States v. Doe, 465 U.S. 605, 613-14 (1984) (finding that the act of producing the documents at issue would involve testimonial self-incrimination, and that requiring such production therefore violated the Fifth Amendment); Fisher v. United States, 425 U.S. 391, 398-99 (1976) (holding that requiring relinquishment of the documents at issue was not a Fifth Amendment violation because no testimonial incrimination was compelled); see also Doe, 465 U.S. at 618 (O'Connor, J., concurring) (contending that "the

This relatively limited level of protection is the result of a long evolution away from a far more protective standard. More than a century ago, in Boyd v. United States,[9] the Supreme Court stated that private papers are an owner's "dearest property."[10] Relying on both the Fourth and Fifth Amendments, in 1886 the Court held that allowing the state to compel production of that property would be "abhorrent to the instincts" of an American and "contrary to the principles of a free government."[11] Only thirty years ago, in Bellis v. United States,[12] the Supreme Court reemphasized that the Fifth Amendment protects "'a private inner sanctum of individual feeling and thought'--an inner sanctum which necessarily includes an individual's papers and effects to the extent that the privilege bars their compulsory production and authentication."[13] Nevertheless, the rule found "abhorrent" in 1886 is now practically the law.[14] Thus, even in Florida where the right to privacy is explicitly mentioned both in the state constitution and in statutes,[15] the Florida Supreme Court has said that the state may justify encroachment of that right if it demonstrates a compelling state interest and that the state has used the least intrusive means to accomplish its goal.[16] And a compelling state interest exists upon a showing that the materials contain information relevant to an ongoing criminal investigation.[17]

The Supreme Court's narrowing interpretations notwithstanding, *Boyd* may not be completely dead. Some courts have suggested, usually in dicta, that *Boyd* has a residual

---

Fifth Amendment provides absolutely no protection for the contents of private papers of any kind").

[9]116 U.S. 616 (1886).

[10]Id. at 627-28.

[11] Id. at 632.

[12]417 U.S. 85 (1974).

[13]Id. at 91 (quoting Couch v. United States, 409 U.S. 322, 327 (1973)).

[14] See Samuel A. Alito, Jr., *Documents and the Privilege Against Self-Incrimination*, 48 U. PITT. L. REV. 27, 29 (1986) (examining the framework then used by the Supreme Court in applying the Fifth Amendment privilege against self-incrimination to compulsory process for documents).

[15]Art. I, § 23, Fla. Const.; cf. Hunter v. State, 639 So.2d 72 (Fla. 5th DCA), rev. denied, 649 So.2d 233 (Fla.1994).

[16]Shaktman v. State, 553 So.2d 148 (Fla.1989).

[17]See State v. Rivers, 787 So.2d 952, 953 (Fla. 2d DCA 2001).

vitality for nonbusiness, nonfinancial, private papers and documents that are kept in the home, if only because the Supreme Court has yet to compel production of such a document.[18] To whatever extent that there remains a constitutional prohibition against the compelled production of diaries, this protection might also extend to the compelled production of stored medical information, especially medical information collected by the subject herself, which is little more than a medical diary.

Even medical records are not protected by the constitution, there are a number of statutory and common-law rules that might prevent the compelled disclosure of PHR held by the patient. Chief among these are evidentiary rules such as the physician-patient and psychiatrist privileges.

State law privilege. The physician-patient privilege originates from state statutes, as it has no common law basis. Legislatures enact the privilege in order that patients will disclose the full details of their conditions to their doctors without fear that the doctor may be forced to release anything embarrassing, humiliating or incriminatory. The privilege blocks both oral testimony as to information obtained in the course of treatment, and also the disclosure of records concerning the patient's treatment kept by the physician or by the hospital from being disclosed without the patient's consent.

In 1828 New York became the first state to adopt a physician-patient evidentiary privilege, a policy later adopted by many other states. As one of the leading cases summarizes it,

> In its current form, the privilege prohibits disclosure of any information acquired by a physician "in attending a patient in a professional capacity, and which was necessary to enable him to act in that capacity." The privilege applies not only to information communicated orally by the patient, but also to "information obtained from observation of the patient's appearance and symptoms, unless the facts observed would be obvious to laymen."[19]

The privilege is not, however, absolute. Courts have carved out exceptions for child custody conflicts, and for other non-criminal matters where the state's interest in doing justice is said to outweigh the patient's privacy interest Other courts have found an exception for objective, nondiagnostic, or "observational" information.[20] The privilege belongs to the patient, not the doctor, but it can be waived -- and is held to be waived by plaintiffs in personal injury cases, as they are deemed to have waived the privilege by bringing the suit and making their physical condition an issue.

---

[18] See LAFAVE, ISRAEL & KING, CRIMINAL PROCEDURE (2d ed.) § 8.12(g).

[19] Dillenbeck v. Hess, 73 N.Y.2d 278, 539 N.Y.S.2d 707 (1989).

[20] 10 A.L.R.4th 552 at § 2[a].

Federal. There is no federal physician-patient privilege. (Some federal statutes even authorize subpoenas in terms that would override the HIPAA regulations,[21] had those applied.) There is, however, a federal evidentiary privilege protecting psychotherapist-patient confidences.[22] Federal courts will follow the state rules in many, but not all, cases.[23] In those cases in which purely federal law applies, Federal Rule of Evidence 501 authorizes courts to create new common law evidentiary privileges,[24] but this is not a common course. Thus, in general, federal courts will mimic state courts where state law applies, but will grant few if any relevant evidentiary privileges outside the statutory psychiatrist-patient privilege.

Applicability of privileges. Ordinarily these privileges, which belong to the patient, are asserted in order to block a doctor or therapist from releasing medical information about the patient. In the case of patient-held PHR, however, a threshold issue is whether the privileges are even relevant, as we are concerned here with data that are not now and may never have been in the medic's control.

Although the two issues are closely related, there is a potentially relevant distinction between (1) data created by the physician and given to the patient and (2) data created by the patient herself with the expectation that it will be given to the physician at a later date. The first case is slightly more straightforward than the second.

---

[21]See, e.g., 18 U.S.C. § 3486; In re Subpoena Duces Tecum, 228 F.3d 341 (4th Cir.2000).

[22]See Jaffee v. Redmond, 518 U.S. 1 (1996).

[23]Federal Rule of Evidence 501 states,

> Except as otherwise required by the Constitution of the United States or provided by Act of Congress or in rules prescribed by the Supreme Court pursuant to statutory authority, the privilege of a witness, person, government, State, or political subdivision thereof shall be governed by the principles of the common law as they may be interpreted by the courts of the United States in the light of reason and experience. However, in civil actions and proceedings, with respect to an element of a claim or defense as to which State law supplies the rule of decision, the privilege of a witness, person, government, State, or political subdivision thereof shall be determined in accordance with State law.

[24]Cf. Northwestern Memorial Hosp. v. Ashcroft, 362 F.3d 923 (CA7 2004) (per Posner, J.) (discussing, but not deciding, creation of new federal common law privilege in context of demand for records of partial birth abortions).

It would be perverse in the extreme to apply a less protective standard to medical records protected by the patient's evidentiary privilege when they are in a doctor's or hospital's hands simply because the patient had chosen to hold copies of the records herself. The privilege, after all, exists to encourage patients to seek medical care and to be frank with their doctors. In addition, a number of state and federal laws, not least HIPAA, require hospitals and doctors to give patients copies of their medical records on demand. To reduce the protection attaching to those records because the patient exercises her right to see and hold those records would undermine the policy underlying both the privilege and the open-records policy.[25] I have found no directly relevant caselaw on this subject, but am nonetheless confident that courts facing situations relating to records in which the physician-patient evidentiary privilege would have applied had the records remained with a doctor or hospital will have little difficulty extending that privilege to records in the patient's own hands.

That said, it bears emphasis that the key principle here is that the extent to which the evidentiary privilege applies is likely to be *the same* as that applied had the data remained in the doctor's hands, not a greater privilege, and that the strength of this privilege varies from state to state. In some states, for example, courts have held that while some "communications" from the patient to the physician, or evidence that the patient might be suffering from an "embarrassing" disease, may be shielded by the physician-patient privilege, other so-called nondiagnostic or purely "observational," unhumiliating information in a patient's records is available for discovery and disclosure.[26]

The case of records created by the patient but not yet shared with a doctor is slightly less straightforward, and outcomes risk being somewhat fact-specific. While the policy considerations described above will come into play, courts likely will seek evidence that the data genuinely were created in order to be given to a physician; evidence of a course of conduct in which the patient routinely gives a copy of the information to a caregiver will go far to satisfying this demand. It is possible, however, that some courts might distinguish between data from a blood pressure or blood sugar recorder automatically created and stored for transmittal as opposed to, for example, a 'health diary' in which the patient recorded her moods and thoughts. (In addition, the residual *Boyd* rule, described above, might apply to the health diary.)

2.2 Other officials

---

[25]See, .e.g., Newman v. Blom, 249 Iowa 836, 89 NW2d 349 (1958), in which the court noted that the policy of the state was to encourage full disclosure and discussion between the patient and the physician of any information needed by the physician in the treatment and care of the patient, and that, in order to facilitate such policy, the statute should be liberally construed.

[26]See *Exemption from Privilege of Nondiagnostic or Purely "Observational" Information in Records*, 10 A.L.R.4th 552 at § 13.

The Supreme Court has held that even in the absence of emergencies persons can be forced to perform nontestimonial acts such as giving handwriting samples,[27] voice samples,[28] and blood samples.[29] None of these precedents, however, apply to stored records. Exigencies, however, often motivate different rules. First responders, officials trying to control a public health emergency, and officials investigating what they term threats to national security all enjoy additional powers beyond those ordinarily available to law enforcement.

In routine public health investigations, if a person refuses to be tested or provide critical information, and the investigators think they might be infected with a dangerous communicable disease, the ordinary response is to treat them as if they were infected, thus avoiding the legal issues surrounding forced disclosure. Thus, it is up to the person either to submit to tests or to provide evidence that they are not infected, which may include enforced isolation during the infectious period; for most infectious diseases a sufficient number of people choose to cooperate to allow health officials to build a model of disease vector.[30] As a result, the issue of stored records rarely if ever arises.

There is, fortunately, no legal precedent regarding responses to bioterrorism. Responding agencies have the authority to conduct administrative searches and to issue subpoenas. Anyone failing to respond to these orders can be fined, or subjected to additional sanctions including incarceration for contempt.

As regards national-security cases involving agents of a foreign power, the federal government has the power to acquire relevant data by means of surreptitious copying, including "black bag" jobs -- breaking and entering. Whether the government claims similar powers regarding US citizens in general, and how easily it classifies US citizens as agents of a foreign power for these purposes is unknown, but is currently the subject of litigation.

2.3 Discovery in Civil Cases

Litigants in civil law suits frequently seek to acquire medical information about other parties to the case. For example, employers may seek medical data to prove an employee was ill and perhaps negligent. Employees may seek information about co-workers in order to support a claim about a hazardous workplace. Parties to divorce or custody cases may seek medical information about another in order to demonstrate their unfitness as parents.

---

[27]See Gilbert v. California, 388 U.S. 263, 266-67 (1967).

[28]See United States v. Wade, 388 U.S. 218, 222- 23 (1967).

[29]See Schmerber v. California, 384 U.S. 757, 767 (1966).

[30]See generally http://biotech.law.lsu.edu/cphl/Models/gon/index.htm.

Divorced spouses may seek information about their non-custodial child in an attempt to prove abuse and thus gain custody.

The possibilities are legion. So too, unfortunately, are the various state-law responses to these myriad situations. The key point for present purposes, however, is simple: in almost all civil discovery cases the location of the data should not alter legal outcomes. The major potential exceptions are the ones discussed above in § 2.2: the application of medical privilege may be subject to an additional hurdle in some cases if courts were to determine that some classes of patient-created data were not covered by it.

2.4 Minors and (Alleged) Incompetents

As a general matter, parents of under-age unemancipated minors have a right to full medical information about their children. (There are some state laws shield laws protecting minors in special cases.) One imagines that doctors and hospitals arranging to have a minor control over her PHR will get the appropriate parental consents, agreements which should address the issue of parental access. Parents seeking access in the face of an agreement not to seek it will probably require a court order, which may not always be forthcoming.

A much more difficult set of question relates to adult persons (or emancipated minors) who may not be fully competent. There is already considerable case law regarding the care of alleged Alzheimer patients for example. Courts tend to be very solicitous of the rights and autonomy of adults threatened with a finding of lack of competency, and will not lightly force them to turn over medical records to those seeking to have them declared incompetent.[31]

3 A Brief Note on the Role of Encryption

Encryption is part of the larger questions of security and authentication, but as a privacy-enhancing technology it does present special problems for compelled third-party access if the holder of the data is unwilling to comply with a court order.

In family law cases particularly, the patient's use of encryption may pose a substantial obstacle to accessing the records if there are no other copies and no provision for "key escrow"[32] -- a back-door access to the encryption key. Parents may be less willing

---

[31]See, e.g., In re Rosa B.-S., 767 N.Y.S.2d 33 (N.Y.A.D. 2 Dept.,2003) (holding that although a guardianship proceeding places the alleged incapacitated person's medical and mental condition in controversy, he or she does not waive the doctor-patient privilege unless he or she has affirmatively placed his or her medical condition in issue).

[32]See generally Part II of A. Michael Froomkin, *It Came From Planet Clipper: The Battle Over Cryptographic Key "Escrow"*, 1996 U. CHI. L. FORUM 15, available online

to have courts apply sanctions to children who refuse to decrypt their data; incompetent persons may be genuinely unable to do so if they have forgotten their passwords or lost a necessary token, and no amount of court sanction may be able to change that.

There is little doubt that ordinarily a party in a civil suit holding otherwise discoverable information can be ordered to decrypt it for the requestor's use. But it is less clear whether the same is true either in criminal cases, or in civil cases in which the recipient of a discovery request seeks to quash on Fifth Amendment grounds. There is no relevant case law or legislation and academic authorities strenuously disagree.[33]

---

http://www.law.miami.edu/~froomkin/articles/planet_clipper.htm

[33]Compare A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip and the Constitution*, 143 U. PENN. L. REV. 709 (1995)), available online www.law.miami.edu/~froomkin/articles/clipper.htm (arguing order would violate Fifth Amendment unless subject were granted full immunity), *with* Orin Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?*, 33 CONN. L. REV. 503 (2001) (arguing that disclosure orders will often be constitutional without immunity grants).