

# Privacy and Fictitious Contracts

David A. Anderson\*

For too long, the law treated privacy as a binary system: matters were either private—and thus protected—or public and unprotected. The Second Restatement of Torts, for example, said that the right of privacy extends “only to publicity given to matters concerning the private, as distinguished from the public, life of the individual.”<sup>1</sup> Thus, it seemed clear to the drafters that there can be no liability for disclosing matters of public record, that it is an invasion of privacy to disclose records that are not open to public inspection, and that “there is no liability when the defendant merely gives further publicity to information about the plaintiff that is already public.”<sup>2</sup>

But of course public and private have never been that clearly cabined, and they certainly are not today. Your medical details are available not only to your physician, but also to the network of medical-service providers and insurance companies with whom you authorized the physician to share them when you signed the check-in form. Your sexual peccadilloes are known to your lover and, quite possibly, to his or her therapist and other confidants, and if you are especially unlucky, to visitors of [dontdatethis.com](http://dontdatethis.com) or its online cousins. The operator of the search engine you use, and the customers it sells its data to, know what subjects you are interested in, and Amazon likely knows what you like to read. Whom you telephone or email overseas may well be known to your government.

The most salutary development in privacy law in the past generation has been the courts’ gradual recognition that privacy must be protected even when it is not complete. The Supreme Court recognized this when it held that FBI rap sheets could be private, for purposes of the Freedom of Information Act, even though they consisted entirely of public record information.<sup>3</sup> Those seeking the information argued for the Restatement view of privacy: that anything in a public record cannot be private. The Court rejected this as “a cramped notion of personal privacy,”<sup>4</sup> noting that “[i]n an organized society, there are few facts that are not at one time or another divulged to another.”<sup>5</sup> The protection accorded privacy, therefore, must depend not on some bright line between public and private, but on “the degree of dissemination of the allegedly private fact and the extent to which

---

\* Fred and Emily Wulff Centennial Chair in Law, University of Texas School of Law.

1. RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (1977).

2. *Id.*

3. *U.S. Dep’t of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 780 (1989).

4. *Id.* at 763.

5. *Id.*

the passage of time rendered it private.”<sup>6</sup> With respect to criminal histories, “[p]lainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.”<sup>7</sup>

The California Supreme Court has been the leader in implementing this more realistic understanding of privacy in tort law. For example, that court held that a tort action for invasion of privacy would lie even if the plaintiff had no expectation of complete privacy. In a workplace, a television reporter posing as a colleague surreptitiously recorded and broadcasted conversations with a worker. The reporter argued that the conversations were not private because they could be overheard by other coworkers. But the court held that even if the plaintiff had no protectable expectation that his conversations would not be overheard, the law could still protect his expectation that they would not be recorded and broadcast to the world.<sup>8</sup>

In another case, the California Supreme Court held that a person injured in a highway crash might have had no protection against being seen and heard by a crowd that gathered on the highway, but could maintain a privacy action against a television crew that recorded her anguished cries by means of a microphone attached to a rescue worker.<sup>9</sup>

These eminently sensible decisions mark a critical turn in the law of privacy. We do not need the law to protect us when we have managed to keep our secrets entirely private. We need help only when the information gets out. Increasingly, it gets out under compulsion—a legal compulsion, as occurs when the law requires us to provide information, or practical compulsion, as when we want to visit an online site or obtain a mortgage or use a credit card. Professor Richards identifies an important reason to expand our power to control the use of information that we have been compelled to surrender: our freedom to explore, develop, and test ideas may be curtailed if the electronic trail we leave in the course of our intellectual investigations is available to anyone who might want to follow it for any purpose.<sup>10</sup>

To my mind, “freedom of thought” and “intellectual privacy” are slightly extravagant names to give this interest. The first is rarely threatened by any means that law can address; thought survives when many other freedoms have been taken away. Intellectual privacy seems to be an umbrella for several more specific values: freedom to seek information, discuss ideas, and advance tentative conclusions without fear of repercussions. But if Professor Richards’ terms endow the matter with

---

6. *Id.*

7. *Id.* at 764.

8. *Sanders v. Am. Broad. Cos., Inc.*, 978 P.2d 67, 85 (Cal. 1999).

9. *Shulman v. Group W Prod., Inc.*, 955 P.2d 469, 497 (Cal. 1998).

10. Neil M. Richards, *Intellectual Privacy*, 87 TEXAS L. REV. 387, 403–04 (2008).

enough gravitas to be taken seriously as an independent reason for giving individuals more control over the trail created by their mental explorations, we ought not quibble about their lack of precision.

What matters is what we do to protect the freedom of intellectual inquiry. I agree that it is not a job for law alone. The example librarians have set is instructive. Without much help from law, the ethic of that profession has done much to protect our freedom to read.<sup>11</sup> I do not see many traces of that ethic in the online world, and that is a pity, because that is where the threats are coming from now. How librarians came to embrace their patrons' interests in intellectual freedom, and what might induce their online successors or counterparts to do so, are subjects that merit urgent attention.

So far as the law's role is concerned, there are two concerns that cry out for attention. Professor Richards identifies one of them: the law must recognize that electronic surveillance poses a different threat than ordinary searches and seizures.<sup>12</sup> The latter are restricted in the interest of protecting privacy and property interests, and to require the police to respect a modicum of citizen autonomy. Surveillance of communications needs to be restricted to protect freedom to speak and to receive information. As Professor Richards urges, the First Amendment, rather than the Fourth, is the more pertinent source of restriction.<sup>13</sup>

The other matter with which law should concern itself is one that Professor Richards gives short shrift. It is the fiction that contract law governs our surrender of information to financial institutions, health care providers, employers, insurers, online merchants, utility companies, and the countless other entities with whom we are obliged to deal.<sup>14</sup> We simply

---

11. Through the American Library Association and the Freedom to Read Foundation, librarians protect readers' rights by fighting for them whether the courts agree or not. *See generally* *United States v. Am. Library Ass'n, Inc.*, 539 U.S. 194 (2003) (rejecting a challenge to federal regulations requiring libraries to block access to pornography); *Doe v. Gonzales*, 386 F. Supp. 2d 66 (D. Conn. 2005) (upholding a challenge to gag orders forbidding Connecticut librarians from revealing that the federal government had sent them "National Security Letters" seeking patrons' library records); *Tattered Cover v. City of Thornton*, 44 P.3d 1044 (Colo. 2002) (in which the Freedom to Read Foundation provided important amicus support for a book store that successfully refused to turn over a patron's records). Their vigilance serves notice that libraries will not betray their readers without a fight.

12. Richards, *supra* note 10, at 432–34.

13. *Id.*

14. *See Adobe Sys. Inc. v. One Stop Micro, Inc.*, 84 F. Supp. 2d 1086, 1089–93 (N.D. Cal. 2000) (holding an end user license agreement valid under California law); *Hotmail Corp. v. Van\$ Money Pie, Inc.*, No. C-98-20064, 1998 WL 388389, at \*6 (N.D. Cal. Apr. 16, 1998) (applying California law and finding the plaintiff likely to prevail on breach of contract claim regarding clickwrap agreement); *cf. In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299 (2005) (enforcing a clickwrap agreement *against* a service provider). Courts and reformers alike seem to accept the premise that users can be contractually bound despite the lack of bargaining and no matter how little freedom the user has to decline. They focus instead on the adequacy of notice. *See generally* Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 PENN ST. L. REV. 587 (2007); David A. DeMarco, Note,

cannot participate in modern life without routinely checking the “I accept” box. Our options are to acquiesce or forgo the service or product.

Preposterously, the law treats our acquiescence as if we had bargained with the entity and reached a mutually agreeable solution, never mind that the information-surrender provisions are non-negotiable and that any other provider would demand similar provisions. This fictitious “contract” then becomes the warrant for passing our information along to other entities with or without our knowledge. If you take the time to read and comprehend the innumerable “privacy policies” that arrive with your credit card bills, bank statements, utility bills, and insurance forms, or that you sign when you seek employment or medical care, you will see that after telling you how much they value your privacy, they say, essentially, “We will do whatever we please, within the limits of the law, with the information you give us.” And the law imposes virtually no limits, again relying on the fiction that we voluntarily surrendered the information and agreed to allow it to be shared.

Professor Richards suggests several steps to ameliorate this situation, including requiring notification of individuals when their data is sold, limiting uses to which data can be put and periods for which it can be retained, and forbidding disclosure of “particularly sensitive types of intellectual data.”<sup>15</sup> In my estimation, that response is far too tepid. The problem is that the law allows private entities to coerce us into furnishing information under the fiction that we are providing it voluntarily. That is the problem that must be attacked. If we accept the legitimacy of that construct, trying to control the uses to which our information is put will always be a struggle. The information becomes a business asset, and the ingenuity, perfidy, and persistence of those who wish to exploit the asset will usually defeat attempts at regulation. We all learn eventually that the only sure way to keep secrets is to not share them. We also know that modern life makes that very hard to do. But the fiction that we voluntarily agree to disclose almost anything that the purveyors of the accoutrements of modern life demand to know makes the control of secrets harder than it needs to be.

---

*Understanding Consumer Information Privacy in the Realm of Internet Commerce: Personhood & Pragmatism, Pop-Tarts & Six-Packs*, 84 TEXAS L. REV. 1013 (2006).

15. Richards, *supra* note 10, at 437.