Article

Information Privacy in a Network Society: Decision Making Amidst Constant Change*

Ming-Li Wang**

ABSTRACT

This article sets out to answer why online privacy protection has been largely ineffective so far, why average people have not been outraged by such failure, and what we should do going forward. The author argues that the two leading privacy regimes in the world have managed to induce over-sweeping privacy policies, for they have underestimated the substantial social change brought about by modern information and communications technologies. Privacy advocates on the other hand have overlooked the ambivalent relationship between modern people who live in a network society and their desire to savor some control over personal information.

This article argues for more patience because long-term solutions cannot be built on quick sand. Before finding real solutions we need more consensus-building dialogues, and to facilitate such discourse we need a little fine-tuning on the balance among the three constitutional powers.

* This article is substantially based on the findings of a research project lead by the author, *Privacy Issues of e-Bathroom Facilities for Next Generation*, which is a part of an interdisciplinary mega-project titled *Innovatory Technology Development and Precursory Humanity Study of e-Bathroom Facilities for Next Generation*, lead by Electric Engineering Professor Yu-Ming Hsin of National Central University, and sponsored by the National Science Commission, Taiwan (project no. NSC 95-2218-E-008 -022). The input from other team members, especially the scientists and social scientists with no legal background has been insightful and is deeply appreciated. Earlier drafts of this article were presented at the Law and Society Association Annual Meeting 2009 (Denver, May 2009) and subsequently at the Asian Constitutional Law Forum 2009 (Taipei, Sept. 2009), where the author received several helpful comments. Two anonymous reviewers provided extremely constructive suggestions, for which the author is very grateful. The author would also like to thank his assistants for their hard works.

** Assistant Professor of Law, Graduate Institute of Industrial Economics, National Central University, Taiwan. E-mail: mlwang@ncu.edu.tw.

Keywords: *Information Privacy, Network Society, Online Privacy Protection, Information and Communications Technologies, Consensus-building Dialogues*

CONTENTS

I. INTRODUCTION

Less than twenty years after its critical transition from a pure research platform into an all-purpose communications infrastructure,[1] the internet has become an integral part of our societal architecture. The convenience of modern information and communications technologies comes at a price. The more our daily lives weave with the fabrics of the net, the greater threat our privacy faces. Indeed privacy concerns have been cited by many as their greatest worries when shopping or socializing online.

Against this background, the research interest of this article was pecked by a series of peculiar and inter-related observations. The first is made here in Taiwan. It was not until 1992 did our Constitutional Court first mentioned people's right to privacy in Interpretation 293. It would then take another decade and more before the first full-blown privacy Interpretation (Interpretation No. 603) came along in 2005.[2] We cannot blame the court for slighting one of the most important basic human rights. As a passive institution, it does not conduct its business according to a set agenda. The relative inaction by the Court in fact is the result of underwhelming public debates about privacy.Second, despite repeated calls for actions by privacy advocates and average netizens[3] around the globe, the gulf between its two leading privacy legal regimes remains as large as it has always been.[4] The attitude of U.S. government is especially puzzling. If it is true that U.S. privacy protection lags behind its European counterparts, as often suggested by commentators,[5] why does its Congress keep quiet? The almighty net power—its muscle was in full display during the 2008 general elections[6]—should have willed numerous pieces of legislation through Congress by now. That has not happened, and it does not seem to matter much. Despite having neglected the popular demand in greater privacy

1. Commercial traffic over the internet officially started in early 1990s; *see* GERALD W. BROCK, THE SECOND INFORMATION REVOLUTION 269-71 (2003).

2. Several decisions in between did mentioned privacy in passing, including J.Y. Interpretation No. 509, 535, 554, 559, 577, 585, 587, 594. Right before J.Y. Interpretation No. 603, J.Y. Interpretation No. 599 issued a preliminary injunction to halt the execution of the finger printing policy before the Court could address its constitutionality.

3. A "netizen" is a "net citizen," a phrase coined in early 90s by Michael Hauben, then a Columbia student enthusiastic about the burgeoning online community. Michael Hauben later wrote an extensive treatise (with his mother Ronda Hauben) on the subject; *see* MICHAEL HAUBEN & RONDA HAUBEN, NETIZENS: AN ANTHOLOGY (1996), *available at* http://www.columbia.edu/~rh120/.

4. *See generally* Marsha Cope Huie, Stephen F. Laribee & Stephen D. Hogan, *The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 391, 403-07 (2002).

5. *See, e.g.*, *id.* at 396-402.

6. *See, e.g.*, Daniel Lyons & Daniel Stone, *President 2.0*, NEWSWEEK (U.S.), Dec. 1, 2008, at 40, *available at* http://www.newsweek.com/id/170347 (describing how Obama harnessed net power to win the election).

protection, America continues to lead in e-commerce and other online activities.

It is tempting to attribute the scarcity of American privacy legislation to legislative malfunction given immense business lobbying power.[7] We cannot easily explain away, however, sustained prosperity and ongoing global expansion of e-commerce and social networking in spite of sub-par privacy protection, at least in America and many other countries. It is as if the people are suffering dissociative identity disorder collectively; they speak one way but act the other. There is an eerie similarity between the under-powered privacy activism in American and the low-key privacy discourse in Taiwan, but their true cause remains to be unveiled.

This article starts its inquiry with a pair of critical examinations of the two dominant privacy legal regimes in the world—the European Union and the United States. The Europeans set the bar high but have fallen victims to the impracticality of their rigid approach, while the Americans have so far underestimated the threat from private actors. The diagnostics will attribute both regimes' ineffectiveness to their inability to grasp the complexity of a fast-forwarding network society.

The puzzles will then be solved in the next section. It starts with an account of how mankind's new baby—privacy—was born into and has grown up in a swift-changing environment, leading to its unsteady personality, followed by a theory of collective ambivalence toward privacy by people. It is the volatile nature of privacy as well as the hurried background scenery changes that have doomed the two leading privacy regimes, and it is the collective ambivalence in people's mind that has made their failure (and the dearth of judicial actions in Taiwan) seemingly inconsequential.

Ambivalence nevertheless does not equate indifference, this article insists, and patience does not equate inaction. Before finding comprehensive long-term solutions we need more consensus-building dialogues, which will be better facilitated by fine-tuning the balance among the three constitutional powers.

II. THE DIGNITY APPROACH: PRINCIPLED BUT IMPRACTICAL

A. *E.U. Privacy Regime*

As Whitman aptly puts, continental Europe sees privacy as an extension of the right to respect and personal dignity, consisting of mainly "rights to

7. *See, e.g.*, Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 70-73 (2000).

one's image, name, and reputation, and what Germans call the right to informational self-determination—the right to control the sorts of information disclosed about oneself."[8] Rooted in such deep respect to personal dignity, the E.U. zone is currently the most assertive champion of privacy right in the world.

Privacy protection has been a continental mandate since the *European Convention for the Protection of Human Rights and Fundamental Freedoms*.[9] The mandate was nevertheless lofty words with little substance in many parts of Europe until the *Personal Data Protection Directive of 1996*.[10] Augmented later by the *Electronic Communications Privacy Directive*[11] and amended by the *Data Retention Directive*,[12] the Privacy Directive outlines a comprehensive system that seeks maximum privacy protection for European citizens.

The Privacy Directive anchors its regulatory structure in the principles set forth in OECD's *Privacy Guidelines*.[13] Personal data can only be collected for "specified, explicit and legitimate purposes."[14] The data subject is bestowed with full autonomy with respect to her personal information. Subject to certain restrictions, processing can be carried out only with the data subject's unambiguous consent,[15] so does transfer to a third country with lesser privacy protection.[16] To ensure informed decision, the data subject is entitled to key information about the nature of the processing.[17] She is also entitled to access her own data[18] and to object to certain processing,[19] along with other rights. Member states have to set up supervisory authority to investigate and intervene when necessary.[20]

The E.U. is proud of their comprehensive approach, so much so that it demands other countries to follow suits, or risk losing data exchange

---

8. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1161 (2004).

9. European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, 213 U.N.T.S. 222 ("Everyone has the right to respect for his private and family life, his home and his correspondence.").

10. Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) [hereinafter *Privacy Directive*].

11. Council Directive 2002/58, 2002 O.J. (L 201) 37 (directive on privacy and electronic communications). This Directive replaces earlier Telecommunications Privacy Directive (Council Directive 97/66, 1998 O.J. (L 24) 1 (EC)).

12. Council Directive 2006/24, 2006 O.J. (L 105) 54 (EC).

13. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [hereinafter *OECD Privacy Guideline*], *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (visited May 24, 2009).

14. Council Directive 95/46/EC, art. 6 para. 1(b), 1995 O.J. (L 281) 31, 40.

15. *Id.*, art. 7(a), at 40.

16. *Id.* art. 26 para. 1(a).

17. *Id.* arts. 10 & 11.

18. *Id.* art. 12.

19. *Id.* art. 14.

20. *Id.* art. 28.

privilege with the E.U. zone.[21] The insistence provoked loud protests from across the Atlantic Ocean at first, but the E.U. did not blink, earning it wide praise from scholars and advocacy groups.[22] After some tussling, a compromise was reached in the form of a "Safe Harbor" framework for U.S. companies so that both sides could save face.[23]

B. *Speed Bumps on the Information Superhighway*

Worthy accolades notwithstanding, the E.U. Privacy Directive was drafted at a time when the full potential of vast computer databases and advanced data-mining techniques was not readily apparent to the general public as well as most policy makers. Even less well understood, however obvious it may seem today, was how profoundly the internet was going to change the way people communicate, socialize, research, express, debate, shop, advertise, entertain, campaign, organize and so forth, let alone how rapidly such changes would take place.

Granted by the time the Privacy Directive was prepared in early 90s, computers had been used to amass an impressive amount of personal data and the internet had been expanding at record speed. Together they elicited enough public fear to set into motion European legislative efforts. The shortsightedness of the eventual legislation was nonetheless seeded much earlier.

As said, the Privacy Directive was anchored in the OECD Privacy Guidelines, which in turn had drawn heavily from a set of principles identified by U.S. Privacy Protection Study Commission in a 1977 report,[24] some of which conceived in early 70s.[25] While later policy makers were no doubt updated on subsequent progress in the field, it is safe to say the cherished privacy principles were largely established when the most privacy-threatening technologies today were still flying under the radar. Personal computing was in its infancy; so were relational database management systems (RDBMS). The term "computer database" conjured up

---

21. *Id.* art. 25 para. 4.

22. *See* Huie et al., *supra* note 4, at 396-97.

23. The "Safe Harbor" framework calls for a voluntary program set up by the U.S. government, which qualified American companies may opt in. To qualify, a company must abide by a set of principles outlined in the E.U. Privacy Directive. Once certified into the Safe Harbor, a company is assumed to be in compliance with the E.U. Directive and thus may exchange data freely with entities inside the E.U. zone. The E.U. Commission Decision authorizing this framework is 2000/520/EC. *See also* Barbara Crutchfield George, Patricia Lynch & Susan J. Marsnik, *U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive*, 38 AM. BUS. L.J. 735, 735-40 (2001).

24. PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY: THE REPORT 500-02 (1977), *available at* http://epic.org/privacy/ppsc1977report/.

25. *Id.* at 500 (an earlier form of the principles were first developed by an Advisory Committee appointed by then Secretary of Health, Education, and Welfare, Elliot L. Richardson in 1972).

images of large flat tables stored on gigantic computer mainframes. The technique most feared by privacy conscious users today—data mining—had not even been invented yet.[26]

Data processing during that era preconditioned on having one of those huge machines and skilled programmers at your disposal. It was a domain exclusive to a select few government agencies and corporate giants—financial institutes chief among them—with ample resources. The types of information they intended to extract from databases were relatively few and unimaginative by today's standard, even less of which could be produced in a timely and economical fashion.[27] Fear nevertheless ran deep in society, with substantial help from popular literatures like Orwell's Nineteen Eighty-Four as well as notorious scandals like Watergate.

Articulated against that kind of technological, economic and social background, the OECD Privacy Guidelines set the bar high with a myriad of principles. From collection, storage, processing to transmission, the Guidelines set guiding principles for the full lifecycle of personal data without specifying how they should be implemented. The potential legal obligations hinted by those principles nonetheless betray the fact that it is designed with gigantic institutions—those that could afford computer mainframes—in mind, not the average Joe.

The kind of regulations the Privacy Directive imposed a decade and a half later, such as the requirement of setting up data controllers and all the obligations that position assumes, inherited much of the same assumptions and intended targets. And yet the world it is supposed to govern has not stood still. The technology bubble of the 90s came and went. Start-ups rise and fall all the time, but the new cyber-landscape they helped create stays and keeps shifting.

Personal computers have replaced mainframes as main data crunchers, shifting innovation to the "end"—in contrast to the "center," where servers reside.[28] The internet has whipped our appetite for free information, in both senses of the word "free" (free beer and free speech). At the same time it has made publishers out of regular surfers. You blog, you publish. You post, you publish. You tweet, you publish. In "me" the information consumer and the producer have merged into one. Together the netizens create mass waves of

26. *See* Sarfaraz M. Manik, History of Data Mining, http://dataminingwarehousing.blogspot.com/2008/10/data-mining-and-warehousing-history-of.html (last modified Oct. 24, 2008) ("Data mining is a fairly new concept which was emerged in the late 1980s.").

27. *See generally* John Gaudin, *The OECD Privacy Principles—Can they survive technological change?, Part I*, 3 PRIVACY L. & POL'Y REP. 143 (1996), http://www.austlii.edu.au/au/journals/PLPR/1996/68.html.

28. It should be noted that current wave of cloud computing is again shifting power to the center, reversing the trend somewhat. But cloud computing works with powerful client machines, not dumb terminals. With personal computers keep beefing up, moreover, there is little chance for end users to give up the power at their disposal.

data exchanges. Much in the same fashion packet switching taking the place of circuit switching, information flow is no longer linear; it comes in all sizes and shapes. It comes from everywhere and goes in all directions, and it moves instantly and constantly.

Somewhere along the routes, bits and pieces—sometimes in large chunks or in whole—linger, on a server here, a client there. The internet that turns everyone into a publisher also makes us data collectors. We might not be doing much different online from what we used to do offline. The mere fact that we are doing these things online has nevertheless rendered them "regulable."[29] Furthermore, for people outside the E.U. zone, online activities have potentially exposed them to the reach of E.U. regulations. While some such activities may be exempted by the "purely personal or household activity" clause[30] of the Directive, it is far from clear whether its scope is broad enough to cover all our regular online activities. Nor can it be assured that no one will fall prey to over-zealous enforcers or frivolous suits. Fringe services grown out of college dorm rooms and based on innovative and yet flaky ideas are even less likely to be categorized as "purely personal or household activities."

The above does not suggest it is wise to flatly leave all new online services or activities alone. "Technology liberates and confines; it creates and it destroys."[31] What makes the net great also makes it dangerous, especially to those less technology sophisticated among us. It is nevertheless a fact that heavy-handed commands and controls tend to frustrate innovation. They are akin to speed bumps on the information superhighway. They might make the road safer, but at the very moment they do so the road has ceased to be a freeway. There is no wonder that they need to open up fast lanes for law enforcement and anti-terrorist intelligence purposes in later amendments.

Even those well established businesses originally targeted by the Directive are not happy with the extra compliance costs,[32] giving rise to the epidemic of sweeping privacy policies. Carefully crafted by lawyers, modern breed of privacy policies is designed to extract a "yes" from the end user at the earliest stage possible, covering as broad a scope of activities as legally allowed, which would be extended automatically to all business partners and their partners, with no expiration date. While enjoying nominal control over

---

29. *See generally* LAWRENCE LESSIG, CODE: VERSION 2.0, 38-82 (2006) (arguing that the internet is moving toward an architecture of control, and life on the net is increasingly more regulable).

30. Council Directive 95/46/EC, art. 3 para. 2 sub-para. 2, 1995 O.J. (L 281) 31, 39 (EC).

31. Lawrence M. Friedman, *The Eye That Never Sleeps: Privacy and Law in the Internet Era*, 40 TULSA L. REV. 561, 577 (2005).

32. *See, e.g.*, Shaffer, *supra* note 7, at 17-20 (elaborating on the costs of E.U. privacy requirements on European Businesses).

her personal data, by a single mouse click the data subject might have signed away every right.[33] Privacy policies are the businesses' own speed lanes.

III. THE FREEDOM APPROACH: FLEXIBLE BUT UNDERWHELMING

A. *American Incrementalism*

One hundred and twenty years after the classic treatise by Warren and Brandeis,[34] there is no longer any doubt that privacy is a basic human right worthy of constitutional protection. Privacy as articulated by the Supreme Court is rooted in individual autonomy, however, not quite the genteel kind championed by Warren and Brandeis.[35] If dignity is the core value anchoring European privacy law, Modern American concept of privacy is driven by its deep insistence on personal liberty—against the state in particular.[36] The expansive reading of privacy generates much controversy in cases involving a woman's right to choose, personal preference in sexual orientation and the like, but its application in personal data protection has been widely embraced.

The *Privacy Act of 1974*[37] is the main federal statute on privacy protection. Subject to certain exceptions, it lays down the ground rule of "no disclosure without consent" for personal information held by federal government agencies,[38] so an individual would not necessarily lose her privacy simply because the government has collected data about her, sometimes against her will or even without her knowledge. The rule does not protect personal information against nondiscretionary disclosure pursuant to the *Freedom of Information Act* (FOIA),[39] but when a FOIA exemption[40] applies—typically exemption 6[41] or exemption 7(C)[42]—the rule forbids discretionary disclosure by an agency.[43]

---

33. *See* Lawrence Lessig, *Coding Privacy*, INDUSTRY STANDARD, Nov. 14, 1999, http://www.lessig.org/content/standard/0,1902,4620,00.html.

34. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

35. *See* Friedman, *supra* note 31, at 571-72.

36. *See* Whitman, *supra* note 8, at 1161-62.

37. Pub. L. 93-579 (codified as amended at 5 U.S.C. § 552a (2006)).

38. There are numerous exceptions; *see* 5 U.S.C. § 552a(b) (2006).

39. 5 U.S.C. § 552 (2006).

40. 5 U.S.C. § 552(b) for the complete list of FOIA exemptions.

41. § 552(b)(6) ("personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy").

42. § 552(7)(C) ("records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information").

43. 5 U.S.C. § 552(b) by itself only exempts certain information from mandatory disclosure, but does not forbid an agency from disclosing it at discretion; *see* The Office of Privacy and Civil Liberties, Department of Justic, Overview of the Privacy Act of 1974, *available at* http://www.usdoj.gov/opcl/1974privacyact-overview.htm (visited Jan. 31, 2010).

As the first statute dedicated to privacy protection in the world, the Privacy Act nevertheless puts only the federal government on a leash. Grievances arising from privacy intrusion by private actors have to be settled in court,[44] where conflicting interests are weighed and balanced. There have been constant calls from privacy advocacy groups for Congress to shore up federal privacy protection against commercial and other private intruders, especially after Europeans got their Privacy Directive in 1996. From time to time Congress does grant their wishes, but only in scattered patch works addressing specific concerns instead of a comprehensive solution, let alone anything close to the European model.[45] After 9/11 the only legislative trend more or less systematic has been steady increase in governmental power to monitor and to search,[46] not at all privacy enhancing.

This incremental approach does have its merits in flexibility and moderation, in its capability to self-correct,[47] and in its capacity to adapt to ongoing social and technological change.[48] It also gives politicians plenty of excuses. They pledge undying support for individual privacy in public, chide corporate greed in hearings, then turn around and decide to make no law, citing their confidence in business self regulation and trust in the court to right the wrongs.

While thankful for being left alone, businesses now face uncertain risks in private litigations. Privacy invasion is a tort. The outcome of a jury trial is as unpredictable as with other torts, if not more so given the difficulty in damage assessment. For businesses, the odds of actually losing in court are slim. Being risk-averse, however, they hate leaving things to chances. The best legal shield they could obtain is prior consents from their customers, which they need anyway in order to dock in the "Safe Harbor." As a result, their lawyers come up with the most over-inclusive privacy policies imaginable that ask the users to consent away anything they may do with your personal data in the future. If this sounds familiar, it is because we are seeing a similar standard practice spurred by the E.U. Privacy Directive as described earlier. With the convenience of copy-pasting on the net, such policies are as easy and costless to produce as never before.

---

44. *See* Robert M. Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, 6 SOFTWARE L.J. 199, 211-12 (1993) (on how the Advisory Committee on Automated Personal Data Systems decided recommending "enforcement of privacy rights through individual court action").

45. *See* James M. Assey, Jr. & Demetrios A. Eleftheriou, *The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?*, 9 COMMLAW CONSPECTUS 145, 149-50 (2001).

46. *See infra* § III.B.

47. *See, e.g.*, Katz v. United States, 389 U.S. 347 (1967).

48. *See, e.g.*, Kyllo v. United States, 533 U.S. 27 (2001).

B. *The Underestimated Threat*

The Europeans may have underestimated the velocity of technological advancement, they at least understand—if only vaguely—where some real dangers lurk. In contrast, American policy makers seem to have a hard time deciphering the qualitative transformation brought about by modern information and communications technologies. If European legislature was somewhat misguided by a set of impractical though noble principles, what has dominated American privacy discourse is a great novel.

Much like what Rachel Carson's Silent Spring did to the environmental movement, George Orwell's Nineteen Eighty-Four has been the main inspiration for modern privacy advocacy.[49] The listless state of lives under the ubiquitous surveillance network deployed by the Big Brother is so well depicted that it is spooky. The year 1984 came and passed without much fanfare only because required technologies were not there yet. As technology marches forward, the threat is getting alarmingly realistic. Generations of privacy advocates are hence inspired and determined to prevent the fiction from becoming a reality.

The security toughening up after 9/11 has only strengthened their determination. The Al Qaeda attacks on American soil not only shocked the world, but also launched a new era in international intelligence warfare. Gone is the aura of invincibility of American military, taking with it the false sense of security on home turf. The way modern terrorists organize and penetrate has made it a necessity to cast a wide and comprehensive net of intelligence gathering—not only abroad but also at home—in order to identify and track potential enemies.

Lead by the USA PATRIOT Act,[50] a string of statutes and executive orders have thus expanded the government's intelligence and investigative power and relaxed preexisting procedural safeguards, at first with overt blessing from the people. The Electronic Communication Privacy Act (ECPA) had just extended existing protection against illegal wiretapping to electronic communication in 1986, only to see large holes punched on it after 9/11.[51] The original privacy protection regime in Europe outlined by the Privacy Directive was also considered a potential hindrance to effective intelligence gathering and sharing, so changes were introduced there, too.[52] In time privacy sensitive people are alarmed. They speak up, albeit gingerly

49. *See* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1394-97 (2001).

50. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT ACT), Pub. L. No. 107-56, 115 Stat. 272 (2001).

51. *See generally* Jamie S. Gorelick, John H. Harwood II & Heather Zachary, *Navigating Communications Regulation in the Wake of 9/11*, 57 FED. COMM. L.J. 351 (2005).

52. Mainly Council Directive 2006/24, 2006 O.J. (L 105) 54 (EC).

at first, and the full debate is restored.

While taming excessive governmental surveillance is a worthy cause, its dominance in American privacy discourse has unnecessarily overshadowed the discussion of another major threat to privacy: massive personal data accumulation and mining. As Solove pointed out, instead of the Big Brother, the world depicted by Franz Kafka in The Trial—full of "thoughtless process of bureaucratic indifference, arbitrary errors, and dehumanization"—might be a greater and more realistic threat to our privacy.[53] With the way technology evolves, moreover, it is only a matter of time before the Big Brother in Nineteen Eighty-Four works with the faceless bureaucrats in The Trial.[54] To some extent, in fact, it is already taking place.

Beyond the government, private actors are even keener to dig deep into the gold mine of boundless personal data. The internet has dramatically lowered the cost of data harvesting, and the coming generation of net-surfing wireless devices will make it easier still. Modern data mining techniques have made it possible to weave meaningless data fragments into revealing information, and more powerful hardware and smarter algorithms will make such applications increasingly feasible and affordable for businesses. Acting together they will erode our privacy in an almost imperceptible way.[55] What we have seen is only the beginning of this development. What only Google is capable of doing might be routine practices in ten to twenty years. It is like an ironic manifestation of the famous motto "information wants to be free" by early "hackers," albeit in a very different context.

IV. RE-APPROACHING PRIVACY

A. *An Elusive Concept*

Information privacy is unusually elusive as a legal concept. In other constitutional rights we have hard cases where the boundaries are tested and contested. In privacy, however, we have something that has not only a very murky "penumbra," but also a fluid "core," borrowing Hart's metaphor.[56] The most well-known "definition" of privacy—the right to be let alone[57]—provides us little guidance despite the ringing tone; it is utterly

53. *See* Solove, *supra* note 49, at 1419-23.

54. *See, e.g.*, John Markoff, *You're Leaving a Digital Trail. What About Privacy?*, N.Y. TIMES, Nov. 30, 2008, at BU1. *See also* James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177 (1997).

55. Bert-Jaap Koops & Ronald Leenes, *'Code' and the Slow Erosion of Privacy*, 12 MICH. TELECOMM. & TECH. L. REV. 115, 176-77 (2005).

56. *See* H. L. A. Hart, *Positivism and the Separation of Law and Morals*, 71 HARV. L. REV. 593, 606-15 (1958).

57. Sometimes termed differently as "the right to be *left* alone," the phrase is best associated with Warren & Brandeis's celebrated work, though they certainly did not invent the concept or the phrase;

unclear what that particular right encompasses in any given society. The "reasonable expectation of privacy" standard has been the best litmus test for privacy adjudication, but the standard fluctuates by nature; its meaning can only be determined in context.[58]

B. *There are several reasons that might account for the mercurial character of privacy. The idea is young; modern legal discourse started merely a little more than a century ago. The philosophical and social roots are not uniform, as evident in earlier discussion. The most important reason, however, lies in the troubling relationship between privacy and technology.*

Information privacy is a fluid concept because its public recognition has coincided with the rise of modern technologies. What troubled Warren and Brandeis in the late nineteenth century was photography, the technology that had begun to tip the balance between reclusive gentlemen and nosy journalists,[59] before the latter morphed into unshakable herds of paparazzi. Heralded and persuasive advocacy notwithstanding, it was an ominous start for the right to privacy, going up against one of the most cherished—if pesky—institution: the press. It was even less encouraging when we see what is feeding this journalistic army—unbounded human curiosity.

When the U.S. Supreme Court first confronted whether and how to protect information privacy on constitutional ground in *Olmstead v. United States*,[60] it was telephone that had blurred traditional physical boundaries between private homes and public streets. While failing one vote short of scoring a victory for privacy, Brandeis—now an Associate Justice on the Supreme Court—nevertheless delivered a powerful dissent that eventually helped turning things around in *Katz*[61] forty years later.

Katz was a landmark not only because it finally curbed unfettered wiretapping by the state, but also it enabled American judiciary to change course and engage privacy advocacy in a more direct manner. The omnipresent "reasonable expectation of privacy" test was also first articulated here, by Justice Harlan in a concurring opinion.[62] And yet by the time *Katz* outlawed unwarranted wiretapping in 1967, another information revolution had already commenced. Untiring and unerring digital computers are the new data crunchers, and the Department of Defense had started

---

see Warren & Brandeis, *supra* note 34, at 195 (quoting Judge Cooly).

58. *See generally* Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005).

59. *See* Warren & Brandeis, *supra* note 34, at 195-96.

60. Olmstead v. United States, 277 U.S. 438 (1928).

61. Katz v. United States, 389 U.S. 347 (1967).

62. *Id.* at 360 (Harlan, J., concurring).

working on a project in the mid sixties that eventually brought us the internet; its first fruits would come to light by the end of the decade.[63] The discourse was only to get more complicated.

When American government conducted its privacy inquiry and when the OECD worked on its privacy guidelines based on established knowledge in mainframe computing, personal computers had begun to take over the world, first in the workplace then in average households. When European scholars and bureaucrats commenced on its quest for a comprehensive data protection directive, the internet revolution had been underway.

Technology is not the only thing that keeps moving. As technology progresses, people adapt and society evolves, which in turn shape future technology progress. With photography—first mechanical then digital—came affordable lasting memories and irrefutable evidence. The former has reshaped family and social gatherings while the latter has brought us amateur investigation.[64] Telephone—first wired then wireless—has redefined social connection and interaction. Kinship and geographical proximity once delineated one's social relationship; today names from all corners fill one's Rolodex. Electronic mass media—first radio then TV broadcasting—has recalibrated after-hour activities. Gone are tea parties under oaks, replaced by family dinners in front of the TV set.[65] Local bounds are further weakened, but would-be strangers across a large area—across oceans, even—are increasingly connected, a trend only to be strengthened by the internet later.

Market, too, never stands still. Innovations bring new businesses, realign competition and redistribute resources. Photography not only made Kodak a giant, but also redefined news reporting. Before anyone notices, a business has emerged in Taiwan that makes glamorous photo albums for young couples before they get married. Telephone speeds up the pace of business. Computers revolutionize information processing, management and storage. ATM, credit cards and complex structured financing are all made possible by modern information and communications technologies.

---

63. For an excellent account of early research efforts commissioned by the U.S. Defense Department which eventually lead to the creation of the internet, see generally KATIE HAFNER & MATTHEW LYON, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET (1996).

64. *See* Lawrence M. Friedman, *Name Robbers: Privacy, Blackmail, and Assorted Matters in Legal History*, 30 HOFSTRA L. REV. 1093, 1114-16 (2002).

65. *See, e.g.*, Barbara Bennett Woodhouse, *Reframing the Debate About the Socialization of Children: An Environmentalist Paradigm*, 2004 U. CHI. LEGAL F. 85, 111 ("Media dominates the family dinner table, with 58 percent of families with children reporting that they have the television on during dinner.").

C. *Amidst such constant technological, social and economical change we live, surrounded by an unbounded web of communications networks. Repeatedly we connect and re-connect, forming layers of relationship, sharing with others what we have, what we know, what we think, and what have been shared with us. In time many have a hard time telling "me" from "others." The line has blurred; welcome to cyberspace. No wonder privacy is hard to define. An Ambivalent Affair.*

In previous sections the author has criticized both U.S. and E.U. regimes for being ill-configured to provide adequate and yet feasible privacy protection in a ubiquitous network society, citing the failure to anticipate the substantial changes modern information and communications technologies would bring as main causes. Law makers are nevertheless professional politicians. They may lack technological prowess, but they are certainly sensitive to people's voices, at least the loud ones. If people are as serious in protecting their privacy as they claim in opinion polls, they should have shouted and dragged their representatives into action. Why that has not happened in two of the most democratic regions in the world is puzzling, or so it seems.

Public choice theories provide us some good hints. After all, those who benefit from the status quo the most are existing law enforcement and intelligence establishments, as well as multinational corporate giants like Google, Amazon, Microsoft and their peers. Those who stand to lose are average netizens and consumers—vast in number but disperse and unorganized in nature. Power, in other words, is not distributed evenly.[66] Should that be the only reality in privacy politics, however, the European Privacy Directive should not have seen the light of day in the first place. The missing piece of the puzzle perhaps lies somewhere most scholars and privacy advocates overlook. Powerless may the people be, they are perhaps less so in politics than in their own heart, confronting their own indetermination.

On one hand, one does like being in charge of her own identity and reputation by controlling the dispersion of personal information;[67] the inner serenity that comes with such control cannot be overstated,[68] for without it "freedom of thought becomes a mocking phrase, and without freedom of thought there can be no free society."[69] Being a social animal, on the other hand, one also enjoys various amounts of information sharing and

66. *See, e.g.*, Lynn A. Stout, *Strict Scrutiny and Social Choice: An Economic Inquiry into Fundamental Rights and Suspect Classifications*, 80 GEO. L.J. 1787, 1805-10 (1992).

67. *See* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 23-25 (1997) (on the value of privacy on individual autonomy).

68. *See id.* at 25-26.

69. Kovacs v. Cooper, 336 U.S. 77, 97 (1949) (Frankfurter, J., concurring).

exchanges. Free information or transparency is a good thing, so long as what is laid bare is not her own life. A big part of "me" is defined by the society, and that very society increasingly demands interactions and connectivity, each generation more so than the last. Only with this understanding could we begin to comprehend why so many people consider texting while driving a necessity.[70]

In this culture people know that their personal information has values to others, and they can and are sometimes—often even—willing to trade given the right "price." We gather personal information ourselves, and we do not see this as inherently immoral or unethical. Most of us hate spammers, but at the same time do not mind learning of a good offer on something we truly desire. We love being able to check out a new boss simply by googling her name, but deep down we know whatever clever tricks Google is pulling to make this work are also exposing us—an unnerving knowledge to say the least.

This ambivalence, acting collectively, accounts for a large part of the inertia in privacy advocacy among the general public. Most are keenly aware of the internal conflict between both wants, but few have a clear compass in how they should be balanced. Privacy advocates like to make it sound like an easy choice. Privacy, they say, is the most important value of a free society. It not only shelters us from tyrannical control, it also provides the inner peace that makes freedom of thought and freedom of expression meaningful. Noble words indeed, but they are about as effective at changing people's behaviors as preaching abstinence in Las Vegas.

D. *Some Collaborating Findings*

For three years ending only recently the author was involved in an interdisciplinary research effort. The project—"E-bath"[71] in short—centered on a futuristic bathroom that would conduct urine tests when you use the toilet, examine your dental health when you brush teeth, sound alarms when you fall to the ground, and monitor water temperatures when you bath. The engineering team tried to make real the required technologies. The computer science team built a centralized control center to coordinate all the actions, and stored and analyzed the data. A sociology team observed the engineering process and measured user feedbacks. The legal team led by the author was in charge of figuring out what privacy implications such a system would

70. *See* Matt Richtel, *Drivers and Legislators Dismiss Cellphone Risks*, N.Y. TIMES, July 19, 2009, at A1.

71. The research findings, including questionnaires, results, and discussions can be found in the final report of the E-bath project, available on the National Science Commission web site, http://www.nsc.gov.tw/.

have, and to make sensible design, legislative and policy suggestions accordingly.

Thanks to the help from the sociology team, we inquired potential users on their privacy concerns with a specific application like the E-bath system. The number of samples we collected is neither large enough nor diverse enough for rigorous statistical analysis, but we have found clear indications of the internal ambivalence described above. Most questionnaire takers value individual privacy, but not in an absolute sense. Giving away some personal data is not only acceptable, but also desirable under the right conditions. A majority of people would like to have access to the health information of their family members collected by the E-bath system, but by the same majority they do not wish theirs made available to their family.

Beyond the ambivalence, we have also seen support of our hypothesis that most people have set preferences on what information they are willing to share, with whom, under what circumstances, and what the recipient may do with it, a set of parameters collectively form what the research team tentatively calls "information privacy domains." These preferences are mainly anchored in the relative closeness of relationship between the data subject and the recipient, but not in a uniform way. There is some information people share more readily with close friends than with their spouse, and vice versa. We also find that people share much more generously when anonymity is guaranteed.[72]

These set preferences necessarily vary from person to person, but many of them converge to a significant degree. They have to. Our cultural upbringing instills much of the original preferences. Social norms and peer influence keep shaping them throughout our lives, while our conscience or religious belief makes the final judgments. None of these lives in a vacuum; they are necessarily a function of many social forces,[73] even more so in a heavily interconnected society like ours.

V. REBALANCING CONSTITUTIONAL POWERS FOR MORE EFFECTIVE PRIVACY DISCOURSE

The most apparent lesson to be learned from the analysis above is we are not ready to address modern privacy challenges in a comprehensive manner just yet. That does not mean we should not start building up a better understanding of the issues that would help us develop long-term solutions sooner rather than later. Nor does it suggest we should give up tackling immediate problems. A few modest adjustments to our constitutional check

72. *Id.*

73. *See generally* Whitman, *supra* note 8, at 1161 (detailing how cultural differences between European and American societies have lead to different understanding of privacy).

and balance among the various powers, the author believes, should go a long way in creating healthy and effective privacy discourse, which in turn will make short-term problem solving easier and long-term solution finding more probable.

A. *Greater Legislative Self-Restraint*

Law does not work in a vacuum. Along with social norms and the market, architecture is also an important part of social control.[74] Architecture was largely overlooked only because it changed slowly and infrequently, to the extent that it was often taken for granted. After the industrial revolution, however, the pace architecture changes has picked up speed, bringing about more frequent social, cultural and economic change. Law alone cannot afford to stand still.

Rising to the occasion, law makers—the good ones at least—would try to hark back to established legal principles, traditional social norms or accepted trade practices, trying to make proper analogies between new social facts with the old. Though it might work reasonably well with other new legal challenges, this method fares rather poorly with privacy issues for two reasons. First, to make sound adjustments, law makers need to see the facts in sufficient clarity. Rapid technological and social change today has made prior prediction increasingly unreliable. Earlier analysis on E.U. privacy law making is a good reminder.

If society is a pool and each technological breakthrough is a stone to be dropped into the water, observing the ripples of a single drop may be easy. Drop several in close range at the same time and the task gets tricky quickly. Now imagine dropping hundreds of stones of varying shapes and sizes in fast sequence, into not a static pool but a moving river full of currents, rocks and fishes—which society really is—and then trying to assess or even predict the ripple effect of any given drop. The task would surely humble even the keenest observers among us. Given the way science and technology advance today, however, that is a task policy makers cannot escape.

As previously suggested, furthermore, information privacy is a relatively young legal concept, practically born and grew with modern information and communications technologies. The U.S. Supreme Court has been heavily criticized for failing to properly define "reasonable expectation of privacy,"[75] but the truth is that very notion defies clear definition.

---

74. *See* LESSIG, *supra* note 29, at 121-25 (on modalities of social control).

75. *See, e.g.*, Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 ¶36-49 (describing the reasonable expectation of privacy test as "unworkable"). *But see* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503 (2007) for an excellent defense of the Supreme Court's approach.

The mercurial character of privacy norms calls for greater legislative self-restraint. From this point of view, the seemingly "lazy" approach of American Congress might turn out to be the preferable one. This is particularly true for a society with relatively little privacy-centered cultural heritage—Taiwan, for instance. It would be unwise—dangerous even—to base Taiwanese privacy law largely on the understanding western societies have on the subject. Large-scale, long-term studies and more public hearings will provide more useful information for the legislature on what privacy actually means to Taiwanese people than German Kommentar, Japanese Codes, or American Supreme Court opinions could. Before such information is sufficient to warrant sweeping rules, problems should be better addressed in a tentative and incremental manner.

B. *Incremental Law Making: The Role of the Executive*

Incremental law making nonetheless is not the legislature's forte. Among the three constitutional branches, the legislature makes decisions by forming large scale consensus, and the decisions it makes are relatively wide-ranging and long-standing in nature. With the number of members in any truly democratic legislature of meaningful size, acting slowly and hesitantly is a given quality by design. While the legislature might—sometimes by necessity—expedite the passage of very narrow laws targeting specific issues, it is never built for quick actions, for which it has to count on the executive branch.

Incremental Law Making: the Role of the Executive Compared to the legislature, administrative agencies are not only better equipped professionally, but also more appropriately configured to make quick and targeted decisions.[76] They have a range of regulatory tools at their disposal, and they are in a better position to pick the right tools, for they are more likely to make decisions in closer proximity to the problem at issue time wise. Moreover, agency rules and measures are easier to adapt and adjust, enabling agencies to experiment and innovate to certain extent, for their mistakes are more easily correctable. Administrative agencies therefore have to be endowed with a little more expansive (semi-)legislative power, and this has to be done with overt blessing from the other two branches.

The legislature therefore should delegate more to administrative agencies. This is not to suggest that the former should start writing blank checks to the latter; the danger of an all-mighty executive branch abusing its power is not lost on the author. Taiwan has just barely turned the page; no

76. *See* Richard B. Stewart, *Reformation of American Administrative Law*, 88 HARV. L. REV. 1669, 1675-88 (1975); JERRY L. MASHAW, DUE PROCESS IN THE ADMINISTRATIVE STATE 18-19 (1985).

one in her right mind would like to turn it back. What this article suggests is more modest and incremental, with a little greater room for discretion left to executive agencies.

In exchange, the legislature could—and should—impose stricter procedural requirements that direct a delegated agency to conduct more public fact finding hearings, e.g., to put more detailed information regarding its policy decisions in records, and to be more proactive in public information disclosure. It could also ask for periodic reports on either specific issues or broad policy concerns that might help formulating long-term policy.

More delegation to executive agencies is probably an advice the legislature could swallow, or even welcome, given their lack of ready answers to many of the challenging privacy issues. If carefully designed, the legislature should retain most of the control it has over executive agencies. There is nonetheless no denial that more legislative delegation means greater power to the executive branch, a shift that begets corruptions and abuses if the balance is not restored properly. To do that, we need some recalibration of the role played by the court.

C. *Incremental Law Making: The Role of the Judiciary*

Compared to politicians, lawyers might be warier of broad legislative delegation. The real attitude of course varies from one legal culture to another. American courts in general, e.g., have less trouble approving broad legislative delegation. Mainstream administrative law theories in Taiwan, on the other hand, consider legislative delegation something that has to be kept to the minimum.

The vaunted principle of express delegation—a principle that has been reiterated in numerous Interpretations by the Grand Justices—requires legislative delegation to be clear and precise.[77] It will have to be loosened to make possible the kind of inter-branch cooperation advocated in previous sub-sections. Instead of insisting on statutory exactness, higher degree of ambiguity should be tolerated when examining provisions authorizing agency actions—rule making in particular.[78]

This article nevertheless does not advocate greater judicial deference.

---

77. It is a doctrine originally derived from German Basic Law, art. 80, § 1, ¶ 2 (called Bestimmtheitsgebot in German) and borrowed by Taiwanese scholars. It is now generally considered a command proscribed by art. 23 of Taiwanese Constitution. The English term employed here is borrowed from the English translation of Interpretation No. 593, *available at* http://jirs.judicial.gov.tw/ENG/FINT/FINTQRY02.asp?cno=593.

78. Note that the requirement of clarity and preciseness in legislative delegation has always been a matter of degree; all the author suggests is for the court to tune it down one notch or two when scrutinizing privacy-related delegations.

On the contrary, it argues for greater judicial scrutiny. Traditional wisdom suggests that the court is neither democratically elected nor professionally competent and hence should refrain from Monday morning quarterbacking.[79] According to the landmark decision *Chevron v. Natural Resources Defense Council*,[80] an administrative interpretation of an ambiguous statutory provision should be "given controlling weight unless they are arbitrary, capricious, or manifestly contrary to the statute" when there is express delegation.[81] Even without explicit delegation, an agency's reading still should be respected as long as it is "reasonable."[82]

Such thinking nevertheless overlooks the value of hindsight—which is available only to the court as far as a particular case is concerned—not just in making it right for the parties involved, but also in facilitating further discourse on related issues.

In the past, it might be reasonable to argue that a non-expert's hindsight can rarely lead to a better decision than an expert's foresight, so on balance the marginal benefit of allowing the court to second guess an agency's doing is simply too small. The balance nonetheless has shifted when considering privacy issues in a network society. While executive agencies still command professional superiority, what trouble the legislature—rapid-changing architecture, elusive norms, fluid market conditions, and complex interactions among the three—have proved to be almost as challenging to regulatory agencies. In this age of constant change, in addition, agencies routinely make decisions in haste, often with insufficient supporting information, professional competence notwithstanding. Even when they are diligent in intelligence gathering, the crystal ball often remains murky even to the brightest experts. Hindsight therefore might have become one of more potent tools when dealing with modern privacy issues, and we need it.

Instead of greater deference to the other branches, therefore, the court should assert itself more often, questioning the judgments of the legislature and administrative agencies with less hesitation. This is particularly important if the court allow more expansive legislative delegation, as implored earlier. With a longer leash, the pit bull has to be watched more closely lest it run amok.

Granted how useful hindsight is depends on many variables, including the pace of technology development and the time difference between the agency's decision and the court's review, among others. All the factors that

---

79. *See, e.g.*, Matthew D. Adler, *Judicial Restraint in the Administrative State: Beyond the Countermajoritarian Difficulty*, 145 U. PA. L. REV. 759, 874-91 (1997).

80. Chevron v. Natural Resources Defense Council, 67 U.S. 837 (1984).

81. *Id.* at 844.

82. *Id. Accord*, J.Y. Interpretation No. 553 (Taiwan). Note that in U.S. Supreme precedents a "reasonable" judicial review standard usually means minimum court intervention.

made the agency's decision making difficult might be just as troubling to the court. A prudent court, therefore, might still choose to respect the agency's judgment in the end. Such deference nevertheless should no longer be taken for granted. More important than righting the wrongs by the other branches with the help of hindsight, the court could help keep the debates open before broad social consensus is formed. If a healthy policy decision cycle can be made out of these dialogues, the legislature, in its slow and careful manner, would be in position to make the final call with all things considered. When this is the case, the resultant statue deserves greater deference by the court, hence completing the fine-tuning of power distribution. The balance should roughly stay the same in the end.

VI. CONCLUSION

Though rooted in different cultural traditions, the two leading privacy regimes in the world have managed to induce over-sweeping privacy policies, for they have underestimated the enormous social change accompanying modern technological development. Privacy advocates on the other hand have overlooked the ambivalent relationship between modern people who live in a network society and their desire to savor some sort of control over personal information. That does not mean people do not care about privacy. In an increasingly transparent society, the right to privacy should only gain greater importance, not less.[83] The hard question is how we could construct an environment that is safe but at the same time does not unduly burden information flow.

Taiwan could, and should, avoid making the same mistakes made by the western world since we have much lighter cultural and legal baggage in this regard. Culturally privacy is a very young social concern. Legally we have few laws and few cases. In short, we have a relatively clean slate to jump start fresh discussions. Given constant change we need to be patient, for long-term solutions cannot be built on quick sand. It would serve our goal of finding a balanced solution better by keeping the dialogues open.

In order to have healthy public discourse on privacy issues, the judiciary has a critical role to play. Unlike the legislative and the executive branches, who routinely gauge public opinions and participate in policy debates (though not always doing a good job), the judiciary feels uneasy to engage in such debates, and understandably so. The world of legal technicalities such as whether an administrative action is authorized by law or whether the authorization is clearly delineated is where the court feels more at home.

---

83. *But see generally* DAVID BRIN, THE TRANSPARENT SOCIETY (1998) (suggesting that transparency is destiny and that is good for society in general).

When it comes to constructive privacy policy debates, however, that is no longer enough. The judiciary is the only of the three bestowed with the benefits of hindsight. In addition to after-the-fact adjudication, therefore, it needs to participate in forward-looking policy making in a more active manner. Instead of greater deference to the legislature or administrative agencies, courts should take a harder look at their decisions, not to lay blame but to nudge relevant policy and regulations in the right direction.

To a degree, this has been the case in the U.S., though not without controversies and certainly not consistently. Civil law countries will have a more difficult time making such an adjustment, either formally or through actual practices. Since we can neither reverse the trend of scientific progress nor slow it down, however, those countries that do come through with the right adjustments stand to reap the reward in making sounder policies. Hopefully Taiwan can make it to the podium, fingers crossed.

REFERENCES

Adler, M. D. (1997). Judicial restraint in the administrative state: Beyond the countermajoritarian difficulty. *University of Pennsylvania Law Review*, *145*, 759-892.

Assey, J. M. Jr., & Eleftheriou, D. A. (2001). The EU-U.S. privacy safe harbor: Smooth sailing or troubled waters?. *CommLaw Conspectus*, *9*, 145-158.

Brock, G. W. (2003). *The second information revolution*. Cambridge, MA: Harvard University Press.

Boyle, J. (1997). Foucault in cyberspace: Surveillance, sovereignty, and hardwired censors. *University of Cincinnati Law Review*, *66*, 177-205.

Brin, D. (1998). *The transparent society*. New York, NY: Perseus Books.

Cate, F. H. (1997). *Privacy in the information age*. Washington, DC: Brookings Institution.

Chevron v. Natural Resources Defense Council, 67 U.S. 837 (1984).

Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

Council Directive 97/66, 1998 O.J. (L 24) 1 (EC).

Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC).

Council Directive 2006/24, 2006 O.J. (L 105) 54 (EC).

European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, (1950), 213 U.N.T.S. 222.

Freiwald, S. (2007). First principles of communications privacy. *Stanford Technology Law Review*, *2007*, 3.

Friedman, L. M. (2002). Name robbers: Privacy, blackmail, and assorted matters in legal history. *Hofstra Law Review*, *30*, 10931132.

Friedman, L. M. (2005). The eye that never sleeps: Privacy and law in the internet era. *Tulsa Law Review*, *40*, 561-577.

Gaudin, J. (1996). The OECD privacy principles—Can they survive technological change?, Part I. *Privacy Law and Policy Report*, *3*, 143-147. Retrieved from http://www.austlii.edu.au/au/journals/PLPR/1996/68.html

Gellman, R. M. (1993). Fragmented, incomplete, and discontinuous: The failure of federal privacy regulatory proposals and institutions. *Software Law Journal*, *6*,199-238.

George, B. C., Lynch, P., & Marsnik, S. J. (2001). U.S. multinational employers: Navigating through the "safe harbor" principles to comply with the EU data privacy directive. *American Business Law Journal*, *38*, 735-783.

Bestimmtheitsgebot [German Basic Law], art. 80, § 1, ¶ 2.

Gorelick, J. S., Harwood, J. H. II, & Zachary, H. (2005). Navigating communications regulation in the wake of 9/11. *Federal Communications Law Journal*, *57*, 351-411.

Hafner, K., & Lyon, M. (1996). *Where wizards stay up late: The origins of the internet*. New York, N.Y.: Simon & Schuster.

Hauben, M., & Hauben, R. (1996). Netizens: An anthology. Retrieved from http://www.columbia.edu/~rh120/

Hart, H. L. A. (1958). Positivism and the separation of law and morals. *Harvard Law Review*, *71*, 593-629.

Huie, M. C., Laribee, S. F., & Hogan, S. D. (2002). The right to privacy in personal data: The EU prods the U.S. and controversy continues. *Tulsa Journal of Comparative and International Law*, *9*, 391-469.

J.Y. Interpretation No. 293 (1992).

J.Y. Interpretation No. 509 (2000).

J.Y. Interpretation No. 535 (2001).

J.Y. Interpretation No. 553 (2001).

J.Y. Interpretation No. 554 (2002).

J.Y. Interpretation No. 559 (2003).

J.Y. Interpretation No. 577 (2004).

J.Y. Interpretation No. 585 (2004).

J.Y. Interpretation No. 587 (2004).

J.Y. Interpretation No. 594 (2005).

J.Y. Interpretation No. 599 (2005).

J.Y. Interpretation No. 603 (2005).

Katz v. United States, 389 U.S. 347 (1967).

Kerr, O. S. (2007). Four models of fourth amendment protection. *Stanford Law Review*, *60*, 503-551.

Koops, B.-J., & Leenes, R. (2005). 'Code' and the slow erosion of privacy. *Michigan Telecommunications and Technology Law Review*, *12*, 115-188.

Kovacs v. Cooper, 336 U.S. 77 (1949).

Kyllo v. United States, 533 U.S. 27 (2001).

Lessig, L. (1999, May 20). Coding privacy. Retrieved from Industry Standard Website, http://www.lessig.org/content/standard/0,1902,4620,00.html

Lessig, L. (2006). *Code 2.0*. New York, NY: Basic Books.

Lyons, D., & Stone, D. (2008, December 1). President 2.0. *Newsweek* (U.S.), p. 40. Retrieved from http://www.newsweek.com/id/170347

Manik, S. M. (2008, October 24). History of data mining. Retrieved from http://dataminingwarehousing.blogspot.com/2008/10/data-mining-and-warehousing-history-of.html

Markoff, J. (2008, November 30). You're leaving a digital trail. What about privacy?. *New York Times*, p. BU1.

Mashaw, J. L. (1985). *Due process in the administrative state*. New Haven, CT: Yale University Press.

Olmstead v. United States, 277 U.S. 438 (1928).

Privacy Act of 1974, 5 U.S.C. § 552 (2006).

Privacy Protection Study Commission. (1977). Personal privacy in an information society: The report 500-02. Retrieved from http://epic.org/privacy/ppsc1977report/

Richtel, M. (2009, July 19). Drivers and legislators dismiss cellphone risks. *New York Times*, p. A1.

Shaffer, G. (2000). Globalization and social protection: The impact of EU and international rules in the ratcheting up of U.S. privacy standards. *Yale Journal of International Law*, *25*, 1-109.

Solove, D. J. (2001). Privacy and power: Computer databases and metaphors for information privacy. *Stanford Law Review*, *53*, 1393-1462.

Stewart, R. B. (1975). Reformation of American administrative law. *Harvard Law Review*, *88*, 1669-1813.

Stout, L. A. (1992). Strict scrutiny and social choice: An economic inquiry into fundamental rights and suspect classifications. *Georgetown Law Journal*, *80*, 1787-1834.

Strahilevitz, L. J. (2005). A social networks theory of privacy. *University of Chicago Law Review*, *72*, 919-988.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act), Pub. L. No. 107-56, 115 Stat. 272 (2001).

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*, 193-220.

Whitman, J. Q. (2004). The two western cultures of privacy: Dignity versus liberty. *Yale Law Journal*, *113*, 1151-1221.

Woodhouse, B. B. (2004). Reframing the debate about the socialization of children: An environmentalist paradigm. *University of Chicago Legal Forum*, 85-149.