Student Note

Locating the Value of Information Privacy in a Democratic Society: A Study of the Information Privacy Jurisprudence of Taiwan's Constitutional Court

Hsiang-Yang Hsieh*

ABSTRACT

This note reconsiders the relationship between information privacy and democracy, arguing that information privacy deserves constitutional protection because it not only ensures an individual's personal interests in his or her personal matters, but also promotes public values central to our democratic society. To make this argument, this note identifies three democratic values inherent to information privacy. First, information privacy limits the government's exercise of power. Second, information privacy secures democracy by providing citizens with certain procedural protections. Third, information privacy secures citizens' freedoms of thought, speech, and other intellectual activities.

This note also explores the information privacy jurisprudence of the Grand Justices of Taiwan's Judicial Yuan, Taiwan's Constitutional Court. Taking Taiwan's experience as an example, this note argues that in order for people to freely think, speak, deliberate, dissent, and participate in the democratic process, their information privacy must be protected. Without information privacy protection, people cannot enjoy a really free and democratic society. Information privacy is thus an important value for a democratic society.

Keywords: *Information Privacy, Democracy, Spatial Privacy, Communicative Privacy, Intellectual Privacy*

* J.S.D. Candidate, School of Law, Washington University in St. Louis. E-mail: hhsieh@wulaw.wustl.edu.

CONTENTS

I. INTRODUCTION

Information privacy has been considered one of the most important values in the human society.[1] While people may evaluate the importance of information privacy in different ways, this note attempts to locate its value in relation to the democratic society. Explaining why information privacy matters for democracy is essential to this note's argument that information privacy not merely secures one's autonomy to control personal information, but also advances public values that are vital to a democratic society. This argument is especially important when information privacy is balanced against other conflicting interests. Those who view privacy as just a personal interest usually subordinate privacy to other competing values. And, people who think in this way are all the more likely to regard information privacy and its nondisclosure protection as being in tension with democracy. This note, however, argues that information privacy is central to democracy in various contexts. Taking Taiwan's experience as an example, this note explores the mutually reinforcing relationship between information privacy and democracy, and reconsiders the significance of information privacy in a democratic society.

This note develops its arguments in six parts. Part I overviews the structure of this note and the problems discussed within it. Part II defines information privacy, and identifies information privacy's democratic value in three contexts. Drawing on these three kinds of democratic value of information privacy, Parts III through V examine the information privacy jurisprudence of Taiwan's Grand Justices of the Judicial Yuan—Taiwan's Constitutional Court. Part III addresses information privacy's democratic value in terms of its limiting of the government's exercise of power. This part discusses *J.Y. Interpretations Nos. 535*,[2] *585*,[3] and *631*.[4] Part IV discusses the "database problem" and information privacy's democratic value in providing procedural safeguards for data subjects. This part examines *J.Y. Interpretations Nos. 293*[5] and *603*.[6] Part V explores

1. For instance, U.S. Supreme Court Justice Brandeis in his dissent in *Olmstead v. United States* has stated that privacy, or the right to be let alone, is "the most comprehensive of rights and the right most valued by civilized men." *See* Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

2. J.Y. Interpretation No. 535 (2001) (Taiwan), *available at* http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=535.

3. J.Y. Interpretation No. 585 (2004) (Taiwan), *available at* http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=585, .

4. J.Y. Interpretation No. 631 (2007) (Taiwan), *available at* http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=631.

5. J.Y. Interpretation No. 293 (1992) (Taiwan), *available at* http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=293.

6. J.Y. Interpretation No. 603 (2005) (Taiwan), *available at* http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=603.

information privacy's democratic value as a means of reinforcing free speech. This part considers *J.Y. Interpretation No. 689*,[7] and rethinks the relationship between information privacy and speech. Part VI concludes this note's arguments.

II. INFORMATION PRIVACY AND ITS RELATIONSHIP TO DEMOCRACY

For the purposes of this note, the right to information privacy means a legal protection for one's autonomy to control the flow of his or her information. This approach to understanding information privacy prevails in the information privacy law of the United States.[8] A paradigm of "information privacy as control" has been developed for decades. Under this paradigm, information privacy is seen as securing one's autonomy to control the disclosure and flow of his or her personal information.[9]

Information privacy is sometimes regarded as being in tension with democratic principles. Consider the dispute that led the Grand Justices to render *J.Y. Interpretation No. 293*. In 1992, the Taipei City Council requested that the Bank of Taipei, a bank owned by Taipei City, produce documents regarding the Bank's non-performing loans, overdue debts, and bad debts.[10] The City Council made this request because it suspected that the Bank had failed to collect some of its customers' overdue debts because of these customers' particular political backgrounds.[11] The Bank refused, contending that the Banking Act prohibited it from disclosing its customers' financial information. The City Council petitioned the Grand Justices for an *J.Y. Interpretation* as to whether the City Council would have authority to ask the city-owned Bank to deliver the requested materials for review. In *J.Y. Interpretation No. 293*, the Grand Justices replied in the affirmative, but only under certain conditions they set forth.[12]

---

7. J.Y. Interpretation No. 689 (2011) (Taiwan), *available at* http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=689.

8. U.S. Dept. of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 763 (1989) ("[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."). *See also* Michael D. Birnhack, *A Quest for a Theory of Privacy: Context and Control*, 51 JURIMETRICS J. 447, 449 (2011); Charles Fried, *Privacy*, 77 YALE L.J. 475, 483 (1968) (emphasizing the notion of "control" when he defines privacy as "control over knowledge about oneself"—not only "control over the quantity of information abroad," but also control over "the quality of the knowledge" about oneself); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1205, 1266 (1998) (citing Clinton Administration's Information Infrastructure Task Force, Principles for Providing and Using Personal Information and stating that "control is at the heart of information privacy").

9. *See*, *e.g.*, ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967) (stating that "[p]rivacy is the claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others").

10. *J.Y. Interpretation No. 293*, (petition).

11. *Id*.

12. *Id*. (holding & reason).

This case illustrates the tension between information privacy and democracy. Out of respect for information privacy, the Bank should not disclose its customers' financial information without their consent. In the interest of democracy, however, under its supervisory authority, the City Council ought legitimately to able to review and ascertain whether the Bank had properly operated its business. As this case suggests, while information privacy often prefers nondisclosure, democratic principles usually favor transparency and disclosure. Some commentators stand on side of democracy, arguing that government and society should be open to citizens. Thomas I. Emerson and others have argued for an "open government," which means that the government should be transparent and accountable to its citizens.[13] Fred H. Cate has emphasized the importance of "the free flow of information."[14] In their view, openness, transparency, accountability, and the free flow of information are important to a self-governing democracy. Those who think in this way may consider information privacy and its nondisclosure protection as being in tension with democracy because they usually regard information privacy as an individual's desire to withhold information that he or she would not like to share with others.[15]

Information privacy, however, is not just a personal value; rather, it advances public values central to our democratic tradition. As Allan F. Westin has stated, information privacy "is an irreducibly critical element in the operations of individuals, groups, and government in a democratic system with a liberal culture."[16] As indicated below, information privacy not only secures the personal interests of each member in the society, but also benefits the society as a whole by restricting the government's unreasonable intrusions and by encouraging citizens to meaningfully engage in the

13. Thomas I. Emerson, *Legal Foundations of the Right to Know*, 1976 WASH. U.L.Q. 1, 14-15 (arguing for a constitutional "right to know in obtaining information from governmental or private sources"). *See also* Wallace Parks, *Open Government Principle: Applying the Right to Know Under the Constitution*, 26 GEO. WASH. L. REV. 1, 3 (1957) (arguing for an open government principle and stating "[t]he accessibility of information about the national executive and administrative agencies and their operations to those engaged in the collection and dissemination of factual and evaluative information to the various 'free publics' and to the Congress is required for our democratic system to function successfully").

14. Fred H. Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877, 881-82 (2000) (suggesting that "the free flow of information" would be "the most important consideration when balancing restrictions on information" and indicating that "the free flow of information" "is not only enshrined in the First Amendment, but frankly in any form of democratic or market economy").

15. *See*, *e.g.*, Richard A. Posner, *An Economic Theory of Privacy*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY 337-38 (Ferdinand D. Schoeman ed., 1984). Eugene Volokh also sees information privacy as an individual interest, stating that information privacy is one's "right to control your communication of personally identifiable information about me," namely "a right to have the government stop you from speaking about me." *See* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1050-51 (2000).

16. WESTIN, *supra* note 9, at 368.

democratic process.

Scholars have identified the democratic values inherent to information privacy in various contexts. Three of these are particularly important and therefore merit discussion here. First, information privacy is essential for democratic traditions because it limits the government's exercise of power. As Priscilla M. Ragan has noted, the constitutional guaranty against the government's unreasonable search and seizure helps the society to "establish the boundaries for the exercise of [the government's] power."[17] By keeping the government off our persons and out of our houses, correspondence, and private conversations, the constitutional protection for privacy preserves a private sphere that is essential for the development of a democratic society.

Second, information privacy secures democratic values by providing citizens with certain procedural protections. As Paul M. Schwartz has observed, information privacy's counterpart in Germany—the right and the principle of "informational self-determination"—suggests a procedural dimension of information privacy that ensures one's participation in the collection and usage of his or her personal information.[18] Schwartz argues for a notion of "privacy as participation," emphasizing information privacy's value to achieving deliberative autonomy and deliberative democracy.[19] This approach to information privacy is especially important when we consider that the government may access public and private databases that store private information about individuals.

Third, information privacy's democratic value can be found in its reinforcement of the freedoms of thought, speech, and other intellectual activities. Neil M. Richards has argued for "intellectual privacy," noting that the government's surveillance and censorship of individuals' intellectual activities could prevent them from thinking differently and generating new ideas.[20] Without privacy protection for individuals' "thinking, reading, and private discussion," he further explains, they cannot deliberate and

17. PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 225-27 (1995). Daniel J. Solove has also argued that the Constitution "protect[s] against random searches of the home because they pose a threat to us all. The value of protecting against such searches emerges from society's interest in avoiding such searches, not from any one particular individual's interest." *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 99 (2008). Scott E. Sundby has offered another approach to understanding the constitutional protection against unreasonable searches and seizures, arguing that the Fourth Amendment, which keeps government officers out of people's "persons, houses, papers, and effects," can be viewed as a constitutional mechanism to maintain "a reciprocal trust between the government and its citizen." *See* Scott E. Sundby, *"Everyman"'s Fourth Amendment: Privacy or Mutual Trust between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1777 (1994).

18. Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 555 (1995).

19. *Id. See also* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1648-54 (1999).

20. Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 403-04 (2008).

participate in any democratic or social process.[21] Therefore, information privacy can be viewed as a precondition for a free and democratic society.

In the following parts this note will draw on the exposition of information privacy's values in these three contexts to examine the jurisprudence of information privacy of Taiwan's Constitutional Court.

III. INFORMATION PRIVACY'S DEMOCRATIC VALUE IN LIMITING THE GOVERNMENT'S EXERCISE OF POWER

A. *J.Y. Interpretations Nos. 535, 585, and 631*

J.Y. Interpretation No. 535 involves a challenge to the constitutionality of the police's stop and inspection practices. Under the then-effective Police Service Act, the police were able to, without a warrant, (1) stop a person in a public place, and then frisk, inspect, and even question him; (2) enter into a private place, and then inspect the place and persons therein.[22] Noting that this practice has interfered with individuals' privacy and other fundamental rights, the Grand Justices held that the practice is constitutional only if it is conducted pursuant to a law which specifically prescribes its requirements and procedures as well as the remedies for unlawful inspections. The Grand Justices further stated that when inspecting places, the police's authority is limited to those places where danger exists or where a reasonable reason indicates that danger may exist. In particular, if the inspected place is a private residence, such a place should be accorded the same protection as a home. When inspecting a person, the police should not exceed the degree necessary for the given circumstances. The Grand Justices also laid down several procedural rules for police inspections, including the requirements that the police should show the checked person their identification, state the purpose of each inspection, and should not take the inspected person to the police station except in the case of some limited exceptions.

Although the Grand Justices mentioned the right to privacy in *J.Y. Interpretation No. 535*, they did not further explain the nature of this right or state on what basis it was grounded. Three years later, in *J.Y. Interpretation No. 585*, the Grand Justices had an opportunity to revisit this "unfinished business." At issue was the constitutionality of the Act of the Special Committee on Investigation of the March 19 Shooting Event. The legislature passed this Act to establish a special agency to investigate a shooting event,

21. *Id.* at 392, 406 (arguing that intellectual privacy is essential to maintain an open society that tolerate people bearing all kind of opinions).

22. For instance, the petitioner of this interpretation alleged that the police stopped him when he was walking on the street at night. After refusing to show identification to the police, he was frisked and questioned by the police. *See* J.Y. Interpretation No. 535 (2001) (Taiwan) (petition), *available at* http://www.judicial.gov.tw/constitutionalcourt/uploadfile/C100/535.pdf.

which happened one day before the 2004 presidential election. The Act set off a fierce constitutional debate because it attempted to delegate to the Commission the broad authority and power to conduct the investigation.

Among the Act's various controversial provisions, the Grand Justices held unconstitutional one provision of the Act that granted the Committee an unlimited interrogatory authority. Under this provision, the Commissioners could pose to the interrogated any question, and the interrogated could not refuse to answer even if that testimony might infringe upon his, her, or another's privacy. The Grand Justices held that this provision infringed on individuals' constitutional right to privacy. According to the Grand Justices, though not explicitly prescribed in the Constitution, the right to privacy deserves constitutional protection because "it is indispensible for human dignity and individuality." They furthermore asserted that, "the right to privacy not only preserves the integrity of personality, but also secures one's personal private sphere free from others' intrusions and one's autonomy to control personal information."[23] The Grand Justices grounded this right as an unenumerated fundamental right protected by Article 22 of the Constitution.

Three years later in 2007, in *J.Y. Interpretation No. 631* the Grand Justices held unconstitutional parts of the Communication Protection and Monitoring Act, which permitted prosecutors to issue a writ of communication monitoring and to conduct warrantless wiretapping. The Grand Justices based this decision mostly on Article 12 of the Constitution, holding that this Article protects individuals' privacy in private communications. Recognizing wiretapping as a form of government interference in fundamental rights, which is much more intrusive than searches and seizures, the Grand Justices held that under Article 12, a writ of communication monitoring should be issued by an impartial and independent judge.

B. *Spatial Privacy, Communicative Privacy, and Information Privacy*

These three interpretations relate to individuals' information privacy defined as the autonomy to control their private information. In each case, the government's purpose when intruding into people's private lives is to gather information from them. When stopping a person on the street, the police asked for the person's identification information. When interrogating a witness, the Special Committee looked for information which would help it "seek the truth" of the shooting event. When monitoring a person's phone conversations, the prosecutor expected to obtain incriminating evidence

23. *Id.* (reasoning sec. 5).

against him. The constitutional protection that the Grand Justices identified in each of these cases ensures people's autonomy to control the flow of their personal information against the government's arbitrary intrusions. Under such constitutional protection, the government could not obtain individuals' private information without complying with the Constitution's requirements.

These interpretations also illustrate the importance of information privacy in limiting the government's exercise of power, thereby securing a private sphere for individuals free from unwanted interference. For instance, the Grand Justices in *J.Y. Interpretation No. 535* attempted to set forth rules for the government as to when, for which purpose, and how it could intrude into a person's private life. In particular, *J.Y. Interpretation No. 535* delineated a concept of "spatial privacy" by emphasizing the significance of the home and other private residences.

Respect for the home's sanctity can be traced back to James Otis's argument in 1761. As a lawyer in colonial Massachusetts who argued against the British authorities' aggressive search and seizure practices, he famously contended, "[a] man's house is his castle; and whilst he is quiet, he is as well guarded as a prince in his castle."[24] The U.S. Supreme Court incorporated Otis's idea that "a man's house is his castle" into its Fourth Amendment[25] jurisprudence in *Silverman v. United States*.[26] The *Silverman* Court stated that the Fourth Amendment secures "the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[27]

Spatial privacy is important for democracy because it enables individuals to retreat from their public lives into a private sphere.[28] "A room of one's own" enables us to isolate ourselves from the public scrutiny in order to think freely, to deliberate and form political judgments, and to generate ideas that are new, unpopular, or even offensive to the society.[29] When people are aware that the government or others are watching or

---

24. James Otis, *Notes of the Argument of Counsel in the Cause of Writs of Assistance, and of the Speech of James Otis*, *in* 2 THE WORKS OF JOHN ADAMS 521, 524-25 (Charles Francis Adams ed., 1856).

25. The Fourth Amendment to the U.S. Constitution provides, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and 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." U.S. CONST. amend. IV.

26. Silverman v. United States, 365 U.S. 505 (1961).

27. *Id.* at 511.

28. WESTIN, *supra* note 9, at 24 ("Personal retreats for securing perspective and critical judgment are also significant for democratic life.").

29. VIRGINIA WOOLF, A ROOM OF ONE'S OWN 2 (1929) ("[A] woman must have money and a room for her own if she is to write fiction . . . ."). *See also* Richards, *supra* note 20, at 413; Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 450 (1980) (arguing that privacy serves as a shelter for people with unfavorable opinions and thus enhance their willingness to "declare their unpopular views in public"). *Cf.* James Griffin, *The Human Right to Privacy*, 44 SAN DIEGO L. REV. 697, 715 (2007).

observing them, they are unlikely to insist on their own beliefs. In such situations, most people will likely change their minds to conform to the watcher's views.

The work of Henry David Thoreau suggests that everyone needs a "Walden Pond" to develop new ideas.[30] In his book *Walden*, Thoreau described how much he enjoyed the solitude at Walden Pond, a place away from the usual lives of most people.[31] Only in a place where we can freely reject society's prevailing views and fully embrace our own beliefs may we generate new and different ideas that contribute to deliberate judgments and the diversity of ideas.

J.Y. Interpretation No. 631 involves privacy in a different sense, that is, communicative privacy. The Grand Justices in *J.Y. Interpretation No. 631* stated that Article 12 of the Constitution secures people's privacy in private communications. We usually expect more privacy protection for our communications in letters, telephone calls, and private conversations. As to letters and other private written correspondences, the U.S. Supreme Court in *Ex parte Jackson* held that sealed letters could not be opened and read by the government without a warrant.[32] As to telephone conversations, the Court in *Katz v. United States* held that the government's overhearing of individuals' telephone conversations constituted a search within the meaning of the Fourth Amendment.[33]

The constitutional protection of private communications is central to democracy. This is because the success of a democracy requires the deliberation and free exchange of ideas on public issues by its citizens. Many people (especially political dissenters) might decline to express their thoughts to others when they are aware that the government might overhear their conversations. In addition, the lack of protection for information privacy may prevent them from sharing ideas, especially when they fear that the ideas in their minds are not ready to be submitted to public criticism.[34] While information privacy is often considered to be one's claim to withhold his or her private information, it can also be understood as one's desire to disclose information to the persons he or she trusts, believing that they will

30. HENRY DAVID THOREAU, *Where I Lived, What I Lived for*, *in* WALDEN 88 (Mercer Univ. ed., 2011) (1854) ("I went to the woods because I wished to live deliberately, to front only the essential facts of life, and see if I could not learn what it had to teach, and not, when I came to die, discover that I had not lived."). *See also* NEIL M. RICHARDS, INTELLECTUAL PRIVACY (forthcoming 2014) (manuscript Ch. 6, at 2) (on file with author).

31. THOREAU, *supra* note 30, at 128.

32. *Ex parte* Jackson, 96 U.S. 727, 733 (1877) ("[T]heir papers, thus closed against inspection, . . . can only be opened and examined under like warrant . . . .").

33. Katz v. United States, 389 U.S. 347, 353 (1967) ("[Government's] activities in electronically listening to and recording [telephone conversations] . . . violated the privacy upon [the petitioner] and thus constituted a 'search and seizure' . . . .").

34. Richards, *supra* note 20, at 424.

keep it in secret.[35] Thinking of information privacy in this way suggests that information privacy encourages individuals to share with others ideas, questions, or conclusions in their minds, while keeping their communications in secret.[36] In this sense, information privacy provides protection for private discussions and exchanges of ideas, in the context of which different thoughts and conclusions usually occur.

Communicative privacy is essential for democracy because the government's surveillance of its citizens has posed a significant threat to free communications. This is why U.S. Supreme Court Justice Brandeis has argued for "a right to be let alone" against the government's wiretapping practice. In his famous dissent in *Olmstead v. United States*, he argued that government wiretapping should be considered as a search under the Fourth Amendment.[37] Emphasizing the significance of the constitutional protection of one's beliefs, thoughts, emotions and sensations, Justice Brandeis argued for a "right to be let alone" against "every unjustifiable intrusion by the government upon the privacy of the individual."[38] Justice Brandeis's argument highlights the importance of constitutional protection of private conversations in which the exchange of ideas usually takes places.

Free discussion is a core value of the freedom of the speech. In *On Liberty*, John Stuart Mill explained why free discussion (the "freedom of the expression of opinion") is important.[39] According to Mill, the freedom of discussion serves as the best way to prevent true beliefs from "becoming a mere formal profession," which is "in danger of being lost," because, without the freedom of discussion, people might hold true beliefs "in the manner of prejudice, with little comprehension or feeling of its rational grounds."[40] When understood in this way, communicative privacy demonstrates its democratic value in encouraging the free exchange of ideas, which reflect people's thoughts on matters of politics, religion, science, the arts, or intimacy.

At the core of the privacy issues presented in *J.Y. Interpretation No. 585* is the question of whether the government may achieve its goals by all means regardless of whether these may interfere with people's fundamental rights and freedoms. We can find the answer to this question by reading *J.Y. Interpretations Nos. 535* (spatial privacy) and *631* (communicative privacy) together, which reveal the value privacy holds in relation to the limitation of the government's exercise of power. The Constitution and the democratic

35. WESTIN, *supra* note 9, at 31.
36. Richards, *supra* note 20, at 421-22.
37. Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).
38. *Id*. at 478.
39. JOHN STUART MILL, ON LIBERTY 33, 69 (J. Gary & G.W. Smith eds.,1991) (1859).
40. *Id.* at 69-70.

values it supports never tolerate the unlimited exercise of government power. Undoubtedly, the government has a legitimate interest in exercising its policing power in order to maintain public order and security. Information privacy, however, along with other fundamental rights, constitutes a constitutional constraint upon the government's policing power. In light of this, *J.Y. Interpretation No. 585* correctly confirmed that granting a government agency a broad, unlimited interrogatory authority violated this constitutional constraint.

IV. THE DATABASE PROBLEM AND THE PROCEDURAL DIMENSION OF INFORMATION PRIVACY

A. *J.Y. Interpretations Nos. 293 and 603*

As indicated above, *J.Y. Interpretation No. 293* revolved around the controversy as to whether the City Council could request that a city-owned Bank deliver to it documents pertaining to customers' information.[41] Although the Bank contended that the Banking Act prohibited it from disclosing its customers' financial information, the Grand Justices held that the City Council had the authority to make such a request in order to perform its duty to supervise and investigate the city-owned Bank. Nevertheless, the Grand Justices set forth conditions for the Bank's disclosure, including the requirements that the City Council must pass a resolution to request the Bank to produce the requested materials; that the Bank must remove customers' names from the documents; and that the City Council must review the documents in a nonpublic session.[42] *J.Y. Interpretation No. 293* was the first time the Grand Justices mentioned the term "the right to privacy." The Grand Justices, however, did not further elaborate as to what the right is, merely stating in passing that the Banking Act's nondisclosure provision attempted to secure bank customers' right to privacy in their financial records.

J.Y. Interpretation No. 603 is a landmark case. At dispute was the Household Registration Act's fingerprint requirement, under which citizens who are fourteen or older must be fingerprinted before being issued a new ID card. The Grand Justices held this requirement unconstitutional because it violated people's constitutional right to information privacy. The Grand Justices stated that the Constitution secures a fundamental right to information privacy, which is essential to one's dignity and integrity of personality. In the reasoning, the Grand Justices further explained that the

41. *See* J.Y. Interpretation No. 293 (1992) (Taiwan), *available at* http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=293.

42. *Id.* (holding & reasoning)..

constitutional right to information privacy secures one's right to determine whether, to what extent, when, to whom, and in which manner to disclose his or her personal information. This right, the Grand Justices added, also guarantees one's right to control and to be informed of the usage of his or her personal information. If his information is inaccurately recorded, according to the Grand Justices, the individual must have a right to correct it. Recognizing that the right to information privacy was not absolute, the Grand Justices held that the legislature may enact a statute to limit this right if this is necessary to accomplish a legitimate purpose. But the legislature must provide specific purposes for the limitation. Adequate data security measures would be required as well. And, if the government attempts to collect individuals' sensitive information, a higher level of legitimacy would be required in order for such collection to pass judicial scrutiny.[43]

The Grand Justices therefore struck down the fingerprint requirement. Noting that the Household Registration Act did not stipulate any purpose for collecting fingerprints, the Grand Justices held that the Act was inconsistent with the constitutional guarantee of information privacy.[44] Defending the Act's constitutionality, the Ministry of Interior contended that the fingerprint requirement did achieve several public interests, such as preventing false claims of ID cards and identifying roadside unconscious patients.[45] The Grand Justices, however, rejected these defenses altogether, considering them insufficient to legitimize the government's compulsory collection of fingerprints. In the Grand Justices' view, fingerprints deserve more protection than other forms of personal data because of their greater sensitivity. Due to the uniqueness and immutability of fingerprints, the Grand Justices explained, once stored in a database and connected to one's identification, fingerprints would enable the government to access one's personal data profile by cross-matching the fingerprints with other personal information.[46]

B. *The Database Problem*

J.Y. Interpretations Nos. 293 and *603* both involve the database problem—an information privacy concern that arises in the context of databases. *J.Y. Interpretation No. 603* involves the question of whether the government may compulsorily collect and store people's fingerprints in a

43. J.Y. Interpretation No. 603 (2005) (Taiwan), *available at* http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=603.

44. *Id.*

45. *Id.* (summary of the MOI's arguments), *available at* http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=603.

46. *Id.* (reasoning).

database. *J.Y. Interpretation No. 293,* on the other hand, is concerned with whether the government may access a publicly owned bank's database containing customers' financial information.

The advent of this database problem can be attributed to the expansion of governments in modern times. The twentieth century witnessed an expansion of the modern state's roles, powers, and functions. As a modern state assumes an active role and takes more responsibility for the wellbeing of its citizens, it must gather more information from its citizens.[47] Governmental agencies collect private information for various purposes. Advances in information technology have enabled the government to collect and process information more efficiently; in particular, new and improved technologies have made it possible to combine all data stored in various databases in various forms into a centralized database. This means, for instance, that when a person submits his income data to a tax-collecting agency, it is possible that this data may be disseminated and stored by another agency for subsequent use.

The U.S. Supreme Court in *Whalen v. Roe* has recognized the database problem and "the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[48] In many respects, as the Court noted, government administration relies on "the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed."[49]

The Grand Justices in *J.Y. Interpretation No. 603* expressed a similar concern related to public databases, and declared that the government could collect and store people's fingerprints in a large-scale database only in the pursuit of certain compelling public interests.[50]

Similarly, private businesses also engage in widespread collection and storage of individuals' personal information. In our everyday lives, we constantly provide personal information to banks, telephone companies, search engines, social network websites, and online stores. These entities keep our records in databases to know us better. Yet, these detailed personal data profiles have become a sellable product on the market,[51] and while most companies issue privacy policies under which our data's confidentiality ought to be respected, this situation still gives rise to some privacy concerns. Among them, data insecurity is most salient, especially after reports of

47. *See*, *e.g.*, Paul M. Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 HASTINGS L.J. 1321, 1331-33 (1992).

48. Whalen v. Roe, 429 U.S. 589, 605 (1977).

49. *Id*.

50. *J.Y. Interpretation No. 603*, (holding).

51. *See*, *e.g.*, Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1156-60 (2005).

several instances of high-profile data leakage. The problem of scam organizations has demonstrated just how worrisome the issue of data insecurity is. In order to fool their victims, members of these organizations usually begin a scam phone call by showing that they already know something private or specific about the victim, and this information was acquired from certain private databases.

We expect the government to regulate private databases and their commercial trading of personal data. Nonetheless, we should not overlook privacy violations arising from the government's access to private databases. The case of *Gonzales v. Google, Inc*. is a good example of this concern.[52] In 2006, the U.S. government requested that Google and other search engines provide the government access to records of their users' search terms and other records.[53] The records that the government obtained from search engine companies not only indicated which websites a user visited and which terms were searched, but also revealed the user's reading habits, intellectual activities, lifestyles, and details concerning other intimate matters. With such access to private databases like search engines or social network websites, the government may easily engage in surveillance of our private activities, online or offline.

C. *The Procedural Dimension of Information Privacy*

The "information privacy as control" paradigm, however, is insufficient for dealing with the database problem. This is because the control approach focuses more on the autonomy question: whether data subjects have consented to the disclosure of their data to the databanks. Data subjects' autonomy, however, is often not fully respected when the subjects provide their information to a database. For instance, when taxpayers file their tax returns with the authorities, they supply a lot of personal information. The government, however, has never attempted to seek consent from taxpayers. In such situations, "information privacy as control" makes little sense

52. Gonzales v. Google, Inc., 234 F.R.D. 674 (N.D. Ca. 2006).

53. The U.S. Department of Justice (DOJ) made such a request because it was preparing to respond to a challenge to the constitutionality of the Child Online Protection Act (COPA) in another pending case, *ACLU v. Gonzales*. *See* Danny Sullivan, *Bush Administration Demands Search Data; Google Says No; AOL, MSN & Yahoo Said Yes*, SEARCH ENGINE WATCH (Jan. 19, 2006), http://searchenginewatch.com/article/2059843/Bush-Administration-Demands-Search-Data-Google-Says-No-AOL-MSN-Yahoo-Said-Yes; *ACLU v. Gonzales,* 478 F. Supp. 2d 775, 778 (E.D. Pa. 2007). To collect information regarding search engine users' search queries, the DOJ served Google, and other search engines, subpoenas which required Google to produce the text of users' search queries. The DOJ hoped that the requested materials could assist the government in defending the COPA, by demonstrating that the statutory restrictions in COPA effectively protect "minors from exposure to harmful materials on the Internet." *See id.* at 679.

because people do not have a meaningful choice at all.[54]

The case of *J.Y. Interpretation No. 293* is another good example illustrating aspects of the database problem. The customers of the city-owned Bank in the case of *J.Y. Interpretation No. 293*, could hardly have conceived of the possibility that the City Council would request that the Bank disclose their information. Instead, they may reasonably expect that the Bank would keep their financial records confidential. In the database context, thus, to address whether each data collector respects each data subject's autonomy might provide less insight for resolving the database problem.

To address this concern, it is helpful to consider information privacy's counterpart in Germany—the right and principle of "informational self-determination." In its 1983 *Census Act Case*, the Federal Constitutional Court of Germany developed a fundamental right of informational self-determination.[55] The Court grounded this right in its jurisprudence of "free development of personality." Noting that data processing technology may threatened one's integrity of personality, the Court found that Article 2 (1) of the Basic Law, in conjunction with Article 1(1),[56] protects a right of informational self-determination, which assures an individual's right to determine whether, when, and how to disclose his or her private information to others.[57]

Emphasizing the significance of informational self-determination, the Court stated that if an individual does not know which information about him or her is known by others in social life, his or her capacity for self-determination will be greatly inhibited. Such a lack of information protection, the Court added, would not only prevent an individual from developing his personality, but would also harm society as a whole. This is because, the Court explained, self-determination is a precondition for a free society, and a free, democratic society is built upon the premise that its citizens can meaningfully act and participate in social processes.[58]

---

54. Fred H. Cate, *Protecting Privacy in Health Research: The Limits of Individual Choice*, 98 CAL. L. REV. 1765, 1776-77 (2010).

55. Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Dec. 15, 1983, 65 Entscheidungen des Bundesverfassungsgerichts [BverfGE] 1 (Ger.) [hereinafter *Census Act*]. *See also* DONALD P. KOMMERS, THE CONSTITUTIONAL JURISPRUDENCE OF THE FEDERAL REPUBLIC OF GERMANY 323-25 (2d ed. 1997).

56. Article 2(2) of the Basic Law provides in part, "[e]very person shall have the right to life and physical integrity." Article 1(1) of the Basic Law provides that "[h]uman dignity shall be inviolable. To respect and protect it shall be the duty of all state authority". The English translation of the Basic Law, *see* BASIC LAW FOR THE REPUBLIC OF GERMANY 15 (Christian Tomuschat & David P. Currieet trans., German Bundestag 2010), *available at* https://www.btg-bestellservice.de/pdf/80201000.pdf.

57. KOMMERS, *supra* note 55, at 324-25 ("Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.").

58. *Id.*

The Court has further developed the principle of informational self-determination. Under this principle, the government may collect individuals' information only pursuant to a law that specifies the purposes and conditions of this information collection practice. Any collection of individual information which may interfere with individuals' informational self-determination must serve as a means necessary to protect public interests and must be consistent with all constitutional principles, such as the principle of proportionality. In addition, the informational self-determination principle requires the government to adopt adequate organizational and procedural measures to ensure that citizens are protected from unwanted invasions of privacy.[59]

The *Census Act* Case suggests a procedural dimension of information privacy. According to the *Census Act* Court, informational self-determination requires that the government or a database ensure that each data subject is informed of which information about him or her is collected and stored in the database. In addition, the government should set forth procedural mechanisms to encourage data subjects to participate in the processing or usage of their information. Informational self-determination also requires some organizational measures to oversee data security within the processing and usage of personal data.

J.Y. Interpretations Nos. 293 and *603* involve this procedural dimension of information privacy. Although the Grand Justices in *J.Y. Interpretation No. 293* might not have articulated a clear notion of information privacy, they implied their perception of data protection by setting forth some procedural requirements. Instead of giving substantive protection—which would have forbid disclosure or required the Bank to seek consent from customers—the Grand Justices set forth procedural requirements under which (1) the City Council must pass a resolution to request the Bank to produce the documents; (2) the Bank should remove the customers' names from the requested materials; and (3) the City Council must review the materials in a nonpublic session.

We can also find procedural protections for information privacy in *J.Y. Interpretations No. 603*. In fact, the rationale and structure of reasoning in *J.Y. Interpretation No. 603* appear to be similar to those of Germany's *Census Act* case. In particular, like Germany's principle of informational self-determination, *J.Y. Interpretation No. 603* also attempted to develop a general data protection principle. For instance, the Grand Justices said that each data subject should have the right to be informed of the collection and usage of his or her information, and when information has been inaccurately recorded, he or she has the right to correct it.

59. *Id.*

These procedural protections are more about procedural rules and organizational design. They thus move the focus of data protection law away from the "information privacy as control" paradigm. As indicated above, Paul M. Schwartz has argued for a "privacy as participation" approach to understanding data protection and information privacy. Under Schwartz's approach, information privacy law should be restructured to include: (1) a statutory definition of databases' obligations as to personal data usage; (2) "the maintenance of transparent processing systems;" (3) a declaration of data subjects' substantive and procedural rights; and (4) an effective oversight mechanism.[60] By refining data protection law in this way, he purports to secure the individual's capacity for decision-making. Schwartz argues that data protection law "must structure the use of personal information so that individuals will be free from state [surveillance] or community intimidation that would destroy their involvement in the democratic life of the community."[61]

Professor Schwartz's argument reminds us of information privacy's democratic value in securing "deliberative autonomy" and "deliberative democracy." Under the theory of deliberative democracy, an ideal democracy depends on its citizens' deliberation and discussion of public issues, which requires the citizens' capacity for "deliberating and judging the justice of basic institutions and social policies, as well as the common good."[62] Equally important, an ideal democracy depends on its citizens' "deliberative autonomy," which demands that citizens possess the capacity for "deliberating about and deciding how to live their own lives."[63]

The data privacy problem, however, has become a threat to individuals' capacity for living their private lives and forming their own judgments. Cases like the *Census Act* decision and *J.Y. Interpretation No. 603* have shown that the government is eager to establish a vast database to store people's personal information. While we may find ourselves displeased about this common practice, it is hardly for us to deny the government's "need" to collect and store our information. People who argue for the government practice of creating and maintaining databases usually point out that systems of public records and databases improve the policymaker's capacity for making good decisions and thus promote the general welfare.[64] This is why we need procedural protections for our privacy. Without information privacy protections against these practices, individuals might

60. Schwartz, *supra* note 18, at 563-65.

61. *Id.* at 561.

62. JAMES E. FLEMING, SECURING CONSTITUTIONAL DEMOCRACY: THE CASE OF AUTONOMY 3, 39 (2006).

63. *Id.* at 3.

64. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 205 (2010).

lose the capacity for making autonomous, independent decisions. As Spiros Simitis has warned, the government's data collection and processing activities "increasingly appears as the ideal means to adapt an individual to a predetermined, standardized behavior that aims at the highest possible degree of compliance with the model [citizen]."[65] In light of this concern, many scholars view information privacy as "prerequisite to the capacity to participate in social discourse." [66] By applying restrictions to the government's data processing practices and encouraging individuals to participate in social processes, information privacy and its procedural protection contribute to a social environment that favors citizen participation and deliberation.

V. THE DEMOCRATIC VALUE OF INFORMATION PRIVACY IN REINFORCING FREE SPEECH

A. *J.Y. Interpretation No. 689*

In *J.Y. Interpretation No. 689,* the Grand Justices grappled with two competing values: privacy and freedom of the press. At issue was the constitutionality of a provision in the Social Order Maintenance Act, which authorizes the police to fine a person who stalks another without justifiable cause and fails to take advice and stop. The petitioner is a journalist who was fined under this provision because he followed celebrities on the street in order to gather information for a news story. He challenged this provision's constitutionality, alleging that it restricted his constitutional right of newsgathering, which is guaranteed as part of freedom of the press.

The Grand Justices upheld the Act's stalking provision. Nonetheless, the Grand Justices said that when a journalist is following and observing a person for reporting a matter of a legitimate concern to public and his or her means of gathering information are not offensive to society, the journalist's stalking cannot be considered as unjustifiable within the meaning of the Act. By so doing, the Grand Justices attempted to resolve a conflict between freedom of the press and privacy.

The matters at hand in *J.Y. Interpretation No. 689* is different from the Grand Justices' previous privacy cases. Here, the privacy violation arose from a private person's interference with the victim's "right to be let alone," not from a state action. Thus, the Grand Justices further articulated the

65. Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 733 (1987).

66. *Id*. at 734. *See also* Schwartz, *supra* note 19, at 1648-58; Danielle Keats Citron, *Fulfilling Government 2.0's Promise with Robust Privacy Protections*, 78 GEO. WASH. L. REV. 822, 842-43 (2010); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423-28 (2000).

meaning and protection of privacy in the reasoning. First, the Grand Justices affirmed the right to privacy as a fundamental right protected by the Constitution. Due to the significance of privacy for human dignity and integrity of personality, the Grand Justices declared, the government has an obligation to prevent violations to privacy, regardless of whether that violation is from the government or a private person.

Second, the Grand Justices found that an individual may not dispossess him or her of this privacy, for instance, simply because he or she is in a public place. Noting that advanced technology has made it easier to monitor others, the Grand Justices formulated a notion of privacy that preserves a private sphere for individuals where they are free from unwanted surveillance. According to the Grand Justices, individuals can still enjoy privacy protection even if they are in public places, as long as they have exhibited an expectation of privacy, and this expectation is regarded as reasonable by society.[67]

B. *The Relationship between Information Privacy and Speech*

J.Y. Interpretation No. 689 illustrates the inherent tension between the nondisclosure protections of information privacy and the values of a free press and free speech. As indicated above, the Grand Justices attempted to strike a balance between these two competing values. By doing so, they refined the boundary between the public and private spheres, and afforded qualified protection to people who are in public areas but have a reasonable expectation of privacy. The Grand Justices' public/private dichotomy can be traced back to *J.Y. Interpretations Nos. 535* and *631*, in which they preserved a private sphere for citizens free from unwanted interference. Although this dichotomy has encountered criticism for its inability to clearly delineate the scope of the privacy right,[68] the dichotomy appears to be especially helpful in cases involving the conflict between privacy and speech. Actually, the idea that the public/private dichotomy would help to balance privacy against free speech came from Warren and Brandeis's 1980 article, "*The Right to Privacy.*"[69] They distinguished public from private, limiting private protection to injuries caused by a speaker's intrusion or disclosure of private

67. The Grand Justices might adopt this approach to privacy by following U.S. Supreme Court Justice Harlan's famous test for the Fourth Amendment privacy right: in order for a defendant to invoke the protection under the Fourth Amendment, he must, first, "have exhibited an actual (subjective) expectation of privacy" and second, the expectation should be "one that society is prepared to recognize as 'reasonable'." Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

68. *See, e.g.*, NISSENBAUM, *supra* note 64, at 113-25.

69. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 214-16 (1890).

matters.[70]

The tensions between information privacy and speech were recognized when privacy was thus "invented" by Warren and Brandeis. This, however, is not the whole picture of the relationship between the two competing values. Information privacy protection reinforces free speech values in some significant but often neglected ways. As discussed above, Neil M. Richards has explained how information privacy protection for our intellectual activities supports free speech values. He notes, "[i]n order to speak, it is necessary to have something to say, and the development of ideas and beliefs often takes place best in solitary contemplation or collaboration with a few trusted confidants."[71] He thus argues for a theory of "intellectual privacy," which articulates a privacy right protecting one's thoughts, reading lists and habits, private communications, and a private sphere where ideas are generated and developed.[72]

Professor Richards's arguments reflect the democratic value in information privacy's supporting of free speech. We may locate the ways in which privacy supports speech in many contexts. For instance, as *J.Y. Interpretation No. 535* has suggested, information privacy protection against unreasonable searches and seizures implies a notion of spatial privacy, which preserves a private sphere where individuals may embrace their beliefs without worrying about public scrutiny. In this sense, information privacy ensures our freedom to develop new thoughts and ideas. Moreover, the communicative privacy in *J.Y. Interpretation No. 631* encourages individuals to share their thoughts and ideas. Information privacy, therefore, not only promotes exchange of ideas, but also reinforces our right to receive new ideas from private, informal discussions with others. In addition, as *J.Y. Interpretations Nos. 293* and *603* have shown, information privacy's procedural dimension protects our data privacy against the government's surveillance and censorship of our private activities. These procedural rules and data protection shore up our capacity to deliberate and participate in social processes. Even in cases involving the press, we can still find information privacy's support for the press in its protection of the offices of the press against the government's unreasonable searches, as well as in its protection for journalists' information sources.[73] The lack of protection for spatial privacy, communicative privacy, and data security will not only restrict our ability to develop our personalities, but also set off chilling

70. *Id.*

71. Richards, *supra* note 20, at 389.

72. *Id*. at 407-26.

73. *See*, *e.g.*, Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 150-51 (2007).

effects which democracy does not tolerate.[74] When we think about the collective significance of these cases together, they demonstrate that information privacy not only protects individuals' personal interest in nondisclosure, but also secures important public interests that are vital to a democratic society. For instance, political dissenters need communicative privacy to further develop their dissenting opinions. They also need privacy protection for their associational activities. These cases thus indicate that to the extent that we need information privacy protection to think, speak, deliberate, dissent, and participate within the context of democratic and social processes, information privacy possesses a demonstrable value in relation to the strengthening of democracy.

VI. CONCLUSION

Taking the Grand Justices' jurisprudence of information privacy as an example, this note reconsiders the relationship between information privacy and democracy. Identifying three of the democratic values inherent in information privacy, this note argues that information privacy can be regarded as a public value that reinforces democracy. As the conventional wisdom focuses too much on information privacy's nondisclosure protection, we often neglect the value of information privacy to democratic society. This note thus argues that when balancing privacy against other competing values (for instance public security), we should not regard privacy as a personal interest and therefore afford it less protection. As this note has shown, in order for people to freely think, speak, deliberate, dissent, and participate in the democratic process, they need protection of their information privacy. Without this, people cannot enjoy a truly free and democratic society. Information privacy, thus, is an important value for a democratic society.

74. *Id*. at 154-59.

REFERENCES

ACLU v. Gonzales, 478 F. Supp. 2d 775 (E.D.Pa. 2007).

Birnhack, M. D. (2011). A quest for a theory of privacy: Context and control. *Jurimetrics: The Journal of Law, Science, and Technology,51*, 447-480.

Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Dec. 15, 1983, 65 Entscheidungen des Bundesverfassungsgerichts [BverfGE] 1 (Ger.)

Cate, F. H. (2000). Principles of internet privacy. *Connecticut Law Review, 32*, 877-896.

Cate, F. H. (2010). Protecting privacy in health research: The limits of individual choice. *California Law Review, 98*, 1765-1804.

Citron, D. K. (2010). Fulfilling government 2.0's promise with robust privacy protections. *George Washington Law Review, 78*, 822-845.

Cohen, J. E. (2000). Examined lives: Informational privacy and the subject as object. *Stanford Law Review, 52*, 1373-1438.

Emerson, T. I. (1976). Legal foundations of the right to know. *Washington University Law Quarterly, 1976*, 1-24.

Ex parte Jackson, 96 U.S. 727 (1877).

Fleming, J. E. (2006). *Securing constitutional democracy: The case of autonomy*. Chicago, IL: University of Chicago Press.

Fried, C. (1968). Privacy. *Yale Law Journal, 77*, 475-493.

Gavison, R. (1980). Privacy and the limits of law. *Yale Law Journal, 89*, 421-471.

Gonzales v. Google, Inc., 234 F.R.D. 674 (N.D. Ca. 2006).

Griffin, J. (2007). The human right to privacy. *San Diego Law Review, 44*, 697-722.

Kang, J. (1998). Information privacy in cyberspace transactions. *Stanford Law Review, 50*, 1193-1294.

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

Kommers, D. P. (1997). *The constitutional jurisprudence of the Federal Republic of Germany* (2nd ed.). Durham, NC: Duke University Press.

J.Y. Interpretation No. 293 (1992) (Taiwan). Retrieved from http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=293

J.Y. Interpretation No. 535 (2001) (Taiwan). Retrieved from http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=535

J.Y. Interpretation No. 585 (2004) (Taiwan). Retrieved from http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=585

J.Y. Interpretation No. 603 (2005) (Taiwan). Retrieved from http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=603

J.Y. Interpretation No. 631 (2007) (Taiwan). Retrieved from http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=631

J.Y. Interpretation No. 689 (2011) (Taiwan). Retrieved from http://www.judicial.gov.tw/constitutionalcourt/EN/p03_01.asp?expno=689

Mill, J. S. (1991). *On liberty.* (J. Gary & G.W. Smith, Eds.). New York, NY: Routledge. (Original work published 1859)

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.

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

Otis, J. (1856). Notes of the argument of counsel in the cause of writs of assistance, and of the speech of James Otis. In C. F. Adams (Ed.), *The works of John Adams* (pp. 521-525). Boston, MA: Little, Brown.

Parks, W. (1957). Open government principle: Applying the right to know under the constitution. *George Washington Law Review, 26*, 1-22.

Posner, R. A. (1984). An economic theory of privacy. In F. D. Schoeman (Ed.), *Philosophical dimensions of privacy* (pp. 333-345). New York, NY: Cambridge University Press.

Regan, P. M. (1995). *Legislating privacy: Technology, social values, and public policy.* Chapel Hill, NC: University of North Carolina Press.

Richards, N. M. (2005). Reconciling data privacy and the First Amendment. *UCLA Law Review, 52*, 1149-1222.

Richards, N. M. (2008). Intellectual privacy. *Texas Law Review, 87*, 387-446.

Richards, N. M. (in press). *Intellectual privacy*. Manuscript submitted for publication.

Schwartz, P. M. (1992). Data processing and government administration: The failure of the American legal response to the computer. *Hastings Law Journal, 43*, 1321-1390.

Schwartz, P. M. (1995). Privacy and participation: Personal information and public sector regulation in the United States. *Iowa Law Review, 80*, 553-618.

Schwartz, P. M. (1999). Privacy and democracy in cyberspace. *Vanderbilt Law Review, 52,* 1609-1702.

Silverman v. United States, 365 U.S. 505 (1961).

Simitis, S. (1987). Reviewing privacy in an information society. *University of Pennsylvania Law Review, 135*, 707-746.

Solove, D. J. (2007). The First Amendment as criminal procedure. *New York University Law Review, 82*, 112-176.

Solove, D. J. (2008). *Understanding privacy*. Cambridge, MA: Harvard University Press.

Sullivan, D. (2006, January 19). Bush administration demands search data; Google says no; AOL, MSN & Yahoo said yes. Retrieved from http://searchenginewatch.com/article/2059843/Bush-Administration-Demands-Search-Data-Google-Says-No-AOL-MSN-Yahoo-Said-Yes

Sundby, S. E. (1994). "Everyman" 's Fourth Amendment: Privacy or mutual trust between government and citizen?. *Columbia Law Review, 94*, 1751-1812.

Thoreau, H. D. (2011). Where I lived, what I lived for. In Mercer University (Ed.), *Walden* (pp. 79-96). Macon, GA: Mercer University Press.

Tomuschat, C., & Currie, D. P. (Trans.). (2010). *Basic law for the Republic of Germany*. Berlin, German: German Bundestag. Retrieved from https://www.btg-bestellservice.de/pdf/80201000.pdf

U.S. Const. amend. IV.

U.S. Dept. of Justice v. Reporters Comm.for Freedom of Press, 489 U.S. 749 (1989).

Volokh, E. (2000). Freedom of speech and information privacy: The troubling implications of a right to stop people from speaking about you. *Stanford Law Review, 52*, 1049-1124.

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

Westin, A. F. (1967). *Privacy and freedom.* New York, NY: Atheneum.

Whalen v. Roe, 429 U.S. 589 (1977).

Woolf, V. (1929). *A room of one's own*. New York, NY: Harcourt Brace Jovanovich.

重新檢視資訊隱私的民主價值

謝 祥 揚

摘 要

本文旨在重新思考資訊隱私與民主社會的關係。本文主張，資訊隱私為重要的基本權利而應受憲法保障，其原因不僅在於資訊隱私與個人自主決定權密切相關，更在於資訊隱私有助於落實諸多重要民主價值。經本文觀察，資訊隱私的民主價值至少有三：一、個人資訊隱私之保障可限制國家權力的行使。二、建構與個人資訊隱私保障的相關程序機制。三、促使人民得以充分享有思想自由、言論自由以及從事其他智慧活動的自由。此外，本文亦分析臺灣司法院大法官資訊隱私相關解釋。藉由臺灣資訊隱私案例之探討，本文進而主張：資訊隱私不僅止於保障人民對於其個人資訊的自我決定權，更進一步確保人民得以自由思考、發表言論、思辨公共議題、發表不同意見、進而得以參與各種民主程序。從而，資訊隱私可謂為現代民主社會所不可或缺，自應受憲法保障。

關鍵詞：資訊隱私、民主、空間隱私、通訊隱私、智慧隱私