South Carolina Law Review

Volume 65 | Issue 2 Article 3

Winter 2013

The Surveillance Society and the Third-Party Privacy Problem

Shaun B. Spencer
University of Massachusetts School of Law - Dartmouth

THE SURVEILLANCE SOCIETY AND THE THIRD-PARTY PRIVACY PROBLEM

Shaun B. Spencer*

This Article examines a question that has become increasingly important in the emerging surveillance society: Should the law treat information as private even though others know about it? This is the third-party privacy problem. Part II explores two competing conceptions of privacy—the binary and contextual conceptions. Part III describes two features of the emerging surveillance society that should change the way we address the third-party privacy problem. One feature, "surveillance on demand," results from exponential increases in data collection and aggregation. The other feature, "uploaded lives," reflects a revolution in the type and amount of information that we share digitally. Part IV argues that the binary conception cannot protect privacy in the surveillance society because it fails to account for the new realities of surveillance on demand and uploaded lives. Finally, Part V illustrates how courts and legislators can implement the contextual conception to deal with two emerging surveillance society problems—facial recognition technology and geolocation data.

I. INTRODUCTION 374

II. THE COMPETING CONCEPTIONS OF PRIVACY 377
A. *The Binary Conception of Privacy* 377
1. *Fourth Amendment Jurisprudence* 377
2. *Tort Law* 380
3. *Statutory Privacy Protection* 382
B. *The Contextual Conception of Privacy* 382
1. *Fourth Amendment Jurisprudence* 383
2. *Tort Law* 385
3. *Statutory Privacy Protection* 388

III. THE SURVEILLANCE SOCIETY 390
A. *Surveillance on Demand* 393
B. *Uploaded Lives* 398

IV. THE BINARY CONCEPTION'S INABILITY TO PROTECT PRIVACY IN THE SURVEILLANCE SOCIETY 401

---

* Assistant Professor, University of Massachusetts School of Law—Dartmouth. I am grateful for the support of the UMass Law Summer Research Grant Program and the UMass Law Faculty Scholarship Colloquium, as well as the contributions of the Albany Law School Scholarship and Teaching Development Workshop. I am also thankful for the thoughtful comments of Ralph Clifford, Spencer Clough, Justine Dunlap, Amitai Etzioni, Hillary Farber, Lawrence Friedman, Francis Larkin, Dylan Malagrino, and Frances Rudko.

A. The Binary Conception's Failure to Distinguish Third Parties as Ends from Third Parties as Means 401
B. The Binary Conception's Failure to Account for the "Anti-Aggregation" Norm 402
C. The Binary Conception's Flawed Reliance on the Myth of Consent ... 404

V. IMPLEMENTING THE CONTEXTUAL CONCEPTION OF PRIVACY 406
A. Facial Recognition Technology 406
B. Geolocation Data 408

VI. CONCLUSION 410

I. INTRODUCTION

This Article examines a question that has become increasingly important in the emerging surveillance society: Should the law treat information as private even though others may know about it? I call this the "third-party privacy problem." When information is available only to the subject of the information and the subject's intended confidants, individuals have no third-party privacy problem because no third parties are involved. The third-party privacy problem arises when the information becomes available beyond the subject and his or her confidants.

Third parties learn information about the subject in several ways. First, the mere act of communicating information may share it with third parties. For example, when I telephone my doctor about a sensitive medical condition, the telephone company records the numbers that I dialed. Second, third parties may observe the subject's activities. For example, when I walk across town to my doctor's clinic, passersby can see me enter the clinic. In both of these situations, I engaged in activities that I may want to keep between myself and my doctor. Yet in both of these situations, third parties have learned about my activities—the phone number that I dialed and the clinic that I entered.

Part II explores two conflicting approaches that have emerged as courts and legislators wrestle with the third-party privacy problem. The first approach is the "binary" conception of privacy.[1] Under the binary conception, courts and legislators decide whether information is private by examining whether anyone

1. *See infra* Part II.A. Many other commentators have described and critiqued a "binary" or dichotomous conception of privacy. *See, e.g.*, HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 113–14 (2010); DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 7 (2007); Danielle Keats Citron, *Fulfilling Government 2.0's Promise with Robust Privacy Protections*, 78 GEO. WASH. L. REV. 822, 826–27 (2010) (citing Alan Freeman & Elizabeth Mensch, *The Public-Private Distinction in American Law and Life*, 36 BUFF. L. REV. 237, 247–50 (1987)); Daniel J. Gervais & Daniel J. Hyndman, *Cloud Control: Copyright, Global Memes and Privacy*, 10 J. ON TELECOMM. & HIGH TECH. L. 53, 77 (2012).

outside the subject or her confidants has access to the information.[2] This Article refers to these outsiders as "third parties." If no third parties have access, the information is private; if third parties have access, the information is public.

The second approach is the "contextual" conception of privacy.[3] Under the contextual conception, courts and legislators decide whether information is private by referring to the norms that surround the situation in which the third party acquired the information.[4] If those norms support the subject's claim to keep the information within the subject's circle of confidants, then the information is private.[5]

Part III describes two features of the emerging surveillance society that change the way courts and legislators should address the third-party privacy problem. The first feature—"surveillance on demand"—results from exponential increases in data collection and aggregation.[6] Data collection technologies have exploded in recent years.[7] In the online world, private and governmental entities store vast databases of individuals' web searches, emails, social network activities, and much more.[8] And in the physical world, a host of digital surveillance tools increasingly record our movements, our driving habits, and even our moods.[9] The cost of building these "digital dossiers"[10] has dropped dramatically because data collection and aggregation have become *de rigeur* in the emerging surveillance state.[11] In addition, data aggregation renders all of this information searchable "on demand" after the fact.[12] Before the surveillance society, a government or private actor had to identify a target in advance and divert the necessary resources to track the target's activities.[13] In the surveillance society, however, interested parties can simply build a digital dossier after the fact.[14]

The second feature—"uploaded lives"—reflects a revolution in both the type of information we share and the manner in which we share it.[15] We live an ever-increasing portion of our lives through third parties. The convenience of cloud computing puts our most sensitive personal information in the virtual hands of

---

2. *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 22 (2008).
3. *See infra* Part II.B. The Author adapted this term from Helen Nissenbaum's argument for "contextual integrity." NISSENBAUM, *supra* note 1, at 3.
4. *See* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 138 (2004).
5. *Id.* at 141.
6. *See infra* Part III.A.
7. NISSENBAUM, *supra* note 1, at 19.
8. *Id.* at 36, 39.
9. *See id.* at 21–35.
10. For a discussion of digital dossiers, see Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1095 (2002).
11. NISSENBAUM, *supra* note 1, at 38–40.
12. *Id.* at 41–42.
13. *See id.* at 38–45.
14. *See id.* at 40–42.
15. *See infra* Part III.B.

third parties, like Google and Amazon, rather than on physical drives that we can keep secure in our homes or offices.[16] Aspects of our social lives have moved onto social networks that are easily shared and searched.[17] Smart phones and cars transmit our locations to third parties.[18] In a host of ways, we are uploading our lives to third-party servers.

Part IV argues that the binary conception of privacy cannot address the third-party privacy problem in the emerging surveillance society. For several reasons, the surveillance society exposes the binary conception as too blunt an instrument. First, the binary conception fails to distinguish between situations in which a third party is a means to an end and situations in which the third party is the end itself.[19] For example, when I telephone my doctor, I do not intend the phone company to be part of that conversation. Similarly, when I write a diary entry and save it to a server in the cloud, I do not intend for Google to read my diary. Yet the binary conception treats such instrumental sharing as equivalent to communicative sharing. As we upload more of our lives to third parties in easily searchable and sharable formats, the binary conception will not protect many previously private realms.

Second, the binary conception fails to account for the "anti-aggregation norm"—the fear of pervasive surveillance by government or private parties.[20] Since large-scale databases first became a possibility, people have balked at the idea of comprehensive databases that could hold all of the data about them.[21]

Finally, the availability of surveillance on demand undermines the binary conception's assumption of consent.[22] The consent assumption presumes that we make informed decisions to provide particular third parties access to our information.[23] For example, if I drive across town, I understand that various passersby may see me along the way, and I therefore consent to each of those individual passersby knowing my location at a particular point in time. In the surveillance society, however, the calculus changes. A host of digital surveillance tools combine to record my movements every step of the way.[24] Aggregating the individual data points creates the same effect as perpetual, around-the-clock surveillance.[25] And this digital data can converge in a single database—accessible to third parties for decades to come.[26] The assumption that I consent to such pervasive third-party surveillance does not hold.

---

16. Gervais & Hyndman, *supra* note 1, at 57.
17. *See* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1149 (2009).
18. *See* NISSENBAUM, *supra* note 1, at 53.
19. *See infra* Part IV.A.
20. *See infra* Part IV.B.
21. Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1394 (2001).
22. *See infra* Part IV.C.
23. *See infra* Part IV.C.
24. NISSENBAUM, *supra* note 1, at 22–27.
25. *See id.* at 42–45.
26. *See id.* at 41.

Part V illustrates how courts and legislators can use the contextual conception to deal with the third-party privacy problem in the surveillance society. The contextual conception of privacy is better calibrated to account for the surveillance society's unique demands. Although it is more complicated to apply, the contextual conception more accurately captures people's expectations. This Part concludes by showing how courts can apply the contextual conception to two emerging issues—facial recognition technology[27] and geolocation data.[28]

II. THE COMPETING CONCEPTIONS OF PRIVACY

A. The Binary Conception of Privacy

Under the binary conception, courts and legislators decide whether information is private by examining whether anyone outside the subject, or the subject's confidants, has access to the information.[29] If no third parties have access, the information is private; if third parties have access, the information is public.[30] This binary conception appears in a variety of constitutional, common law, and statutory approaches to privacy.

1. Fourth Amendment Jurisprudence

The Supreme Court's Fourth Amendment jurisprudence offers the most prominent example of the binary conception of privacy. Courts determine whether there has been a Fourth Amendment "search" by asking whether the government has intruded on an area where the defendant had a "reasonable expectation of privacy."[31] In *Katz v. United States*,[32] the Supreme Court held that a person speaking on a public telephone had a justifiable expectation of privacy in his conversation, and that the government violated this expectation by wiretapping the telephone.[33] In an often-cited concurrence, Justice Harlan explained that "reasonableness" entails a two-part, expectation-driven test.[34] First, the defendant must have an actual or subjective expectation of privacy.[35]

---

27. *See infra* Part V.A.
28. *See infra* Part V.B.
29. *See, e.g.*, United States v. Miller, 425 U.S. 435, 442–43 (1976) (citing 12 U.S.C. § 1829b(a)(1) (2012); United States v. White, 401 U.S. 745, 751–52 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427, 438 (1963)) ("All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.").
30. *See* NISSENBAUM, *supra* note 1, at 113; SOLOVE, *supra* note 2, at 22.
31. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
32. 389 U.S. 347.
33. *Id.* at 353.
34. *Id.* at 361 (Harlan, J., concurring).
35. *Id.*

Second, the expectation must be "one that society is prepared to recognize as 'reasonable.'"[36]

Under the Court's third-party doctrine, however, one cannot expect privacy in information shared with third parties, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[37] Thus, in *United States v. Miller*,[38] agents of the Bureau of Alcohol, Tobacco, and Firearms presented allegedly defective grand jury subpoenas to two of Miller's banks.[39] The banks made Miller's account records available to the agents.[40] The records provided one or two investigatory leads, and the grand jury later indicted Miller.[41] After copies of Miller's checks were introduced at trial, the district court denied Miller's motion to suppress, and the jury found Miller guilty on charges related to whiskey distilling and tax evasion.[42] The Fifth Circuit reversed, holding that procuring bank records through a defective subpoena violated the Fourth Amendment.[43] The Supreme Court granted the government's petition for certiorari.[44]

The Court held that subpoenaing the bank's records was not an unreasonable search or seizure in violation of the Fourth Amendment.[45] Miller argued that he had a reasonable expectation of privacy in his bank records because he only made them available to his banks for a limited purpose.[46] The Court rejected Miller's argument, quoting its statement in *Katz* that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[47] The Court reasoned that Miller's checks, financial statements, and deposit slips

---

36. *Id.*

37. United States v. Miller, 425 U.S. 435, 443 (1976) (citing United States v. White, 401 U.S. 745, 751–52 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427, 438 (1963)).

38. 425 U.S. 435.

39. *Id.* at 437–39.

40. *Id.* at 438.

41. *Id.*

42. *Id.* at 436–37. The charges were for "possessing an unregistered still, carrying on the business of a distiller without giving bond and with intent to defraud the Government of whiskey tax, possessing 175 gallons of whiskey upon which no taxes had been paid, and conspiring to defraud the United States of tax revenues." *Id.* at 436 (citing 18 U.S.C. § 1371 (2012); 26 U.S.C. §§ 5179, 5601 (2006); 26 U.S.C. § 5205 (repealed 1984)).

43. *Id.* at 437.

44. United States v. Miller, 421 U.S. 1010 (1975) (granting certiorari).

45. *Miller*, 425 U.S. at 440.

46. *Id.* at 442. Miller also argued that, because the Bank Secrecy Act required the bank to maintain Miller's records, the combination of the Bank Secrecy Act and the subpoenas allowed the government to circumvent the protections that the Fourth Amendment would have provided had the government sought documents directly from Miller. *Id.* at 441. The Court rejected that argument as well. *Id.* at 443 (citing Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 52–53 (1974); United States v. White, 401 U.S. 745, 751–52 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427, 438 (1963)).

47. *Id.* at 442 (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

merely contained information that Miller "voluntarily conveyed" to the banks and their employees, and that one who reveals his affairs to another takes the risk that the other will convey that information to the government.[48] The Court relied on prior cases holding that the Fourth Amendment did not protect information conveyed to others—even on the assumption that the information would be used only for a limited purpose and held in confidence.[49]

The Court reaffirmed its binary approach three years later in *Smith v. Maryland*.[50] In *Smith*, police suspected Smith of robbery and of placing obscene and threatening phone calls to the robbery victim.[51] The police asked the telephone company to install a pen register[52] at the company's central offices to record the numbers dialed from the phone in Smith's home.[53] The pen register revealed a call to the victim's home, and police subsequently obtained a warrant to search Smith's home.[54] At trial, Smith moved to suppress all evidence obtained and derived from the pen register.[55] The trial court denied the motion, and the jury convicted Smith.[56]

The Supreme Court held that Smith had no reasonable expectation of privacy for the numbers that he dialed.[57] The Court reasoned that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company" when they make a call, and that the phone company records the numbers dialed and uses them for a variety of reasons.[58] Smith, therefore, "assumed the risk" that the telephone company would reveal to the police the numbers that he dialed.[59]

Thus, under the third-party doctrine, sharing information with a third party removes any expectation of privacy as to that information.[60] The third-party

---

48. *Id.* at 442–43 (citing *White*, 401 U.S. at 751–52).

49. *Id.* at 443 (citing *White*, 401 U.S. at 751–52; *Hoffa*, 385 U.S. at 302; *Lopez*, 373 U.S. at 438).

50. 442 U.S. 735 (1979).

51. *See id.* at 737.

52. The Court noted that "[a] pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed." *Id.* at 736 n.1 (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1977)).

53. *Id.* at 737 (citations omitted).

54. *Id.* (citations omitted).

55. *Id.* (citations omitted).

56. *Id.* at 737–38 (citations omitted).

57. *Id.* at 743 (quoting Katz v. United States, 389 U.S. 347, 361 (1967)).

58. *Id.* at 742.

59. *Id.* at 745.

60. *Id.* at 743–44; *see also* United States v. Miller, 425 U.S. 435, 442, 443 (1976) (citing United States v. White, 401 U.S. 745, 751–52 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427, 438 (1963)). In her concurrence in *United States v. Jones*, Justice Sotomayor urged for reconsideration of the third-party doctrine, recognizing it as "ill suited to the digital age." 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring). For a thorough discussion of the development of the third-party doctrine, see generally Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*,

doctrine prevails not only in the federal courts, but also in at least eighteen states.[61]

2. Tort Law

Courts and commentators also rely on the binary conception of privacy in the common law tort context. An early example appears in Dean William Prosser's famous 1960 article titled *Privacy*.[62] Discussing what he labeled "intrusion," Dean Prosser observed:

> On the public street, or in any other public place, the plaintiff has no right to be alone, and it is no invasion of his privacy to do no more than follow him about. Neither is it such an invasion to take his photograph in such a place, since this amounts to nothing more than making a record, not differing essentially from a full written description, of a public sight which any one present would be free to see.[63]

Similarly, when describing the public disclosure of private facts, Dean Prosser explained that "no one can complain when publicity is given to information about him which he himself leaves open to the public eye, such as the appearance of the house in which he lives, or to the business in which he is engaged."[64] Elaborating on this point, he observed:

> [A]nything visible in a public place may be recorded and given circulation by means of a photograph, to the same extent as by a written description, since this amounts to nothing more than giving publicity to what is already public and what any one present would be free to see.[65]

---

56 MERCER L. REV. 507, 510–21 (2005) (citations omitted) (arguing that the third-party doctrine should be reexamined and clarified in light of current technological advances).

61. Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 395 tbl.1 (2006). As of 2006, Henderson noted that eleven states had rejected the third-party doctrine, and another ten states may reject it. *Id.*

62. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960).

63. *Id.* at 391–92 (citing Berg v. Minneapolis Star & Tribune Co., 79 F. Supp. 957, 963 (D. Minn. 1948); Gill v. Hearst Publ'g Co., 253 P.2d 441, 445 (Cal. 1953); Chappell v. Stewart, 33 A. 542, 542–53 (Md. Ct. App. 1896); Lyles v. State, 330 P.2d 734, 745 (Okla. Crim. App. 1958)).

64. *Id.* at 394.

65. *Id.* at 394–95 (citing *Berg*, 79 F. Supp. at 962; Humiston v. Universal Film Mfg. Co., 178 N.Y.S. 752, 758–59 (App. Div. 1919); Merle v. Sociological Research Film Corp., 152 N.Y.S. 829, 831–32 (App. Div. 1915); *Lyles*, 330 P.2d at 739; Sports & Gen. Press Agency, Ltd. v. "Our Dogs" Publ'g Co., [1916] 2 K.B. 880 at 884 (Eng.)).

Not surprisingly, in the wake of Dean Prosser's influential article,[66] portions of the 1965 Restatement (Second) of Torts also embodied a binary conception of privacy.[67] For example, section 652B describes "intrusion upon seclusion" as intentionally intruding on another's solitude, seclusion, or private affairs.[68] Comment c explains that no liability arises for examining what is "open to the public eye" or "exhibited to the public gaze."[69] Similarly, section 652D addresses liability for "public disclosure of private facts."[70] Comment b precludes liability for publicizing what the plaintiff "leaves open to the public eye."[71]

The binary conception of privacy is also present in numerous common law tort cases. For example, in *Mark v. Seattle Times*,[72] a television cameraman walked up a driveway to a pharmacy and videotaped the pharmacist through the window.[73] Although the pharmacy was closed at the time, the court reasoned that there was no intrusion upon seclusion because the cameraman filmed from a place open to the public and any passerby could have viewed the scene recorded by the camera.[74]

The court applied the same approach to digital data in *Interscope Records v. Duty*.[75] In that case, various record companies sued Lindsay Duty for copyright infringement based on her sharing of music through the peer-to-peer file-sharing network, Kazaa.[76] Duty counterclaimed for, among other things, intrusion upon seclusion.[77] Duty claimed that the record companies invaded her privacy by accessing the "share" file on her computer.[78] The court, however, dismissed Duty's claim for intrusion upon seclusion because Duty's share file was accessible to the public and, therefore, could not support the tort's seclusion element.[79]

---

66. *See generally* Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887 (2010) (discussing the importance and impact of Dean Prosser's article in the development of the law of tort privacy).

67. *See* RESTATEMENT (SECOND) OF TORTS §§ 652B, 652D (1977).

68. *Id.* § 652B.

69. *Id.* cmt. c.

70. *Id.* § 652D.

71. *Id.* § 652D cmt. b. *But see infra* Part II.B.2 (discussing other Restatement comments evidencing a contextual conception of privacy).

72. 635 P.2d 1081 (Wash. 1981).

73. *Id.* at 1094–95.

74. *Id.* at 1095 (citing McLain v. Boise Cascade Corp., 533 P.2d 343, 347 (Or. 1975)).

75. No. 05CV3744-PHX-FJM, 2006 WL 988086 (D. Ariz. Apr. 14, 2006).

76. *Id.* at *1.

77. *Id.* at *3.

78. *Id.* (citations omitted).

79. *Id.*

3. Statutory Privacy Protection

As Professors Paul Schwartz and Daniel Solove have described, some privacy statutes condition protection on whether the information in question is accessible to the public.[80] The Gramm-Leach-Bliley Act of 1999 (GLBA), for example, prevents financial institutions from disclosing "nonpublic information" about a consumer without giving the consumer notice and an opportunity to opt out.[81] *Nonpublic information* excludes any information that is not "publicly available" as defined by regulation.[82] The applicable regulation defines *publicly available information* as "any information that you have a reasonable basis to believe is lawfully made available to the general public from: (i) . . . government records; (ii) [w]idely distributed media; or (iii) [d]isclosures to the general public that are required to be made by Federal, State, or local law."[83] Similarly, the Illinois Children's Privacy Protection and Parental Empowerment Act prohibits the sale or purchase of personal information concerning a child without parental consent.[84] *Personal information*, however, does not include "[i]nformation found in publicly available sources."[85]

Both of these statutes take the type of all-or-nothing approach dictated by the binary conception of privacy. Under these statutes, if the information becomes available to the general public, the information is not entitled to protection.[86]

B. The Contextual Conception of Privacy

Unlike the binary conception's bright line approach, the contextual conception considers the particular circumstances in which the information was shared.[87] Helen Nissenbaum captured this contextual conception in her argument for an approach to privacy based on "contextual integrity."[88] Nissenbaum rejected the binary conception of privacy.[89] She reasoned that

---

80. Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1830 (2011). Schwartz and Solove argued that the "publicly available" approach is problematic because "[t]he public or private status of data often does not match up to whether it can identify a person or not." *Id.*

81. 15 U.S.C. § 6802(a), (b) (2012).

82. 15 U.S.C. § 6809(4)(A), (B) (2012).

83. 16 C.F.R. § 313.3(p)(1) (2013).

84. 325 ILL. COMP. STAT. 17/10 (2012).

85. *Id.* at 17/5. Similarly, Connecticut law imposes a duty to safeguard any personal information about another person. CONN. GEN. STAT. § 42-471(a) (Supp. 2010). However, the definition of *personal information* does not include "publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media." *Id.* § 42-471(c).

86. *See* 325 ILL. COMP. STAT. 17/5 (2012); CONN. GEN. STAT. § 42-471(c) (Supp. 2010).

87. *See* Nissenbaum, *supra* note 4, at 137–38.

88. *Id.* at 136–46 (citations omitted).

89. *See id.* at 155–57.

"personal information revealed in a particular context is always tagged with that context and never 'up for grabs' as other accounts would have us believe of . . . information gathered in public places."[90]

Instead, according to Nissenbaum, contextual integrity exists in any situation involving the disclosure of information in which two types of norms are maintained: "norms of appropriateness" and "norms of information flow."[91] First, *norms of appropriateness* dictate what information is appropriate to reveal in a given context.[92] Second, *norms of information flow* dictate whether the flow of information is one-way or two-way and whether the information can be shared with others.[93] In some contexts, people expect shared information to be held in strict confidence or limited to a small group of confidants.[94] In others, people expect that the information may be widely disseminated.[95]

1. Fourth Amendment Jurisprudence

Today, many examples of the contextual conception appear in practice alongside the binary conception. In search and seizure jurisprudence, for example, numerous states have relied upon their own constitutions to reject the binary approach of the Supreme Court's third-party doctrine.[96] As Professor Stephen Henderson's thorough examination of this subject reveals, state courts have been willing to find a reasonable expectation of privacy in bank records,[97] telephone records,[98] and garbage left for curbside collection,[99] despite the fact

---

90. *Id.* at 143.

91. *Id.* at 138. According to Nissenbaum, "there is no place not governed by at least some informational norms." *Id.* at 139.

92. *Id.* at 138.

93. *See id.* at 140–43 (citing MICHAEL WALZER, SPHERES OF JUSTICE: A DEFENSE OF PLURALISM AND EQUALITY 320 (1983)).

94. *Id.* at 142.

95. *See id.* at 141–43 (citing 45 C.F.R. §§ 164.103–.534 (2011); WALZER, *supra* note 93, at 320).

96. Henderson, *supra* note 61, at 396–400 tbl.2 & nn.118–28.

97. *Id.*; *see, e.g.*, Burrows v. Superior Court, 529 P.2d 590, 593 (Cal. 1974) (holding that one retains a reasonable expectation of privacy in bank records); People v. Lamb, 732 P.2d 1216, 1220 (Colo. 1987) (en banc) (recognizing a bank customer's expectation of privacy); Winfield v. Div. of Pari-Mutuel Wagering, 477 So. 2d 544, 548 (Fla. 1985) (interpreting state law to reflect an individual's expectation of privacy in financial records); State v. McAllister, 875 A.2d 866, 875 (N.J. 2005) (recognizing the Federal Government's efforts to protect privacy rights in bank records).

98. *See, e.g.*, People v. Blair, 602 P.2d 738, 746 (Cal. 1979) (en banc) (holding that people enjoyed a reasonable expectation of privacy in telephone numbers dialed from a hotel room and that it was reasonable to believe these records were collected for billing purposes only); People v. Timmons, 690 P.2d 213, 215 (Colo. 1984) (en banc) (affirming the suppression of wiretap and pen register evidence obtained with a faulty search warrant); Shaktman v. State, 553 So. 2d 148, 151–52 (Fla. 1989) (recognizing the state must have a compelling reason to intrude upon telephone calls because pen registers intrude upon fundamental privacy interests); State v. Mollica, 554 A.2d 1315, 1322 (N.J. 1989) (finding that a hotel using phone records for billing "does not diminish the individual occupant's expectation of privacy in connection with personal use"); State v. Hunt, 450

that those records and items were exposed to third parties. These courts rejected the idea that sharing information with a third party automatically waives any expectation of privacy and, instead, looked to the particulars of the context.[100]

Recently, a majority of the Supreme Court applied a decidedly conceptual approach to the expectation of privacy in public places. In *United States v. Jones*,[101] law enforcement officers placed a Global Positioning System (GPS) tracking device on the defendant's car and monitored the car's movements for four weeks.[102] The government used the GPS data to help obtain a drug trafficking conviction, but the defendant appealed based on the lack of a valid warrant to attach the GPS tracking device.[103] The Supreme Court held that the government's GPS monitoring constituted a Fourth Amendment search that required a valid warrant.[104] Writing for the Court, Justice Scalia relied on the physical trespass associated with attaching a GPS device to a car.[105] Justice Alito, concurring in the judgment, reasoned that around-the-clock surveillance of one's location for a month violates a reasonable expectation of privacy.[106] Justice Sotomayor wrote a separate concurrence in which she joined the Court's opinion, but also adopted Justice Alito's position that such long-term GPS surveillance violated a reasonable expectation of privacy.[107]

Justice Alito's concurrence represents a decidedly contextual approach to locational privacy. Had Justice Alito taken a purely binary approach, he would have followed the reasoning of *United States v. Knotts*,[108] in which the Court held that the law enforcement agents' use of a beeper to track the defendant's vehicle did not constitute a Fourth Amendment search because one has no expectation of locational privacy while on a public road.[109] Instead, Justice Alito considered the context of the particular search—a month of continuous

---

A.2d 952, 955–56 (N.J. 1982) (citing Katz v. United States, 389 U.S. 347, 352 (1967)) (comparing the right of privacy for phone calls to the right of privacy in one's home).

99. *See, e.g.*, People v. Edwards, 458 P.2d 713, 718 (Cal. 1969) (en banc) (holding that the defendants enjoyed a reasonable expectation of privacy in their garbage); State v. Hempele, 576 A.2d 793, 810 (N.J. 1990) (holding that an expectation of privacy in garbage is reasonable and is protected by the Constitution).

100. *See supra* notes 97–99 and accompanying text.

101. 132 S. Ct. 945 (2012).

102. *Id.* at 948.

103. *See id.* at 948–49 (citing United States v. Maynard, 615 F.3d 544, 566–68 (2010)).

104. *Id.* at 949.

105. *Id.* at 950. Justice Scalia delivered the opinion of the Court and was joined by Chief Justice Roberts and Justices Kennedy and Thomas. *Id.* at 947.

106. *Id.* at 964 (Alito, J., concurring). Justice Alito was joined by Justice Ginsburg, Justice Breyer, and Justice Kagan. *Id.* at 957. Justice Alito's concurrence took the position that *Katz v. United States* eviscerated the trespass doctrine. *Id.* at 959 (citing Katz v. United States, 389 U.S. 347, 353 (1967)). Justice Alito also suggested a potential exception that would permit long-term monitoring for investigations involving "extraordinary offenses." *Id.* at 964.

107. *Id.* at 954, 955 (Sotomayor, J., concurring).

108. 460 U.S. 276 (1983).

109. *Id.* at 281–82, 285.

surveillance.[110] He recognized a reasonable expectation that one would not be subject to "long-term" monitoring because, before GPS technology, real-world constraints made long-term monitoring extremely costly and impractical.[111]

Justice Sotomayor went even further than Justice Alito by questioning the continuing viability of the third-party doctrine.[112] She found the third-party doctrine "ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[113] Given this reality, Justice Sotomayor refused to assume that disclosing information to some member of the public for a limited purpose eliminated Fourth Amendment protection.[114]

2. *Tort Law*

In their seminal article *The Right to Privacy*,[115] Samuel Warren and Louis Brandeis adopted a contextual approach, rather than a binary one.[116] Their discussion of the right to prevent one's "public portraiture" recognized that one could maintain a right to privacy even after displaying one's image to others by walking on a public street.[117]

Although the Restatement (Second) of Torts contains language applying a binary approach,[118] it contains other language applying a contextual approach. For example, section 652B protects against intrusion upon seclusion.[119] Comment b to section 652B observes that the information in question need not be completely inaccessible to third parties.[120] Instead, a defendant can intrude

---

110. *Jones*, 132 S. Ct. at 963 (Alito, J., concurring).

111. *Id.* at 963–64.

112. *Id.* at 957 (Sotomayor, J., concurring).

113. *Id.*

114. *Id.*; *see also* Henderson, *supra* note 61, at 378 (citing Henderson, *supra* note 60, at 524–28) (citations omitted) (proposing that the third-party doctrine should apply only to information shared with the third party for that party's use); Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1311 (2012) (observing that current Fourth Amendment doctrine "places far fewer hurdles in front of the police when they use the fruits of somebody else's surveillance than when they do the surveillance themselves"). Professor Ohm identified the same problem as I do, but proposed a different solution. *See* Ohm, *supra* at 1310–11. Professor Ohm suggested that privacy is doomed due to the emerging surveillance society and the government's ability to "piggy-back" on private, third-party surveillance. *Id.* at 1311. His proposed solution is to untether the Fourth Amendment from privacy and, instead, reinterpret the Fourth Amendment as a protection of liberty from government power. *Id.* at 1311–12. I take the opposite approach by urging that the binary conception of privacy be abandoned altogether. *See infra* Parts IV & V.

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

116. *Id.* at 206–20.

117. *Id.* at 213–14.

118. *See* RESTATEMENT (SECOND) OF TORTS § 652A (1977).

119. *Id.* § 652B.

120. *Id.* cmt. b.

upon one's seclusion by examining that person's bank account, which necessarily involves information that has been shared with a third party.[121]

Several California tort cases illustrate the contextual approach to privacy. In *Shulman v. Group W Productions, Inc.*,[122] a helicopter medical crew rescued the plaintiffs after their car went off of a highway.[123] A television cameraman accompanied the medical crew and filmed the rescue and transport to the hospital.[124] In addition, the rescue nurse's microphone recorded conversations with one of the plaintiffs at the scene of the accident and in the rescue helicopter.[125] Group W Productions later used video and sound from the rescue in a television show.[126] The plaintiffs sued for intrusion upon seclusion, and the trial court granted the defendant's motion for summary judgment; the case then reached the Supreme Court of California on appeal.[127]

The court first evaluated the plaintiffs' claim that filming them at the accident scene was an intrusion upon seclusion.[128] Although the court rejected this claim, the court did not adopt a binary approach in reasoning that there was no expectation of privacy in a public place.[129] Instead, the court examined the norms and customs surrounding the interaction at issue.[130] First, the court noted that journalists commonly film accident scenes and rescues.[131] Second, the court noted that California statutes exempt the press from certain emergency closure orders.[132] Based on these circumstances, the court held that filming at the accident scene was not an intrusion upon the plaintiffs' seclusion.[133]

Next, the court held that filming the plaintiffs inside the rescue helicopter could intrude upon their seclusion.[134] Again, the court relied on the norms and customs surrounding the interaction[135]: "Although the attendance of reporters and photographers at the scene of an accident is to be expected, we are aware of no law or custom permitting the press to ride in ambulances or enter hospital rooms during treatment without the patient's consent."[136]

Finally, the court held that recording the plaintiffs' communications with the rescue nurse could constitute an intrusion upon seclusion.[137] The court again

---

121. *Id.*
122. 955 P.2d 469 (Cal. 1998).
123. *Id.* at 474.
124. *Id.* at 474–75.
125. *Id.* at 475.
126. *Id.*
127. *Id.*
128. *Id.* at 490.
129. *Id.* at 490–91.
130. *See id.*
131. *Id.* at 490.
132. *Id.*
133. *Id.*
134. *Id.*
135. *See id.*
136. *Id.*
137. *Id.* at 491.

based its conclusion on the norms and customs surrounding the interaction.[138] Because the accident occurred "in a ditch many yards from and below the rural superhighway," it was extremely unlikely that any passersby on the road could have overheard the conversations.[139] The court also noted that "existing legal protections for communications," such as the physician–patient privilege and the California Invasion of Privacy Act, supported a conclusion that one of the plaintiffs reasonably expected her conversations to remain private.[140]

Shortly after deciding *Shulman*, the California Supreme Court elaborated on its contextual approach in *Sanders v. American Broadcasting Cos.*[141] In *Sanders*, an ABC reporter took a job as a telephone psychic and wore a hidden camera in the workplace.[142] The reporter's camera recorded her conversations with several coworkers, including the plaintiff, Sanders.[143] Sanders sued ABC for intrusion upon seclusion.[144]

ABC argued that Sanders could not claim to have been "secluded" because his conversations were accessible to his coworkers.[145] The court, however, rejected the binary notion that an expectation of privacy must be absolute to enjoy protection.[146] Instead, the court examined the context in which this intrusion occurred.[147] First, the court noted that Shulman's conversations were accessible only to his coworkers—not to the general public.[148] Second, the court noted that one may enjoy a reasonable expectation of privacy from electronic recording of one's conversations, even when certain third parties may overhear these conversations.[149] Such "secret monitoring denies the speaker an important aspect of privacy of communication—the right to control the nature and extent of the firsthand dissemination of his statements."[150] Explicitly rejecting the binary conception, the court explained:

> [P]rivacy, for purposes of the intrusion tort, is not a binary, all-or-nothing characteristic. There are degrees and nuances to societal recognition of our expectations of privacy: the fact the privacy one

138. *See id.*
139. *Id.*
140. *Id.* at 491–92 (CAL. PENAL CODE § 632 (West 2007)).
141. 978 P.2d 67 (Cal. 1999).
142. *Id.* at 69.
143. *Id.*
144. *Id.*
145. *See id.* at 73, 78.
146. *Id.* at 73–74.
147. *Id.* at 77.
148. *Id.*
149. *Id.* at 72.
150. *Id.* (quoting Shulman v. Grp. W Prods., Inc., 955 P.2d 469, 492 (Cal. 1998)).

expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law.[151]

3. Statutory Privacy Protection

The contextual approach finds favor in statutory regimes as well. For example, the Federal Video Voyeurism Prevention Act prohibits capturing an image of an individual's "private area . . . under circumstances in which the individual has a reasonable expectation of privacy."[152] The individual may enjoy a reasonable expectation of privacy not only where "a reasonable person would believe that he or she could disrobe in privacy," but also in any circumstance in which a reasonable person would believe that his or her "private area" would not be "visible to the public, regardless of whether that person is in a public or private place."[153] A Delaware statute governing the installation of video cameras in schools takes a similarly contextual approach to privacy.[154] The statute provides that "in no event shall video cameras be used at any time or at any location which would violate a student's reasonable expectation of privacy including, but not limited to, locker rooms, areas where students may disrobe and lavatories."[155]

A Pennsylvania statute concerning GPS surveillance implements the contextual conception of privacy in a different context.[156] The statute gives courts authority to order GPS surveillance by law enforcement on "probable cause that criminal activity has been, is or will be in progress and that the use of a mobile tracking device will yield information relevant to the investigation of the criminal activity."[157] The statute, however, limits the ability to monitor the device in certain circumstances[158]: "Movement of the tracking device within an area protected by a reasonable expectation of privacy shall not be monitored absent exigent circumstances or an order supported by probable cause . . . ."[159]

---

151. *Id.*

152. 18 U.S.C. § 1801(a) (2012). The Act applies only in the territorial or maritime jurisdiction of the United States. *Id.*

153. *Id.* § 1801(b)(5). Although the federal statute applies only "in the special maritime and territorial jurisdiction of the United States," more than half of the states have enacted some form of an anti-voyeurism statute. *Id.* § 1801(a); *see, e.g.*, Timothy J. Horstmann, Comment, *Protecting Traditional Privacy Rights in a Brave New Digital World: The Threat Posed by Cellular-Phone Cameras and What States Should Do to Stop It*, 111 PENN ST. L. REV. 739, 742–46 (2007) (citations omitted) (discussing the laws of the twenty-six states that have adopted anti-voyeurism statutes); Antonietta Vitale, Note, *Video Voyeurism and the Right to Privacy: The Time for Federal Legislation Is Now*, 27 SETON HALL LEGIS. J. 381, 393-400 (2003) (citations omitted) (analyzing state voyeurism statutes).

154. *See* DEL. CODE ANN. tit. 14, § 4121 (2007).

155. *Id.*

156. 18 PA. STAT. ANN. § 5761 (West Supp. 2011).

157. *Id.* § 5761(c)(4).

158. *Id.* § 5761(g).

159. *Id.*

Of course, legislation need not be keyed to reasonable expectations to embody the contextual conception. The predominant legislative approach to privacy in the United States is sector-specific, with protection for some types of data but no protection for many others.[160] Many of these sector-specific protections provide examples of legislators examining the context in question and deciding that the balance should tip in favor of privacy. For example, Congress passed the Driver's Privacy Protection Act of 1994 (DPPA)[161] in the wake of the 1989 stalking and murder of actress Rebecca Schaeffer by a deranged fan who found her address through the department of motor vehicles.[162] The DPPA prohibited states from releasing drivers' personal information for certain purposes without the drivers' consent, but allowed states to presume such consent unless the drivers opted out.[163] A 1999 amendment changed the DPPA's protection scheme to opt in so that states could not release the information without drivers' express consent.[164]

Similarly, in the wake of the controversial confirmation hearings following Judge Robert Bork's Supreme Court nomination, Congress passed the Video Privacy Protection Act of 1988 (VPPA).[165] During the hearings, many were shocked to learn that a journalist from Washington, D.C.'s *City Paper* had obtained a printout of the movies Judge Bork rented from his neighborhood video store.[166] Though many remember the controversy over a journalist obtaining Judge Bork's video rental records in the hope of demonstrating that he rented pornographic films, fewer remember that the records revealed nothing controversial.[167] As it turned out, most of the 146 movies he rented were Disney movies and Hitchcock films.[168] Today, the VPPA allows civil suits against any videotape service providers who knowingly disclose the titles of videos rented by their customers.[169] Videotape service providers may, however, disclose the names of videos to law enforcement agencies pursuant to a warrant, grand jury

---

160. *See* Robert M. Gellman, *Can Privacy Be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules*, 41 VILL. L. REV. 129, 130 (1996) ("The United States approach to privacy is sometimes termed 'sectoral,' with separate and uncoordinated laws applying to some personal records, and no laws applying to other records." (citing Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 500 (1995))).

161. Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322, § 300002, 108 Stat. 2099 (1994) (codified as amended at 18 U.S.C. § 2721 (2012)).

162. Jennifer S. Lee, *Welcome to the Database Lounge: Bars and Shops Find Pay Dirt in Scannable Driver's Licenses, and Your Age Isn't All They Want*, N.Y. TIMES, Mar. 21, 2002, at G1.

163. Driver's Privacy Protection Act § 300002.

164. Department of Transportation and Related Agencies Appropriation Act of 2000, Pub. L. No. 106-69, § 350(c)–(e), 113 Stat. 986, 1025 (1999).

165. Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (1988) (codified as amended at 18 U.S.C. § 2710 (2012)).

166. *See* SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 72 (2000).

167. *Id.*

168. *Id.*

169. 18 U.S.C. § 2710(b)(1) (2012).

subpoena, or court order, and may disclose the subject matter of the rented videos for the purpose of marketing goods directly to the consumer, so long as the consumer has a chance to opt out.[170]

The DPPA and VPPA are just two examples of the contextual conception of privacy at work. In each case, Congress limited the sharing of data in the hands of third parties by engaging a context-specific balancing of the competing interests at play in each situation.[171]

III. THE SURVEILLANCE SOCIETY

Scholars have predicted the rise of the surveillance society for several decades. For example, in a 1998 article, Dr. Roger Clarke described what he called "dataveillance," which is the systematic monitoring of people's actions or communications through the application of information technology.[172] That same year, Dr. David Brin predicted a future of pervasive surveillance from video cameras, airborne drones, and massive aggregations of consumer data.[173] As the digital revolution continued, many others followed in their footsteps.[174]

In many ways, the surveillance society is already here.[175] For example, our computers share extensive data with third parties. Some of that sharing occurs when we post personal information on social networking sites like Facebook.[176] Much of the sharing, however, is less voluntary. For example, search engines

---

170. *Id.* § 2710(b)(2)(C), (b)(2)(D)(ii).

171. *See* Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (1988) (codified as amended at 18 U.S.C. § 2710 (2012)); Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322, § 300002, 108 Stat. 2099 (1994) (codified as amended at 18 U.S.C. § 2721 (2012)).

172. Roger A. Clarke, *Information Technology and Dataveillance*, 31 COMM. OF THE ACM 498, 498 (1988), *available at* www.anu.edu/au/people/Roger.Clarke/DV/CACM88.html.

173. *See* DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? 5–8 (1998).

174. *See generally* DAVID LYON, SURVEILLANCE AFTER SEPTEMBER 11 (2003) (discussing the intensification, integration, and globalization of surveillance since the September 11, 2001 attacks); DAVID LYON, THE ELECTRONIC EYE: THE RISE OF SURVEILLANCE SOCIETY (1994) (addressing the implications of living in a "surveillance society"); CLIVE NORRIS & GARY ARMSTRONG, THE MAXIMUM SURVEILLANCE SOCIETY: THE RISE OF CCTV 212–14 (1999) (discussing an advanced "neural network" for processing digital video in the law enforcement context); ROBERT O'HARROW, JR., NO PLACE TO HIDE (2005) (painting a comprehensive picture of how much information has been and will be gathered through surveillance tools available to governments and businesses); David Wood, *Foucault and Panopticism Revisited*, 3 SURVEILLANCE & SOC'Y 234, 235–36 (2003), *available at* http://www.surveillance-and-society.org/articles1(3)/editorial.pdf (summarizing several journal articles organized under the common theme of Panopticism, or constant surveillance, popularized by the modern French philosopher, Michel Foucault); Ohm, *supra* note 114, at 1318 (referring to a "new surveillance society").

175. *See, e.g.*, Jennifer Valentino-Devries, *The Economics of Surveillance*, WALL ST. J. DIGITS BLOG (Sept. 28, 2012, 10:30 PM), http://blogs.wsj.com/digits/2012/09/28/the-economics-of-surveillance/ (offering an excellent summary of various third-party surveillance and data collection techniques).

176. Grimmelmann, *supra* note 17, at 1149–51 (explaining how Facebook paints a complete picture of its users' lives through the information it collects).

like Google monitor the queries we type and the websites we visit.[177] And the Internet service providers on whom we rely for essential connectivity record the websites we visit, the files we download, and the people whom we email or message.[178]

Everyday transactions, both online and in real space, convey a plethora of data to third parties.[179] Our credit and debit card activity provides "a virtual dossier of our daily activities."[180] Merchants have access to our weekly grocery orders, medical and prescription drug purchases, the books we buy, the movies we rent, and the causes to which we contribute.[181]

Even our cars share increasing amounts of data.[182] Law enforcement agencies, as well as private "repo men," are using license plate readers that log the location and time of day of each license plate that passes before the reader's electronic eye.[183] Over one-third of police departments were already using automated license plate readers by 2010.[184] Cars are now being built with "black boxes" similar to those in commercial airliners.[185] These black boxes can monitor speed and location, as well as communicate data about our driving performance,[186] to our auto insurance carriers. GPS devices are often built into cars,[187] and traffic cameras and electronic toll collection stations can track where and when we travel.[188]

Finally, our bodies are beginning to share increasing amounts of information. Facial recognition technology has been improving rapidly in recent

---

177. *See, e.g.*, Quentin Hardy & Matt Richtel, *Don't Ask? Internet Still Tells*, N.Y. TIMES, Nov. 22, 2012, at A1 (depicting how users enter information that may be too private to even disclose to friends into search engines, such as Google and Bing).

178. NISSENBAUM, *supra* note 1, at 27–31.

179. *See, e.g.*, Henderson, *supra* note 61, at 390 (discussing several examples of how people convey data to third parties in everyday transactions).

180. *Id.*

181. *Id.*

182. *See, e.g.*, Julia Angwin & Jennifer Valentino-DeVries, *New Tracking Frontier: Your License Plates*, WALL ST. J., Sept. 29, 2012, *available at* http://online.wsj.com/article/SB10000872396390443995604578004723603576296.html ("The rise of license-plate tracking is a case study in how storing and studying people's everyday activities . . . has become the default rather than the exception.").

183. *Id.*

184. CYNTHIA LUM ET AL., GEORGE MASON UNIV. CTR. FOR EVIDENCE-BASED CRIME POLICY, LICENSE PLATE RECOGNITION TECHNOLOGY (LPR): IMPACT EVALUATION AND COMMUNITY ASSESSMENT 13 (2010), http://gemini.gmu.edu/cebcp/lpr_final.pdf (noting that over one-third of Police Executive Research Forum (PERF) members had adopted License Plate Recognition Technology).

185. Donald W. Garland & Carol M. Bast, *Is the Government Riding Shotgun? Recent Changes in Automobile Technology and the Right to Privacy*, 46 CRIM. L. BULL. 295, 295–96 (2010).

186. *Id.*

187. *See id.* at 295; Henderson, *supra* note 61, at 385 n.75.

188. Henderson, *supra* note 61, at 390.

years as computer processing speed has increased.[189] For example, Alessandro Acquisti led a study that illustrated the potential of facial recognition technology when combined with cloud computing and data aggregation.[190] He first photographed people using a laptop computer.[191] He then used facial recognition software to match those images to Facebook profiles, thereby determining their identity.[192] Matching the photographs to the Facebook profiles took under three seconds, and the accuracy rate was about 33%.[193] Finally, Acquisti used data available on those social networking sites to determine the students' dates of birth, interests, and the last five digits of their social security numbers.[194] Facial recognition and other biometric identification techniques are only increasing.[195]

This disparate array of data collectors poses a challenge for privacy advocates because they cannot point to any master plan—sinister or otherwise—behind the surveillance society.[196] No single "big brother" is gathering data.[197] When one considers individual data collection practices, it is easy to treat each practice in isolation as relatively harmless and largely defensible. Yet, in the aggregate, the data collection system creates a nearly unimaginable wealth of data to be mined.[198]

This Article turns next to two aspects of the emerging surveillance society that impact how we must handle the third-party privacy problem: the phenomena of surveillance on demand and uploaded lives.

---

189. Valentino-DeVries, *supra* note 175 ("Consider facial recognition technology. Five years ago, it only worked in very controlled settings such as passport checkpoints. . . . Within the past 18 months, the software has improved to allow faces to be matched even in regular snapshots and online images . . . . This is in part because as computers become faster, the complicated geometric analysis involved in analyzing faces can be done more quickly.").

190. ALESSANDRO ACQUISTI, RALPH GROSS & FRED SUTZMAN, FACES OF FACEBOOK: PRIVACY IN THE AGE OF AUGMENTED REALITY, Presented at Black Hat (Aug. 4, 2011), *available at* http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/acquisti-faces-BLACKHAT-draft.pdf.

191. *Id.*

192. *Id.*

193. *Id.*

194. *Id.*

195. *See* Valentino-DeVries, *supra* note 175 (discussing improvement in facial recognition technology).

196. *See, e.g.*, Alan Greenblatt, *Our Surveillance Society: What Orwell and Kafka Might Say*, NPR (Jun. 8, 2013), http://www.npr.org/2013/06/08/189792140/our-surveillance-society-what-orwell-and-kafka-might-say ("It's not just the corporations performing surveillance . . . average citizens . . . are also tracking and documenting each other's movements in real life these days.").

197. *See id.*

198. *See, e.g.*, Patrick Tucker, *Has Big Data Made Anonymity Impossible?*, MIT TECH. REV. (May 7, 2013), http://www.technologyreview.com/news/514351/has-big-data-made-anonymity-impossible/ ("[T]he amount of data created each year has grown exponentially: it reached 2.8 zettabytes in 2012, a number that's as gigantic as it sounds, and will double again by 2015 . . . ."); *see also* NISSENBAUM, *supra* note 1, at 36–38.

A. Surveillance on Demand

We find a classic example of pervasive surveillance in Jeremy Bentham's ideal vision of a prison: the Panopticon.[199] The Panopticon's purpose was to change prisoners' behavior through "the illusion of constant surveillance."[200] Bentham envisioned a central tower with windows on all sides, surrounded by a ring of cells occupied by the prisoners.[201] The cells open inward, and an inspector in the central tower can monitor and speak to any prisoner at any time.[202] The Panopticon controls behavior because prisoners know their behavior can be constantly monitored, but cannot know when the inspector is monitoring them.[203]

Today's digital data collection and storage facilitate a more pervasive Panopticon. Because digital data are easily stored and searchable,[204] today's watchers can decide whom they would like to observe after the fact, and then search for the relevant data.[205] This aspect of today's surveillance society resembles the "time shifting" made possible by video cassette recorders and digital video recorders.[206] Rather than watching what happens to be on television at a given moment, time-shifting viewers can watch any program from

---

199. *See generally* MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 195–308 (Alan Sheridan trans., 1977) (discussing the surveillance context of Bentham's Panopticon).

200. REG WHITAKER, THE END OF PRIVACY: HOW TOTAL SURVEILLANCE IS BECOMING A REALITY 33 (1999) (quoting Miran Božovic, *Introduction* to JEREMY BENTHAM, THE PANOPTICON WRITINGS 16 (Miran Božovic ed., 1995)). Bentham trumpeted his idea as a "new mode of obtaining power of mind over mind, in a quantity hitherto without example." *Id.* at 34 (quoting BENTHAM, *supra* at 30). Reg Whitaker termed the modern state of widespread surveillance as the "Participatory Panopticon." *Id.* at 139.

201. *Id.* at 32.

202. *Id.* at 32–33.

203. *Id.* An elaborate system of "lanterns and apertures" renders the Inspector a silhouette so the prisoners cannot see his face. *Id* at 33. Focault noted that "[h]e who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection." FOUCAULT, *supra* note 199, at 202–03.

204. The cost for businesses to "store and use a gigabyte of information for a year dropped from $18.95 in 2005 to $1.68 in 2012, and it's expected to drop to just 66 cents in 2015." Valentino-DeVries, *supra* note 175.

205. *See* JOHN VILLASENOR, CTR. FOR TECH. INNOVATION AT BROOKINGS, RECORDING EVERYTHING: DIGITAL STORAGE AS AN ENABLER OF AUTHORITARIAN GOVERNMENTS 1 (Dec. 14, 2011), *available at* http://www.brookings.edu/~/media/research/files/papers/2011/12/14%20digital%20storage%20villasenor/1214_digital_storage_villasenor.pdf ("These enormous databases of captured information will create what amounts to a surveillance time machine, enabling state security services to retroactively eavesdrop on people in the months and years before they were designated as surveillance targets.").

206. *See, e.g.*, Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 421 (1984) (describing "time shifting" as "us[ing] a [video recorder] principally to record a program he cannot view as it is being televised and then to watch it once at a later time").

any channel at any moment in the past—subject to the programs they decide to record and the available storage capacity.[207] The surveillance society, however, automatically records virtually all channels at all times, and there appears to be no limit as to how much data the many collection entities can store.[208] The "channels" being recorded in the surveillance society are ever expanding.[209] For example, the total quantity of the world's recorded data doubled every year from the mid-1990s to 2008.[210] According to the big data management company Zettaset, a staggering 2.5 quintillion bytes of Big Data are captured daily from consumers and "80% of data captured today is . . . posts to social media sites, purchase transaction records, and cell phone GPS signals."[211] Acxiom, a leading data broker, claims to have data concerning "500 million active consumers worldwide, with about 1500 data points per person."[212]

Private data brokers aggregate information from various private databases to create consumer profiles for sale to private or public parties.[213] In a recent response to questions from members of Congress, Acxiom reported collecting the following types of information:

- Identifying information such as name, address, land and mobile phone, email, social security number, and driver's license number;
- Court and public agency records such as criminal history, bankruptcies, judgments, liens, and licenses;
- Demographic information such as date of birth, race, ethnicity, religious affiliation, marital status, presence of children in the household, education, occupation, and political party affiliation;
- Financial indicators such as estimated net worth, estimated income, and type of credit cards used;

---

207. *See id.* at 422–23.

208. *See, e.g.*, David Von Drehle, *The Surveillance Society*, TIME (Aug. 1, 2013), http://nation.time.com/2013/08/01/the-surveillance-society (explaining that it is more cost effective for intelligence agencies to record everything and analyze the data at a later date).

209. *See id.*; *see also* Glen Greenwald, *XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet,'* THE GUARDIAN (July 31, 2013), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data ("A top secret [NSA] program allows analysts to search . . . through vast databases containing emails, online chats and the browsing histories of millions of individuals . . . .").

210. Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 317 (2008) (citing JEFFREY W. SEIFERT, CONG. RESEARCH SERV., RL 31798, DATA MINING AND HOMELAND SECURITY: AN OVERVIEW 2 (2007), *available at* http://www.fas.org/sgp/crs/intel/RL31798.pdf).

211. *See What is Big Data and Hadoop?*, ZETTASET, http://www.zettaset.com/info-center/what-is-big-data-and-hadoop.php (last visited Nov. 17, 2013).

212. Natasha Singer, *You for Sale*, N.Y. TIMES, June 17, 2012, at BU1, *available at* http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?_r=0.

213. *See* Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1157 (2005).

- Health information such as interests in particular conditions or diseases; and
- Lifestyle indicators such as shopping preferences, media usage, and types of social media used.[214]

In the past, it was impractical for the government to search for data about every citizen, and this technological barrier effectively limited the government's data mining efforts to situations involving some particularized suspicion.[215] Today, however, with the rise of large-scale private data collection and aggregation, the government can now conduct many more automated investigations—for example, it can easily find all of the people who bought books about particular topics.[216] In fact, as Professor Christopher Slobogin explained, many governmental data mining efforts rely largely on "commercial data brokers[ ] to provide their input, which is then analyzed by government officials."[217] These data brokers offer a plethora of data about individuals:

> [Such data] includ[es] basic demographic information, income, net worth, real property holdings, social security number, current and previous addresses, phone numbers and fax numbers, names of neighbors, driver records, license plate and VIN numbers, bankruptcy and debtor filings, employment, business and criminal records, bank account balances and activity, stock purchases, and credit card activity.[218]

Thus, the government can aggregate in one place all of the individual pieces of information that people convey to many different third parties over many years, which can now be used for "unrelated, unexpected, and typically undesired purpose[s]."[219]

Information released by Google offers one example of the government's reliance on third-party data. Google fields ever-increasing numbers of such requests from the government each year.[220] For example, the following chart shows the total number of government data requests sent to Google for the six-

---

214. Letter from Jennifer Barrett Glasgow, Global Privacy & Pub. Policy Exec., Acxiom Corp., to Representative Edward Markey, U.S. House of Representatives (Aug. 15, 2012) [hereinafter Acxiom Response], *available at* http://geekslop.com/main/wp-content/uploads/2012/11/Acxiom_response_to_lawmakers.pdf.

215. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 181 (2004).

216. *Id.*; *see also* Solove, *supra* note 21, at 1400–13 (providing an excellent summary of the history of public and private databases).

217. Slobogin, *supra* note 210, at 320.

218. *Id.*

219. Henderson, *supra* note 61, at 392.

220. *Transparency Report*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/data (last visited Nov. 14, 2013).

month periods ending from December 2009 to June 2013.[221] Where the data are available, the chart also shows the percentage of requests with which Google complied.[222]

Table 1: U.S. State and Federal Government Requests for Google User Data[223] – 2009-2012

End Date of Six-Month Period	Number of Government Requests	Percentage in Which Google Supplied Data
12/31/2009	3,580	(not available)
6/30/2010	4,287	(not available)
12/31/2010	4,601	94%
6/30/2011	5,950	93%
12/31/2011	6,321	93%
6/30/2012	7,969	90%
12/31/2012	8,438	88%
6/30/2013	10,918	82%

Cellular telephone providers face even more government requests for information than Google.[224] In 2011, cellular telephone providers responded to at least 1.3 million requests for information about cellular telephone subscribers.[225] As long as the government does not seek information about the content of the call, the government can request information about where the cellular phone was located at a particular time, or whom a person called or emailed on a particular day.[226] To obtain such information, the Electronic Communications Privacy Act merely requires the government to persuade a judge that there are "reasonable grounds to believe" that the information sought is "relevant and material to an ongoing criminal investigation."[227]

Government reliance on commercial data is not limited to criminal investigations. As Edward Snowden revealed in 2013, the National Security Agency (NSA) has received telephone records for virtually every domestic telephone subscriber for years.[228] The NSA obtained these records pursuant to

221. *Id.*

222. *Id.*

223. *Id.*

224. *Compare* Adam Liptak, *The Public Is Left in the Dark When Courts Allow Electronic Surveillance*, N.Y. TIMES, July 24, 2012, at A15 ("[C]ell phone carriers responded to at least 1.3 million requests for subscriber information last year."), *with supra* Table 1 (noting that Google received 12,271 requests for user data from governments in 2011).

225. Liptak, *supra* note 224.

226. *Id.*; *see also* 18 U.S.C. § 2703(c), (d) (2012).

227. § 2703(d).

228. *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Subscribers Daily*, THE GUARDIAN, June 5, 2013, *available at* http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; Administration White Paper, *Bulk Collection of Telephony*

Foreign Intelligence Service Court (FISC) orders directing all major telephone providers to give the NSA "telephony metadata" for all of their customers' telephone calls.[229] This metadata includes the telephone numbers of incoming and outgoing calls, as well as the time and duration of every call.[230] Further, the records are not limited to international calls; they include calls between domestic numbers.[231] The Central Intelligence Agency (CIA) has also accessed private telephone records in its investigations, although it has done so through a private contract, rather than a court order.[232] Unlike the NSA's bulk collection program, the CIA's contract does not call for copies of all telephone records.[233] Instead, when the CIA finds a telephone number of a terrorist overseas, the CIA provides that number to AT&T, which searches its records and provides the NSA with call logs for the terrorist's number.[234]

The unprecedented scope of today's data mining raises the stakes for courts and legislators trying to address the third-party privacy problem. Adopting the binary approach will give both governments and private data brokers free rein to build extensive digital dossiers on every citizen.[235] The binary conception fuels the third-party doctrine, which allows the government to circumvent the Fourth Amendment and gather data that would otherwise be available only through a search of the individual citizen's records.[236] The binary conception would also counsel against protection for the data we are increasingly placing in the hands of third parties.[237]

Metadata Under Section 215 of the USA PATRIOT Act 1–2 (Aug. 9, 2013), *available at* http://op.bna.com/der.nsf/id/sbay-9aeu73/$File/Administration%20White%20Paper%20Section%20215.pdf.

229. *See* Greenwald, *supra* note 228; *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [Redacted] (*In re Bulk Metadata Collection Program*), No. BR-13-109, 1–2 (FISA Ct. Oct. 11, 2013), *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf.

230. *See In re Bulk Metadata Collection Program*, No. BR-13-109, at 2 & n.2; Administration White Paper, *supra* note 228, at 7.

231. Administration White Paper, *supra* note 228, at 3.

232. Charlie Savage, *CIA Is Said to Pay AT&T for Call Records*, N.Y. TIMES, Nov. 7, 2013, at A1, *available at* http://www.nytimes.com/2013/11/07/us/cia-is-said-to-pay-att-for-call-data.html.

233. *Id.*

234. *Id.*

235. *See, e.g.*, Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 595–96 (2004) (discussing privacy concerns arising from digital profiles of private citizens containing confidential information).

236. *See id.* at 621–22 (citing Yuval Dror, *Big Brother is Watching You– and Documenting*, HAARETZ, Feb. 20, 2003, www.haaretz.com/print-edition/features/big-brother-is-watching-you-and-documenting-1.18491) (arguing that private data brokers circumvent traditional Fourth Amendment protections by aggregating vast amounts of information on almost any adult and making the aggregated data available to law enforcement).

237. *See id.* at 622.

B. Uploaded Lives

Increasingly, we are living our lives in "the cloud." *Cloud computing* refers to providing computing services through the Internet, rather than on a local drive.[238] Examples of cloud computing include web-based email services like Gmail,[239] online storage services like Carbonite,[240] and business applications like Google Apps for Business.[241] Cloud computing's benefits include "faster deployment of computing resources, a decreased need to buy hardware or to build data centers, and more robust collaboration capabilities."[242]

The move to cloud computing marks a paradigm shift in computer and Internet usage. Prior to widespread Internet usage, data was kept largely on central or mainframe computers, or on isolated individual computer hard drives.[243] Widespread Internet adoption enabled a shift to what Professor Daniel Gervais and Daniel Hyndman call a "connection paradigm," in which the Internet acted as a network connecting computers.[244] Under the connection paradigm, users worked with data and software on their own computers and used the Internet to "transmit processed data between two or more computers."[245] Cloud computing marks a shift to an "amalgamation paradigm."[246] For Gervais and Hyndman, this amalgamation paradigm means that users' devices are mere tools to access "private and commercial content amalgamated on server farms operated by major intermediaries."[247] The cloud computer works with data located on external computers one does not own or control and which that person cannot even locate.[248]

Examining how cloud computing arose may suggest where it is headed. As Internet bandwidth gradually increased, there came a point when relatively low-bandwidth software could function as effectively in the cloud as on the user's computer.[249] Early examples were web-based email providers, which did not

---

238. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-10-513, INFORMATION SECURITY: FEDERAL GUIDANCE NEEDED TO ADDRESS CONTROL ISSUES WITH IMPLEMENTING CLOUD COMPUTING 2 (2010).

239. *See Gmail*, GOOGLE, http://www.gmail.com (last visited Nov. 14, 2013).

240. *See* CARBONITE, http://www.carbonite.com (last visited Nov. 14, 2013).

241. *See* GOOGLE APPS FOR BUSINESS, http://www.google.com/enterprise/apps/business (last visited Oct. 7, 2013).

242. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-10-513, INFORMATION SECURITY: FEDERAL GUIDANCE NEEDED TO ADDRESS CONTROL ISSUES WITH IMPLEMENTING CLOUD COMPUTING 1 (2010).

243. *See* Gervais & Hyndman, *supra* note 1, at 55.

244. *Id.*

245. *Id.* at 57 (citing Nelson Minar & Marc Hedlund, *A Network of Peers: Peer-to-Peer Models Through the History of the Internet*, *in Peer to Peer: Harnessing the Power of Disruptive Technologies* 3 (Andy Oram ed., 2001)).

246. *Id.* at 55.

247. *Id.*

248. *Id.* at 57.

249. *Id.* (citing Arif Mohamad, *A History of Cloud Computing*, COMPUTERWEEKLY.COM (Mar. 27, 2009), http://www.computerweekly.com/feature/A-history-of-cloud-computing).

even require a constant flow of data.[250] As bandwidth expanded, cloud-based services—such as YouTube—arose that could stream video and audio instantly.[251] Gervais and Hyndman predict that, with ever evolving bandwidth and network infrastructure, the cloud will expand to new areas.[252] They see the probable "end game" as "one in which all digital content is either stored exclusively on, or at least backed up on, the Cloud."[253]

Cloud-based computer services are exploding in popularity.[254] A 2010 survey predicted that some five billion devices would be connected to the Internet in September 2010 and that an astonishing twenty-two billion devices would be connected by 2020.[255] An increasing percentage of those Internet connected devices are smartphones.[256] A 2012 survey found that social media usage accounts for nearly one-third of all the time that smartphones are connected to the Internet.[257] Email ranks second, constituting 16% of smartphone usage time.[258]

This rise of cloud computing is changing the types of information that we entrust to third parties. Gervais and Hyndman predict that "soon everything digital will be in the Cloud, including our personal data."[259] The cloud already holds our songs,[260] books,[261] and movies.[262] We have also entrusted significant

250. *Id.* at 57–58.

251. *Id.* at 58.

252. *Id.*

253. *Id.*

254. Paul Lanois, *Privacy in the Age of the Cloud*, J. INTERNET L., Dec. 2011, at 3, 3 (noting that use of cloud-computing services grew by more than 60% from spring 2010 to 2011).

255. Press Release, HIS Elecs. & Research, Internet Connected Devices About to Pass the 5 Billion Milestone (Aug. 19, 2010), *available at* http://imsresearch.com/press-release/Internet_Connected_Devices_About_to_Pass_the_5_Billion_Milestone.

256. *Id.*

257. *Social Media Dominates Smartphone Internet Time, Accounting for Almost One-Third of Minutes*, GFK (Dec. 17, 2012), http://www.gfk.com/us/news-and-events/News/Pages/Social-Media-Dominates-Smartphone-Internet-Time.aspx.

258. *Id.* In contrast to smartphone users, laptop and desktop computer users do not spend as much time on social media. *Id.* The study showed that laptop and desktop users spend their time online in the following manner: 18% on social media, 18% on email, 13% on online video, and 11% on searches. *Id.* In addition, the trend is for smartphone users to account for a greater percentage of total Internet connection time. *Id.* In 2011, computers accounted for 83% of Internet time, compared to 12% for smartphones. *Id.* In 2012, however, that gap closed to 73% for computers and 17% for smartphones. *Id.* Tablets accounted for 3% in 2011 and 6% in 2012; Internet TVs accounted for 2% in 2011 and 4% in 2012. *Id.*

259. Gervais & Hyndman, *supra* note 1, at 54.

260. *See, e.g.*, *iTunes*, APPLE, http://www.apple.com/itunes/features/#everywhere (providing that all music purchased from or added to iTunes can be accessed from all of the user's other devices through the cloud) (last visited Nov. 15, 2013).

261. *See, e.g.*, *id.* (stating that ebooks and audiobooks purchased through iTunes can be accessed through iCloud).

262. *See, e.g.*, *id.* (stating that movies purchased through iTunes accounts can be accessed by all of that users devices through the cloud).

personal information to the cloud, like financial information[263] and tax records.[264] We are increasingly backing up our data to the cloud.[265] We post vast amounts of personal communications, thoughts, feelings, and photographs on social media, such as Facebook, Twitter, and Instagram.[266] And with Google Apps offering the most popular software services online,[267] and Google's new Chromebook laptops poised to use web-based storage, rather than a local hard drive,[268] we are shifting toward creating data in the cloud in the first place.[269]

Cloud computing will also bring about a structural change to the "shareability" of our data.[270] When data exist on devices under our control, we must take steps to share that data. However, once the data migrate into the hands of cloud-based third parties, sharing becomes the default.[271] In fact, it may prove impossible to make our data disappear completely.[272]

The end result of all of this cloud-based sharing is that we are uploading substantial portions of our lives to third parties.[273] This paradigm shift to cloud computing makes third parties an extension of ourselves. Cloud computing takes what was once done on a local hard drive and places it in the hands of third

---

263. *See, e.g.*, *Your Financial Life, All in One Place*, MINT, http://www.mint.com/what-is-mint (providing that users can access all of their financial data online from any device) (last visited Nov. 15, 2013).

264. *See, e.g.*, TURBOTAX, http://turbotax.intuit.com (providing online product services to allow customers to access their tax records from anywhere) (last visited Nov. 15, 2013).

265. *See* Eric A. Taub, Storing Your Files Inside the Cloud, N.Y. TIMES, Mar. 2, 2011, at B7, *available at* http://www.nytimes.com/2011/03/03/technology/personaltech/03basics.html?pagewanted=all&_r=0.

266. *See* Lanois, *supra* note 254, at 3.

267. *See Apps Marketplace*, GOOGLE, https://www.google.com/enterprise/marketplace/?pli=1 (last visited Nov. 15, 2013).

268. *See Introducing Chromebook*, GOOGLE, http://www.google.com/intl/en/chrome/business/devices/features-different.html (last visited Nov. 15, 2013).

269. *See, e.g.*, *id.* ("Chromebooks have a cloud storage service called Google Drive built-in so you can save your work safely in the cloud. Traditional computers often require you to back up your files manually.").

270. Gervais & Hyndman, *supra* note 1, at 55.

271. *Id.* at 79.

272. *Id.* at 78 ("Once personal data is in the Cloud, there is no way to know with certainty where it is stored, which laws apply to that storage, and who might see it. In certain cases, it may simply not be possible to truly delete the information."); *see also* Jeffrey Rosen, *The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google*, 80 FORDHAM L. REV. 1525, 1533 (2012) (discussing efforts in the European Union to enact a "right to be forgotten").

273. *See* Henderson, *supra* note 61, at 390 (discussing the various ways that people upload sensitive information to third parties); *see also* Alex Williams, *Here I Am Taking My Own Picture*, N.Y. TIMES, Feb. 19, 2006, § 9 (SundayStyles), at 1 (describing "digital self-portraits"); Jonathan Zittrain, *Net Neutrality as Diplomacy*, YALE L. & POL'Y REV. INTER ALIA (May 1, 2010, 10:00 AM), http://yalelawandpolicy.org/sites/default/files/YLPRIA29_Zittrain.pdf ("The Internet is . . . the paramount way we communicate with one another, and the means by which we establish our own digital selves.").

parties.[274] Electronic data on static media under our control are shareable, but data in the cloud are already shared.[275]

Part III has illustrated two significant features of the surveillance society: surveillance on demand and uploaded lives. Next, Part IV explains why these changes render the binary conception ineffective to address the third-party privacy problem.

IV. THE BINARY CONCEPTION'S INABILITY TO PROTECT PRIVACY IN THE SURVEILLANCE SOCIETY

The binary conception allows for only two states: private and not private. This indiscriminating approach overlooks the varying degrees of privacy expectations that individuals actually hold. In particular, the binary conception fails to account for three features of how people think about privacy. First, the binary conception ignores the difference between sharing with third parties as ends and sharing with third parties as mere means. Second, the binary conception ignores the anti-aggregation norm—our deep-seated aversion to mass surveillance. Finally, the binary conception rests upon a flawed assumption of consent.

A. The Binary Conception's Failure to Distinguish Third Parties as Ends from Third Parties as Means

Sometimes we share information with third parties with the expectation that those third parties will receive and convey that information. When I update a website hosted by, for example the uber-advertised service GoDaddy.com, I share information with GoDaddy.com with the expectation that GoDaddy.com will receive my information and make it available to anyone browsing my website. Or when I "tweet," I share information with Twitter with the expectation that Twitter will make my tweet available to any Twitter user who chooses to "follow" me.

In contrast, there are many situations in which we share information with third parties but do not intend for those third parties to pass our information along to others. For example, when we engage in online banking, we willingly share information with the bank, but we do not expect the bank to share that information with third parties. Similarly, when we use cloud-based backup providers like Carbonite to store our backup data, or when we create and store documents in the cloud using Google Docs, we do not expect our files to be

---

274. *See, e.g.*, Gervais & Hyndman, *supra* note 1, at 55 ("[U]ser computers and devices are merely tools used to access private and commercial content amalgamated on server farms operated by major intermediaries . . . .").

275. *See, e.g.*, *id.* at 57 ("[W]ith Cloud computing, the user stores (uploads) and accesses (downloads) data located on external computers that the user does not own, does not control, and cannot locate.").

shared with third parties. These cloud-computing services are merely tools that we use to accomplish purposes unrelated to sharing our data.

The binary conception of privacy ignores this distinction and treats all third-party access as a waiver of privacy.[276] In the context of the third-party doctrine, Professor Henderson urges that courts apply this doctrine only when information was provided for the third party's use—thus distinguishing information recipients from mere couriers.[277] Similarly, in Justice Marshall's dissent in *Smith v. Maryland*,[278] he observed that "[t]hose who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[279]

B. The Binary Conception's Failure to Account for the Anti-Aggregation Norm

George Orwell's *Nineteen Eighty-Four*[280] and Franz Kafka's *The Trial*[281] offer popular illustrations of our societal aversion to the all-knowing watcher.[282] As Professor Solove explains, Orwell presented a vision of "Big Brother [a]s an all-knowing, constantly vigilant government that regulates every aspect of one's existence—even one's private thoughts."[283] The Big Brother metaphor "understands privacy in terms of power."[284] Kafka presented a different but equally disturbing vision.[285] According to Professor Solove, "Kafka depicts an indifferent bureaucracy, where individuals are pawns, not knowing what is happening, having no say or ability to exercise meaningful control over the process."[286] Kafka's protagonist, Josef K., embodies "the sense of helplessness, frustration, and vulnerability one experiences when a large bureaucratic organization has control over a vast dossier of details about one's life."[287] Both of these dystopian visions embody a societal fear of pervasive surveillance: the *anti-aggregation norm*.

---

276. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting) ("[T]he Court determines that individuals who convey information to third parties have 'assumed the risk' of disclosure to the government." (citing *id.* at 744–45 (majority opinion))).

277. Henderson, *supra* note 61, at 526.

278. 442 U.S. 735 (1979).

279. *Id.* at 749 (Marshall, J., dissenting).

280. GEORGE ORWELL, NINETEEN EIGHTY-FOUR (Secker & Warburg 1999) (1949).

281. FRANZ KAFKA, THE TRIAL (Edwin Muir & Willa Muir trans., definitive ed., Everyman's Library 1992) (1925).

282. *See* Solove, *supra* note 21, at 1395–99 (citations omitted).

283. *Id.* at 1413.

284. *Id.* at 1415.

285. *See id.* at 1421.

286. *Id.*

287. *Id.*

Lawmakers and legal academics often invoke "Orwellian" or "Kafkaesque" metaphors in their discussions of pervasive government surveillance.[288] Today, however, societal concerns about the all-knowing "other" are not limited to government actors.[289] Professor Solove observed that, while life in the digital age has brought "a dizzying amount of information":

> [I]t has also placed a profound amount of information about our lives in the hands of numerous entities. These digital dossiers are increasingly becoming digital biographies, a horde of aggregated bits of information combined to reveal a portrait of who we are based upon what we buy, the organizations we belong to, how we navigate the Internet, and which shows and videos we watch.[290]

Similarly, Professor Ohm warns that the proliferation of both public and private databases and the ability to "re-identify" what were thought to be anonymous data combine to simulate a "database of ruin" that contains harmful information about everyone.[291]

This anti-aggregation norm figured prominently into the Supreme Court's rejection of long-term, warrantless GPS surveillance in *United States v. Jones*.[292] In the Court's prior vehicle surveillance cases, the Court had reasoned that tracking by traditional visual observation for several days was not a search for Fourth Amendment purposes.[293] In *Jones*, however, five members of the Court distinguished those traditional methods from long-term GPS surveillance.[294] In his concurrence, Justice Alito reasoned:

> [T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses,

---

288. *See, e.g.*, *id.* at 1395–99 (citations omitted) ("Journalists, politicians, and jurists often describe the problem created by databases with the metaphor of Big Brother . . . ."); *see also* Parker B. Potter, Jr., *Ordeal by Trial: Judicial References to the Nightmare World of Franz Kafka*, 3 PIERCE L. REV. 195, 256–71 (2005) (discussing cases in which judges cited both Orwell and Kafka). *But see* Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1128–33 (2006) (citations omitted) (book review) (critiquing the utility of Kafka's *The Trial* as a metaphor for database privacy issues).

289. *See, e.g.*, Solove, *supra* note 10, at 1095 ("The government is increasingly contracting with private sector entities to acquire databases of personal information.").

290. *Id.*

291. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1748 (2010).

292. 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.").

293. *Id.* at 951–52 & n.6 (majority opinion) (citing United States v. Karo, 468 U.S. 705, 707–08, 713 (1984); United States v. Knotts, 460 U.S. 276, 278, 279, 281–82, 284 (1983)).

294. *Id.* at 964 (Alito, J., concurring); *id.* at 955–56 (Sotomayor, J., concurring).

> society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.[295]

Justice Sotomayor recognized the anti-aggregation norm even more explicitly in her concurrence.[296] She observed that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations," and that the "Government can store such records and efficiently mine them for information years into the future."[297] Justice Sotomayor would have addressed the reasonable expectation of privacy issue by asking whether people "reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[298]

Implicit in Justice Sotomayor's reasoning is the failure of the binary conception of privacy. By simply asking whether each piece of data is known to any third party, the binary conception of necessity ignores the anti-aggregation principle. It ignores the difference between knowing a few individual pieces of data about a person, and knowing all of the data about that person.

C. The Binary Conception's Flawed Reliance on the Myth of Consent

The binary conception rests largely on the assumption that allowing any third-party access to one's data means consent to any future sharing of one's data. In *United States v. Miller*,[299] for example, the Court reasoned that the third-party doctrine denied any expectation of privacy for data shared with a third party, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[300] Despite this expectation, the Court reasoned that "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[301]

This assumption of consent, however, does not comport with reality. As Justice Marshall observed in his dissent in *Smith v. Maryland*, "Implicit in the

---

295. *Id.* Justices Ginsburg, Breyer, and Kagan joined Justice Alito in his concurrence. *Id.* at 957.

296. *See id.* at 956 (Sotomayor, J., concurring).

297. *Id.* at 955–56 (citing United States v. Pineda-Moreno, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, J., dissenting)).

298. *Id.* at 956.

299. 425 U.S. 435 (1976).

300. *Id.* at 443 (citing United States v. White, 401 U.S. 745, 752 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427, 438 (1963)).

301. *Id.* (citing *White*, 401 U.S. at 751–52).

concept of assumption of risk is some notion of choice."[302] For several reasons, however, the realities of the surveillance society preclude any notion of choice. First, the imbalance of bargaining power precludes consumer choice.[303] Social networking sites like Facebook, as well as major email and messaging services like Gmail and Twitter, have become "unavoidable" for millions of users.[304] Gervais and Hyndman argue that this leads to such a disparity in bargaining power that, "As a matter of contract law, the differential in bargaining power arguably affects the validity of major waivers of protection in license and other end-user agreements."[305] As a practical matter, this imbalance in bargaining power precludes people from withholding data about themselves from third parties.[306]

Second, even if individuals had sufficient bargaining power to choose, they would lack the information necessary to exercise that power wisely. Consumers are entirely unaware of the existence of some data collection practices.[307] For example, researchers discovered in 2011 that iPhones and iPads were keeping a log of information about their owners' geolocation and transferring that log to computer hard drives when synced—all without their owners' knowledge.[308] Similarly, the Federal Trade Commission reported that consumers are often unaware of the types of data that data brokers gather, the purposes for which those data are used, and even the existence of data brokers.[309] With regard to other practices, consumers may have a general awareness of the data collection, but lack the information to make an informed choice.[310] For example, Professor James Grimmelmann has explained in detail why Facebook users have no meaningful way to assess the risk that the information they share on Facebook will be used beyond their Facebook "friends."[311] Instead of basing their decisions on hard data, the users instead rely on a collection of heuristics that

---

302. 442 U.S. 735, 749 & n.1 (1979) (Marshall, J., dissenting) ("Lacking the Court's apparently exhaustive knowledge of this Nation's telephone books and the reading habits of telephone subscribers . . . I decline to assume general public awareness of how obscene phone calls are traced.").

303. *See* Gervais & Hyndman, *supra* note 1, at 79.

304. *See id.*

305. *Id.*

306. *See* Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 898–900 (2002) (citations omitted).

307. *See* Nick Bilton, *Tracking File Found in iPhones*, N.Y. TIMES, Apr. 21, 2011, at B1.

308. *Id.*

309. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS, at iv, 68 (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

310. *See, e.g.*, Grimmelmann, *supra* note 17, at 1160 ("The social dynamics of social network sites do more than just give people a reason to use them notwithstanding the privacy risks. They also cause people to *misunderstand* those risks.").

311. *Id.* at 1160–64 (citing ROBERT B. CIALDINI, INFLUENCE: THE PSYCHOLOGY OF PERSUASION 114–66 (2007); PATRICIA WALLACE, THE PSYCHOLOGY OF THE INTERNET 14–19 (1999); Dan M. Kahan et al., *Fear of Democracy: A Cultural Evaluation of Sunstein on Risk*, 119 HARV. L. REV. 1071, 1083 (2006) (book review)).

understate the risk.[312] Similarly, with regard to data gathered from Internet browsers, only 38% of consumers say they are even "generally aware of ways they themselves can limit how much information about them is collected by a website."[313]

V. IMPLEMENTING THE CONTEXTUAL CONCEPTION OF PRIVACY

Although implementing the contextual conception of privacy may prove complicated, it can help courts and legislators deal with new technologies more effectively than the binary conception. This Article concludes with two illustrations of how the contextual conception can apply to several emerging surveillance society issues: facial recognition and geolocation data.

A. Facial Recognition Technology

Facial recognition technology converts images of faces into sets of measurements and then compares those measurements against an existing database of measurements to try to find a matching face.[314] Facial recognition technology could be combined with existing networks of public and private video surveillance cameras.[315] The technology can also be used with networks of drones, which could provide surveillance at a fraction of the cost of using more traditional methods.[316] And the database of facial images is not limited to images that law enforcement can create—it can be drawn from publicly available websites such as social networking sites.[317]

---

312. *Id.* at 1164.

313. KRISTIN PURCELL ET AL., PEW INTERNET & AM. LIFE PROJECT, PEW RESEARCH CTR., SEARCH ENGINE USE 2012, at 25 (2012), *available at* http://pewinternet.org/~/media/Files/Reports/2012/PIP_Search_Engine_Use_2012.pdf.

314. Adam Schwartz, *Chicago's Video Surveillance Cameras: A Pervasive and Poorly Regulated Threat to Our Privacy*, 11 NW. J. TECH. & INTELL. PROP. 47, 50 ¶ 17 (2013) (citing LUCAS D. INTRONA & HELEN NISSENBAUM, CTR. FOR CATASTROPHE PREPAREDNESS & RESPONSE, N.Y. UNIV., FACIAL RECOGNITION TECHNOLOGY: A SURVEY OF POLICY AND IMPLEMENTATION ISSUES 11, 15–17 (2009), *available at* http://www.nyu.edu/ccpr/pubs/Niss_04.08.09.pdf).

315. *See id.* at 50 ¶¶ 14, 17. Researchers are now working on techniques to reliably track subjects as they pass from the view of one camera to the next. *See generally* Riccardo Mazzon & Andrea Cavallaro, *Multi-Camera Tracking Using a Multi-Goal Social Force Model*, 100 NEUROCOMPUTING (SPECIAL ISSUE) 41 (2013), *available at* http://www.sciencedirect.com/science/article/pii/S092523121200327X (citations omitted) (describing methods by which peoples' movements can be tracked across multiple cameras); Kevin Hartnett, *Watching You Between Surveillance Cameras and Other Recent Highlights from the Ideas Blog*, BOSTON GLOBE, Feb. 3, 2013, at K12 (discussing the research on developing an algorithm that predicts people's paths).

316. *See* Yochi J. Dreazen, *From Pakistan, with Love*, NAT'L J., Mar. 13, 2011, at 40; Ellen Nakashima & Craig Whitlock, *Air Force's New Tool: 'We Can See Everything,'* WASH. POST, Jan. 2, 2011, at A1.

317. *See What Facial Recognition Technology Means for Privacy and Civil Liberties Before the Subcomm. on Privacy, Tech. and the Law of the S. Comm. on the Judiciary*, 112th Cong. 2, 4–6

If a major city combined facial recognition capability with a network of surveillance cameras monitoring public spaces, it could face a Fourth Amendment challenge. A court applying the binary conception likely would dispense quickly with such a challenge. Under the traditional third-party doctrine, one could have no reasonable expectation of privacy in a face exposed to public view.

The contextual conception, however, would permit a more nuanced approach by recognizing norms that the binary conception ignores. First, exposing our faces to public view is generally not an end in itself, but merely a means to an essential public good—the ability to travel from one location to another.[318] Second, pervasive facial recognition triggers the anti-aggregation norm that Justices Sotomayor and Alito recognized in *United States v. Jones*.[319] Unconnected strangers noting your passage at various points on your journey is qualitatively different from a pervasive system tracking your every movement in public. Finally, there can be no meaningful consent to such a pervasive video surveillance system because the scope of the surveillance is difficult to conceive,[320] and because people must travel on public ways to function in modern society.[321] All of these norms would weigh in favor of a reasonable expectation that the government cannot build a searchable database of places at which every face travels within its video surveillance network.

Legislators will also make different decisions based on which conception of privacy they adopt.[322] Under the binary conception, they would not be likely to restrict surveillance using facial recognition technology because there would be little motivation to protect citizens who are already in public view.[323] On the other hand, legislators applying a contextual conception might take a more nuanced approach. Recognizing that people have not meaningfully consented to such pervasive surveillance, legislators could prohibit law enforcement from using facial recognition techniques in criminal cases, unless supported by a warrant backed by probable cause.[324] In addition, legislators could recognize the anti-aggregation norm by prohibiting law enforcement from creating a general database of facial recognition images, while still allowing them to search for a

---

(2012), *available at* http://www.judiciary.senate.gov/pdf/12-7-18AcquistiTestimony.pdf (testimony of Professor Alessandro Acquisti, Carnegie Mellon University).

318. *See* Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting) ("It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative.").

319. *See* United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

320. *See id.* at 964 (Alito, J., concurring).

321. *See Smith*, 442 U.S. at 750 (Marshall, J., dissenting).

322. *See* Spencer, *supra* note 306, at 858 ("We cannot ignore . . . the role of social expectations in the legislative process.").

323. *See id.* at 860 ("[U]nless the public has a strong desire for privacy in a particular area, attempts to pass legislation establishing that area as a private sphere are doomed to fail.").

324. *Cf.* S. 3287, 112th Cong. §§ 3, 6 (2012) (prohibiting the use of drones to gather evidence of criminal conduct absent a warrant supported by probable cause, as well as the use of any evidence obtained in violation of the act).

particular individual's facial characteristics after obtaining a warrant backed by probable cause.[325]

B. Geolocation Data

Both government and private entities are increasingly seeking access to geolocation data.[326] Geolocation data can identify the location of wireless devices like cell phones.[327] Although mobile phones are one popular source, geolocation data can also come from tablets, laptops, traditional desktops, and even cars.[328] Geolocation data can also be found in photographs that we post online; indeed, a Raytheon engineer has developed software to map a subject's travels based on metadata within people's Facebook photographs.[329] Once disparate geolocation data are collected by individual entities, data brokers can aggregate them and provide a comprehensive database of people's travels.[330]

Given the tremendous amount of data that private data warehouses can gather, consumers may seek relief under various common law theories—assuming no statutory violation has occurred—such as intrusion upon seclusion, public disclosure of private facts, or unfair trade practices.[331] If the court adopts the binary conception, however, the court could take an approach similar to the

---

325. *Cf.* 105 ILL. COMP. STAT. 5/34-18.34 (2013) (providing that, if a school collects facial recognition evidence about a student, the school must only use it for identification and fraud prevention, must destroy it within thirty days of the student's graduation, and must not share the information without consent from the student (or the student's guardian) or a court order).

326. *See e.g.*, Thomas Garry et al., *Intelligent Transportation Systems: Personal Data Needs and Privacy Law*, 39 TRANSP. L.J. 97, 98 (2012) ("Global positioning systems ('GPS') technology . . . is now commonplace in cellular phones, cars, bicycle computers, and even runners' watches.").

327. *See id.*; *see also* Tracie E. Wandell, *Geolocation and Jurisdiction: From Purposeful Availment to Avoidance and Targeting on the Internet*, 16 J. TECH. L. & POL'Y 275, 291–95 (2011) (citations omitted) (discussing technologies used to identify locational data of Internet users).

328. Garry et al., *supra* note 326, at 98.

329. *See* Ryan Gallagher, *Defence Giant Builds 'Google for Spies' to Track Social Networking Users*, THE GUARDIAN (London), Feb. 11, 2013, at 1.

330. *See* Lior Jacob Strahilevitz, *Signaling Exhaustion and Perfect Exclusion*, 10 J. ON TELECOMM. & HIGH TECH. L. 321, 325 (2012) ("By aggregating data from multiple databases and geolocation services, and using data mining techniques to find whatever patterns exist, companies like Verizon and Apple can piece together consumer profiles that make FICO scores look exceptionally crude."); *see also* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1014 (2010) ("A very different dynamic exists with electronic data. Data sent, stored, and received over the Internet can be copied repeatedly, instantly, and freely. It can be zipped around the world in a split second, and it can be stored anywhere and without cost. The data does not occupy any physical space, and it can be divided up and distributed anywhere.").

331. *See* Gervais & Hyndman, *supra* note 1, at 86 ("These [license and other end-user agreements] are often enforced through and are subject to state consumer protection laws. As such, abuse or misuse of personal information, can be considered a form of unfair or deceptive business practice."); Spencer, *supra* note 306, at 851–57 (citations omitted) (discussing the tort law of privacy protection).

third-party doctrine. Under such an approach, the court would reason that there was no invasion of privacy or any aspect of unfairness because consumers entrusted their data to vendors without promises that the third parties could never access their data.

As with the facial recognition example, the contextual conception will permit consideration of social norms that the binary conception disregards. First, although consumers may share their geolocation data when they use navigation apps in their phones or cars, or browse the Internet with their laptops, that data sharing is merely the means to navigating their day-to-day lives.[332] Second, when data warehouses combine all geolocation data from all available sources—both real world and online—about each consumer, they offend the anti-aggregation norm. When consumers share data with each individual vendor or service provider, they are comfortable sharing that information with the vendor or provider because it may improve their service or form part of their transaction, and they are not sharing a complete, 24/7 virtual map of their lives.[333] Thus, consumers still may object to massive aggregation of all of their data. Finally, given the complexities of the marketplace for consumer data, consumers cannot be said to consent in any meaningful way to pervasive data aggregation when they do business with each individual vendor or service provider.[334] These three context-specific concerns—which the binary conception ignores—would favor treating the aggregation of consumer geolocation data as an invasion of privacy.

Geolocation data have already drawn Congress's attention, although Congress has not yet passed geolocation legislation.[335] A purely binary approach would counsel against regulation of the third-party collection or sharing of geolocation data because consumers have shared their data with third parties.

The contextual conception, however, suggests the need for legislative action. One attempt at such action appeared in the Location Privacy Protection Act of 2012 (LPPA), which was introduced in the 112th Congress by Senator Franken and reported with amendments by Senator Leahy.[336] The LPPA would restrict the collection and sharing of geolocation data from devices such as mobile phones and automobiles.[337] The Act would also prevent private entities—like cellular phone providers and GPS navigation system providers—from collecting or sharing consumers' geolocation data without "express authorization."[338]

---

332. *See* Henderson, *supra* note 60, at 526 (noting a distinction between revealing information to a third party for that party's use and revealing information to a third party as a means to an end).

333. *See* Garry et al., *supra* note 326, at 115 ("Most individuals having [sic] a strong stated preference for maintaining the privacy of their movement and travel habits.").

334. *See* Gervais & Hyndman, *supra* note 1, at 79 ("Either [users] don't use the service and risk being left out in the cold, or they use the service and trust the provider not to use their information in some undesirable way."); Spencer, *supra* note 306, at 892 ("Consumers are generally unaware of the variety of ways that businesses collect information about them.").

335. *See* Location Privacy Protection Act of 2012, S. 1223, 112th Cong. (2012).

336. *Id.*

337. *Id.* § 3.

338. *Id.*

Express authorization would require the consumer's express written consent after receiving a notice—separate from the general terms of service—of (1) the information to be collected, (2) the specific individuals with whom the information may be shared, and (3) the means by which the consumer may revoke consent.[339]

This legislative limitation on collecting and sharing geolocation data would recognize the contextual norms at play. First, by requiring express consent to the gathering of geolocation data, the bill would recognize that a consumer, as a general matter, does not set out to share geolocation data. Any sharing that takes place is merely incidental because the geolocation data sharing is merely a means to the consumer's end of completing a transaction or using a service. Second, by requiring the vendor to obtain the consumer's consent and to identify the specific entities with whom it proposes to share the data, the bill would recognize the anti-aggregation norm. And third, by ensuring that consumers receive explicit notice of the information to be gathered and the parties with whom it may be shared, the bill would make it more likely that any geolocation data would not be collected or shared without meaningful consent.

VI. CONCLUSION

The emerging technology of the 1890s prompted Warren and Brandeis to reshape the existing approaches to protecting one's information and likeness.[340] The rapid changes in today's surveillance society require that we do the same with regard to the third-party privacy problem. Changes in technology are driving more and more of our data into the hands of third parties, and those data are becoming increasingly easy to collect, aggregate, and mine. If the binary conception guides how courts and legislators approach the third-party privacy problem, the result will be that sharing data with one third party means sharing that data with *all* third parties. Only the contextual conception captures what the binary conception ignores. The binary conception cannot distinguish sharing as a means to an end from sharing as the end itself. And the binary conception ignores society's long-held anti-aggregation norm and relies on a flawed assumption of consent. The adaptability of the contextual conception will allow judges and legislators to balance more accurately the competing concerns affected by any given data-sharing situation.

339. *Id.*

340. Warren & Brandeis, *supra* note 115, at 195.