The Digital Person
Technology and Privacy in the Information Age

Daniel J. Solove
the digital person
Ex Machina: Law, Technology, and Society
General Editors: Jack M. Balkin and Beth Simone Noveck

The Digital Person
Technology and Privacy in the Information Age
Daniel J. Solove
the digital person

Technology and Privacy in the Information Age

daniel j. solove

NEW YORK UNIVERSITY PRESS New York and London
In loving memory of
my grandma,
Jean
Contents

Acknowledgments ix

1 Introduction 1
   The Problems of Digital Dossiers 2
   Traditional Conceptions of Privacy 7
   Rethinking Privacy 8
   A Road Map for This Book 9

2 The Rise of the Digital Dossier 13
   A History of Public-Sector Databases 13
   A History of Private-Sector Databases 16
   Cyberspace and Personal Information 22

3 Kafka and Orwell: 27
   Reconceptualizing Information Privacy 27
   The Importance of Metaphor 27
   George Orwell’s Big Brother 29
Franz Kafka's Trial 36
Beyond the Secrecy Paradigm 42
The Aggregation Effect 44
Forms of Dehumanization: Databases and the Kafka Metaphor 47

4 The Problems of Information Privacy Law 56
The Privacy Torts 57
Constitutional Law 62
Statutory Law 67
The FTC and Unfair and Deceptive Practices 72
A World of Radical Transparency: Freedom of Information Law 73
The Law of Information Privacy and Its Shortcomings 74

5 The Limits of Market-Based Solutions 76
Market-Based Solutions 76
Misgivings of the Market 81
The Value of Personal Information 87
Too Much Paternalism? 90

6 Architecture and the Protection of Privacy 93
Two Models for the Protection of Privacy 93
Toward an Architecture for Privacy and the Private Sector 101
Reconceptualizing Identity Theft 109
Forging a New Architecture 119

7 The Problem of Public Records 127
Records from Birth to Death 127
The Impact of Technology 131
The Regulation of Public Records 132

8 **Access and Aggregation:**

  Rethinking Privacy and Transparency 140

  The Tension between Transparency and Privacy 140
  Conceptualizing Privacy and Public Records 143
  Transparency and Privacy:
    Reconciling the Tension 150
  Public Records and the First Amendment 155

iii government access

9 **Government Information Gathering** 165

  Third Party Records and the Government 165
  Government–Private-Sector Information Flows 168
  The Orwellian Dangers 175
  The Kafkaesque Dangers 177
  Protecting Privacy with Architecture 186

10 **The Fourth Amendment, Records, and Privacy** 188

  The Architecture of the Fourth Amendment 188
  The Shifting Paradigms of
    Fourth Amendment Privacy 195
  The New *Olmstead* 200
  The Emerging Statutory Regime and Its Limits 202

11 **Reconstructing the Architecture** 210

  Scope: System of Records 211
  Structure: Mechanisms of Oversight 217
  Regulating Post-Collection Use of Data 221
  Developing an Architecture 222
12 Conclusion

Notes 229
Index 267
About the Author 283
It is often said that books are written in solitude, but that wasn’t true for this one. The ideas in this book were created in conversation with many wise friends and mentors. I owe them immense gratitude. Michael Sullivan has had an enormous influence on my thinking, and he has continually challenged me to strengthen my philosophical positions. Paul Schwartz has provided countless insights, and his work is foundational for the understanding of privacy law. Both Michael’s and Paul’s comments on the manuscript have been indispensable. I also must thank Judge Guido Calabresi, Naomi Lebowitz, Judge Stanley Sporkin, and Richard Weisberg, who have had a lasting impact on the way I think about law, literature, and life.

Charlie Sullivan deserves special thanks, although he disagrees with most of what I argue in this book. He has constantly forced me to better articulate and develop my positions. I may never convince him, but this book is much stronger for making the attempt.

So many other people are deserving of special mention, and if I were to thank them all to the extent they deserve, I would more than double the length of this book. Although I only list their names, my gratitude extends much further: Anita Allen, Jack Balkin, Carl Coleman, Howard Erichson, Timothy Glynn, Rachel Godsil, Eric Goldman, Chris Hoofnagle, Ted Janger, Jerry Kang, Orin Kerr, Raymond Ku, Erik Lillquist, Michael Risinger, Marc Rotenberg, Richard St. John, Chris Slobogin, Richard Sobel, Peter Swire, Elliot Turrini, and Benno Weisberg.
I greatly benefited from the comments I received when presenting my ideas, as well as portions of the manuscript, at conferences and symposia at Berkeley Law School, Cornell University, Emory Law School, Minnesota Law School, Seton Hall Law School, Stanford Law School, and Yale Law School.

My research assistants Peter Choy, Romana Kaleem, John Spaccarotella, and Eli Weiss provided excellent assistance throughout the writing of this book. Dean Pat Hobbs and Associate Dean Kathleen Boozang of Seton Hall Law School gave me generous support. Don Gastwirth, my agent, shepherded me through the book publishing process with great enthusiasm and acumen. With unceasing attention, constant encouragement, and superb advice, he helped me find the perfect publisher. Deborah Gershenowitz at NYU Press believed in this project from the start and provided excellent editing.

Finally, I would like to thank my parents and grandparents. Their love, encouragement, and belief in me have made all the difference.

This book incorporates and builds upon some of my previously published work: *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 Stanford Law Review 1393 (2001); *Access and Aggregation: Privacy, Public Records, and the Constitution*, 86 Minnesota Law Review 1137 (2002); *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 Southern California Law Review 1083 (2002); and *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 Hastings Law Journal 1227 (2003). These articles are really part of a larger argument, which I am delighted that I can now present in its entirety. The articles are thoroughly revised, and parts of different articles are now intermingled with each other. The argument can now fully unfold and develop. Privacy issues continue to change at a rapid pace, and even though these articles were written not too long ago, they were in need of updating. The arguments originally made in these articles have been strengthened by many subsequent discussions about the ideas I proposed. I have been forced to think about many issues more carefully and with more nuance. My understanding of privacy is a work in progress, and it has evolved since I began writing about it. This book merely represents another resting place, not the final word.
The Architecture of the Fourth Amendment

The Purposes and Structure of the Fourth Amendment. For better or for worse, we currently regulate law enforcement in the United States with a constitutional regime, comprised primarily by the Fourth, Fifth, and Sixth Amendments. A significant part of this regime applies to government information gathering. The Fifth Amendment affords individuals a privilege against being compelled to testify about incriminating information. The Fourth Amendment regulates the government’s power to obtain information through searches and seizures. Specifically, the Amendment provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.¹

Although the Fourth Amendment applies to government activity in both the civil and criminal contexts,² it is limited to activities that constitute “searches” and “seizures.” Certain activities, such as seeing things exposed openly to public view, are not searches.³ The Fourth
Amendment only governs searches where an individual has “a reasonable expectation of privacy.”

If the Fourth Amendment applies, a search or seizure must be “reasonable.” Although technically the two clauses of the Fourth Amendment are separate, the Court has interpreted the requirement that a search or seizure be reasonable as related to the warrant requirement. To obtain a warrant, the police must demonstrate to a neutral judge or magistrate that they have “probable cause,” which means they must provide “reasonably trustworthy information” that the search will reveal evidence of a crime. Generally, searches and seizures without a warrant are per se unreasonable—which means that they are deemed invalid. This has become known as the “per se warrant rule.”

The Court has made numerous exceptions to the per se warrant rule. For example, the Court held in Terry v. Ohio that the police could stop and frisk an individual without a warrant or probable cause. Further, the Court has held that “special needs” in schools and workplaces make the warrant and probable cause requirements impracticable. In the words of legal scholars Silas Wasserstrom and Louis Michael Seidman, the per se warrant rule “is so riddled with exceptions, complexities, and contradictions that it has become a trap for the unwary.”

The Fourth Amendment is enforced primarily through the exclusionary rule. Evidence obtained in violation of the Amendment must be excluded from trial. Without the exclusionary rule, Justice Holmes observed, the Fourth Amendment would be a mere “form of words.” According to law professor Arnold Loewy: “The exclusionary rule protects innocent people by eliminating the incentive to search and seize unreasonably.” The exclusionary rule, however, has long been a sore spot in Fourth Amendment jurisprudence, engendering extensive debate over its desirability and efficacy.

Fourth Amendment Scope: Privacy. As applied by the Court, the Fourth Amendment has focused on protecting against invasions of privacy, although some commentators contend this focus is misguided. According to legal scholar William Stuntz, criminal procedure is “firmly anchored in a privacy value that had already proved inconsistent with
the modern state." Stuntz, privacy vis-à-vis the government is impracticable given the rise of the administrative state, with its extensive health and welfare regulation. Stuntz asserts that robust Fourth Amendment protection of privacy will prevent the government from regulating industry, uncovering white-collar crime, and inspecting industrial facilities. The government must collect information to enforce certain regulations, such as securities laws and worker safety protections. “By focusing on privacy,” Stuntz argues, “Fourth Amendment law has largely abandoned the due process cases’ concern with coercion and violence.” “The problem,” argues Stuntz, “is not information gathering but [police] violence.”

Legal scholar Scott Sundby offers a different critique of the Fourth Amendment’s focus on privacy. Although designed to expand Fourth Amendment protection, privacy has “turned out to contain the seeds for the later contraction of Fourth Amendment rights.” “The Fourth Amendment as a privacy-focused doctrine has not fared well with the changing times of an increasingly nonprivate world and a judicial reluctance to expand individual rights.”

However, Sundby assumes that “privacy” means what the Court says it means. Many current problems in Fourth Amendment jurisprudence stem from the Court’s failure to conceptualize privacy adequately, both in method and substance. Methodologically, the Court has attempted to adhere to a unified conception of privacy. Conceptualizing privacy by attempting to isolate its essence or common denominator has inhibited the Court from conceptualizing privacy in a way that can adapt to changing technology and social practices. Substantively, the Court originally conceptualized privacy in physical terms as protecting tangible property or preventing trespasses. The Court then shifted to viewing privacy with the secrecy paradigm. In each of these conceptual paradigms, the Court has rigidly adhered to a single narrow conception and has lost sight of the Fourth Amendment’s larger purposes.

In contrast, I contend that the Fourth Amendment provides for an architecture, a structure of protection that safeguards a range of different social practices of which privacy forms an integral dimension. Those like Stuntz and Sundby who contend that the Fourth Amendment should not concern itself with privacy fail to see the importance
of privacy in the relationship between the government and the People. The private life is a critical point for the exercise of power. Privacy shields aspects of our lives and social practices where people feel vulnerable, uneasy, and fragile, where social norms and judgment are particularly oppressive and abrasive. It is also implicated when information relates to our basic needs and desires: finances, employment, entertainment, political activity, sexuality, and family. Indeed, the great dystopian novels of the twentieth century—George Orwell’s *1984*, Aldous Huxley’s *Brave New World*, and Franz Kafka’s *The Trial*—all illustrate how government exercises of power over the private life stifle freedom and well-being.

Although Stuntz contends that the Fourth Amendment must forsake privacy because of the rise of the administrative state, this is the very reason why protecting privacy is imperative. The administrative state threatens to equip the government with excessive power that could destroy the Framers’ careful design to ensure that the power of the People remains the strongest.24 In particular, the extensive power of modern bureaucracies over individuals depends in significant part on the collection and use of personal information. While Stuntz is correct that the Fourth Amendment should not be cabined exclusively to protecting privacy and should address other values such as coercion and violence, he errs in treating privacy and police coercion as mutually exclusive.25

Robust Fourth Amendment protection need not be inconsistent with the administrative state, as a significant amount of modern administrative regulation concerns business and commercial activities which lack Fourth Amendment rights equivalent to those guaranteed to individuals.26 Stuntz retorts that for individuals to have a meaningful protection of privacy, they must be provided with privacy within institutions, which “is almost the same as giving the institution itself a protectible privacy interest.”27 Beyond this, Stuntz contends, “a great deal of government information gathering targets individuals,” such as the information that is gathered in tax forms.28 However, one need not adopt an all-or-nothing approach to Fourth Amendment privacy. The Fourth Amendment does not categorically prohibit the government from compelling certain disclosures by individuals or institutions. If it did, then the tax system and much corporate regulation
would be nearly impossible to administer. But the fact that the government can compel certain disclosures does not mean that it can compel people to disclose the details of their sexual lives or require them to send in their diaries along with their tax forms. The government’s power to inspect factories for safety violations does not mean that the government should be able to search every employee’s office, locker, or bag. Therefore, although misconceptualizing privacy, the Court has correctly made it a focal point of the Fourth Amendment.

**Fourth Amendment Structure: Warrants.** Before eroding it with dozens of exceptions, the Court made the Fourth Amendment’s warrant requirement one of the central mechanisms to ensure that the government was responsibly exercising its powers of information collection. Some critics, however, view warrants as relatively unimportant in the Fourth Amendment scheme. According to constitutional law expert Akhil Amar, the Fourth Amendment “does not require, presuppose, or even prefer warrants—it limits them. Unless warrants meet certain strict standards, they are per se unreasonable.”

Amar contends that the colonial revolutionaries viewed warrants with disdain because judges were highly influenced by the Crown and warrants immunized government officials from civil liability after conducting a search. Therefore, according to Amar, “[t]he core of the Fourth Amendment, as we have seen, is neither a warrant nor probable cause, but reasonableness.”

Amar is too dismissive of warrants. Merely looking to colonial precedents is insufficient, because the Fourth Amendment did not follow colonial precedents (since general searches were rampant) but rejected them. My aim, however, is not to quarrel about original intent. Even if Amar is right about the Framers’ intent, warrants are an important device in our times since, as Scott Sundby observes, “the Founders could not have foreseen the technological and regulatory reach of government intrusions that exists today.”

The warrant requirement embodies two important insights of the Framers that particularly hold true today. First, the warrant requirement aims to prevent searches from turning into “fishing expeditions.” Accordingly, the warrant clause circumscribes searches and
seizures. As the Fourth Amendment states, a warrant must describe with “particular[ity] . . . the place to be searched and the persons or things to be seized.”

The Framers included the warrant clause because of their experience with writs of assistance and general warrants. A writ of assistance was a document that allowed British customs officials to force local officials and even private citizens to search and seize prohibited goods. Writs of assistance didn’t need to specify a particular person or place to be targeted; anyone could be searched under their authority; and they resulted in “sweeping searches and seizures without any evidentiary basis.” Like writs of assistance, general warrants had a very broad scope, and they did not need to mention specific individuals to target or specific locations to be searched. They “resulted in ‘ransacking’ and seizure of the personal papers of political dissenters, authors, and printers of seditious libel.” As Patrick Henry declared: “They may, unless the general government be restrained by a bill of rights, or some similar restrictions, go into your cellars and rooms, and search, ransack, and measure, everything you eat, drink, and wear. They ought to be restrained within proper bounds.”

Second, warrants reflect James Madison’s vision of the appropriate architecture for a society in which the power of the People remains paramount. Writing about separation of powers in Federalist No. 51, Madison observed:

But what is government itself but the greatest of all reflections on human nature? If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controuls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: You must first enable the government to controul the governed; and in the next place, oblige it to controul itself. A dependence on the people is no doubt the primary controul on the government; but experience has taught mankind the necessity of auxiliary precautions.

The profound insight of Madison and the Framers was that by separating government powers between different entities and pitting
them against each other, government could be controlled. As legal scholar Raymond Ku aptly observes, the Framers adopted the Fourth Amendment based on concerns about limiting executive power.42 Madison was acutely aware that the “parchment barriers” of the Constitution would fail to check government encroachments of power, and he explained how both the legislative and executive branches could overstep their bounds.43 He arrived at an architectural solution: Power should be diffused among different departments of government, each afforded “the necessary constitutional means, and personal motives, to resist encroachments of the others.” Government will be kept in check only if its parts consist of “opposite and rival interests.” As historian Gordon Wood describes the Madisonian vision:

It was an imposing conception—a kinetic theory of politics—such a crumbling of political and social interests, such an atomization of authority, such a parceling of power, not only in the governmental institutions but in the extended sphere of the society itself, creating such a multiplicity and a scattering of designs and passions, so many checks, that no combination of parts could hold, no group of evil interests could long cohere. Yet out of the clashing and checking of this diversity, Madison believed the public good, the true perfection of the whole, would somehow arise.45

The warrant requirement reflects Madison’s philosophy of government power by inserting the judicial branch in the middle of the executive branch’s investigation process.46 Although warrants have been criticized as ineffective because judges and magistrates often defer to the police and prosecutor’s determination, criminal procedure expert Christopher Slobogin aptly contends that warrants raise the “standard of care” of law enforcement officials by forcing them to “document their requests for authorization.”47 According to Stuntz, warrants make searching more expensive, because they require law enforcement officials to “draft affidavits and wait around courthouses.”48 Because officers must devote time to obtaining a warrant, they are unlikely to use them unless they think it is likely that they will find what they are looking for.49 As Justice Douglas has explained for the Court:
The Fourth Amendment has interposed a magistrate between the citizen and the police. This was done neither to shield criminals nor to make the home a safe haven for illegal activities. It was done so that an objective mind might weigh the need to invade that privacy in order to enforce the law. The right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals. Power is a heady thing; and history shows that the police acting on their own cannot be trusted. And so the Constitution requires a magistrate to pass on the desires of the police before they violate the privacy of the home.50

Further, the requirement of prior approval prevents government officials from “dreaming up post hoc rationalizations”51 and judges from experiencing hindsight bias when evaluating the propriety of a search after it has taken place.52

My purpose is not to defend the existing structure of the Fourth Amendment as perfect. For the purposes of this discussion, it is sufficient to agree (1) that the Fourth Amendment regime serves an important function by establishing an architecture that aims to protect privacy in addition to other values, and (2) that one of the central features of this architecture requires neutral and external oversight of the executive branch’s power to gather and use personal information.

Even if its efficacy is limited, the structure of the Fourth Amendment is better than a void. Few commentators have suggested that the Fourth Amendment be repealed or that its larger purposes in controlling government power are inimical to a well-functioning society. Outside the realm of the Fourth Amendment is a great wilderness, a jungle of government discretion and uncontrolled power. Thus, the issue of the applicability of the Fourth Amendment is an important one, and to that issue I now turn.

The Shifting Paradigms of Fourth Amendment Privacy

Some notion of privacy has always been the trigger for Fourth Amendment protection, at least since the late nineteenth century. In 1886, in Boyd v. United States,53 an early case delineating the meaning
of the Fourth and Fifth Amendments, the government attempted to subpoena a person’s private papers for use in a civil forfeiture proceeding. The Court held that the subpoena violated the Fourth and Fifth Amendments, since it invaded the individual’s “indefeasible right of personal security, personal liberty and private property.”

Commentators have characterized *Boyd* as protecting property and as consistent with the exaltation of property and contract during the *Lochner* era. The *Lochner* era was a period of Supreme Court jurisprudence lasting from about 1899 through 1937. The case that epitomized this era was *Lochner v. New York*, where the Court struck down a law restricting the number of hours that bakery employees could work to 60 a week. The Court concluded that the law infringed upon the constitutional guarantee of liberty of contract. When the Court also nullified many other progressive laws and New Deal statutes for similar reasons, it was denounced for adhering too strictly to an ideology of laissez faire and unbridled commercial activity.

Although *Boyd* certainly furthers the ideology of the *Lochner* Court, it should not merely be dismissed as the product of *Lochner*-like activism. *Boyd* follows a conception of privacy that the Court consistently adhered to in the late nineteenth century and the first half of the twentieth century. Under this conception, the Court viewed invasions of privacy as a type of physical incursion. For example, nine years prior to *Boyd*, in 1877, the Court held in *Ex Parte Jackson* that the Fourth Amendment applied to the opening of letters sent through the postal system: “The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be.” Additionally, privacy also concerned physical bodily intrusions. In *Union Pacific Railway Company v. Botsford*, an 1891 case concerning privacy but not directly involving the Fourth Amendment, the Court held that a court could not compel a female plaintiff in a civil action to submit to a surgical examination:

> The inviolability of the person is as much invaded by a compulsory stripping and exposure as by a blow. To compel any one, and especially a woman, to lay bare the body, or to submit it to
the touch of a stranger, without lawful authority, is an indignity, an assault, and a trespass.59

Consistent with Boyd and Ex Parte Jackson, the Court readily recognized the injury caused by physical intrusions such as trespassing into homes, rummaging through one’s things, seizing one’s papers, opening and examining one’s letters, or physically touching one’s body. Indeed, in 1890, when Warren and Brandeis authored their famous article The Right to Privacy, they observed that the law, which had long recognized physical and tangible injuries, was just beginning to recognize incorporeal ones.60 Warren and Brandeis argued that privacy was more than simply a physical intrusion, a view increasingly recognized in the common law of torts in the early twentieth century. However, in its Fourth Amendment jurisprudence, the Court held fast to its physical intrusion conception of privacy.

The Court’s view that Fourth Amendment privacy constituted protection from physical intrusions came to a head in 1928 in Olmstead v. United States.61 There, the Court held that the tapping of a person’s home telephone outside a person’s house did not run afoul of the Fourth Amendment because it did not involve a trespass inside a person’s home: “The Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.”62 Olmstead relied upon the Court’s physical intrusion conception of privacy. Since there was no trespassing, opening, or rummaging, there was no invasion of Fourth Amendment privacy.

Justice Louis Brandeis vigorously dissented, chastising the Court for failing to adapt the Constitution to new problems. He observed: “When the Fourth and Fifth Amendments were adopted, the form that evil had theretofore taken had been necessarily simple.”63 The government “could secure possession of [a person’s] papers and other articles incident to his private life—a seizure effected, if need be, by breaking and entry.”64 But technological developments, Brandeis argued, have created new threats to privacy:
[T]ime works changes, brings into existence new conditions and purposes. Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.\(^{65}\)

The Court, however, continued to follow the *Olmstead* conception of privacy in subsequent cases. In *Goldman v. United States*, for example, the police placed a device called a “detectaphone” on the wall next to a person’s office, enabling them to eavesdrop on the conversations inside the office. The Court concluded that since there had been no physical trespass into the office, the Fourth Amendment had not been violated.\(^{66}\)

In 1967, nearly 40 years after *Olmstead*, the Court in *Katz v. United States* finally abandoned the physical intrusion conception of privacy and adopted the Fourth Amendment approach employed today. *Katz* involved the electronic eavesdropping of a telephone conversation made by a person in a phone booth. Explicitly overruling *Olmstead* and *Goldman*, the Court declared: “What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”\(^{67}\)

The Court’s approach to determining the applicability of the Fourth Amendment emerged from Justice Harlan’s concurrence in *Katz*. The “reasonable expectation of privacy test” looks to whether (1) a person exhibits an “actual or subjective expectation of privacy” and (2) “the expectation [is] one that society is prepared to recognize as ‘reasonable.’”\(^{68}\)

Brandeis’s dissent in *Olmstead* only partially won the day in *Katz*. Instead of adopting a conception of privacy that was adaptable to new technology, as the reasonable expectation of privacy test initially promised to be, the Court rigidified its approach with a particular conception of privacy—the secrecy paradigm. The Court based this new conception on the language in *Katz* that privacy turned on what a person exposed to the public. In this way, privacy was conceptual-
ized as a form of secrecy, and people couldn’t have a reasonable expectation of privacy in information that was not kept secret.

The full implications of this new conception of privacy are discussed in the next section. Before turning to this issue, it is important to observe the effects of the Court’s failure to reconceptualize privacy in *Olmstead*. As a result of the nearly 40 years between *Olmstead* and *Katz*, there was little control over the burgeoning use of electronic surveillance, one of the most powerful technological law enforcement tools developed during the twentieth century. The Fourth Amendment stood by silently as this new technology proliferated.

At the time of *Olmstead*, many viewed wiretapping with great unease. Justice Holmes called it a “dirty business.” Even J. Edgar Hoover, who later became one of the greatest abusers of wiretapping, testified in 1929 that wiretapping was “unethical” and that he would fire any FBI employee who engaged in it.

In 1934, just six years after *Olmstead*, Congress enacted §605 of the Federal Communications Act, making wiretapping a federal crime. However, §605 was practically impotent. It did not apply to wiretapping by state police or private parties. Nor did it apply to bugging. Further, it only precluded the disclosure of tapped communications in court proceedings. Thus, the FBI could wiretap so long as it didn’t try to use any of the results in court.

Gradually, presidents gave the FBI increasing authority to wiretap. In World War II, the FBI gained authorization to engage in wiretapping to investigate national security threats. Later, the authorization expanded to encompass domestic security. The fear of communism during the 1950s allowed the FBI to intensify its use of electronic surveillance.

Widespread abuses began to occur. Hoover’s misconduct was egregious. He wiretapped critics of the FBI, enemies of his political allies, and practically anybody whose political views he disliked. As discussed earlier, he engaged in massive electronic surveillance of Martin Luther King, Jr. Presidents also misused the FBI’s wiretapping power for their own political purposes. President Nixon ordered extensive wiretapping, including surveillance of his own speechwriter, William Safire. Presidents Kennedy and Johnson also ordered electronic surveillances inappropriately. With regard to
pre-\textit{Katz} wiretapping by the states, an influential study led by Samuel Dash concluded that 90 percent of state wiretapping lacked court authorization and that state regulation of wiretapping had been largely ineffective against abuses.\textsuperscript{77}

Thus, for 40 years, the government’s power to engage in electronic surveillance fell outside of the reach of the Fourth Amendment, and the legislation that filled the void was ineffective. Today, history is in the process of repeating itself. The Court has made a mistake similar to \textit{Olmstead}, and it is one with severe and far-reaching implications.

\textbf{The New \textit{Olmstead}}

Although we have moved from the \textit{Olmstead} physical intrusion conception of privacy to a new regime based upon expectations of privacy, there is a new \textit{Olmstead}, one that is just as shortsighted and rigid in approach. The Court’s new conception of privacy is the secrecy paradigm. If any information is exposed to the public or if law enforcement officials can view something from any public vantage point, then the Court has refused to recognize a reasonable expectation of privacy.

For example, in \textit{Florida v. Riley}, the Court held that a person did not have a reasonable expectation of privacy in his enclosed greenhouse because a few roof panels were missing and the police were able to fly over it with a helicopter.\textsuperscript{78} In \textit{California v. Greenwood}, the police searched plastic garbage bags that the defendant had left on the curb to be collected by the trash collector. The Court held that there was no reasonable expectation of privacy in the trash because “[i]t is common knowledge that plastic bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public.”\textsuperscript{79} Trash is left at the curb “for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through [the] trash or permitted others, such as the police, to do so.”\textsuperscript{80}

Consistent with this conception of privacy, the Court held that there is no reasonable expectation in privacy for information known or exposed to third parties. In \textit{United States v. Miller}, federal agents
presented subpoenas to two banks to produce the defendant’s financial records. The defendant argued that the Fourth Amendment required a warrant, not a subpoena, but the Court concluded that the Amendment didn’t apply. There is no reasonable expectation of privacy in the records, the Court reasoned, because the information is “revealed to a third party.” Thus, “checks are not confidential communications but negotiable instruments to be used in commercial transactions. 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.”

The Court used similar reasoning in *Smith v. Maryland*. Without a warrant, the police asked a telephone company to use a pen register, which is a device installed at the phone company to record the numbers dialed from the defendant’s home. The Court concluded that since people “know that they must convey numerical information to the phone company,” they cannot “harbor any general expectation that the numbers they dial will remain secret.”

*Miller* and *Smith* establish a general rule that if information is in the hands of third parties, then an individual lacks a reasonable expectation of privacy in that information, which means that the Fourth Amendment does not apply. Individuals thus probably do not have a reasonable expectation of privacy in communications and records maintained by ISPs or computer network administrators. The third party record doctrine stems from the secrecy paradigm. If information is not completely secret, if it is exposed to others, then it loses its status as private. *Smith* and *Miller* have been extensively criticized throughout the past several decades. However, it is only recently that we are beginning to see the profound implications of the third party doctrine. *Smith* and *Miller* are the new *Olmstead* and *Goldman*. Gathering information from third party records is an emerging law enforcement practice with as many potential dangers as the wiretapping in *Olmstead*. “The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping,” Justice Brandeis observed in his *Olmstead* dissent. “Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court,
and by which it will be enabled to expose to a jury the most intimate occurrences of the home.\footnote{86}

That day is here. The government’s harvesting of information from the extensive dossiers being assembled with modern computer technology poses one of the most significant threats to privacy of our times.\footnote{87}

The Emerging Statutory Regime and Its Limits

Throughout the twentieth century, when the Supreme Court held that the Fourth Amendment was inapplicable to new practices or technology, Congress often responded by passing statutes that afforded some level of protection. Through a series of statutes, Congress has established a regime regulating government access to third party records. This regime erects a particular architecture significantly different from that of the Fourth Amendment. Unfortunately, this regime is woefully inadequate.

Procedural Requirements to Obtain Information. The most significant deficiency is that a majority of the statutes permit government access to third party records with only a court order or subpoena—a significant departure from the Fourth Amendment, which generally requires warrants supported by probable cause to be issued by a neutral and detached judge. Unlike warrants, subpoenas do not require probable cause and can be issued without judicial approval. Prosecutors, not neutral judicial officers, can issue subpoenas.\footnote{88} According to Stuntz: “[W]hile searches typically require probable cause or reasonable suspicion and sometimes require a warrant, subpoenas require nothing, save that the subpoena not be unreasonably burdensome to its target. Few burdens are deemed unreasonable.”\footnote{89} According to legal scholar Ronald Degnan, subpoenas are not issued “with great circumspection” and are often “handed out blank in batches and filled in by lawyers.”\footnote{90} As Stuntz contends, federal subpoena power is “akin to a blank check.”\footnote{91}

Prosecutors can also use grand jury subpoenas to obtain third party records.\footnote{92} Grand jury subpoenas are “presumed to be reasonable” and may only be quashed if “there is no reasonable possibility
that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury investigation.”93 As Stuntz observes, grand jury subpoenas “are much less heavily regulated” than search warrants:

As long as the material asked for is relevant to the grand jury’s investigation and as long as compliance with the subpoena is not too burdensome, the subpoena is enforced. No showing of probable cause or reasonable suspicion is necessary, and courts measure relevance and burden with a heavy thumb on the government’s side of the scales.94

Therefore, courts “quash or modify” subpoenas only “if compliance would be unreasonable or oppressive.”95 Further, “judges decide these motions by applying vague legal standards case by case.”96

Court orders under most of the statutes are not much more constrained than subpoenas. They typically require mere “relevance” to an ongoing criminal investigation, a standard significantly lower and looser than probable cause.

The problem with subpoenas and court orders is that they supply the judiciary with greatly attenuated oversight powers. The role of the judge in issuing or reviewing subpoenas is merely to determine whether producing records is overly burdensome. With this focus, financial hardship in producing information would give courts more pause when reviewing subpoenas than would threats to privacy. The role of the judiciary in court orders is also quite restricted. Instead of requiring probable cause, court orders require the government to demonstrate that records are “relevant” to a criminal investigation, a much weaker standard. In short, judicial involvement with subpoenas and court orders amounts to little more than a rubber stamp of judicial legitimacy.

Wiretapping and Bugging. When the Court held in *Olmstead* that the Fourth Amendment did not apply to wiretapping, Congress responded six years later by enacting §605 of the Federal Communications Act of 1934. As discussed earlier, §605 was far too narrow and limited. In 1968, a year after the Court in *Katz* declared that the Fourth Amendment applied to wiretapping, Congress enacted Title III of the
Omnibus Crime Control and Safe Streets Act,97 which greatly strengthened the law of wiretapping, extending its reach to state officials and private parties. In 1986, Congress amended Title III with the Electronic Communications Privacy Act (ECPA). The ECPA restructured Title III into three parts, known as the “Wiretap Act,” which governs the interception of communications; the “Stored Communications Act,” which covers access to stored communications and records; and the “Pen Register Act,” which regulates pen registers and trap and trace devices.98

The Wiretap Act covers wiretapping and bugging. It applies when a communication is intercepted during transmission. The Act has strict requirements for obtaining a court order to engage in electronic surveillance.99 In certain respects, the Wiretap Act’s requirements are stricter than those for a Fourth Amendment search warrant.100 It also requires that the surveillance “minimize the interception of communications” not related to the investigation. The Act is enforced with an exclusionary rule.101

However, the interception of electronic communications not involving the human voice (such as email) is not protected with an exclusionary rule. Although the Wiretap Act has substantial protections, it covers ground already protected by the Fourth Amendment. In areas not protected by the Fourth Amendment, the architecture of the statutory regime is much weaker and more porous.

**Stored Communications.** Communications service providers frequently store their customers’ communications. ISPs temporarily store email until it is downloaded by the recipient. Many ISPs enable users to keep copies of previously read email on the ISP’s server, as well as copies of their sent emails. Since a third party maintains the information, the Fourth Amendment may not apply.102

The Stored Communications Act provides some protection, but unfortunately it is quite confusing and its protection is limited. Electronic storage is defined as “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof,” and “any storage of such communication by an electronic communication service for purposes of backup protection.”103 This definition clearly covers email that is waiting on the ISP’s
server to be downloaded. But what about previously read email that remains on the ISP’s server? According to the Department of Justice’s (DOJ) interpretation of the Act, the email is no longer in temporary storage, and is therefore “simply a remotely stored file.” The Act permits law enforcement officials to access it merely by issuing a subpoena to the ISP. And in contrast to the Wiretap Act, the Stored Communications Act does not have an exclusionary rule.

Communications Service Records. The Stored Communications Act also regulates government access to a customer’s communications service records, which consist of the customer’s name, address, phone numbers, payment information, and services used. One of the most important pieces of information in ISP records is the customer’s identity. An ISP may have information linking a customer’s screen name to her real name. Thus, an ISP often holds the key to one’s ability to communicate anonymously on the Internet. The government often wants to obtain this information to identify a particular speaker. To access customer records, the government must obtain a court order, which requires “specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation.” Further, since the Act lacks an exclusionary rule, information obtained in violation of the law can still be introduced in court.

Pen Registers, Email Headers, and Websurfing. The Pen Register Act attempts to fill the void left by Smith v. Maryland by requiring a court order to use a pen register or trap and trace device. Whereas a pen register records the phone numbers a person dials from her home, a trap and trace device creates a list of the telephone numbers of incoming calls. The USA-PATRIOT Act, passed in 2001 shortly after the September 11th attacks, expanded the scope of the Pen Register Act. The definition of a pen register now extends beyond phone numbers to also encompass addressing information on emails and IP addresses. An IP address is the unique address assigned to a particular computer connected to the Internet. All computers connected to the Internet have one. Consequently, a list of IP addresses accessed
reveals the various websites that a person has visited. Because websites are often distinctively tailored to particular topics and interests, a comprehensive list of them can reveal a lot about a person’s life. The court order to obtain this information, however, only requires the government to demonstrate that “the information likely to be obtained . . . is relevant to an ongoing criminal investigation.” Courts cannot look beyond the certification nor inquire into the truthfulness of the facts in the application. Once the government official makes the proper certification, the court must issue the order. As one court has observed, the “judicial role in approving use of trap and trace devices is ministerial in nature.” Finally, there is no exclusionary rule for Pen Register Act violations.

Financial Records. Two years after United States v. Miller, Congress filled the void with the Right to Financial Privacy Act (RFPA) of 1978, which requires the government to obtain a warrant or subpoena to access records from banks or other financial institutions. However, the subpoena merely requires a “reason to believe that the records sought are relevant to a legitimate law enforcement inquiry.” When subpoena authority is not available to the government, the government need only submit a formal written request for the information.

In addition to banks, credit reporting agencies have detailed records for nearly every adult American consumer. Under the Fair Credit Reporting Act (FCRA) of 1970, a consumer reporting agency “may furnish identifying information respecting any consumer, limited to his name, address, former addresses, places of employment, or former places of employment, to a governmental agency.” Thus, the government can simply request this information without any court involvement. And the government can obtain more information with a court order or grand jury subpoena. Since the FCRA focuses on credit reporting agencies, it doesn’t prohibit the recipients of credit reports from disclosing them to the government.

Although the RFPA and FCRA protect financial information maintained by banks and credit reporting agencies, the government can obtain financial information from employers, landlords, merchants, creditors, and database companies, among others. Therefore, finan-
cial records are protected based only on which entities possess them. Thus, the statutory regime merely provides partial protection of financial data.

**Electronic Media Entertainment Records.** The statutory regime protects records pertaining to certain forms of electronic media entertainment. Under the Cable Communications Policy Act (Cable Act) of 1984, a government official must obtain a court order in order to obtain cable records. The government must offer “clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case.” People can “appear and contest” the court order. This standard is more stringent than the Fourth Amendment’s probable cause and warrant requirements. However, there is no exclusionary rule under the Cable Act.

In addition to cable records, the statutory regime also protects videotape rental records. The Video Privacy Protection Act (VPPA) of 1988 states that a videotape service provider may disclose customer records to law enforcement officials “pursuant to a warrant . . . , an equivalent State warrant, a grand jury subpoena, or a court order.” Unlike the Cable Act, the level of protection under the VPPA is much less stringent.

Although the statutory regime protects the records of certain forms of electronic media entertainment, it fails to protect the records of many others. For example, records from music stores, electronics merchants, and Internet media entities are afforded no protection.

**Medical Records.** Our medical records are maintained by third parties. Could the third party doctrine extend to medical records? On the one hand, given the considerable privacy protection endowed upon the patient-physician relationship, the third party doctrine may stop at the hospital door. On the other hand, the doctrine applies to records of financial institutions, which also have a tradition of maintaining the confidentiality of their customers’ information. Unless the patient-physician relationship is distinguished from banks, the third party doctrine logically could apply to medical records. However, the Supreme Court has yet to push the doctrine this far.
The federal health privacy rules under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 apparently view medical records as falling under the third party doctrine. The rules permit law enforcement officials to access medical records with a mere subpoena.\textsuperscript{124} Health information may also be disclosed “in response to a law enforcement official’s request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person.”\textsuperscript{125}

Moreover, not all health records are covered by HIPAA. Only records maintained by health plans, health care clearinghouses, and health care providers are covered.\textsuperscript{126} Although doctors, hospitals, pharmacists, health insurers, and HMOs are covered, not all third parties possessing our medical information fall under HIPAA. For example, the sale of nonprescription drugs and the rendering of medical advice by many Internet health websites are not covered by HIPAA.\textsuperscript{127} Therefore, while certain health records are protected, others are not.

\textit{Holes in the Regime}. Federal statutes provide some coverage of the void left by the inapplicability of the Fourth Amendment to records held by third parties. Although the statutes apply to communication records, financial records, entertainment records, and health records, these are only protected when in the hands of particular third parties. Thus, the statutory regime does not protect records based on the type of information contained in the records, but protects them based on the particular types of third parties that possess them.

Additionally, there are gaping holes in the statutory regime of protection, with classes of records not protected at all. Such records include those of merchants, both online and offline. Records held by bookstores, department stores, restaurants, clubs, gyms, employers, and other companies are not protected. Additionally, all the personal information amassed in profiles by database companies is not covered. Records maintained by Internet retailers and websites are often not considered “communications” under the ECPA; the government can access these records and the ECPA doesn’t apply. Thus, the statutory regime is limited in its scope and has glaring omissions and gaps. Further, the statutes are often complicated and confusing, and their
protection turns on technical distinctions that can leave wide fields of information virtually unprotected.

Therefore, the current statutory regime is inadequate. As warrants supported by probable cause are replaced by subpoenas and court orders supported by “articulable facts” that are “relevant” to an investigation, the role of the judge in the process is diminished to nothing more than a decorative seal of approval. And since there are numerous holes in the regime, there are many circumstances when neither court orders nor subpoenas are required. The government can simply ask for the information. An individual’s privacy is protected only by the vague and toothless privacy policies of the companies holding their information.