2008

The Constitution in the National Surveillance State

Jack M. Balkin

Essay

The Constitution in the National Surveillance State

Jack M. Balkin†

Late in 2005, the *New York Times* reported that the Bush administration had ordered the National Security Agency (NSA) to eavesdrop on telephone conversations by persons in the United States in order to obtain information that might help combat terrorist attacks.[1] The secret NSA program operated outside of the restrictions on government surveillance imposed by the 1978 Foreign Intelligence Surveillance Act (FISA)[2] and is thought to be only one of several such programs.[3] In 2007, Congress temporarily amended FISA to increase the

† Knight Professor of Constitutional Law and the First Amendment, Yale Law School. This essay was originally given as the William B. Lockhart Lecture at the University of Minnesota Law School on October 10, 2006. My thanks to Bruce Ackerman, Orin Kerr, Seth Kreimer, Sandy Levinson, Tracey Meares, and Tal Zarsky for comments on a previous draft, and to Leah Belsky for research assistance.

1. James Risen, *Bush Lets U.S. Spy on Callers Without Courts,* N.Y. TIMES, Dec. 15, 2007, at A1. *See generally* JAMES RISEN, STATE OF WAR: THE SECRET HISTORY OF THE CIA AND THE BUSH ADMINISTRATION 39–60 (2006).

On January 17, 2007, Attorney General Gonzales wrote to Senators Patrick Leahy and Arlen Specter, respectively the Chairman and Ranking Minority Member of the Senate Judiciary Committee, stating that the administration would conduct the Terrorist Surveillance Program under the approval of the Foreign Intelligence Surveillance Court using new "complex" and "innovative" court orders. Letter from Alberto R. Gonzales, Attorney Gen., to Patrick Leahy and Arlen Specter, Senators (Jan. 17, 2007), *available at* http://www.talkingpointsmemo.com/docs/nsa-doj-surveillance/.

2. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 26 (1978) (codified as amended in scattered sections of 50 U.S.C.).

3. On the variety of NSA domestic surveillance programs, which blur the line between domestic and foreign intelligence, see Siobhan Gorman, *NSA's Domestic Spying Grows As Agency Sweeps Up Data*, WALL ST. J., Mar. 10, 2008, at A1 (describing the NSA's monitoring of a wide range of personal data from credit card transactions and e-mail to Internet searches and travel records, as well as "an ad-hoc collection of so-called 'black programs' whose existence is undisclosed").

President's power to listen in on conversations where at least one party is reasonably believed to be outside the United States.[4] In June 2008, Congress passed a new set of amendments to FISA, which allow the President to engage in a broad range of electronic surveillance without seeking warrants against particular individual targets of surveillance.[5] At the same time, Congress effectively immunized telecommunications companies that had participated in the secret NSA program.[6]

In July 2007, New York City announced that it planned to mount thousands of cameras throughout Lower Manhattan to monitor vehicles and individuals.[7] Some cameras will be able to photograph and read license plates and send out alerts for suspicious cars.[8] The system of cameras will link to a series of pivoting gates installed at critical intersections, giving government officials the ability to block off traffic through electronic commands.[9] New York's new plan—called the Lower Manhattan Security Initiative—is based on London's "Ring of Steel," a security and surveillance system around London's central core that features thousands of surveillance cameras.[10] New York is hardly alone;[11] the Department of Homeland Security has been quietly channeling millions of dollars to local governments around the country to create hi-tech camera networks that can be linked with private surveillance systems.[12]

4. Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (2007).

5. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436, 2437–78 (2008) (to be codified in 50 U.S.C. §§ 1801–12).

6. §§ 801–04, 122 Stat. 2467–70.

7. Cara Buckley, *Police Plan Web of Surveillance for Downtown*, N.Y. TIMES, July 9, 2007, at A1.

8. *Id.*

9. *Id.*

10. *See* Michael McCahill & Clive Norris, *CCTV in London* 6–11 (Urbaneye, Ctr. For Criminology and Criminal Justice, Univ. of Hull, Working Paper No. 6, 2002), *available at* http://www.urbaneye.net/results/ue_wp6.pdf; SURVEILLANCE STUDIES NETWORK, A REPORT ON THE SURVEILLANCE SOCIETY (2006), http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf; Manav Tanneeru, *'Ring of Steel' Coming to New York*, CNN, Aug. 3, 2007, http://www.cnn.com/2007/TECH/08/01/nyc.surveillance/index.html.

11. *See* Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1351–52 (2004) (noting the proliferation of cameras in New York, Baltimore, Washington, D.C., and Chicago).

12. Charlie Savage, *United States Doles Out Millions for Street Cameras*,

The secret NSA program and New York's Lower Manhattan Security Initiative reflect a larger trend in how governments do their jobs that predates the September 11, 2001 attacks and the Bush administration's declaration of a "war on terror."[13] During the last part of the twentieth century, the United States began developing a new form of governance that features the collection, collation, and analysis of information about populations both in the United States and around the world. This new form of governance is the National Surveillance State.

In the National Surveillance State, the government uses surveillance, data collection, collation, and analysis to identify problems, to head off potential threats, to govern populations, and to deliver valuable social services. The National Surveillance State is a special case of the Information State—a state that tries to identify and solve problems of governance through the collection, collation, analysis, and production of information.

The war on terror may be the most familiar justification for the rise of the National Surveillance State,[14] but it is hardly the sole or even the most important cause. Government's increasing use of surveillance and data mining is a predictable result of accelerating developments in information technology.[15] As technologies that let us discover and analyze what is happening in the world become ever more powerful, both governments and private parties will seek to use them.[16]

The question is not whether we will have a surveillance state in the years to come, but what sort of surveillance state

BOSTON GLOBE, Aug. 12, 2007**,** at A1 ("Since 2003, the Department has handed out some $23 billion in federal grants to local governments for equipment and training to help combat terrorism . . . [including] millions on surveillance cameras, transforming city streets and parks into places under constant observation.").

13. Jack M. Balkin & Sanford Levinson, *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 FORDHAM L. REV. 489, 490 (2006).

14. *See* Andrew Cohen, *The Legal War on Terror: White House Describing Surveillance in Military Terms*, CBS NEWS, Jan. 22, 2006, http://www.cbsnews.com/stories/2006/01/22/opinion/courtwatch/main1227481.shtml.

15. *Cf.* James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1464–68 (2004).

16. *See id.* at 1468–69 (describing government use of privately collected data). *See generally* U.S. GEN. ACCOUNTING OFFICE, GAO-04-548, DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES (2004), *available at* http://www.gao.gov/new.items/d04548.pdf [hereinafter U.S. GEN. ACCOUNTING OFFICE] (reporting widespread use of privately collected data).

we will have. Will we have a government without sufficient controls over public and private surveillance, or will we have a government that protects individual dignity and conforms both public and private surveillance to the rule of law?

The National Surveillance State is a way of governing. It is neither the product of emergency nor the product of war. War and emergency are temporary conditions. The National Surveillance State is a permanent feature of governance, and will become as ubiquitous in time as the familiar devices of the regulatory and welfare states.[17] Governments will use surveillance, data collection, and data mining technologies not only to keep Americans safe from terrorist attacks but also to prevent ordinary crime and deliver social services.[18] In fact, even today, providing basic social services—like welfare benefits—and protecting key rights—like rights against employment discrimination—are difficult, if not impossible, without extensive data collection and analysis.[19] Moreover, much of the surveillance in the National Surveillance State will be conducted and analyzed by private parties.[20] The increased demand for—and the in-

17. *See* Balkin & Levinson, *supra* note 13, at 520–23.

18. *See id.* at 525–26; *see also* Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 440–44 (2008).

19. While surveillance is usually portrayed as a tool for social control, it is also a means by which governments respect and realize citizenship to the extent that it enables the implementation of the welfare state and the rights and benefits that go with it. As David Lyon explains:

> [T]he surveillance systems of advanced bureaucratic nation-states are not so much the repressive machines that pessimists imply, but the outcome of aspirations and strivings for citizenship. If government departments are to treat people equally, . . . then those people must be individually identified. To exercise the right to vote, one's name must appear on the electoral roll; to claim welfare benefits, personal details must be documented. Thus, . . . the individuation that treats people in their own right, rather than merely as members of families or communities, means "freedom from specific constraints but also greater opportunities for surveillance and control on the part of a centralized state."

See DAVID LYON, THE ELECTRONIC EYE 32-33 (1994) (quoting NICHOLAS ABERCROMBIE, SOVEREIGN INDIVIDUALS OF CAPITALISM (1994)).

Governments, of course, have long been in the business of collecting and analyzing statistics to facilitate governance. The famous Domesday Book, commissioned in 1086 by William the Conqueror, sought to assess the land and resources owned in England to facilitate tax collection in order to raise the necessary capital to support armies in defense of the realm. It included exhaustive compilations of landholders, their tenants, the properties they owned, and their values both before and after the Conquest, thus providing a snapshot of the country's social and economic state.

20. *See* U.S. GEN. ACCOUNTING OFFICE, *supra* note 16, at 11; Dempsey &

creased use of—public and private surveillance cannot be explained or justified solely in terms of war or emergency.[21]

The National Surveillance State grows naturally out of the Welfare State and the National Security State; it is their logical successor. The Welfare State governs domestic affairs by spending and transferring money and by creating government entitlements, licenses, and public works.[22] The National Security State[23] promotes foreign policy through investments in defense

Flint, *supra* note 15, at 1468–73 (describing government use of privately collected data).

21. Balkin & Levinson, *supra* note 13, at 520–23 ("The National Surveillance State arose from a number of different features whose effects are mutually reinforcing. The most obvious causes are changes in how nations conduct war and promote their national security . . . . Equally important [however] . . . are new technologies of surveillance, data storage, and computation . . . .").

22. Although the Welfare State as a mode of governance is often identified with the New Deal, its techniques and mechanisms arose earlier. *See generally* THEDA SKOCPOL, PROTECTING SOLDIERS AND MOTHERS: THE POLITICAL ORIGINS OF SOCIAL POLICY IN THE UNITED STATES (1992) (rooting contemporary principles of social welfare policy in nineteenth-century pension benefits for veterans and their families); STEPHEN SKOWRONEK, BUILDING A NEW AMERICAN STATE: THE EXPANSION OF NATIONAL ADMINISTRATIVE CAPACITIES 1877–1920 (1982) (describing the development of parts of the machinery of the modern state in the era before the New Deal). On the constitutional problems posed by the welfare state, see PAUL BREST ET AL., PROCESSES OF CONSTITUTIONAL DECISIONMAKING 1593–1800 (5th ed. 2006) (discussing constitutional disputes over rights to government services and benefits, unconstitutional conditions, and due process requirements); ROBERT G. MCCLOSKEY, THE AMERICAN SUPREME COURT 174–205 (Sanford Levinson ed., 2d ed. 1994) (discussing the constitutional implications of the rise of the welfare state in the twentieth century; materials on the Welfare State written by Sanford Levinson).

23. The National Security State arose in the wake of World War II in the context of the American struggle against the Soviet Union during the cold war. This required, among other things, substantial new investments in defense spending and military technology, the stationing of American forces around the world, and a new emphasis on intelligence capabilities. A characteristic piece of legislation is the National Security Act of 1947, Pub. L. No. 253, ch. 343, 61 Stat. 495 (codified as amended in scattered sections of 50 U.S.C.), which reorganized the military and intelligence services and created the Department of Defense, the National Security Council, and the Central Intelligence Agency. For historical accounts of the causes and growth of the National Security State, see MICHAEL J. HOGAN, A CROSS OF IRON: HARRY S. TRUMAN AND THE ORIGINS OF THE NATIONAL SECURITY STATE 1945–1954 (1998); DANIEL YERGIN, SHATTERED PEACE: THE ORIGINS OF THE COLD WAR AND THE NATIONAL SECURITY STATE (1977). For legal and constitutional accounts, see William M. Wiecek, *America in the Post-War Years: Transition and Transformation*, 50 SYRACUSE L. REV. 1203 (2000); William M. Wiecek, *The Legal Foundations of Domestic Anticommunism: The Background of* Dennis v. United States, 2001 SUP. CT. REV. 375 (2001).

industries and defense-related technologies, through creating and expanding national intelligence agencies like the CIA and the NSA, and through the placement of American military forces and weapons systems around the globe to counter military threats and project national power.

The Welfare State created a huge demand for data processing technologies to identify individuals—think about all the uses for your Social Security Number—and deliver social services like licenses, benefits, and pensions.[24] The National Security State created the need for effective intelligence collection and data analysis.[25] It funded the development of increasingly powerful technologies for surveillance, data collection, and data mining, not to mention increasingly powerful computer and telecommunications technologies.[26] American investments in defense technologies spurred the electronics industry,

24. The United States government played an important role in promoting the development of data processing technology. A former office worker for the census, Herman Hollerith, invented the computer punch card to help tabulate statistics about populations in the United States. SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 17 (2000). The tabulating machine company Hollerith founded eventually became known as the International Business Machine Company, or IBM. *Id.* at 18. The creation of the modern welfare state, with its vast array of new government employees and beneficiaries of government programs, created a demand for the services of IBM and similar companies, and the Social Security number eventually became a central identifier for the federal and state governments. Initially created to provide unique identifiers for all individuals collecting benefits, social security numbers were then adopted by many states for administration of income taxes, drivers licenses, student IDs, and library cards. Eventually the private sector began to use the numbers for consumer credit reporting. *Id.* at 19–25, 33; *see also* SOCIAL SECURITY ADMIN., PUBL'N. NO. 21-059, SOCIAL SECURITY: A BRIEF HISTORY (2007), *available at* www.ssa.gov/history/pdf/2005 pamphlet.pdf.

Similar developments occurred in Europe, as record-keeping requirements morphed from providing proof of identity to underpinning personal rights and governmental obligations, including pensions and allowances for families of military personnel. The expansion of the welfare state created a need for statistics to facilitate planning of delivery of social services, for letting citizens know about services available to them, for enforcing traffic laws, and for identifying criminal suspects. *See* Edward Higgs, *The Rise of the Information State: The Development of Central State Surveillance of the Citizen in England, 1500–2000*, 14 J. HIST. SOC. 175, 185–86 (2001).

25. *See* Cate, *supra* note 18, at 444–52.

26. *See id.* at 456–59. *See generally* JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE (2004) (exploring the threats to privacy and promotion of social conformity through emerging surveillance technology).

the computer industry, and eventually, the birth of the Internet itself.[27]

By the time the Internet went commercial in the mid-1990s, the National Surveillance State was already well in gear. Telecommunications, computing, data storage, and surveillance technologies have become ever more potent, while their costs have steadily declined.[28] It is unthinkable that governments would not seek to use these technologies to promote the public good; it is even more unthinkable that private parties would not try to harness them as well. In fact, much, if not most surveillance and information collection these days is in private hands. Corporations invest heavily in security and surveillance, especially to protect sensitive information in their computer networks.[29] Private security cameras still outnumber those operated by the government.[30] Many businesses make money from collecting, analyzing, and selling consumer data; in fact, governments increasingly purchase information from corporations instead of collecting it themselves.[31]

In the National Surveillance State, the line between public and private modes of surveillance and security has blurred if not vanished. Public and private enterprises are thoroughly intertwined.[32] The NSA program would be impossible without the

27. *See* Internet Society, A Brief History of the Internet and Related Networks (2007), http://www.isoc.org/internet/history/cerf.shtml.

28. *See* Patricia L. Bellia, *The Memory Gap in Surveillance Law*, 75 U. CHI. L. REV. 137, 142–53 (2008) (describing trends which "make indefinite data retention feasible for businesses and individuals alike").

29. *See, e.g.*, LAWRENCE A. GORDON ET AL., COMPUTER SECURITY INSTITUTE, COMPUTER CRIME AND SECURITY SURVEY 5–6 (2006), *available at* http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf.

30. *See* Dean E. Murphy, *As Security Cameras Sprout, Someone's Always Watching*, N.Y. TIMES, Sept. 29, 2002, at A33 ("The Security Industry Association estimates that at least two million closed-circuit television systems are in the United States. A survey of Manhattan in 1998 by the American Civil Liberties Union found 2,397 cameras fixed on places where people pass or gather, like stores and sidewalks. All but 270 were operated by private entities, the organization reported. CCS International, a company that provides security and monitoring services, calculated last year that the average person was recorded 73 to 75 times a day in New York City.").

31. *See* JAY STANLEY, AM. CIVIL LIBERTIES UNION, THE SURVEILLANCE-INDUSTRIAL COMPLEX: HOW THE AMERICAN GOVERNMENT IS CONSCRIPTING BUSINESSES AND INDIVIDUALS IN THE CONSTRUCTION OF A SURVEILLANCE SOCIETY 12, 26 (2004), *available at* http://www.aclu.org/FilesPDFs/surveillance_report.pdf; U.S. GEN. ACCOUNTING OFFICE, *supra* note 16, at 8–11.

32. *See, e.g.*, ROBERT O'HARROW, JR., NO PLACE TO HIDE 1–10 (2005) (detailing links of cooperation between private information collection industries and government); Dempsey & Flint, *supra* note 15, at 1468–70 (noting gov-

assistance of telecommunications companies; the government now requires that new communications technologies be designed with back ends that facilitate government surveillance.[33] Federal programs also encourage linking private security cameras with comprehensive government systems like those planned in Manhattan.[34] Corporate data collectors and commercial data mining operations are a major source of information on individuals' tastes, preferences, histories, and behaviors that governments can harness.[35] Government and businesses are increasingly partners in surveillance, data mining, and information analysis.[36] Moreover, the architecture of the Internet—and the many possible methods of attack—requires governments, corporations, and private parties to

ernment use of commercial data for intelligence and counterterrorism purposes).

33. Communications Assistance for Law Enforcement Act of 1994 (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. §§ 1001–10 (2006)). CALEA mandates that telecommunications services design their technology so it can be wiretapped by the government pursuant to a lawful authorization or a court order, in a manner which enables the government to access call-identifying information, and which allows the transmission of the intercepted information to the government. 47 U.S.C. § 1002(a)(1); *see* Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH 6, para. 84 (2003); Emily Hancock, *CALEA: Does One Size Still Fit All?*, *in* CYBERCRIME: DIGITAL COPS IN A NETWORKED ENVIRONMENT 184–203 (Jack M. Balkin et al. eds., 2007) [hereinafter CYBERCRIME].

34. *See* Buckley, *supra* note 7 (describing coordination of public and private cameras in Lower Manhattan Security Initiative).

35. *See* Cate, *supra* note 18, at 435 (explaining how "advances in digital technology have greatly expanded the volume of personal data created as individuals engage in everday activities").

36. *See, e.g.*, Verne Kopytoff, *Google Now Has a Lot More To Do With Intelligence*, S.F. CHRON., Mar. 30, 2008, at C6 (detailing Google's multiple services for the government). According to Kopytoff, Google's customers include not only the intelligence agencies, but also "the National Oceanographic and Atmospheric Administration, the U.S. Coast Guard, the National Highway Traffic Safety Administration, the State of Alabama and Washington D.C." *Id.* It sells "virtually the same products to companies as it does to government agencies." *Id.*; *see also* ROSEN, *supra* note 26, at 108 (explaining how Silicon Valley companies work with the government to enable data collection techniques and other new technologies to serve government). Silicon Valley entrepreneurs, Rosen reports, are working toward a "killer app" useful for both business and for national security that "will allow government agencies to access and share information about Americans that is currently stored in different databases—from our chat-room gossip to our shopping history to our parking tickets, and perhaps even to our payment history for child-support checks." *Id.* at 107.

work together to protect network security and head off threats before they occur.[37]

Increased focus on surveillance and prevention becomes inevitable once digital information technologies become widely dispersed. Criminal organizations and terrorist groups can use many of the same information and surveillance technologies that governments and legitimate businesses do.[38] Terrorist groups that lack fixed addresses can use new information technologies to communicate and plan assaults.[39] Hackers can attack networks from afar.[40] A new breed of criminals employs digital networks to commit old-fashioned crimes like embezzlement and to commit new crimes like identity theft and denial of service attacks.[41] Cyberattacks can not only bring down financial institutions; they can also target the nation's defense systems.[42] Digital technologies simultaneously pose new prob-

37. For example, the FBI's InfraGard program seeks cooperation between government, business, and academia to protect computer networks and Internet infrastructure. InfraGard, About InfraGard, http://www.infragard.net/about.php?mn=1&sm=1-0 (last visited Oct. 14, 2008); *see also Current and Projected National Security Threats to the United States: Before the S. Select Comm. on Intelligence*, 109th Cong. 33 (2005) (statement of Robert S. Mueller, III, Director, Fed. Bureau of Investigation), *available at* http://www.fbi.gov/congress/congress05/mueller021605.htm (describing a central mission of the FBI as "proactively target[ing] threats to the US, inhibiting them, and dissuading them before they become crimes").

38. *E.g.*, PHILIP BOBBITT, TERROR AND CONSENT 55–57 (2008) (describing how new information technologies facilitate international terrorism).

39. *See id.*; GABRIEL WEIMANN, TERROR ON THE INTERNET 106 (2006) (describing Al Qaeda's use of the Internet); Audrey Kurth Cronin, *Behind the Curve: Globalization and International Terrorism*, 27 INT'L SECURITY 30, 46–48 (2002–03) (explaining challenges created by changes in means, methods and organization of terrorist networks due to new technology); Robert F. Worth, *TheirSpace*, N.Y. TIMES, June 25, 2006, at 21 (reviewing WEIMANN, *supra*).

40. *See* BOBBITT, *supra* note 38, at 95; Daniel E. Geer, Jr., *The Physics of Digital Law: Searching for Counterintuitive Analogies*, *in* CYBERCRIME, *supra* note 33, at 13–36.

41. *See* BOBBITT, *supra* note 38, at 55–57; Scott Charney, *The Internet, Law Enforcement, and Security*, *in* 2 PRACTICING L. INST., FIFTH ANNUAL LAW INSTITUTE 943–44 (Ian C. Ballon et al. eds., 2001) (detailing the increasing vulnerabilities and threats to the state that are enabled by new technologies); Geer, *supra* note 40 (noting basic problems of network security that facilitate attacks); Doreen Carvajal, *High-Tech Crime Is an Online Bubble That Hasn't Burst*, N.Y. TIMES, Apr. 7, 2008, at C2.

42. *See, e.g.*, O'HARROW, *supra* note 32, at 10 (noting that while America's technological capability could serve as a weapon abroad, its use could also "spin out of control" in the hands of enemies).

lems for governments and create new opportunities for identifying threats and meeting them in advance.[43]

Older models of law enforcement have focused on apprehension and prosecution of wrongdoers after the fact and the threat of criminal or civil sanctions to deter future bad behavior.[44] The National Surveillance State supplements this model of prosecution and deterrence with technologies of prediction and prevention. Computer security tries to identify potential weaknesses and block entry by suspicious persons before they have a chance to strike.[45] Private companies and government agencies use databases to develop profiles of individuals who are likely to violate laws, drive up costs, or cause problems, and then deflect them, block them, or deny them benefits, access, or opportunities.[46] The government's "No Fly" and "Selectee" watch lists and its still-planned Secure Flight screening program collect information on passengers and create profiles that seek to block dangerous people from boarding planes.[47] Gover-

43. *See* BOBBITT, *supra* note 38, at 55–58.

44. *See, e.g.*, Charney, *supra* note 41, at 944 (discussing the traditional model of law enforcement before the advent of new information technologies).

45. *See* Geer, *supra* note 40, at 14–15 (providing an overview of how computer security systems deal with risks posed by hackers).

46. *See, e.g.*, Cate, *supra* note 18, at 442–44 (describing how the FBI uses various databases for law enforcement).

47. For descriptions of the "No Fly" and "Selectee" watch lists, see Transportation Security Administration (TSA): Frequently Asked Questions, http://www.tsa.gov/research/privacy/faqs.shtm (last visited Oct. 14, 2008); *60 Minutes: Unlikely Terrorists on No Fly List* (CBS television broadcast Oct. 8, 2006), *available at* http://www.cbsnews.com/stories/2006/10/05/60minutes/main2066624.shtml; *see also* 49 U.S.C. § 114(h) (Supp. V 2006) (creating statutory authorization for creation of these passenger lists). These watch lists, in turn, are subsets of a much larger Terrorist Screening Database. *See* Federal Bureau of Investigation, Terrorist Screening Center: Frequently Asked Questions, http://www.fbi.gov/terrorinfo/counterrorism/faqs.htm (last visited Oct. 14, 2008).

The TSA has been working on a more elaborate system, the Secure Flight Screening Program, for some time. *See* Intelligence Reform and Terrorism Prevention Act of 2004 § 4012, 49 U.S.C. § 44903(j)(2)(A) (Supp. V 2006) (directing the Secretary of Transportation to "ensure that the Computer-Assisted Passenger Prescreening System, or any successor system—(i) is used to evaluate all passengers before they board an aircraft"). Its predecessor, the automated Computer-Assisted Passenger Prescreening System (CAPPS II), was suspended in August 2004 due to strong criticism, and was replaced by Secure Flight, whose implementation, in turn, has been delayed due to public criticism. *See, e.g.*, *Aviation Security: Significant Management Challenges May Adversely Affect Implementation of the Transportation Security Administration's Secure Flight Program: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 109th Cong. 8–11 (2006) (statement of Cathleen A. Berrick, Director, Homeland Security and Justice Issues), *available at*

nance in the National Surveillance State is increasingly statistically oriented, *ex ante* and preventative, rather than focused on deterrence and *ex post* prosecution of individual wrongdoing.[48] Such tendencies have been around for at least a century, but new technologies for surveillance, data analysis, and regulation by computer code and physical architecture have made them far easier to put into effect.

The National Surveillance State seeks any and all information that assists governance; electronic surveillance is not its only tool. Governments can also get information out of human bodies, for example, through collection and analysis of DNA, through locational tracking, and through facial recognition systems.[49] The Bush administration's detention and interrogation practices seek to get information out of human bodies through old-fashioned detention and interrogation techniques, including techniques that are tantamount to torture.[50] In the National

http://www.gao.gov/new.items/d06374t.pdf; Matthew L. Wald & John Schwartz, *Screening Plans Went Beyond Terrorism*, N.Y. TIMES, Sept. 14, 2004, at A35 (detailing how the Department of Homeland Security attempted to expand the CAPPS II program to serve broader police purposes); Electronic Privacy Information Center, Spotlight on Surveillance: Secure Flight Should Remain Grounded Until Security and Privacy Problems Are Resolved (2007), http://epic.org/privacy/surveillance/spotlight/0807/default.html.

48. As Nimrod Kozlovski explains:

> The new policing aims to prevent and preempt crime rather than to prosecute it. By predicting when, how, and by whom a crime will be committed, it aims to enable efficient intervention. Automated tools constantly monitor the environment to match users' risk profiles against dynamically identified patterns of criminal behavior. Patterns of previous computer crimes are coded as "crime signatures." These "signatures" . . . monitor for anomalies or deviations from "normal" behavior. The patterns of "normal" behavior are coded and an algorithm watches for a certain level of deviation from them. The systems aim to be able to disarm the attacker, redirect his actions to a "safe zone," block or modify his communication, or even strike back.

Nimrod Kozlovski, *Designing Accountable Online Policing*, *in* CYBERCRIME, *supra* note 33, at 110.

49. *See, e.g.*, Noah Shachtman, *The New Security: Cameras That Never Forget Your Face,* N.Y. TIMES, Jan. 25, 2006, at G6 (describing the use of facial recognition systems in New York City); Grant Gross, *Lockheed Wins 10-year FBI Biometric Contract*, WASH. POST, Feb. 13, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/02/13/AR2008021301655_pf.html (detailing the rise of biometric systems).

50. *See* Dana Priest, *Covert CIA Program Withstands New Furor*, WASH. POST, Dec. 30, 2005, at A1 (explaining the origins of interrogation program and "authorized techniques," such as waterboarding, hard slapping, isolation, sleep deprivation, liquid diets, and stress positions); Brian Ross & Richard Esposito, CIA's Harsh Interrogation Techniques Described, ABC NEWS (Nov. 18, 2005), http://abcnews.go.com/WNT/Investigation/story?id=1322866 (describing additional interrogation techniques—forced standing, hypothermia, and noise

Surveillance State, bodies are not simply objects of governance; they are rich sources of information that governments can mine through a multitude of different technologies and techniques.

Decades ago Michel Foucault argued that modern societies had become increasingly focused on watching and measuring people in order to control them, to normalize their behavior and to make them docile and obedient.[51] His famous example was Jeremy Bentham's idea of a Panopticon—a prison designed so that the prisoners could always be watched but would not know exactly when.[52] By making surveillance ubiquitous, governments and private organizations could discourage behavior they deemed unusual or abnormal.

Today's National Surveillance State goes beyond Foucault's Panoptic model. Government's most important technique of control is no longer watching or threatening to watch. It is analyzing and drawing connections between data. Much public and private surveillance occurs without any knowledge that one is watched. More to the point, data mining technologies allow the state and business enterprises to record perfectly innocent behavior that no one is particularly ashamed of and draw surprisingly powerful inferences about people's behavior, beliefs, and attitudes.[53] Over time, these tools will only become more effective. We leave traces of ourselves continually, including our location, our communications contacts, our consumption choices—even our DNA.

bombardment); Associated Press, White House Defends Use of Waterboarding, MSNBC (Feb. 6, 2008), http://www.msnbc.msn.com/id/23030663/ (revealing that President had ordered waterboarding in the past and might do so again); *see also* Dana Priest, *Officials Relieved Secret Is Shared*, WASH. POST, Sept. 7, 2006, at A17 [hereinafter Priest, *Officials Relieved*] (describing revelation of secret CIA black sites); Jan Crawford Greenburg et al., Sources: Top Bush Advisors Approved 'Enhanced Interrogation,' ABC NEWS (Apr. 9, 2008), http://abcnews.go.com/TheLaw/LawPolitics/story?id=4583256&page=1 (describing how senior Bush administration officials discussed and approved "enhanced interrogation techniques" to be used against high-value detainees).

51. *See generally* MICHEL FOUCAULT, DISCIPLINE AND PUNISH 195–217 (Alan Sheridan trans., Pantheon Books 1977) (describing the rise of the disciplinary society).

52. *See id.* at 200–02 (discussing Bentham's idea of a Panopticon).

53. *See* Kozlovski, *supra* note 48, at 114 ("Investigators increasingly focus on 'noncontent' data such as traffic data and automated system logs, enabling them to create maps of associations, and to visualize non-trivial connections among events."); Gorman, *supra* note 3 (explaining that NSA "now monitors . . . domestic emails and Internet searches as well as bank transfers, credit-card transactions, travel and telephone records" received from private companies or other agencies, which are analyzed for suspicious patterns).

Data mining allows inferences not only about the direct subjects of surveillance, but about *other people* with whom they live, work, and communicate.[54] Instead of spying on a particular person, data about other persons combined with public facts about a person can allow governments and private businesses to draw increasingly powerful inferences about that person's motives, desires, and behaviors.[55]

The problem today is not that fear of surveillance will lead people to docile conformity, but rather that even the most innocent and seemingly unimportant behaviors can increase knowledge about both ourselves and others.[56] Normal behavior does not merely acquiesce to the state's power; it may actually amplify it, adding information to databases that makes inferences more powerful and effective. Our behavior may tell things about us that we may not even know about ourselves. In addition, knowledge about some people can generate knowledge about others who are not being directly watched. Individuals can no longer protect themselves simply by preventing the government from watching them, for the government may no longer need to watch *them* to gain knowledge that can be used against them.

Equally important, the rise of the National Surveillance State portends the death of amnesia. In practice, much privacy protection depends on forgetting. When people display unusual or embarrassing behavior, or participate in political protests in public places, their most effective protection may be that most people don't know who they are and will soon forget who did what at a certain time and place. But cameras, facial recognition systems, and location tracking systems let governments

54. *See* Gorman, *supra* note 3 (discussing social network analysis and other data analysis techniques). *See generally* Dempsey & Flint, *supra* note 15, at 1464–66 (explaining pattern-based searching and link analysis).

55. *See* Eric Lichtblau, *F.B.I. Data Mining Reached Beyond Initial Targets,* N.Y. TIMES, Sept. 9, 2007, at A1 (describing the practice of "link analysis").

56. *See* Dempsey & Flint, *supra* note 15, at 1464 (explaining that the point of data mining is to search "based on the premise that the planning of terrorist activity creates a pattern or 'signature' that can be found in the ocean of transactional data created in the course of everyday life"); Ira S. Rubinstein et al., *Data Mining and Internet Profiling, Emerging Regulatory and Technological Approaches,* 75 U. CHI. L. REV. 261, 261 (2007) ("[T]o identify and preempt terrorist activity, intelligence agencies have begun collecting, retaining, and analyzing voluminous and largely banal transactional information about the daily activities of hundreds of millions of people."); Ellen Nakashima, *From Casinos to Counterterrorism,* WASH. POST, Oct. 22, 2007, at A1 (describing data mining and surveillance techniques of casinos).

and businesses compile continuous records of what happens at particular locations, which can be collated with records of different times and places. The collation and analysis of events allows public and private actors to create locational and temporal profiles of people, making it easier to trace and predict their behaviors.[57] Older surveillance cameras featured imprecise, grainy images, and the recordings were quickly taped over. New digital systems offer ever greater fidelity and precision,[58] and the declining cost of digital storage means that records of events can be maintained indefinitely and copied and distributed widely to other surveillance systems around the country or even around the globe.[59] Ordinary citizens can no longer assume that what they do will be forgotten; rather, records will be stored and collated with other information collected at other times and places.[60] The greatest single protector of privacy—amnesia—will soon be a thing of the past. As technology im-

57. *See* Nakashima, *supra* note 56 (describing how a casino investigator can assemble a mosaic of visitor's moves for the past two weeks; this technology is used to better target high rollers for special treatment and others for promotions).

58. *See* NEW YORK CIVIL LIBERTIES UNION, WHO'S WATCHING?: VIDEO CAMERA SURVEILLANCE IN NEW YORK CITY AND THE NEED FOR PUBLIC OVERSIGHT 7 (2006), http://www.nyclu.org/pdfs/surveillance_cams_report_121306.pdf (describing cameras today as having a "super-human" vision, including capabilities to tilt, pan, and rotate to better follow an individual, and capability to zoom to see the pages of a book or even a text message on a screen of a cell phone).

59. *See* Bellia, *supra* note 28, at 141 (describing trends toward an "architecture of perfect memory" where low cost of storing vast quantities of data and ease of conversion of nondigital information to digital form remove many of the incentives to destroy data, increasingly held by third parties); Robert O'Harrow Jr. & Ellen Nakashima, *National Dragnet Is a Click Away*, WASH. POST, Mar. 6, 2008, at A1 (reporting on the new N-DEx database intended to become a "one-stop shop" enabling federal law enforcement, counterterrorism and intelligence analysts to automatically examine the enormous caches of local and state records); Walter Pincus, *NSA Gave Other Agencies Info from Surveillance,* WASH. POST, Dec. 31, 2005, at A8 ("Information captured by the National Security Agency's secret eavesdropping . . . has been passed on to other government agencies, which cross-check the information with tips and information collected in other databases . . . .").

60. *See* Saul Hansell, *U.S. Wants Internet Companies to Keep Web-Surfing Records,* N.Y. TIMES, June 2, 2006, at A15 (reporting on Justice Department's request to Internet companies to retain records on the Web-surfing and email activities of their customers for up to two years); O'Harrow & Nakashima, *supra* note 59 (describing commercial data-mining system used by police investigators to "find hidden relationships among suspects and instantly map links among people, places, and events"); Pincus, *supra* note 59 (revealing that other agencies used "records obtained from NSA in combination with wide-ranging databases to look for links and associations").

proves and storage costs decline, the National Surveillance State becomes the State that Never Forgets.[61]

The National Surveillance State poses three major dangers for our freedom. Because the National Surveillance State emphasizes *ex ante* prevention rather than *ex post* apprehension and prosecution, the first danger is that government will create a parallel track of preventative law enforcement that routes around the traditional guarantees of the Bill of Rights. The Bush administration's military detention practices and its NSA surveillance program are two examples. The administration justified detaining and interrogating people—including American citizens—in ways that would have violated traditional legal restraints on the grounds that it was not engaged in ordinary criminal law enforcement.[62] It sought intelligence that would prevent future attacks and wanted to prevent terrorists from returning to the battlefield.[63] Similarly, the administration defended warrantless surveillance of people in the United States by arguing that the President was not engaged in criminal prosecutions but in collection of military intelligence designed to fight terrorism.[64]

61. *See* Bellia, *supra* note 28, at 137–38, 148–49 (noting that our surveillance and information privacy laws say little about data retention and that much of what they say provides incentives for indefinite retention).

62. *See* Military Order No. 222, Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism, 66 Fed. Reg. 57,833 (Nov. 13, 2001) (ordering the detention of persons whom the President has reason to believe (1) are current or former members of al-Qaeda, (2) have engaged in, aided, abetted, or conspired to commit terrorist acts or are preparing to do so, or (3) have harbored such a person, and delegating the authority over trials of these individuals to military commissions under the purview of the Secretary of Defense); Brief for the Respondents at 16, Yaser Esam Hamdi v. Rumsfeld, 542 U.S. 507 (2004) (No. 03-6696) (justifying the detention of Hamdi, a United States citizen, as the capture of "a classic battlefield detainee").

63. *See* Priest, *Officials Relieved*, *supra* note 50 (reporting the CIA's assertion that it needed "to harshly interrogate prisoners to extract time-sensitive information about possible terrorists attacks"); David Stout, *Rumsfeld Defends Plan to Hold War Detainees*, N.Y. TIMES, Mar. 28, 2002, at A18 (reporting a statement of Defense Secretary Donald H. Rumsfeld that preventing Afghan war prisoners from returning to the battlefield was justification for a plan to hold some prisoners even if they were acquitted in military tribunals); Press Release, President George W. Bush, President Discusses Creation of Military Commissions to Try Suspected Terrorists (Sept. 6, 2006) (defending detention and interrogation practices necessary to gain intelligence to stop terrorist attacks and arguing that "we have an obligation to the American people, to detain these enemies and stop them from rejoining the battle").

64. *See* Letter from William E. Moschella, Assistant Attorney Gen., Dep't of Justice, to the Senate Select Comm. on Intelligence and House Permanent Select Comm. on Intelligence (Dec. 22, 2005), *reprinted in* 81 IND. L.J. 1360,

The second danger posed by the National Surveillance State is that traditional law enforcement and social services will increasingly resemble the parallel track. Once governments have access to powerful surveillance and data mining technologies, there will be enormous political pressure to use them in everyday law enforcement and for delivery of government services. If data mining can help us locate terrorists, why not use it to find deadbeat dads, or even people who have not paid their parking tickets?[65] If surveillance technologies signal that certain people are likely threats to public order, why not create a system of preventive detention outside the ordinary criminal justice system?[66] Why not impose sanctions outside the criminal law, like denying people the right to board airplanes or use public facilities and transportation systems? And if DNA analysis can identify people who will likely impose high costs on public resources, why not identify them in advance and exclude them from public programs and other opportunities? The more powerful and effective our technologies of surveillance and analysis become, the more pressure the government will feel to route around warrant requirements and other procedural hurdles so that it can catch potential troublemakers more effectively and efficiently before they have a chance to cause any harm.

Private power and public-private cooperation pose a third danger. Because the Constitution does not reach private parties, government has increasing incentives to rely on private

1363 (2006) (characterizing communication intercepts by NSA as falling into a category of "special needs" outside the ordinary criminal process); U.S. Dep't of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President (Jan. 19, 2006), *reprinted in* 81 IND. L.J. 1374, 1410–12 (2006) [hereinafter Legal Authorities] ("[C]ollecting foreign intelligence is far removed from the ordinary criminal law enforcement action to which the warrant requirement is particularly suited.").

65. For discussions of "mission creep" in the use of data mining and surveillance technologies, see MARY DEROSA, CTR. FOR STRATEGIC AND INT'L STUDIES, DATA MINING AND DATA ANALYSIS FOR COUNTERTERRORISM 16 (2004), http://www.cdt.org/security/usapatriot/20040300csis.pdf; TECHNOLOGY & PRIVACY ADVISORY COMM., SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM 39–40 (2004), *available at* http://www.cdt.org/security/usapatriot/20040300tapac.pdf.

66. *See* Jack L. Goldsmith & Neal Katyal, Op-Ed., *The Terrorists' Court,* N.Y. TIMES, July 11, 2007, at A19 (proposing "a comprehensive system of preventive detention" overseen by a national security court, which could use evidence "too difficult to present in open civilian court without compromising intelligence sources and methods").

enterprise to collect and generate information for it.[67] Corporate business models, in turn, lead companies to amass and analyze more and more information about people in order to target new customers and reject undesirable ones. As computing power increases and storage costs decline, companies will seek to know more and more about their customers and sell this valuable information to other companies and to the government.

If some form of the National Surveillance State is inevitable, how do we continue to protect individual rights and constitutional government? Today's challenge is similar to that faced during the first half of the twentieth century, when government transitioned into the Welfare State and the National Security State. Americans had to figure out how to tame these new forms of governance within constitutional boundaries. It is no accident that this period spawned both the New Deal—with its vast increase in government power—and the Civil Rights Revolution. The more power the state amasses, the more Americans need constitutional guarantees to keep governments honest and devoted to the public good.

We might begin by distinguishing between an authoritarian information state and a democratic information state.[68] Authoritarian information states are information gluttons and information misers. Like gluttons they grab as much information as possible because this helps maximize their power. Authoritarian states are information misers because they try to keep the information they collect—and their own operations—secret from the public. They try to treat everything that might

67. *See* Birnhack & Elkin-Koren, *supra* note 33, para. 41, 43 (explaining that online service providers are being recruited to serve governmental purposes because "they are not tied, nor restricted, to any national border" and because they are also "more flexible in watching online activities since they are not subject to the same scrutiny which applies to the State and its agents"); *see also* Laura K. Donohue, *Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1142 (2006) (listing the wide range of personal data traded by the private sector, access to which is also purchased by government agencies); Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 320 (2008) ("[M]any [government] programs rely in whole or in part on private companies, called commercial data brokers, to provide their input, which is then analyzed by government officials.").

68. *Cf.* ALAN F. WESTIN, PRIVACY AND FREEDOM 23–26 (1967) (distinguishing between authoritarian and democratic models of privacy); Lewis Mumford, *Authoritarian and Democratic Technics*, 5 TECH. & CULTURE 1, 1–8 (1964) (noting a long historical dialectic between "authoritarian" and "democratic" modes of technological development).

embarrass them or undermine their authority as state secrets, and they multiply secret rules and regulations, which lets them claim to obey the law without having to account for what they do. In this way they avoid accountability for violating people's rights and for their own policy failures. Thus, information gluttony and information miserliness are two sides of the same coin: both secure governments' power by using information to control their populations, to prevent inquiry into their own operations, to limit avenues of political accountability, and to facilitate self-serving propaganda.[69]

By contrast, democratic information states are information gourmets and information philanthropists. Like gourmets they collect and collate only the information they need to ensure efficient government and national security. They do not keep tabs on citizens without justifiable reasons; they create a regular system of checks and procedures to avoid abuse. They stop collecting information when it is no longer needed and they discard information at regular intervals to protect privacy. When it is impossible or impractical to destroy information—for example, because it is stored redundantly in many different locations—democratic information states strictly regulate its subsequent use. If the information state is unable to forget, it is imperative that it be able to forgive.

Democratic information states are also information philanthropists because they willingly distribute much valuable information they create to the public, in the form of education, scientific research, and agricultural and medical information. They allow the public access to information about their laws and their decision-making processes so that the public can hold government officials accountable if they act illegally or arbitrarily or are corrupt or inefficient. They avoid secret laws and secret proceedings except where absolutely necessary. Democratic states recognize that access and disclosure help prevent governments from manipulating their citizens. They protect individual privacy because surveillance encourages abuses of power and inhibits freedom and democratic participation. Thus being an information gourmet and an information philanthropist are also connected: both help keep governments open and responsible to citizens; both further individual autonomy and democracy by respecting privacy and promoting access to knowledge.

69. *See* WESTIN, *supra* note 68, at 23 ("The modern totalitarian state relies on secrecy for the regime, but high surveillance and disclosure for other groups.").

You might think the Fourth Amendment[70] would be the most important constitutional provision for controlling and preventing abuses of power in the National Surveillance State. But courts have largely debilitated the Fourth Amendment to meet the demands of the Regulatory and Welfare States, the National Security State, and the War on Drugs.[71] Much government collection and use of personal data now falls outside the Fourth Amendment's protection—at least as the courts currently construe it. The Supreme Court has held that there is no expectation of privacy in business records and information that people give to third parties like banks and other businesses;[72] in the digital age this accounts for a vast amount of personal information. Most e-mail messages are copied onto privately held servers, making their protection limited if not nonexistent.[73] Courts have also held that the Fourth Amendment poses few limits on foreign intelligence surveillance, which is largely regulated by FISA;[74] as a result, the executive branch

70. U.S. CONST. amend. IV.

71. *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 202 (2004) (noting that the Supreme Court has limited Fourth Amendment protections when faced with new practices and new technologies); Paul Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 HASTINGS L.J. 1321, 1323 (1992) (arguing that the United States has failed to develop an appropriate law of data protection for the activist state); *cf.* William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 442, 444–46 (1995) (noting how strong privacy protections require strong limits on government and arguing that the rise of a powerful administrative state inevitably limited Fourth and Fifth Amendment protections).

72. *See* Smith v. Maryland, 442 U.S. 735, 742–43 (1979) (holding that records of telephone numbers dialed are not subject to constitutional protection); United States v. Miller, 425 U.S. 435, 446 (1976) (holding that there is no expectation of privacy in bank records held by a third party).

73. *See, e.g.*, Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 460–64 (5th Cir. 1994) (holding that stored e-mails not intercepted contemporaneously with transmission are not protected under federal privacy laws).

74. *See* Foreign Intelligence Surveillance Act, 50 U.S.C.A. §§ 1801–1811 (West 2002 & Supp. 2007), *as amended by* FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (2008); *see also* United States v. Truong Dinh Hung, 629 F.2d 908, 913–15 & n.4 (4th Cir. 1980) (discussing the "foreign intelligence exception" to the Fourth Amendment); United States v. Butenko, 494 F.2d 593, 604–05 (3d Cir. 1974) (en banc) (upholding presidential power to engage in warrantless surveillance to gather foreign intelligence information); United States v. Brown, 484 F.2d 418, 425–27 (5th Cir. 1973) (noting that the President may authorize wiretaps for the purpose of foreign surveillance); *In re* Sealed Case, 310 F.3d 717, 737–46 (FISA Ct. Rev. 2002) (holding that a FISA provision permitting government to conduct surveillance of agent of foreign power, if foreign intelligence is a "significant purpose" of

has increasingly justified domestic surveillance by asserting that it is a permissible byproduct of foreign intelligence gathering.[75]

Currently, governments are free to place cameras in public places like streets and parks because there is no expectation of privacy there.[76] Governments can also collect information that people leave out in the open, like their presence on a public street; or abandon, like fingerprints, hair, or skin cells.[77] Moreover, because the Fourth Amendment focuses on searches and seizures, it places few limits on collation and analysis, including data mining.[78] The Fourth Amendment does not require governments to discard any information they have already lawfully collected. Digital files, once assembled, can be copied and augmented with new information indefinitely for later analysis and pattern matching. Finally, whatever constitutional limits might restrain government do not apply to private parties, who can freely collect, collate, and sell personal information back to the government free of Fourth Amendment restrictions, effectively allowing an end-run around the Constitution.

We should try to change some of the weaknesses in current Fourth Amendment doctrine. But legislative, administrative,

such surveillance, did not violate Fourth Amendment). *But cf.* Zweibon v. Mitchell, 516 F.2d 594, 600 (D.C. Cir. 1975) (en banc) (noting the importance of judicial scrutiny to safeguard against illegal domestic surveillance of persons not associated with foreign countries).

75. Legal Authorities, *supra* note 64, at 1409–14.

76. *See* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 236 n.106 (2002) (listing cases holding that video surveillance by public cameras is not a search because there is no reasonable expectation of privacy).

77. *See* California v. Greenwood, 486 U.S. 35, 40–41 (1988) (finding no expectation of privacy in trash in garbage bags left on the street); United States v. Dionisio, 410 U.S. 1, 15 (1973) (collecting fingerprints not found to be a search); Abel v. United States, 362 U.S. 217, 241 (1960) (holding that items left in hotel room wastepaper basket were abandoned goods and government collection did not violate the Fourth Amendment). The precise question of how to deal with "abandoned DNA" is still open to debate. *Compare* Edward J. Imwinkelried & D.H. Kaye, *DNA Typing: Emerging or Neglected Issues*, 76 WASH. L. REV. 413, 440 (2001) ("[T]he better course is to treat human cells left in public places like fingerprints . . . ."), *with* Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857, 882–83 (2006) (conceding that there is probably no current Fourth Amendment protection but arguing for legislation regulating covert collection of DNA).

78. *See* SOLOVE, *supra* note 71, at 201; Slobogin, *supra* note 67, at 330–31.

and technological solutions may be far more important means of guaranteeing constitutional freedoms in the National Surveillance State. These laws and technologies will probably do far more to enforce the constitutional values underlying the Fourth Amendment and the Due Process Clause.

Congress must pass new superstatutes to regulate the collection, collation, purchase, and analysis of data. These new superstatutes would have three basic features. First, they would restrict the kinds of data governments may collect, collate, and use against people. They would strengthen the very limited protections of e-mail and digital business records, and rein in how the government purchases and uses data collected by private parties. They would institutionalize government "amnesia" by requiring that some kinds of data be regularly destroyed after a certain amount of time unless there were good reasons for retaining the data. Second, the new superstatutes would create a code of proper conduct for private companies that collect, analyze, and sell personal information. Third, the new superstatutes would create a series of oversight mechanisms for executive bureaucracies that collect, purchase, process, and use information.

Oversight of executive branch officials may be the single most important goal in securing freedom in the National Surveillance State. Without appropriate checks and oversight mechanisms, executive officials will too easily slide into the bad tendencies that characterize authoritarian information states. They will increase secrecy, avoid accountability, cover up mistakes, and confuse their interest with the public interest.

Recent events in the Bush administration suggest that legislative oversight increasingly plays only a limited role in checking the executive. Meaningful oversight is most likely to occur only when there is divided government. Even then the executive will resist sharing any information about its internal processes or about the legal justifications for its decisions. A vast number of different programs affect personal privacy and it is unrealistic to expect that Congress can supervise them all. National security often demands that only a small number of legislators know about particularly sensitive programs and how they operate, which makes it easy for the administration to co-opt them.[79] The Bush administration's history demonstrates

79. As Marty Lederman points out, the post-Watergate oversight system was designed to make Congress as well as the courts "effective check[s] against unfettered executive power." Marty Lederman, *Is There Any Way to*

the many ways that Presidents can feign consultation with Congress without really doing so.[80]

Judicial oversight need not require a traditional system of warrants. It could be a system of prior disclosure and explanation and subsequent regular reporting and minimization. This is especially important as surveillance practices shift from operations targeted at individual suspected persons to surveil-

Fix Legislative Oversight of Intelligence Operations?, BALKINIZATION, Mar. 31, 2008, http://balkin.blogspot.com/2008/03/is-there-any-way-to-fix-legislative.html. However, as our current system has developed, Congress has found few ways of detecting and responding to executive misbehavior. The administration offers information only to a very small and select number of legislators. *See* CHARLIE SAVAGE, TAKEOVER: THE RETURN OF THE IMPERIAL PRESIDENCY AND THE SUBVERSION OF AMERICAN DEMOCRACY 242 (2007). Its messengers are professional intelligence and uniformed military officers with whom legislators have already developed trusted relationships that they do not wish to undermine. Briefings are highly classified and often occur after questionable conduct has already begun, so that legislators are put in the difficult position of demanding a halt to existing programs that the administration claims are crucial for national security. *See* JACK GOLDSMITH, THE TERROR PRESIDENCY: LAW AND JUDGMENT INSIDE THE BUSH ADMINISTRATION 206 (2007). The administration assures legislators that any legal questions have already been thoroughly vetted by administration lawyers (for example, in the Office of Legal Counsel) without explaining the basis of the legal analysis in detail, offering competing arguments on the other side, or revealing the existence of dissenting views within the Executive branch. In addition, the administration tells legislators that they may not disclose what they learn about these programs to anyone, including their own staffs—much less any outside experts who might actually help them assess the legality and wisdom of the administration's conduct. That is because any discussions of the legality of administration practices would disclose classified information that might be useful to the enemy or otherwise compromise national security. As a result, legislators generally don't know what the problems are, and even if they suspect that they exist, there is very little they can do about them. *See* Marty Lederman, *The Government Institution Most in Need of Comprehensive Reform*, BALKINIZATION, Dec. 9, 2007 http://balkin.blogspot.com/2007/12/government-institution-most-in-need-of.html.

80. *See* Heidi Kitrosser, *Congressional Oversight of National Security Activities: Improving Information Funnels*, 29 CARDOZO L. REV. 1049, 1060 (2008) (noting that recent controversies in the Bush administration show that "administrations do not necessarily comply with statutory directives to share information, and individual congresspersons may acquiesce in, even facilitate, such non-compliance."). For recent reform proposals, see NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 419–23 (2004) (arguing for reform of congressional oversight); Anne Joseph O'Connell, *The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World*, 94 CAL. L. REV. 1655, 1730–35 (2006) (arguing for increased legislative oversight); Jack Goldsmith, *The Laws in Wartime*, SLATE, Apr. 2, 2008, http://www.slate.com/id/2187870/pagenum/2/ (presenting a list of proposals for continuing aggressive counterterrorism policies while increasing legislative oversight).

lance programs that do not begin with identified individuals and focus on matching and discovering patterns based on the analysis of large amounts of data and contact information.[81] We need a set of procedures that translate the values of the Fourth Amendment (with its warrant requirement) and the Fifth Amendment's Due Process Clause[82] into a new technological context. Currently, however, we exclude more and more executive action from judicial review on the twin grounds of secrecy and efficiency. The Bush administration's secret NSA program is one example; the explosion in the use of administrative warrants that require no judicial oversight is another.[83] Yet an independent judiciary plays an important role in making sure that zealous officials do not overreach. If the executive seeks greater efficiency, this requires a corresponding duty of greater disclosure before the fact and reporting after the fact to determine whether its surveillance programs are targeting the right people or are being abused. Judges must also counter the executive's increasing use of secrecy and the state secrets privilege to avoid accountability for its actions. Executive officials have institutional incentives to label their operations as secret and beyond the reach of judicial scrutiny. Unless legislatures

81. *See* Orin S. Kerr, *Updating the Foreign Intelligence Surveillance Act*, 75 U. CHI. L. REV. 225, 234 (2008) (noting that "today's surveillance tends to be divorced from the identity and location of the parties to the communication" due to changes in communications technology).

82. U.S. CONST. amend. V.

83. *See* DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006 158 (2008), *available at* http://www.usdoj.gov/oig/special/s0803b/final.pdf (finding expansion of use of national security letters against U.S. persons in a three-year period and detailing abuses of the power to obtain records without a warrant); DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FBI'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS IN 2006 85 (2008), *available at* http://www.usdoj.gov/oig/special/s0803a/final.pdf (discussing instances in which the FBI received additional information that it was not authorized to receive by FISA court order); DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS 31–35 (2007), *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf (describing underreporting of number of NSL requests issued and number of legal violations); Electronic Privacy Information Center, National Security Letters (2008), http://epic.org/privacy/nsl/default.html; Barton Gellman, *The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans*, WASH. POST, Nov. 6, 2005, at A1 (describing "an exponentially growing practice of domestic surveillance under the USA Patriot Act"); R. Jeffrey Smith, *FBI Violations May Number 3,000, Official Says*, WASH. POST, Mar. 21, 2007, at A7 (noting as many as 600 "cases of serious misconduct" involving national security letters between 2003 and 2006).

and courts can devise effective procedures for inspecting and evaluating secret programs, the Presidency will become a law unto itself.

Given the limits of legislative and judicial oversight, oversight within the executive branch will prove especially crucial. Congress can design institutional structures that require the executive to police itself and make regular reports about its conduct. For example, if Congress wants to bolster legal protections against warrantless surveillance, it might create a cadre of informational ombudsmen within the executive branch—with the highest security clearances—whose job is to ensure that the government deploys information collection techniques legally and nonarbitrarily.[84] Unfortunately, the Bush administration has made extreme claims of inherent presidential power that it says allow it to disregard oversight and reporting mechanisms.[85] Rejecting those claims about presidential power will be crucial to securing the rule of law in the National Surveillance State.

Finally, technological oversight will probably be an indispensable supplement to legal procedures. The best way to control the watchers is to watch them as well. We should construct surveillance architectures so that government surveillance is regularly recorded and available for audit by ombudsmen and executive branch inspectors.[86] Records of surveillance can, in

84. *See, e.g.*, Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy Decisionmaking in Administrative Agencies*, 75 U. CHI. L. REV. 75, 96 (2008) (noting importance of independent "embedded privacy experts" in Department of Homeland Security "specifically charged with advancing privacy among competing agency interests, located in a central position within the agency decisionmaking structure, drawing on internal relationships and external sources of power, and able to operate with relative independence"); *cf.* Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L.J. 2314, 2314–19 (2006) (arguing for mechanisms to create checks and balances within the executive branch in the foreign affairs area); Neal Kumar Katyal, *Toward Internal Separation of Powers*, 116 YALE L.J. 106 (Pocket Part 2006) (same).

85. *See* GOLDSMITH, *supra* note 79, at 123–26, 202–10; SAVAGE, *supra* note 79, at 132–34; Dawn E. Johnsen, *What's a President to Do? Interpreting the Constitution in the Wake of Bush Administration Abuses*, 88 B.U. L. REV. 395, 400–01 (2008) (discussing the Bush administration's decision not to comply with some federal statutes based on a theory of broad executive authority); Marty Lederman, *The Theory of a Preclusive Commander-in-Chief Power is Alive and Well*, BALKINIZATION, Jan. 30, 2008, http://balkin.blogspot.com/2008/01/theory-of-preclusive-commander-in-chief.html.

86. *See, e.g.*, DEROSA, *supra* note 65, at 19 (discussing audit technology as a method of protecting privacy and preventing abuse); TECHNOLOGY & PRIVACY ADVISORY COMM., *supra* note 65, at 50–52 (recommending audit systems

turn, be subjected to data analysis and pattern matching to discover any unusual behavior that suggests abuse of procedures. These technological audits can automate part of the process of oversight; they can assist ombudsmen, executive officials, Congress, and the courts in ensuring that surveillance practices stay within legal bounds. We can prevent some kinds of abuse by technological design; at the very least, technology can force disclosure of information that executive officials would otherwise keep hidden.

The Administrative and Welfare States raised problems not only for the Constitution, but also for the rule of law itself. The same is true for the National Surveillance State. Changing methods of governance demand new strategies to preserve constitutional values and democratic self-government. We mastered at least some of the problems caused by the rise of the Administrative and Welfare States; we must hope that we can do so the same for the National Surveillance State, which is already here.

for data mining programs); Kozlovski, *supra* note 48, at 126–28 (arguing for technological systems of accountable policing, including logging of information collected, who has access to it and what searches have been performed); Rubinstein et al., *supra* note 56, at 269 ("[A]n audit system is needed to provide a complete and tamper-proof record of the searches that have been conducted and the identity of the analysts involved.").