**ALEX KOZINSKI***
**STEPHANIE GRACE**†

# The (Continued) Assault on Privacy: A Timely Book Review Forty Years in the Making

For many of us, the name "Arthur Miller" instantly brings us back to the long law school nights spent cuddling up with our favorite civil procedure textbook. For others, it conjures up images of Miller's media persona, from *Miller's Court* to Court TV to *Good Morning America*. And, for the unfortunate few, mere mention of the name triggers anew the terror struck into their hearts the moment they spotted the venerable practitioner at opposing counsel's table or on the signatory line of a response brief. Throughout the years, Miller has been a prolific and engaged teacher, academic, celebrity and advocate, making invaluable contributions to legal discourse and the practice of law. And today, as many of Miller's colleagues and admirers comment on his enviable body of work, we have selected but one to celebrate the occasion—a work that has not only endured the test of time, but embraced it.

The year was 1971. Nixon was president, *Patton* won the Academy Award, and gas was 36 cents a gallon. And, while many of us were squandering our time making celebrity appearances on *The Dating Game* or waiting to be born, the one and only Arthur Miller was carefully crafting scholarship considering the grave implications the computer would have on modern conceptions of personal privacy.

* Chief Judge of the United States Court of Appeals for the Ninth Circuit.

† His former law clerk, now a litigation associate in the San Diego office of Latham and Watkins LLP.

And so *The Assault on Privacy: Computers, Data Banks, and Dossiers*[1] was born.

Why this book? Because in a world of Twitter and Facebook where few things—save canned peas and British royalty—have a shelf life beyond the nanosecond of their conception, *The Assault on Privacy* has proved to be a seminal masterpiece in privacy for the twentieth century and beyond. Penned at the dawn of the computer age, the book ably grapples with the dangers presented by the accumulation and centralization of personal information in official and private databases.[2] The efforts of these "data-maniacs"—those individuals who can't "perceiv[e] anything but the intrinsic value of data" and will stop at nothing to amass it—Miller forewarned, pose a dire threat to the "informational privacy" of the person whose information is sought to be extracted, dissected, stored, disseminated or otherwise used.[3]

Chapter by chapter, the book lucidly details the direct threats to privacy in the early digital age, from the "murky business" of the credit bureaus collecting and selling information about millions of Americans;[4] to the aggressive and relentless efforts of administrative agencies to "extract more and more facts about the American citizenry"[5] by way of diagnostics, questionnaires and surveys; to the federal government's push for a crime-fighting "National Data Center."[6]

Importantly, the threat Miller so clearly articulates isn't merely that information will be wrongfully disseminated or otherwise misused—though that risk is thoughtfully addressed as well—but the more immediate danger to the "individual's ability to control the circulation of information relating to him," which is threatened by the testing, surveying, storing and centralizing itself.[7] As Miller eloquently explains, "when an individual is deprived of control over the spigot that governs the flow of information pertaining to him, in some measure he becomes subservient to those people and institutions that

---

[1] ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS (1971).

[2] *See id.*

[3] *Id.* at 22–23.

[4] *Id.* at 69.

[5] *Id.* at 128 (quoting 115 CONG. REC. H859 (daily ed. Feb. 6, 1969) (statement of Rep. Betts)).

[6] *Id.* at 54–67.

[7] *Id.* at 25.

are able to manipulate it."[8] And while the danger of hackers and fraudsters hovers continuously on the horizon, it is this "intrinsically valuable aspect[] of individual privacy"[9] that remains most fragile as we have moved seamlessly from machine-readable punch cards to computing in a cloud.

Nowadays, of course, we're all so inured to the idea of being surveyed, observed, scrutinized, poked and prodded that one might wonder how such antiquated notions of "privacy" are possibly applicable to our goldfish-bowl society. Indeed, Miller himself anticipated "that the growing omnipresence of the computer may have a numbing effect on the . . . values subsumed under the heading 'personal privacy.'"[10] And his prediction was surely borne out: In a world where people proudly blog about their sexual exploits[11] and plastic surgeries,[12] it's hard to imagine being seriously offended by such benign inquiries as a census question asking whether you have a clothes dryer in your home.[13] But our desensitization has only gone so far, and, at least as to those narrow categories of our own lives we still hold private, we must heed Miller's warning and remain most vigilant against the government's veracious appetite for information—lest the data-maniacs run wild over the few civil liberties we have left.

Our National DNA Database is a case in point. The tale begins in 2000, when Congress first required federal law enforcement officers to extract DNA samples from those convicted of serious federal crimes—murder, rape, etc.—for preservation in a revolutionary new database called the Combined DNA Index System or CODIS.[14] States could also deposit offender DNA into the data bank to be compared and exchanged with samples collected from all over the nation. Almost immediately, the database proved useful in solving cold crimes and new cases alike, and Congress never looked back.

---

[8] *Id.*

[9] *Id.* at 23.

[10] *Id.* at 53.

[11] *See* Jeffrey Rosen, *Your Blog or Mine?*, N.Y. TIMES MAG. (Dec. 19, 2004), http://www.nytimes.com/2004/12/19/magazine/19PHENOM.html.

[12] *See, e.g.*, *Meet the Girls: Popular Ladies Blogs*, MYFREEIMPLANTS.COM, http://MyFreeImplants.com/meet-the-girls/ladies-blogs (last visited Mar. 7, 2012).

[13] *See* MILLER, *supra* note 1, at 127.

[14] *See* DNA Analysis Backlog Elimination Act of 2000, 42 U.S.C. § 14135a(a) (2000). *See generally* United States v. Kincade, 379 F.3d 813, 845–46 (9th Cir. 2004) (en banc) (Reinhardt, J., dissenting).

Succumbing to, as Miller calls it, "the hypnotic attraction for electronic record-keeping,"[15] Congress soon amended the law to collect and preserve DNA from anyone convicted of *any* felony,[16] and, just two years after that, again expanded the Act to cover arrestees and immigration detainees.[17] States eagerly followed suit, rapidly expanding the reach of their DNA swabs to arrestees, misdemeanants, even juveniles.[18] Today, just twelve short years after its initial conception, CODIS holds the DNA of over ten million individuals, including over 139,000 from Oregon alone.[19] If the government's insatiable demand for DNA continues, we will all find ourselves in the DNA database sooner or later.

Indeed, the government may not even need the DNA of each and every one of us, since familial matching means DNA can identify not only the suspect, but the relatives of the suspect as well.[20] Nor is the use of the DNA database necessarily limited to identification purposes. Given that we leave a trail of genetic bread crumbs everywhere we go, DNA can be collected to reconstruct where we've been and who we were with. Moreover, the DNA sample itself has the potential to reveal massive amounts of personal information including our sex, race, genetic defects, behavioral propensities, predisposition to disease and perhaps even sexual orientation.[21]

Though the privacy implications may be too obvious to overlook today, Miller foresaw the seductive danger of a centralized, universal

---

15 MILLER, *supra* note 1, at 4.

16 *See* 42 U.S.C. § 14135a(d) (2004).

17 *See* Bail Reform Act, 18 U.S.C. § 3142(b) (2006).

18 *See* Ju-Hyun Yoo, Note, *The Science of Identifying People by Their DNA, A Powerful Tool for Solving Crimes, Including Cold Cases from the Civil Rights Era*, 22 SYRACUSE SCI. & TECH. L. REP. 53, 60 (2010) (noting that, as of 2009, "twenty-eight states collect DNA from juvenile offenders, nine collect DNA from those convicted of certain misdemeanors, and fifteen from arrestees").

19 *See CODIS–NDIS Statistics*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/lab/codis/ndis-statistics#Army (last visited Mar. 7, 2012).

20 *See* Kelly Lowenberg, *Applying the Fourth Amendment When DNA Collected for One Purpose Is Tested for Another*, 79 U. CIN. L. REV. 1289, 1317 (2011).

21 *See* United States v. Kincade, 379 F.3d 813, 850 (9th Cir. 2004) (en banc) (Reinhardt, J., dissenting). Judge Gould made this connection as well: "In our age in which databases can be 'mined' in a millisecond using super-fast computers, in which extensive information can, or potentially could, be gleaned from DNA (even the 'junk' DNA currently used), and in which this data can easily be stored and shared by governments and private parties worldwide, the threat of a loss of privacy is real, even if we cannot yet discern the full scope of the problem. A related concern was voiced more than two decades ago, long before the advent of DNA profiling. *See generally* Arthur R. Miller, *The Assault on Privacy* 24–54 (1971)." *Id.* at 842 (Gould, J., concurring).

data bank four decades sooner. The issue of the day was universal fingerprinting, but the fundamental threat remains the same:

> It is axiomatic that the power the government can acquire through widespread surveillance or information control might be used to constrict individual freedom and that pressures in that direction must be resisted. Arguments or supplications couched in terms of governmental economy or administrative efficiency cannot justify every bureaucratic demand for greater power to extract, manipulate, store, and disseminate personal data . . . . Unless we maintain our vigilance against today's pressures, we may find ourselves confronted by something akin to the Chinese Communist Party's program to register and monitor every household in China.[22]

Thus, although universal fingerprinting may have gone out of style along with purple velour trousers and disco music, the need to zealously guard against the threats posed by advancing technology—and those who aren't afraid to use it—has not.

This is not to deny that there are benefits to the digitization of even very private information. As Miller repeatedly acknowledges, "the new information technology has enormous long-range beneficial consequences for society"[23]—benefits that we have earned and are entitled to enjoy. Thus, the question becomes not how to limit or eradicate this intrusive technology, but how to "strike a balance between the rights of the individual and the need for societal efficiency."[24] Under this framework, the only real danger lies in the temptation to embrace new technology with such vigor that privacy considerations are relegated to footnote status or eliminated altogether.

Today's pedal-to-the-metal push for the adoption of electronic medical records illustrates precisely this concern. Most of us still consider our medical records private. It's really nobody's business, after all, that you've been diagnosed with erectile dysfunction or suffer from hemorrhoids. Yet Miller recognizes the upside of storing such records in a central, electronic location: "[I]f a person falls ill while away from home, a local doctor could use the patient's birth number to retrieve his medical history and drug reactions from a central medical data bank."[25] And four decades later, it was with

---

[22] MILLER, *supra* note 1, at 205.

[23] *Id.* at 7–8.

[24] *Id.* at 239.

[25] *Id.* at 4.

these very goals in mind that Congress enacted legislation requiring all medical records to be digitized by 2014.[26]

But admirable as these goals may be, not enough attention has been paid to the confidentiality and security of such personal information. Indeed, the very features that make the policy useful—the centralization and immediate accessibility of the data bank—also increase by orders of magnitude the number of people who can gain access to the confidential information. Accordingly, the danger of computer-savvy hackers, conventional thieves and good-old-fashioned nosy neighbors gaining illicit access to our records takes on urgent significance in the digital age.

Experience with electronic medical records at the state and local levels confirms the legitimacy of these fears. In 2009 a hacker demanded $10 million ransom from Virginia after breaking into its state-run drug abuse database and stealing 8.3 million patient records.[27] And in 2010 a Bronx thief stole 1.7 million electronic health files from an unlocked record management company's van.[28] The numbers speak for themselves: The federal government's "Wall of Shame"—a Department of Health and Human Services compilation of security breaches affecting more than 500 patients—lists over *300* hospitals, insurance companies and health care professionals reporting such privacy breaches in the past two years alone.[29]

There are the curious to worry about as well. As Miller recognized, "many of us are congenital gossipers[ who] show a prurient interest in the details and misfortunes in the lives of others."[30] But the curious cat in all of us has had serious

---

[26] *See* 42 U.S.C. § 1395w-4(a)(7)(A)(i)–(ii) (2006 & Supp. 2011); *see also Obama Pledges Electronic Medical Records for Everyone Within Five Years*, DIABETES HEALTH (Jan. 20, 2009), http://www.diabeteshealth.com/read/2009/01/19/6053/obama-pledges-electronic-medical-records-for-everyone-within-five-years.

[27] Brian Krebs, *Hackers Break into Virginia Health Professions Database, Demand Ransom*, WASH. POST (May 4, 2009), http://voices.washingtonpost.com/securityfix/2009/05/hackers_break_into_virginia_he.html.

[28] *See* N.Y.C. Health and Hosps. Corp., *Press Release: HHC Reports Theft of Personal Health Information*, NYC.GOV (Feb. 11, 2011), http://www.nyc.gov/html/hhc/html/pressroom/pr-20110211-data-theft.shtml.

[29] U.S. Dep't of Health and Human Servs., *Breaches Affecting 500 or More Individuals*, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html (last visited Mar. 7, 2012); *see also* Milt Fruedenheim, *Breaches Lead to Push to Protect Medical Data*, N.Y. TIMES (May 30, 2011), http://www.nytimes.com/2011/05/31/business/31privacy.html?_r=1&ref=business&pagewanted=all.

[30] MILLER, *supra* note 1, at 47.

repercussions for medical privacy: In 2008, UCLA fired over a dozen employees for unauthorized snooping into Britney Spears's medical records after she was admitted for psychiatric problems, even though the hospital sent an email the morning she arrived reminding employees that they weren't permitted to peruse records unless caring directly for a patient.[31] The hospital was confronted with the same issue just months earlier, when it was revealed that an administrative specialist "accessed [Farah Fawcett's] records more often than her own doctors" and sold news of her cancer relapse to tabloids for $4600.[32] Though gossip and the bribery used to obtain it are age-old predicaments, the temptation to sneak a peek will loom ever larger once health employees across the United States come to realize that a few clicks of a mouse can reveal intimate details on neighbors, celebrities and teenage-daughters' boyfriends alike.

Congress has taken a rather nonchalant attitude towards privacy. There are no provisions, for example, requiring patient data to be encrypted, meaning that a misplaced laptop or thumb drive could easily lead to the public disclosure of thousands of medical files.[33] And a recent audit by the Department of Health and Human Services of seven hospitals revealed gaping security issues, ranging from "inadequate password settings [and] computers that did not log users off after periods of inactivity" to a "data backup room[ whose] back door lock had been taped over."[34] Although a pending regulation could give patients the right to see who has viewed their medical record *after* the fact,[35] there are no requirements that the patient be notified, much less consent, *before* his data is handed over to a third

---

31 Charles Ornstein, *Hospital to Punish Snooping on Spears*, L.A. TIMES (Mar. 15, 2008), http://articles.latimes.com/2008/mar/15/local/me-britney15.

32 Charles Ornstein, *Farrah Fawcett: 'Under a Microscope' and Holding onto Hope*, L.A. TIMES (May 11, 2009), http://www.latimes.com/la-et-fawcett-interview11-2009may11,0,3538939.story.

33 *See Electronic Medical Records Rarely Encrypted: Expert*, THE HUFFINGTON POST (Nov. 10, 2011), http://www.huffingtonpost.com/2011/11/10/electronic-medical-records-encrypted-data-breach_n_1086129.html.

34 DANIEL R. LEVINSON, DEP'T OF HEALTH AND HUMAN SERVS., NATIONWIDE ROLLUP REVIEW OF THE CENTERS FOR MEDICARE & MEDICAID SERVICES HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 OVERSIGHT 3, 6–7 (May 16, 2011), *available at* http://oig.hhs.gov/oas/reports/region4/40805069.pdf.

35 *See* Kelly Kennedy, *Greater Patient Access to Records Proposed*, USA TODAY (June 9, 2011), http://www.usatoday.com/news/washington/2011-06-09-patient-health-records_n.htm.

party.[36] By pressing relentlessly towards digitization without considering the consequences for personal privacy, Congress is shirking its duty to truly engage in the deliberative process, and, ultimately, to ensure that privacy protections are in place before all of our sensitive information is uploaded to the medical community at large. Its failure to do so is yet another clear symptom of the data-mania Miller diagnosed almost a half century ago.

Yet another area where Miller's predictions have been borne out is with regard to data sharing as Big Business. Miller's warning that "[w]e must begin to realize what it means to live in a society that treats information as an economically desirable commodity and a source of power"[37] is more true today than ever: Knowledge may be power, but information is money.

To a certain extent, we've accepted the fact that there is a booming market in our personal data. At this point, we've all grown complacent to the constant bombardment of tracking cookies and targeted pop-ups that seem a bit too keen on our Internet excursions. Even the coupons printed on our grocery store receipts—perhaps $1 off Midol and buy one, get one free Dove chocolates—seem creepily one step ahead of next week's anticipated purchases.

What we may be less aware of, however, is how our own government has figured into the equation. As Miller notes, government investigators and local law enforcement have always been avid consumers in the marketplace of information, at least as loyal customers of the credit bureaus.[38] And, as the information economy has expanded, so too have the government's purse strings. Verizon, for instance, has admitted that it "receives tens of thousands of requests for customer records, or other customer information from law enforcement" each year.[39] Facebook gets ten to twenty police requests a day.[40] And the information doesn't come cheap: Cox Communications, the third-largest cable provider in the United States,

---

[36] *See* MILLER, *supra* note 1, at 86–88 (describing similar shortcomings of the Fair Credit Reporting Act).

[37] *Id.* at 23.

[38] *See id.* at 83.

[39] *See* Christopher Soghoian, *8 Million Reasons for Real Surveillance Oversight*, SLIGHT PARANOIA (Dec. 1, 2009), http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html (quoting letter from Todd S. Schulman, Assistant Gen. Counsel, Verizon, to Arleta D. Cunningham, Office of Gen. Counsel, U.S. Marshals Serv. (Sept. 14, 2009), *available at* http://files.cloudprivacy.net/verizon-price-list-letter.PDF).

[40] Nick Summers, *Walking the Cyberbeat*, NEWSWEEK (April 30, 2009), http://www.thedailybeast.com/newsweek/2009/04/30/walking-the-cyberbeat.html.

for example, charges law enforcement anywhere from $40 for basic information, including identifying individuals based on IP address, to $3500 for 30 days of wiretapping.[41]

Government is also a major patron of the commercial data brokers, which have all but replaced the credit bureaus as the government's go-to source for information. Such firms quietly collect massive quantities of personal information on individuals and then sell the data to corporations, attorneys, insurers, employers, collection agencies, news media and, you guessed it, the government. In 2005, for example, four government agencies—the Department of Justice, State Department, Department of Homeland Security and the Social Security Administration—spent $30 million on information from data brokers.[42] And ChoicePoint, one of the largest data-collection firms, had "multimillion dollar contracts with at least thirty-five federal agencies, including the [IRS] and the FBI."[43] Today, there are databases containing trillions of records on virtually every American, available for easy perusal by law enforcement everywhere.[44] The growing omnipresence of the data brokers is particularly disconcerting given that the industry is still largely unregulated, meaning that government officials can use the firms to avoid privacy protection laws that would limit their ability to gather and share the information themselves.[45] As a result, any efforts to cabin Big Brother's watchful eye would be incomplete without extending such efforts to "Big Brother's Little Helpers"[46] as well.

Nor is the government's role limited to that of a hungry consumer. As Miller explains, our trusted government officials have a long

---

41 *Notice to Parties Serving Subpoenas on Cox Communications*, COX COMMC'NS, http://ww2.cox.com/aboutus/policies/lea-information.cox (last visited Mar. 7, 2012).

42 *See* Jayni Foley, Note, *Are Google Searches Private? An Originalist Interpretation of the Fourth Amendment in Online Communication Cases*, 22 BERKELEY TECH. L.J. 447, 447 n.5 (2007).

43 Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 363 (2006).

44 *See* Ann Woolner, *Ex-Drug Smuggler Turned Data Miner Reclaims Field He Created*, BLOOMBERG BUSINESSWEEK (Sept. 15, 2011), http://www.businessweek.com/news/2011-09-15/ex-drug-smuggler-turned-data-miner-reclaims-field-he-created.html.

45 *See* Corey Ciocchetti, *Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information*, 10 VAND. J. ENT. & TECH. L. 553, 581 n.80 (2008).

46 *See* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595 (2004).

history of "vending information about us behind our backs."[47] State departments of motor vehicles, for example, have been selling out car owners for just about as long as there have been cars, just as the Federal Aviation Administration has sold lists of airline pilots, and the IRS has sold aggregate statistics about taxpayers to direct-target advertisers.[48]

As Miller accurately predicted, the gravy train hasn't stopped yet: States continue to make millions selling personal information of drivers stored in their Department of Motor Vehicles databases,[49] and universities have cashed in by "selling student mailing lists to banks and credit card companies."[50] Indeed, some K-12 public schools have been all too eager to milk the informational cash cow, offering to distribute surveys by businesses to their students—for a fee.[51] Although there has been some federal legislation that attempts to curb these abuses,[52] the laws are riddled with exceptions. The Driver's Privacy Protection Act, for example, purports to protect private information, but has more than a dozen exceptions, including allowing disclosures to other agencies, private investigators and those conducting market research.[53] Legislation or not, cash-strapped schools, agencies and local governments will continue to find a way to profit from peddling their informational wares, as they always have.

So where does all this leave us? Should we throw our hands up to the futility of it all and quietly accept our fate? Certainly not. Although, as Miller explained, the law has been "laggard in coming to grips with the broader ramifications of the computer," we must counteract the sheer momentum of rapidly advancing technology by devoting our "human resources to help solve the difficult problem of

---

47 *See* MILLER, *supra* note 1, at 82.

48 *Id.*

49 *See, e.g.*, John Estus et al., *Oklahoma Brings in Millions by Selling Personal Data*, NEWSOK (Apr. 5, 2010), http://newsok.com/oklahoma-brings-in-millions-by-selling-personal-data/article/3451253.

50 Lynn M. Daggett, *FERPA in the Twenty-First Century: Failure to Effectively Regulate Privacy for All Students*, 58 CATH. U. L. REV. 59, 100 & n.238 (2008).

51 *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1823 (2011).

52 *See, e.g.*, Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721–2725 (2006); Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (2006 & Supp. 2011); *see also* Protection of Pupil Rights Amendment, 20 U.S.C. § 1232h (2006).

53 18 U.S.C. § 2721.

balancing privacy and efficiency."[54] If we can strike this balance, or at least take seriously the need to do so, there may yet be hope for the "personal privacy [that] is fundamental to our democratic tradition of individual autonomy."[55]

This advice could not be more timely. It is exceedingly rare for a book, particularly one about computers, to be as relevant four decades after its publication as the date it was written. Its continued relevance stands testament to the fact that although technology may change dramatically—from universal fingerprinting to DNA databases and credit bureaus to data brokers—our fundamental notions of privacy and the need to balance such concerns with the demands of the modern state do not. It also stands testament to the wisdom of the author. Although we have largely ignored Miller's cautionary words so far, there is still time to lay claim to the precious private spheres that remain. And we must. If we don't stand up to the data-maniacs today, we may soon find ourselves bowing to the "dossier dictatorship" of tomorrow.

*The Assault on Privacy* is thus not simply a well-documented snapshot of the challenges facing society at the dawn of the computer era, but a shrewd and continuing reminder of the perennial issues we must confront in an ever-evolving, technologically-driven society; its author, in turn, is not merely a prolific and engaged teacher, academic, celebrity and advocate, but a prophet in his own time.

---

54 MILLER, *supra* note 1, at 259.

55 *Id.*