JAMES B. RULE

The Whole World Is Watching

In an increasingly monitored world, how can consumers and citizens reclaim ownership of their private lives?

Early in 2010, *The Guardian* reported plans by the British Police and Home Office for a remarkable new venture in domestic surveillance. Unmanned aerial drones, now used for tracking insurgents in Pakistan and Afghanistan, are to be adapted (unarmed, one hopes) to monitor Britain's civil population. An initial aim of the project is crowd control during the 2012 London Olympics. Thereafter, these high-tech surveillance engines are to become a permanent feature of state security and law enforcement—much to the distress of civil libertarians and privacy advocates, who immediately objected to the plans.

But no one can say this is especially new. With an estimated 1.7 million video cameras deployed on the ground, George Orwell's homeland can probably already claim world leadership in state-sponsored monitoring of its population.

JAMES B. RULE *is Distinguished Affiliated Scholar at the Center for the Study of Law and Society at the University of California, Berkeley. His most recent book is* Privacy in Peril.

And the intensification of all forms of institutional tracking of individuals isn't restricted to Britain—it is occurring the world over. All told, the United States has probably contributed more to these trends than any other country as both the creator and exporter of different means of government and corporate surveillance. The sheer variety of forms implicated in this monitoring is striking. They include real-time recording of consumers' buying habits and finances; tracking of travelers' movements by air, train, and road; monitoring of private citizens' telecommunications; and the mass harvesting of tidbits of personal data from social sites like Facebook.

The seemingly relentless pace of innovation in surveillance cannot be ascribed to any one interest, policy, organizational purpose, or political mood. Instead, it suffuses all manner of relations between institutions and individuals, from the allocation of welfare-state benefits to the pursuit of suspected terrorists.

The result has been change in the very texture of everyday life. Being "alone" is not what it used to be. Our whereabouts, our financial transactions, our uses of the World Wide Web, and countless other data routinely register in the automated consciousness of corporate and state bureaucracies. More importantly, the results of such monitoring in turn shape the treatment we receive from these organizations—sometimes in ways that we know, and often in ways we hardly imagine.

Many observers dismiss these developments with a shrug: The fate of personal privacy in the face of institutional data-gathering may be hopeless, they hold, but such a development is not really serious. The collection of personal data supports all sorts of valued corporate conveniences and public policies, from easy credit to protection from terrorist threats. The fact that my most intimate medical information is held by a distant bureaucracy is hardly a loss, the argument goes, so long as the people who handle it don't really know me in any personal way. And why should I care if government agencies track my communications, movements, or expenditures if I have nothing to hide? We ought to be grateful for these developments, and not challenge them with anachronistic values like privacy.

Such nonchalance shortchanges both the complexity of the changes we are enmeshed in and their repercussions in our everyday lives. In every realm of life, the flow (and restriction) of personal information confers advantage and disadvantage between parties, opening some possibilities and closing others. In face-to-face relationships, as elsewhere, we do not readily disclose information about areas of our lives in which we feel weak, troubled, or ashamed. Nor do we reveal information that could confer strategic advantage on the other party, like the maximum we are willing to pay in a purchase we are negotiating,

for example. For all sorts of reasons, we cherish the ability to control sensitive information about ourselves.

Thus, even those who profess themselves unconcerned about privacy are apt to object when unauthorized use of their information works against *them*. They will not appreciate finding themselves the losers, for example, in "target pricing"—the practice in which online retailers raise or lower prices offered to different customers for identical items on the basis of their past buying habits. They will be displeased if they discover that their bosses have accessed their medical files from the company health-care plan, and used their medical data as bases for decisions on pay or promotions. They will feel aggrieved on finding themselves subjected to marketing appeals for embarrassing products or services—incontinence supplies, treatments for sexual dysfunction—on the strength of their past website visits or consumer choices. They will wax indignant if they discover that the prices they are quoted for insurance coverage are raised because the insurer has discovered that they have low *credit scores*, which supposedly correlate with greater likelihood of filing insurance claims. And they will be outraged if they find themselves victims of "universal default"—creditors' policy of raising a customer's rates in one credit account based on reports that the amounts of credit used in *other* credit accounts have risen.

In these cases and countless others, people resent receiving unfavorable treatment on the basis of information about themselves that they consider "nobody else's business." The trouble is, notions of what information constitutes anyone's own "business" are in headlong transformation. We live in a world in which possibilities for accessing personal data are mutating in ways that institutions, unsurprisingly, exploit to their own advantage. What disclosures and uses of personal data are held "reasonable" under such circumstances is constantly up for grabs. That is why the need for serious public conversations about privacy is so urgent.

Classic visions of liberal society stress judicious limitations of institutional power, both governmental and corporate, coupled with preservation of individual autonomy and freedom of choice. We accept that institutions like the IRS have investigative powers sufficient to collect most taxes owed, most of the time. But we recoil—I hope—at an idea like unlimited IRS monitoring of all taxpayers' e-mails and phone conversations aimed at registering key words associated with tax evasion. Such (hypothetical, but quite feasible) measures could be very effective in spotting underreporting of taxable income. But even greatly increased compliance with tax obligations is not worth such sweeping losses to privacy.

Restricting police searches to instances when there is "probable cause" or "reasonable suspicion," or requiring court orders for government entry into private premises, reflects this same determination to balance public powers against the need to defend a private sphere of life. It is indispensable that properly designated government agencies have powers to collect specific personal information when evidence points to specific needs for it. But we should be alarmed at information-gathering routines where government investigators troll frictionlessly through broad categories of personal information—telecommunications, purchase records, travel data—just in case something interesting presents itself. In the fluid informational world that we inhabit, that is unfortunately the prevailing direction of change.

The costs of this drift toward ever-more-pervasive surveillance are felt not only by those personally targeted—those whose "confidential" medical records are disclosed, for example, or those whose travels are tracked by Homeland Security officials. The sheer existence of these surveillance systems generates chilling effects experienced by all members of civil society. In this respect, privacy values are holistic—like the values of freedom of expression. Even if I, individually, feel no hesitation about speaking out, I suffer in a world where others are intimidated against articulating their concerns, grievances, and visions of the public good. By the same token, public confidence that certain realms of life are defended from public scrutiny enriches civic culture for all.

Our whereabouts, financial transactions, and countless other data are routinely delivered to corporate and state bureaucracies.

Privacy advocates hardly wish to stop those determined to disseminate information about themselves from doing so (though we might want to insist on legal guarantees that would protect the right to reverse such decisions after the fact). What advocates seek above all is to enhance meaningful individual *choice and control* over release and use of personal data. We want to help find ways for institutions to get their work done while relying on as little personal information as possible. And where disclosure of personal data is deemed necessary, we seek to have specific data supplied for specific purposes—and no others.

The ultimate disaster, in this view, is a world in which any personal information provided in specific settings for specific purposes becomes available to all institutions for all purposes. We're not there yet, and many voices are rising against the possibility. But the forces promoting such easy flow of personal data include some of our most powerful institutions.

Don't Blame Technology

What has triggered this pervasive appetite for institutional tracking of what used to be called private life? And where are the resulting changes taking us?

Folk explanations often indict "technology" as the master cause, as though computing could by itself redirect human interests and intentions. And obviously one can point to many ways in which new departures in surveillance depend on developments in information technology. But not all systems that *might* be created for knowing more are *likely* to be created. Prevailing political interests are decisive in shaping which technological possibilities will become reality.

Consider the achievements of today's systems for tracking and evaluating the so-called credit-worthiness of American consumers. This country's consumer credit reporting industry ascribes to the great majority of adult Americans a three-digit score epitomizing their potential profitability as charge-account customers, credit card users, or mortgage applicants. As in virtually all systems of mass surveillance, credit tracking and scoring enables institutions to make ever-finer distinctions in their treatment of the people they deal with.

But note that American consumers have no remotely comparable monitoring system to help them choose among retailers, products, and services. This is hardly for lack of need. A consumer-friendly tracking system could furnish the same comprehensive, instantaneously available data to buyers that credit reporting provides to lenders and retailers. True, populist approaches to information technology have benefitted consumers in recent years: One can comparison shop for a new car on one's iPhone, for example, or access user reviews of restaurants. But to do for consumers what the credit reporting industry does for retailers seeking data *on* consumers, a system would have to go much further. Instead of compiling a few reviews of products and services from self-selected consumers, a strong consumer-oriented system would have to elicit reactions from most users, or at least a highly representative sample of them. And these ratings should not simply reflect consumers' immediate experience; they should provide reliable information on how satisfied consumers of long-lasting products are, say, after five years. For complex products like cars and computers, a system would provide information on how long different components will last, on average, before requiring major repairs. It would provide instant answers to questions like, "What are the average projected total repair bills on a new Chevrolet Volt over a five-year period? And how do these figures compare with those of other new models?"

All of this would cost money, though consumer savings would likely make up for the public costs. What's more problematic is that such a system would

require manufacturers and sellers to provide crucial data. They will, of course, insist that such information is *proprietary*—that is, they own it, and they're not giving it up. The reasons for such resistance are obvious: Better information for consumers spells potential disadvantage for sellers.

The dramatic discrepancies between these two surveillance potentials—one an ultra-sophisticated reality, the other grossly underdeveloped—are by no means imposed by technology. They reflect sponsorship. This country's lending and retail industries are simply better organized and more resourceful interests than consumers. Seeing the profits promised by discriminating among prospective customers based on finely grained information, the industry has willingly made the vast investments necessary to create, collect, massage, and repackage consumers' account data for sale. Thus, creation and extension of large-scale surveillance follow well-worn grooves of political and economic power. Only institutions—and well-heeled ones at that—can mobilize the vast capital costs and cultivate the public acquiescence necessary to create comprehensive systems for monitoring large populations.

Surveillance and Symbiosis

Think of institutional surveillance as a kind of manufacturing process where the "products" are decisions about how to deal with individual consumers or citizens, and the raw material consists of personal information on the individuals concerned. Recent decades have generated a steady stream of new sources of these crucial raw materials, including the Internet and mobile telephony, the growing array of tax collection data, the intensified monitoring of air travel and other forms of transport, and the increasingly sophisticated automated monitoring of telecommunications. Analysis and exploitation of such personal data make it possible to target individuals with just the right ad at just the right moment, direct the right intervention from Homeland Security personnel, or provide the right form of medical care given a patient's history and entitlements.

The cumulative effect is to render ever-wider domains of everyday experience subject to monitoring by distant institutional decision-makers. The more realms of typical Americans' lives are subject to systematic documentation, the broader the scope for such decision-making. Near-universal registration of births and deaths became complete in the first quarter of the twentieth century. By mid-century, the IRS and Social Security had begun to track employment and incomes of most American adults. Around the same time, credit reporting grew to monitor the finances of perhaps half of American families.

Computing played no role in the advent of such monitoring, but it has since lent vast momentum to its development. The 1980s brought the beginnings of

the Internet, eventually spawning new troves of information on users' interests, communication patterns, and activities. The 1990s saw the explosion of mobile telephones, generating new systems of accounting for Americans' movements and whereabouts, as well as their communications patterns. The new millennium has yielded mushrooming social networking sites, attracting willing new sources of personal information, along with the attentions of countless organizations determined to find profitable uses for it.

If the pace of such innovation appears to be accelerating, it is largely because surveillance feeds on itself. The more of it there is, the more opportunities there are for leveraging the effects of such documentation across institutional lines. Boundaries between government and corporations don't much matter here. Personal data have long since become a valuable commodity, and trade flourishes vigorously across the public-private frontier. Credit reporting agencies troll through public records for data on bankruptcies. Insurance companies purchase millions of dollars worth of data on drivers, vehicles, accidents, and citations from state motor vehicle departments. Government investigators, from law enforcement and anti-terror agencies to the IRS, thrive on the fine detail of consumers' purchasing data supplied by credit card companies and other financial institutions. Among the biggest consumers of such commercially generated background reports are government agencies engaged in their own surveillance operations, notably the Justice Department and the Department of Homeland Security.

Virtually all mass surveillance systems enable institutions to make ever-finer distinctions about people, but people have no remotely comparable system.

Conspiring with these trends are changes in the cultural role of computing. If we think of media in Marshall McLuhan's terms as "extensions of man," then social networking sites are extensions of people's (apparently insatiable) desire to know and be known by others. It has become a truism that participants in these sites are often confounded by the unintended uses of personal data they themselves furnish. Evgeny Morozov, a skeptical observer of the political role of computing, reports mining of social network sites by state security agencies in countries like Iran and his native Belarus to identify supporters of the political opposition.

What's disturbing is that newer generations seem increasingly resigned to the proposition that personal information, once yielded, slips permanently out of one's control. This does not have to be true. But the actual interests and practices governing disclosure, given the absence of broad legal rights over one's own data, are often extremely difficult to discern. Privacy statements put forward

by websites and companies often acknowledge, on close scrutiny, data-holders' virtually unconstrained discretion to disseminate and exchange personal data. Thus, legislation like the Health Insurance Portability and Accountability Act is officially described as assuring "the confidentiality, integrity and availability of electronic protected health information," when in fact it ratifies broad disclosure of patients' data without their permission and even against their interests.

This discouraging reality inspires dicta like the one attributed to Sun Microsystems co-founder Scott McNealy: "You have zero privacy anyway. Get over it." Such willing fatalism reinforces the convictions of many Americans that personal information has somehow permanently escaped from human control.

The Official Response: Privacy Codes

Since the 1960s, anxiety over these trends has fueled demand for law and policy to protect privacy. Throughout the world's prosperous liberal societies, policy elites and concerned publics have embraced the conviction that personal information is too important to be left to the sole discretion of the institutions that collect and store it. Treatment of personal data held in file has thus emerged as a public issue requiring appropriate legislation, court action, and institution-building.

The result has been global proliferation of privacy codes, devoted to specifying the rights and responsibilities of institutions and individuals in the treatment of personal data. As of 2011, more than 60 countries around the world—including most recently Argentina and South Korea—have adopted such measures.

Despite significant variation from country to country, the world's privacy codes show marked similarities. Most establish individual rights that apply to data held by both governments and private organizations. Virtually all require that organizations maintaining personal data systems give public notice of their activities and take responsibility for the legal operation of their systems. Organizations are enjoined to restrict their collection and use of personal data to what is required for the official purposes of record-keeping (a notoriously elastic notion). Institutional holders of personal data must typically allow individuals to access their own files and, often, challenge the accuracy of data and the uses made of them. And to back up the codes, nearly every country that has one has a data-protection commission, an ombudsman-like agency with a commissioner and (usually quite small) support staff. These commissions serve as the public voice of privacy concerns, reminding institutions of their obligations under privacy law, responding to citizen complaints, and mediating disputes over treatment of personal information.

In a striking bit of American exceptionalism, the United States remains nearly alone among the world's liberal democracies *without* such an independent data-protection commission. Moreover, its privacy codes are fairly

restricted compared to those of other countries. Specific rights of access and challenge are provided in stand-alone legislation governing records held in such diverse settings as consumer credit, video rentals, health care delivery, and financial accounts. But U.S. law establishes no broad rights protecting personal data held throughout the private sector, and only limited rights over government-held records. In the absence of a national data commissioner, aggrieved individuals are expected to act on their own to seek redress under these laws.

For all that recommends them, privacy codes rarely challenge basic premises of institutional surveillance. They implicitly accept the legitimacy of institutional collection and use of personal data, in response to what are often vaguely bracketed as organizational "needs" for such information. They set down specific rights and responsibilities for organizations—often dubbed "fair information practices"—based on a faintly liberal model of informed choice. Where provision of personal data is not mandated by law, individuals are expected to grant their formal consent to its use, presumably in exchange for valued services from the organization. In practice, however, the interpretation of "consent" often proves as elastic as that of the official purposes for which data are collected.

For some optimistic observers, following ground rules based on fair information practices solves the essential ethical and political problems posed by large-scale personal data collection. But such views are myopic. Yes, where personal data systems exist, we are normally better off with fair information practices in place. But at best, privacy codes address only a subset of the consequential issues raised by institutional surveillance.

For one thing, privacy codes are rarely applied to surveillance operations of the coercive and investigative branches of state power. Uses of personal data by police, tax collectors, espionage and counterterrorism agencies, and the like remain virtually untouched by the codes. To be sure, even the strongest privacy advocates would agree that investigators pursuing verifiable dangers should be permitted significant measures of secrecy for their work. But to stop short of any constraints over who is tracked, when, and for how long obviously places vast swathes of state surveillance beyond the reach of privacy considerations.

Far more important, the world's privacy codes are virtually silent on the most pressing questions of all: How much institutional surveillance should we permit in the first place? What constitute adequate grounds for creating these vast systems of human tracking? What forms of personal data, if any, are simply too revealing, too intrusive, or too dangerous to justify assembling into systems for institutional monitoring?

The reflexive response to such questions—more often implicit than stated—is that organizations resort to surveillance as a result of "needs" for personal data. In an Information Society, one often hears, the flow of all kinds of data is a fundamental necessity. Personal information is the basis for efficiencies that nearly everyone values, from easy access to credit to safety in air travel to cost-effective tax collection. But bureaucratic needs for personal information are not like the body's needs for oxygen—deprivation does not bring death. Beyond a certain low threshold, doing with less personal information hardly brings these systems to a halt. This holds as much for government institutions as for corporations. Certainly the IRS needs access to some basic forms of personal data in order to enforce basic tax obligations—income data from employers, interest data from mortgage-holders, etc. But an IRS—or a Justice Department or a Department of Homeland Security—that could monitor a continuous feed of *all* data on *all* Americans' financial affairs, from every credit or debit card purchase to every stock transfer or utility payment, would trigger chilling effects felt by everyone.

The Progressives' Dilemma

Dilemmas on where and how to limit intrusive surveillance for "good" purposes have not always brought out the best in progressives. For many, the greatest promise of government lies in the enhancement of its powers to do good—by knowing more about the governed, for example, or by refining means to alter the circumstances of their lives. Such themes seamlessly merge with Information Society affirmations that more information is bound ultimately to foster wiser, more enlightened government. Thus, a fully comprehensive compilation of all medical data on all Americans—as promoted by both the Bush and Obama Administrations—would in this view amount to a win for all, if only managed so as to avoid "abuse" of personal information.

But we should remain skeptical about such effusive liberal visions. History has shown that it is not so easy to wring politics out of administration. One may have the sturdiest faith in the liberal intentions of those who create new surveillance systems. But political climates change, whereas the powers conferred by such systems endure.

Such prospects are hardly speculative. This country's past shows regular recurrences of repressive periods in public life, including such nasty episodes as the Palmer Raids at the end of World War I and the FBI-led campaigns against alleged Communist sympathizers in the 1950s and Martin Luther King Jr. and his followers in the 1960s. Given the reality of such swings in American life—and the evident pressures even in the best of times to share the resources

of surveillance systems for "legitimate" purposes—can Americans afford to be so complacent about the encroachment of institutional surveillance into every nook and cranny of daily existence?

The trouble is that we reach these realizations only after the systems are faits accomplis. If we hope to do better, we must weigh in advance the long-term trajectories of such incremental developments. At some point nearly everyone must agree that institutional access to personal information becomes threatening and excessive, even if the institutions are ones we basically support. There has to be a line demarcating certain categories of personal data, or realms of personal life, as no legitimate concern of interested institutions. And such definitions must arise only through public debate and reflection, rather than being relegated to bureaucratic planners and designers of information systems.

The Alternative: Serious Privacy Protection

The right choices on such questions will render American life considerably more privacy-friendly. The most basic tools for implementing such choices involve the legal status of personal information. Consider Americans' "personal papers," records protected under the Fourth Amendment from "unreasonable search and seizure." Today this constitutional protection still applies to documents and other possessions physically held in Americans' homes, such that court orders are required before state investigators can enter one's premises and seize materials of interest. But the definition of personal files has changed more than a little since the framing of the Constitution. It is all but impossible to live a normal life without accumulating vast troves of personal information in systems maintained by banks, credit card and telecommunications companies, and other third-party record-keepers. Such data do not enjoy constitutional protection from investigators' access; instead, access is governed by statute law. This means that state agencies often need not seek court approval to access such data. In practice, many investigations of this kind are not even reported publicly, to Congress or any other party.

A simple but sweeping step would be for Congress to extend constitutional protection to these "personal papers"—normally computer records—held by outside institutions. Such a far-reaching change would by no means place such information beyond the reach of investigators who have convincing need for it. The measure would simply require advance approval of such seizures from an independent judiciary, thereby providing protection against vague fishing expeditions, attempted harassment through unfounded investigations, and other privacy-eroding dangers. Except where courts agreed in advance, this step should provide those being investigated with a chance to challenge investigators' demands before searches could go forward.

Extension of Fourth Amendment protections would trigger massive opposition from the vast investigative establishment of the government, from local prosecutors all the way up to Washington. And we would be deluding ourselves if we imagined that government's current free hand in these matters has no popular support: Many ordinary Americans have been convinced that unobtrusive and unchecked government delving through personal data sources is essential to their own safety from terrorists or other evil-doers. A broad public debate on the issue would grant liberals the chance to insist that protection of personal data files from warrantless state scrutiny is consistent with a law-abiding and secure social order. It's an argument that true conservatives in the tradition of Burke and de Tocqueville would also support, along with many centrists and others concerned for separation of powers and rule of law.

Other simple but far-reaching changes could yield similar shifts in the balance of power between institutions and individuals. Perhaps the most basic step would be the creation of a property right over commercial exploitation of personal information. Given such a right, no sale or trade of personal data for commercial purposes would be possible without express authorization from the person concerned. The underlying principle would be the classic privacy-friendly idea: no disclosure as the default condition, with alternatives available to those who prefer disclosure. Simply by doing nothing, anyone would be protected against use of his or her data for such purposes. Thus ordinary citizens would have the same lock on commercialization of their names and lives now enjoyed only by celebrities.

A basic step would be the creation of a property right over commercial use of personal information, requiring consent from the person concerned.

Any such right would have to be carefully circumscribed. It should never apply to uses of personal information in public discourse, such as in political campaigns, public debate, or even private gossip. Nor should it offer protection against the sale of legitimate debts, for example, to debt collection agencies. Nor should rights over anyone's information be permanently alienable, so that corporations or other interests could somehow buy up people's privacy rights in perpetuity. Legal scholars such as Paul Schwartz at the University of California, Berkeley School of Law have proposed detailed road maps for how such a privacy-friendly right would work in practice.

Who would be the losers in such a fundamental shift in control over personal data? Only the corporate interests that now profit from capturing and exploiting

such data for nothing. Long-established industries from retailing to consumer credit reporting to direct marketing would rise in unison if confronted with any serious threat to the free access they now enjoy to Americans' data. No less energized would be representatives of the new Information Economy, from obscure start-ups to giants like Google and Facebook.

Even short of these sweeping proposals, progressives could put forward privacy-friendly measures that would garner much popular support. We could propose that those subjected to government monitoring—of their accounts, phone and e-mail exchanges, and the like—automatically be apprised of what has occurred soon after the fact, absent a showing that such notification would be harmful to a legitimate ongoing investigation. Even this modest concession would have the salutary effect of politicizing government surveillance and demonstrating how pervasive it actually is.

In the private sector, progressives could propose that every credit applicant have the option, when opening an account, to block dissemination of data from that account to outside interests, notably credit reporting industries. Such a privacy-friendly right, long a baseline principle in some consumer societies, would shield consumers from well-founded fears of pressure to settle disputed debts, or having one's account reported as delinquent.

Presented as measures on behalf of ordinary Americans against remote and high-handed institutions, proposals like these could garner much populist enthusiasm. But there is no denying that they will be a heavy political lift. To change our privacy culture in any programmatic way, progressives will have to acknowledge that some uses of personal information are simply too sweeping to embrace, even when profitable, convenient, or effective as vectors of government power. And this means affirming that some desirable results of constantly knowing more about the lives of more and more people will have to be foregone. Some criminals will escape, some potential terrorists will go unmonitored, some devious taxpayers will go undetected, some bad credit risks will get a break, and on and on. In short, there will be tragedies. This is not a prospect that any politician relishes discussing in public.

But properly understood, the present state of affairs is still more unpalatable. Without realizing it, we have slipped into a world where institutional access to personal data has become a default condition. This transition has occurred incrementally, without national reflection on the world we are fostering. The fact that people so readily yield their data to impersonal institutions should hardly be taken as affirmation of their support for an un-private world, any more than driving should be taken as evidence of enthusiasm for global warming. Loss of control over personal data presents itself to most people not as a choice to be

made so much as the normal condition of everyday life. Progressives need to challenge the premises of such a world and seek to extend meaningful choice in these respects.

Nobody really desires a world where any bit of information captured in any way by any institution is automatically available to all—much as we approach that world by daily increments. For any hope of doing better, we need to start with serious public soul-searching on the politics of surveillance. D