OP-ED CONTRIBUTOR NEW YORK TIMES

The Price of the Panopticon

By JAMES B. RULE

Published: June 11, **2013**

BERKELEY, Calif. — THE revelation that the federal government has been secretly gathering records on the phone calls and online activities of millions of Americans and foreigners seems not to have alarmed most Americans. A poll conducted by the Pew Research Center over the four days immediately after the news first broke found that just 41 percent of Americans deemed it unacceptable that the National Security Agency "has been getting secret court orders to track telephone calls of millions of Americans to investigate terrorism."

We privacy watchers and civil libertarians think this complacent response misses a deeply worrying political shift of vast consequence. While President Obama has conveniently described the costs of what appears to be pervasive surveillance of Americans' telecommunications connections as "modest encroachments on privacy," what we are actually witnessing is a sea change in the kinds of things that the government can monitor in the lives of ordinary citizens.

The N.S.A. dragnet of "connection data" — who communicates with whom, where, how often and for how long — aims at finding patterns between calls or messages, and between parties with given characteristics, which correlate with increased odds of terrorist activity. These patterns can in turn cue authorities to focus attention on possible terrorists.

The success rate in these operations is a matter of intense speculation, given the authorities' closemouthed stance on the matter. But no serious analyst can doubt that such steps may be helping to pinpoint terrorist acts in advance, as supporters, like Senator Dianne Feinstein, Democrat of California, have insisted.

The question, though, is what comes next? Government planners have apparently invested billions of dollars to develop these new surveillance capabilities. Given the open-ended nature of this country's relentless campaign against terrorism and other declared evils, it would be naïve to imagine that the state's grip on "big data," achieved at such cost, would be allowed to atrophy in the foreseeable future. It is far more likely that new uses — and, inevitably, abuses — will be found for these surveillance techniques.

This is true even if the Obama administration's goals are benign. Institutions and techniques predictably outlive the intentions of their creators. J. Edgar Hoover went before

Congress in 1931 to declare that “any employee engaged in wiretapping will be dismissed from the service of the bureau.” A few decades later, F.B.I. agents were in full pursuit of alleged Communist sympathizers, civil rights workers and the Rev. Dr. Martin Luther King Jr. — using wiretapping, break-ins and other shady tactics.

We must also ask how far we want government to see into our private lives, even in the prevention and punishment of genuine wrongdoing. The promise that one especially egregious sort of crime (terrorism) can be predicted and stopped can tempt us to apply these capabilities to more familiar sorts of troublesome behavior.

Imagine that analysis of telecommunications data reliably identified failure to report taxable income. Who could object to exploiting this unobtrusive investigative tool, if the payoff were a vast fiscal windfall and the elimination of tax evasion? Or suppose we find telecommunications patterns that indicate the likelihood of child abuse or neglect. What lawmaker could resist demands to “do everything possible” to act on such intelligence — either to apprehend the guilty or forestall the crime.

Using surveillance for predictive modeling to prevent all sorts of undesirable or illegal behavior is the logical next step. These possibilities are by no means a fantastical slippery slope — indeed, the idea of pre-empting criminals before they act was envisioned by Philip K. Dick’s short story “The Minority Report,” later a movie starring Tom Cruise.

Some privacy watchers have dismissed N.S.A. activities as surveillance boondoggles, unlikely to significantly prevent terrorism. That is not my view. Terrorism is an authentic danger — as are dangerous driving, communicable diseases, gun violence and countless other behaviors and tendencies that could, in principle, be combated by closer monitoring of Americans’ communication.

But do we need, and should we tolerate, a government so powerfully and deeply embedded in our once private lives as to spot manifestations of such evils anywhere and everywhere, perhaps even before they occur? How ready and able are we to fend off the overextension and abuse of that knowledge? Who watches the watchers? And how are we to weigh the prospective losses to communal bonds and trust in our communities and our institutions, in a world without the buffer against state intervention that privacy affords?

American life has swung before between repressive and permissive climates. The swing toward surveillance, begun by George W. Bush, has only continued under his successor. But

even those Americans who think the supposed trade-off between privacy and security is "worth it" need to ponder all the likely consequences.

James B. Rule is a sociologist and a scholar at the University of California, Berkeley, School of Law.

A version of this op-ed appeared in print on June 12, 2013, on page A27 of the New York edition with the headline: The Price of the Panopticon.