2009

The National Surveillance State: A Response to Balkin

Orin S. Kerr

Response Article

The National Surveillance State: A Response to Balkin

Orin S. Kerr†

In his recent Lockhart lecture, published in this journal as *The Constitution in the National Surveillance State*,[1] Jack Balkin warns of a "new form of governance" that he calls "the National Surveillance State."[2] Balkin argues that new technologies have triggered a new approach to governance that changes what government can do and how it does it.[3]

According to Balkin, the National Surveillance State "grows naturally out of the Welfare State and the National Security State"[4] and "seeks any and all information that assists governance."[5] The National Surveillance State is threatening because it focuses on prevention ex ante rather than prosecution ex post, and because it can use private/public partnerships to circumvent constitutional limits on government.[6] Balkin leaves us with a question: Will the National Surveillance State be an "authoritarian information state" that controls us, or a "democratic information state" that we the citizenry control?[7]

† Professor, George Washington University Law School. Thanks to the editors of the *Minnesota Law Review* for inviting me to publish this response.

1. Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1 (2008).

2. *Id.* at 3.

3. *See id.* ("Government's increasing use of surveillance and data mining is a predictable result of accelerating developments in information technology.").

4. *Id.* at 5.

5. *Id.* at 11.

6. *See id.* at 15–17 (describing the "three major dangers for our freedom" posed by the National Surveillance State).

7. *See id.* at 17–18.

Like Balkin, I would insist on the latter.[8] But I think Balkin's essay somewhat misses the point of the changes he describes. In my view, we aren't seeing a "new form of governance." The form of governance remains very much the same. Rather, what Balkin describes is part of a broader societal shift away from human observation and towards computerization. The widespread use of computers and the introduction of digital information have caused important changes in how individuals can learn what others are doing. The government's reaction to these changes, while highly visible, is only a small part of the picture.

In this brief response, I will explain why the changes Balkin details should be understood as a technology problem instead of a governance problem. Technology has changed, and the law should shift in response. This approach is both more accurate and more likely to prove politically appealing; it suggests solutions that draw support from a wide political base rather than a narrow one.

I. THE SHIFT TO COMPUTERIZATION

In the past, information ordinarily was collected and shared using the human senses. We generally knew what we knew because we had either seen it directly or heard it from someone else. Knowledge was based entirely on personal observation. If you wanted to know what was happening, you had to go out and take a look. You had to see what was happening and observe it with your own eyes, or at least speak to those who had done so to get a second-hand account. The human senses regulated everything.

That is gradually changing. More and more, our daily lives are assisted by and occur through computer networks.[9] Computer networks are extraordinary tools for doing remotely what we used to have to do in person. It seems like we barely need to leave home anymore. We wake up in the morning and check Facebook, using the network to send and receive messages. We make our purchases online, using the network to select and order goods. If we go outside and head to lunch—yes, some people

8. *See id.* at 25 (hoping that the United States can surmount the problems caused by the National Surveillance State in order to "preserve constitutional values and democratic self-government").

9. *See, e.g.*, Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 309 (2005) (describing how the shift to computerization has affected criminal activity and investigations).

do actually still "go outside"—we probably pay for the meal with a credit card. All of these routine steps are facilitated by computer networks.

If you're interested in knowing what's happening in a computer network, the human senses alone aren't enough. You can't just look around in the network. You can't just listen to hear what's happening. Instead, knowing what's happening requires collecting and analyzing data from the networks themselves. The network contains information zipping around the world, and the only way to know what is happening is to analyze it. Specifically, some device must collect the information, and some device must manipulate it.[10] The result is a substitution effect: Work that used to be done entirely by the human senses now must be done in part by tools.

The shift from information collection via the human senses to information collection via tools means a general switch in how a person or institution might learn what is happening in the world. The old powers are out: Institutions can no longer simply send an individual out and ask him to collect information with his senses. Instead, devices must be installed and configured to collect the data. And once collected, the information must be processed and analyzed so that it makes sense to whomever wants to use it to understand what is happening on the network. In the computer network environment, the work traditionally performed by the human senses is increasingly done by computer data collection and analysis.

Professor Balkin looks at these changes and sees a new form of government, a new "National Surveillance State."[11] But these changes are not so much a "new form of governance" as a new playing field for the old one. The government's goals haven't changed. Just as before, the public wants the government to catch bad guys. Just as before, the public wants terrorists caught and criminals prosecuted. But that old job must now be done in a new way. The switch to networks means that information must be obtained and then analyzed using tools. Someone must install the tools; someone must configure them; and someone must analyze them.

10. *See* Balkin, *supra* note 1, at 7–11 (discussing the ways in which data from a whole variety of networks is collected and analyzed).

11. *See id.* at 3.

II. THE NEW PLAYING FIELD AND POLITICAL APPEAL

Why does it matter whether we see the changes as a "new form of governance" or just a new playing field? It matters because it points to a different solution for a different audience. Balkin sees a governance problem, so he looks to the traditional governance solutions: Judicial review, legislative oversight, and oversight within the executive branch.[12] His approach appeals to a civil-libertarian audience. The "National Surveillance State" evokes George Orwell's *Nineteen Eighty-Four*,[13] and it calls on us to remain vigilant against the traditional threat of excessive government power.[14] But surely a civil-libertarian audience is already on board with Balkin's agenda. That audience needs no prompting to demand more oversight of government surveillance and data mining.

In contrast, framing the issue as a technology problem can appeal to a much broader political audience. It enables reformers to make an institutionally conservative argument for change: If technology has changed, the law should change with it to restore the status quo ante. Instead of inspiring civil-libertarians, the argument appeals to a Burkean conservative commitment to prior institutional settlements. Further, it focuses attention on technical issues that can draw broad agreement rather than ideological claims that tend to trigger disagreement and distrust.

Consider an example. In an era of human observation, the law focuses almost exclusively on information collection. When a person observes evidence, it is relatively difficult to share and analyze it. The information is stored only in the human mind, and the person who knows it must consciously decide to share that information with a particular person at a particular time. It takes energy. Further, over time memory fades, and the information disappears along with it. These practical realities tend to impose natural limits on how much and when evidence that is collected will be used and distributed. Computers, however, are not so limited. They are remarkably efficient tools for distributing and preserving data. They can store everything, distribute data anywhere in an instant, and configure data in a way that can be broadly subjected to many different types of analysis for many different reasons.

12. *See id.* at 20–25.

13. GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949).

14. *See id.* at 24 ("The best way to control the watchers is to watch them as well.").

The shift to computerization presents an easy case for the expanded role of use restrictions in privacy law. When the law imposes a use restriction, it imposes limitations on what an entity can do with information after it has been collected.[15] In the past, the law focused on evidence collection: The frailty and imperfection of the human mind made use restrictions generally unnecessary.[16] But computers have brought the cost of total memory to zero, and that shift means that the law must now play the role that the practicalities of human observation once played. The argument doesn't depend on public fear of the executive branch, as does the notion of the new "National Surveillance State."[17] Rather, it is based on the simple dynamic of technological change: To restore the status quo, the law should make hard what technology has made easy.

The technological narrative also carves out a natural role for oversight focused on efficacy. It reminds us that surveillance and data mining are always goal-dependent: When assessing a particular program, the focus must be on what works. If a surveillance tool or program doesn't work, it shouldn't be used. This seems obvious, but tends to become lost in practice. I recently served on a committee of the National Academy of Sciences that studied the problem of government data mining, and I was struck by how often programs exist with no evidence of whether they actually work.[18] In my view, the mindset that allows such programs to exist without analyzing their efficacy

15. *See, e.g.*, Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49, 77–92 (1995) (describing how the transformation of Fourth Amendment jurisprudence has led to controversial use restrictions on seized information).

16. At least this is the case when the law regulates evidence collection. Use restrictions have played an important role where the law has regulated evidence collection very lightly, as in the case of grand jury secrecy. *See* FED. R. CRIM. P. 6(e)(2).

17. *See* Balkin, *supra* note 1, at 21 ("Without appropriate checks and oversight mechanisms, executive officials . . . . will increase secrecy, avoid accountability, cover up mistakes, and confuse their interest with the public interest.").

18. Indeed, the committee's recommendations focused heavily on how to ensure that such programs actually work and can therefore justify the privacy threats they raise. *See* NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., PROTECTING INDIVIDUAL PRIVACY IN THE STRUGGLE AGAINST TERRORISTS: A FRAMEWORK FOR PROGRAM ASSESSMENT 86 (2008) ("U.S. government agencies should be required to follow a systematic process . . . to evaluate the effectiveness, lawfulness, and consistency with U.S. values of every information-based program . . . for detecting and countering terrorists before it can be deployed, and periodically thereafter.").

sees such programs as a governance issue, not a technology issue: The programs exist because data mining is just something the government does. To borrow Balkin's phrase, it is part of the National Surveillance State. But viewing data mining as a technology problem instead of a governance problem forces every data mining program to justify its existence: It exposes data mining as simply a new tool to achieve a traditional end, focusing attention on whether each particular data mining program can in fact achieve that end.

CONCLUSION

In his essay, Professor Balkin asks whether the National Surveillance State will control us or whether we the citizenry will control it.[19] This framing of the problem leaves the answer distressingly uncertain: It presents the State with a life of its own that only the popular will can tame. I am much more optimistic. The shift to computerization has changed the playing field of traditional government functions. In the new environment, some things that were hard have become easy; some things that were easy have become hard. It will take time for the legal system to appreciate the shift. Network technologies are new, and user experiences limited. But over time we will see that the basic game hasn't changed. New laws are needed to respond to technological change. But the government's functions remain the same regardless of technology: Technology has changed how the government does its job, but the job itself remains. As before, the legal restrictions on government practices are up to lawmakers, not the State itself—National Surveillance or otherwise.

19. *See* Balkin, *supra* note 1, at 4 ("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?").