A TWENTY-FIRST CENTURY FRAMEWORK FOR DIGITAL PRIVACY

WHITE PAPER SERIES

Introduction: A Twenty-First Century Framework for Digital Privacy

JEFFREY ROSEN

NATIONAL CONSTITUTION CENTER

NATIONAL CONSTITUTION CENTER

Introduction: A Twenty-First Century Framework for Digital Privacy

By Jeffrey Rosen*

At the beginning of the twenty-first century, breathtaking changes in technology pose stark challenges to privacy and security. Private companies collect massive amounts of consumer data—information that often contains intimate details about our personal lives, from the people that we email to the apps that we use to the websites that we visit. Law enforcement often seeks to access this information when investigating suspected criminals and terrorists, and the data itself is highly mobile, with companies able to send it across borders at the tap of a button. At the same time, hackers threaten our personal data through cyberattacks, and sophisticated users shield the contents of their data from law enforcement through the use of cutting-edge encryption tools.

Concerns span the ideological spectrum. Libertarian conservatives and civil-libertarian liberals are united in their suspicion of state surveillance, while conservatives suspect regulation of the consumer sphere and progressives are concerned about concentrated corporate power. At the same time, judges and legislators have been remarkably slow to respond to the new threats cyberspace poses. There have been no great Supreme Court cases on data privacy since the 1980s; the statutory framework for regulating consumer privacy is incomplete and uncertain; and few judges or legislators have been willing to tackle the crucial challenge of translating the Constitution and key privacy laws in light of new technologies.

Advances in technology raise numerous important (and difficult) legal questions:

- How can we strike the right balance between security and privacy in the digital age?
- How might we translate Fourth Amendment doctrine in light of technological advances and changing consumer expectations of privacy?
- What constitutional and statutory protections should there be for data stored in the Cloud, and under what circumstances and with what constraints should the government get access to it?
- Does the government have to tell consumers when it searches their email accounts or accesses their data?
- And whose law should govern access to data in our borderless world—a world where data is often stored on servers in other countries and can be transferred across borders at the snap of a finger?

The National Constitution Center, with the support of Microsoft, has assembled leading scholars and thought leaders to publish a series of five white papers, entitled *A Twenty-First Century Framework for Digital Privacy*. We've asked these contributors to reflect on the challenges that new technologies pose to existing constitutional doctrine and statutory law and to

propose solutions—doctrinal, legislative, and constitutional—that translate the Constitution and federal law in light of new technologies. The overarching question we asked contributors to address is how best to balance privacy concerns against the need for security in the digital age. These contributors represent diverse points of view and experiences and their papers reflect the Constitution Center's commitment to presenting the best arguments on all sides of the constitutional issues at the center of American life.

In *Digital Divergence*, David Kris examines advances in technology, and he challenges the view that balancing privacy and security is a zero-sum game. Instead, he argues that new technologies threaten *both* privacy *and* security. While privacy faces familiar threats such as mass data collection and government surveillance, Kris argues that we shouldn't ignore the risks posed to security in the digital age. Far from a "golden age" of government surveillance, Kris sees a digital world where advances in technology have made it easier for sophisticated criminals and terrorists to carry out illegal acts and more difficult for government agents to conduct effective surveillance—due, in part, to the massive volume of data, data's mobility, and the use of cutting-edge encryption tools. In short, more and more data is generated—most of it useless to law enforcement, but that data is still susceptible to large-scale cyberattacks. Kris frames this problem as one of "digital divergence"—namely, that the advance of digital technology has harmed both privacy and security—and examines constitutional and statutory changes that might follow from this trend.

In *Administering the Fourth Amendment in the Digital Age*, Jim Harper critiques the limited privacy protections provided by current Fourth Amendment doctrine and calls on courts to adopt a new approach—one guided by Justice Pierce Butler's forgotten dissent in *Olmstead v. United States*. Harper rejects an approach that focuses on society's "reasonable expectations of privacy" and calls on courts to adopt one that protects privacy at least as much as the Founding generation did—protections that hew closely to the Fourth Amendment's text and recognize data, information, and communications as a key form of property. In particular, he urges courts to administer the Fourth Amendment methodically, by (1) determining whether there has been a "seizure," defined as an invasion of a property right, or a "search," defined as acting with a "purpose of finding something"; (2) analyzing whether the government agent seized or searched something protected by the Fourth Amendment—namely, a person, house, paper, or effect; and, finally, (3) asking if the seizure or search was reasonable—an inquiry that should focus on the reasonableness of the *government's* actions rather than the reasonableness of the *defendant's* privacy preferences. Harper argues that this approach would place judges back in the familiar position of applying the law to the facts of a specific case.

In *Policing and The Cloud*, Christopher Slobogin offers his own approach to balancing privacy and security in the digital age—an approach that focuses on context and proportionality. He argues that given the personal nature of the information stored in the Cloud, law enforcement shouldn't be able to access it at will. Instead, Slobogin advocates for an approach that is sensitive to the context of the specific government action or request. While a warrant may not be appropriate in all circumstances, a mere subpoena may not be sufficient, either. For instance, when the government requests non-public information about a specific person, courts should weigh the level of intrusion involved in the request against the level of suspicion. As the level of intrusion and the amount of data requested increases, so should the level of justification—up to

and including, perhaps, a warrant. Slobogin's goal is to construct rules that will allow the government to harness the Cloud's investigative potential, while also limiting the opportunities for government abuses.

In *Secret Government Searches and Digital Civil Liberties*, Neil Richards tackles the issue of what he describes as "secret government searches"—namely, examples of government surveillance that remain a secret to the search target. These can be physical or digital, carried out with a warrant or without, and unknown to everyone but the government or facilitated by a private company that is prohibited from notifying the target. Richards places these secret searches in historical, technological, and constitutional context and argues that they are unprecedented, historically and technologically, and inconsistent with key constitutional values, including freedom of thought, freedom of expression, and freedom from unreasonable searches and seizures.

Finally, in *Whose Law Governs in a Borderless World?: Law Enforcement Access to Data Across Borders*, Jennifer Daskal explores the challenges posed by the mobility of data. Today, legal rules covering government access to data treat location as king. And yet, data can move across borders and around the world instantly, can be held in multiple places at once, and can be accessed remotely from across the world. Daskal argues that a better rule would shift the focus away from data location and consider a variety of other factors, including target location and nationality, the location of the provider, and the strength of the government's interest. For Daskal, these factors better reflect the interests at stake in cross-border data disputes, including privacy, security, and sovereignty.

** Tom Donnelly, Senior Fellow for Constitutional Studies at the National Constitution Center, contributed to this article and directed this project.*