

JEFFREY ROSEN

1

*Introduction:
Technological Change and the
Constitutional Future*

At the beginning of the twenty-first century, changes in technology are posing stark challenges to our legal and constitutional values. From free speech to privacy, from liberty and personal autonomy to the privilege against self-incrimination, from the definition of personhood to the state's authority to protect security, basic constitutional principles are under stress from technological advances unimaginable even a few decades ago, let alone in the founding era. Consider a few cases that might plausibly confront the Supreme Court in the year 2025:

—In response to popular demand, Facebook decides to post live feeds from public and private surveillance cameras so they can be searched online. After Facebook grants the request, anyone in the world can log onto the Internet, select a particular street view on Facebook, and zoom in on a particular individual. The user can then back-click to retrace that person's steps since she left the house in the morning or forward-click to see where she is headed. With facial recognition technology, a user can click on an image of a stranger, plug the image into a Facebook or Google database to identify her by name, and then follow her movements from door to door. Imagine that this ubiquitous surveillance is challenged as a violation of the Fourth Amendment, which prohibits unreasonable searches and seizures of our "persons, houses, papers, and effects." Under existing doctrine, the Fourth Amendment may not be construed to regulate Facebook, a private corporation, and even if there were enough state action to trigger the Constitution, the Court has come close to saying that we have no expectations of privacy in public places.

—As genetic selection becomes more advanced, couples who use in vitro fertilization are increasingly selecting embryos on the basis of sex, height, sexual

orientation, and even intelligence. In response to concerns about the new eugenics, several states enact laws banning genetic screening for nontherapeutic purposes. These laws are then challenged before the Supreme Court as a violation of the personal liberty and autonomy protected by the due process clause of the Constitution. Existing case law, however, offers little guidance about whether the right to have offspring, recognized in cases such as *Roe v. Wade*, includes an unlimited right to select the characteristics of those offspring.

—As brain scans become increasingly sophisticated, they are becoming de rigueur in death penalty trials, where defense lawyers routinely seek to introduce functional magnetic resonance imaging (fMRI) scans to prove that their clients were unable to control their violent impulses—a kind of “my brain made me do it” defense. Under the relaxed evidentiary standards for capital sentencing, this evidence is usually admitted, and lawyers predict that “neuro-law” evidence will increasingly transform the legal system, calling into question traditional ideas of moral responsibility. Some scholars already claim that neuroscience should lead the legal system to jettison retribution as a goal of criminal punishment, since it’s unfair to hold people responsible for actions that are predetermined by their brains rather than chosen by their free will. Imagine that in 2025 scans can predictably identify people with dangerous propensities to violence. And imagine that a state predicates a civil commitment on the results of scans. Should the Supreme Court strike down efforts to hold people responsible for their propensities rather than their actions as an unconstitutional bill of attainder, or is punishment for propensity different from the procedure that concerned the framers of the Constitution—namely, laws that outlawed specific persons, rather than actions, without the benefit of a judicial trial?

As these examples show, a series of constitutional provisions—including the First, Fourth, Fifth, and Fourteenth Amendments—provide no clear answers, at least as currently interpreted, to the question of how we can preserve American values in the face of dramatic and rapid technological change. Part of the challenge arises from a world in which private corporations have more power over free speech and privacy than any president, king, or Supreme Court justice; part arises from gaps in the Supreme Court’s constitutional doctrine itself, which arose in response to very different challenges in the pre-Internet age.

Of course, the project of keeping the Constitution technologically current is not new. The most creative constitutional thinkers have long struggled to adapt constitutional values to changes in technology. Justice Louis Brandeis offers the paradigmatic example. As early as 1928, in a case called *Olmstead v. United States*, the Supreme Court first encountered the constitutionality of wiretaps. When the federal government began to tap phones in an effort to

enforce prohibition, a bootlegger named Roy Olmstead protested that the wiretaps violated his rights under the Fourth Amendment. In a literal-minded majority opinion, Chief Justice William Howard Taft disagreed. The Fourth Amendment, he said, was originally understood to forbid only searches or seizures accompanied by physical trespass. The agents had not trespassed on Olmsted's property when they placed wiretaps on the phone lines in the streets near his house, Taft held, and conversations were not tangible "effects" that could be searched or seized.

In a visionary dissenting opinion, Brandeis grappled with the issue of translating late-eighteenth-century values in a twentieth-century world. As private life had begun to be conducted over the wires in the age of radio, he observed, telephone conversations contained even more intimate information than sealed letters, which the Supreme Court had held in the nineteenth century could not be opened without a warrant. To protect the same amount of privacy that the framers of the Fourth and Fifth Amendments intended to protect, Brandeis concluded, it had become necessary to translate those amendments into the twentieth century, extending them to prohibit warrantless searches and seizures of conversations over the wires, even if the violations occurred without physical invasions.

In a remarkably prescient passage, Brandeis then looked forward to the age of cyberspace, predicting that technologies of surveillance were likely to progress far beyond wiretapping. "Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home," he wrote. In anticipation of those future innovations, Brandeis challenged his colleagues to translate the Constitution once again to take account of the new technologies, or else risk protecting less privacy and freedom in the twenty-first century than the framers of the Constitution expected in the eighteenth century.

The technologies that Brandeis imagined have now come to pass—and they do not only affect privacy; they affect a broad range of constitutional values. At the same time, these new technologies are having an impact on vastly greater numbers of people than Brandeis could have imagined possible. In the late 1890s, in the most famous article on the right to privacy ever written, Brandeis had worried about new technologies—the Kodak camera and the tabloid press—that were threatening the privacy of aristocrats and celebrities by spreading idle gossip. Today, in an age when 500 million members share billions pieces of content on Facebook each month, all of us face a kind of scrutiny through gossip and ill-advised photos and videos that Brandeis's celebrities could not have imagined.

Yet judges today are generally reluctant to take up Brandeis's challenge to translate legal and constitutional doctrines in light of new technologies. Furthermore, the task of doing so should not be left exclusively to judges or to constitutional doctrine. Sometimes, Congress has kept constitutional values current with legislation. The hard work of applying the Fourth Amendment to wiretapping was ultimately done not by judges but by the U.S. Congress, which in 1968 passed the federal wiretapping law and, a decade later, passed the Foreign Intelligence Surveillance Act. Sometimes, regulatory agencies have taken the lead, such as the Federal Communication Commission's embrace of the principal of network neutrality—namely, the idea that Internet service providers must treat all data equally and may not block or delay any content or applications. And sometimes, keeping the Constitution up to date may require amendments that update the constitutional text itself.

The Brookings Project on Technology and the Constitution was set up to identify, in a nonpartisan and nonideological manner, the range of options for constitutional translation—from courts and legislatures to regulators and new technologies. We asked leading thinkers to imagine the concrete threats that different technologies would pose to constitutional and legal values in the year 2025 and then invited them to select the balance of regulatory, legal, and technological responses that they thought could best preserve the values they considered most important. We chose contributors from very different philosophical and ideological backgrounds in the hope of discovering whether contemporary ideological disputes would map onto the futuristic scenarios. (In some areas, they did; in others, they did not.) This volume is testament both to the possibility of creative thinking about constitutional translation and to the difficulty of ensuring that the most promising solutions are adopted in practice.

The book proceeds in four parts. The first focuses on surveillance, data mining, and the Fourth Amendment. The second looks at the future of free expression and privacy. The third examines the constitutional implications of brain scan technologies. And the fourth explores various aspects of genetic engineering.

The first part, "The Future of Surveillance," begins with Christopher Slobogin's envisioning a future in which the police increasingly use global positioning system (GPS) tracking and other virtual searches. Slobogin argues that the Supreme Court's interpretation of the Fourth Amendment has failed to anticipate virtual searches and investigative techniques that do not require physical access to premises, people, papers, or effects. Slobogin argues that the Supreme Court, rather than focusing on individuals' expectations of privacy, should instead adopt a proportionality principle: for every state action that

implicates the Fourth Amendment, he says, the government should demonstrate cause—a level of certainty that evidence of wrongdoing will be found—more or less proportionate to the intrusiveness of the search.

Orin Kerr also imagines the increasing use of surveillance and data-mining technologies; he speculates that the government in the future might monitor all subway riders as they enter and exit the station by collecting their fingerprints. Although this MONITOR system might help to foil terrorist plots by preventing people on watch lists from entering the station, he says, it might also be misused, allowing criminal investigators to track people in an effort to solve low-level crimes. Kerr says that rather than restricting the collection of data, legislators should pay greater attention to the use of data after they are collected.

Jack Goldsmith describes an even more ambitious monitoring program to meet the threat of a cyber attack. Sometime in the near future, he says, the government might mandate the use of a government-coordinated intrusion-prevention system throughout the domestic network that would electronically monitor all communications, including private ones. Although the program would be controversial, Goldsmith argues that massive government snooping in the network can be made lawful and constitutional if Congress and the president adopt credible safeguards, including independent scrutiny by the Foreign Intelligence Surveillance Court, privacy-protecting “minimization” procedures, oversight mechanisms, and sunset provisions.

My chapter begins part 2 of the book, “The Future of Free Expression and Privacy.” I argue that in the twenty-first century, lawyers for Google and Facebook have more control over free speech and privacy than any president, judge, or king. I begin by imagining Open Planet, a decision by Facebook to link all public and private surveillance cameras and to put them live and online. Under existing Supreme Court case law, Open Planet might not violate the Fourth Amendment, but there are a series of other arguments for restricting ubiquitous surveillance. I then examine three other technologies—body scanners at airports, a web that never forgets, and controversial YouTube videos—and argue that in each case, political activism and federal regulations may be as important as constitutional doctrine in translating and preserving values of privacy and free speech.

Tim Wu argues that anyone who wants to understand free speech in the twenty-first century needs to know how the concept has expanded over time. The first free speech tradition focused on threats from government; the second, he argues, focuses on threats from private intermediaries, such as radio and broadcast networks and Internet platforms such as Google and Facebook. Wu imagines a merger between Google and AT&T, followed by an effort

to crush its political opponents and favor its political supporters. Now that the future of free speech will be determined by concentrated, private intermediaries, he argues, regulatory agencies such as the Federal Communications Commission have more influence over speech than Supreme Court justices, and he urges the commission to use this power to prevent content discrimination by the private actors who control the lines.

In his “Mutual Aid Treaty for the Internet,” Jonathan Zittrain notes that today, most people have direct access to the web, but that their online lives are controlled by consolidating search engines, content providers, and social networking sites. Greater online centralization means greater vulnerability to cyber attacks and threats to free speech: for example, Zittrain notes, a world where all of the world’s books are stored in a centralized online Google depository means that a court order to delete a particular book because it infringes copyright would cut off access to all the world’s readers. Zittrain argues that the key to solving this centralization problem, which he calls the “Fort Knox” problem, is to make the current decentralized web a more robust one by reforging the technological relationships between sites and services. Zittrain’s model is mutual aid treaties among states, which create redundancy and security.

In part 3, “The Future of Neurolaw,” Stephen Morse reflects on how neuroscience is attempting to transform legal notions of personal responsibility. Functional imaging and genetic evidence, he says, may be introduced more often, in coming years, in criminal cases outside of capital sentencing. Morse begins by imagining a young man who kills a fellow driver in an expression of road rage and, at trial, is found to have a predisposition to violent behavior. Morse considers and rejects neuroscience’s radical challenge to responsibility, which treats people as victims of neuronal circumstances. If this view of personhood is correct, say Morse, it would indeed undermine all ordinary conceptions of responsibility and even the coherence of law itself.

In a similar vein, O. Carter Snead argues that advances in cognitive neuroscience have resurrected old arguments about human agency, moral responsibility, and the proper ends of criminal punishment. He begins by imagining that neuroimaging evidence of a predisposition to antisocial behavior, introduced at the sentencing phase of a capital trial, might be invoked to argue more frequently for the death penalty. Once retributive justice is off the table, Snead says, juries may be urged to execute criminals for the sole purpose of preventing them from committing the crimes to which they are neurologically predisposed. Like Morse, Snead wants to resist the radical conceptual challenge that neuroscience poses for criminal punishment in the United States.

Part 4 of the book, “Genetic Engineering and the Future of Constitutional Personhood,” focuses on genetic engineering and the future of constitutional

personhood. John Robertson begins with an examination of the coming legal challenges facing the constitutional doctrine of procreative liberty. He imagines a futuristic setting in which a gay couple, eager to have a male child who shares the sexual orientation of both parents, arranges to have “gay gene” sequences inserted into embryos created through in vitro fertilization. Robertson writes that by 2030, the logic of procreative freedom should lead courts to recognize a broad constitutional right of prospective parents to use the available technologies to have the family they choose.

Eric Cohen and Robert George imagine a future in which people could engineer genetic replicas of themselves or in which individuals could know what diseases they will suffer in the decades ahead. The new genetics, they argue, are rooted in a desire for self-understanding, new medical therapies, genetic engineering, the prediction of disease, and efforts to choose some lives and reject others. But each of these desires for personal autonomy presents profound moral and ethical questions about what it means to be human, raising the specter of a new eugenics. Instead of endorsing a constitutional solution to the potential excesses of genetic autonomy, Cohen and George prefer legislative solutions, including a national ban on human cloning and the patenting of human embryos, state-level prohibitions on the destruction of embryos for research, and a new regulatory body that monitors the safety of new reproductive technologies and has the power to restrict them in the interest of protecting children.

James Boyle hypothesizes that in the next century, it is likely that constitutional law will have to classify artificially created entities that have some but not all of the attributes we associate with human beings. Boyle imagines two entities with human attributes—Hal, a computer with artificial intelligence, and Vanna, a genetically engineered sex doll. Treating Hal and Vanna as full constitutional persons, Boyle argues, might have implications for the debates over fetal and corporate personhood that could discomfit liberals and conservatives alike. Instead of protecting Hal and Vanna with broad expansions of constitutional rights, and instead of trying to legislate the problem out of existence, Boyle argues, it may make more sense to muddle through with less abstract constitutional and statutory regulation.

Benjamin Wittes imagines that in coming years, biothreats—especially those emanating not from governments but from individuals—will present a profound challenge to the Constitution and the nation’s basic assumptions about security. Imagining a genetically engineered small pox virus designed by a suicidal grad student terrorist, Wittes examines the continued proliferation of bioterrorism technologies and speculates that it will lead to a significant erosion of the federal government’s monopoly over security policy. Rather

than intrusive government monitoring that might cripple legitimate research, Wittes argues, the most effective defenses against bioterrorism may come from technological developments and from encouraging alert researchers, companies, and citizens to take on security responsibilities.

Finally, in a forward-looking epilogue, Lawrence Lessig argues that predicting the future in constitutional law is difficult because constitutional meaning comes just as much from what everyone knows to be true (both in the past and today) as from what the framers actually wrote. Yet “what everyone knows is true” changes over time, and in ways that are impossible to predict, even if quite possible to affect. To translate and protect values such as privacy and security in the face of unknown threats that will confront us in the future, Lessig says, we should adopt technologies today that will increase our range of choices tomorrow—such as an identity layer built into the Internet that would allow dangerous individuals to be identified but only with a court order. If we wait until after the threat has materialized, Lessig warns, adopting these thoughtful technologies of balance may not be politically feasible.

The contributors to this volume, in short, suggest a broad range of options for translating constitutional and legal values in light of new technologies. For some contributors—such as Slobogin and Robertson—courts should take the lead in constitutional translation; for others—Kerr, Goldsmith, and Cohen and George, for example—the most important actors will be legislators, not judges. Wu points to the importance of administrative regulation; Wittes and Zittrain emphasize voluntary cooperation; I stress the importance of political activists, working in conjunction with courts, legislators, and administrators. And Lessig describes how technological choices can shape the contours of the constitutional debate.

There is no question that the Constitution will change in response to developing technology in the future, as it has always changed in the past. But as the chapters in this volume suggest, it is far from clear how that change will take place, what form it will take, and how effective the changes will be. Citizens disagree vigorously and plausibly about whether judges should take the lead in adapting constitutional values to changing technologies or whether the more effective and democratically legitimate responses should come from the political branches or the private sector. Instead of endorsing a single approach, contributors to this volume have identified a range of options that judges, technologists, and legislators have as they struggle to respond to technological change. The result, we hope, is a provisional blueprint for translating constitutional and legal values into the twenty-first century.