THE FUTURE
OF THE CONSTITUTION

May 2, 2011

David Malan – Connections within a social network.

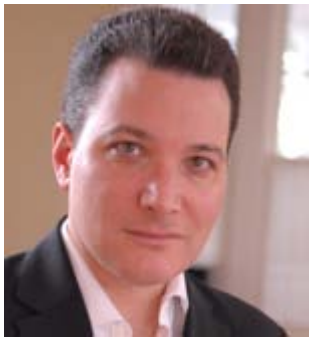
The Deciders: Facebook, Google, and the Future of Privacy and Free Speech

Jeffrey Rosen

Governance Studies
at BROOKINGS

INTRODUCTION

It was 2025 when Facebook decided to post live feeds from public and private surveillance cameras, so they could be searched online. The decision hardly came as a surprise. Ever since Facebook passed the 500 million-member mark in 2010, it found increasing consumer demand for applications that allowed users to access surveillance cameras with publicly accessible IP addresses. (Initially, live feeds to cameras on Mexican beaches were especially popular.) But in the mid-2020s, popular demand for live surveillance camera feeds were joined by demands from the U.S. government that an open circuit television network would be invaluable in tracking potential terrorists. As a result, Facebook decided to link the public and private camera networks, post them live online, and store the video feeds without restrictions on distributed servers in the digital cloud.



Jeffrey Rosen is a nonresident senior fellow in Governance Studies at Brookings. He is also a professor of law at The George Washington University and the legal affairs editor of *The New Republic*.

Once the new open circuit system went live, anyone in the world could log onto the Internet, select a particular street view on Facebook maps and zoom in on a particular individual. Anyone could then back click on that individual to retrace her steps since she left the house in the morning or forward click on her to see where she was headed in the future. Using Facebook's integrated face recognition app, users could click on a stranger walking down any street in the world, plug her image into the Facebook database to identify her by name, and then follow her movements from door-to-door. Since cameras were virtually ubiquitous in public and commercial spaces, the result was the possibility of ubiquitous identification and surveillance of all citizens virtually anywhere in the world—and by anyone. In an enthusiastic launch, Mark Zuckerberg dubbed the new 24/7 ubiquitous surveillance system "Open Planet."

Open Planet is not a technological fantasy. Most of the architecture for implementing it already exists, and it would be a simple enough task for Facebook or Google, if the companies chose, to get the system up and running: face recognition is already plausible, storage is increasing exponentially; and the only limitation is the coverage and scope of the existing cameras, which are growing by the day. Indeed, at a legal Futures Conference at Stanford in 2007, Andrew McLaughlin, then the head of public policy at Google, said he expected Google to get requests to put linked surveillance networks live and online within the decade. How, he, asked the audience of scholars and technologists, should Google respond?

If "Open Planet" went live, would it violate the Constitution? The answer is that it might not under Supreme Court doctrine as it now exists—at least not if it were a purely-private affair, run by private companies alone and without government involvement. Both the First Amendment, which protects free speech, and the Fourth Amendment, which prohibits unreasonable searches and seizures, only restrict actions by the government. On the other hand, if the government directed Open Planet's creation or used it to track citizens on government-owned, as well as private-sector, cameras, perhaps Facebook might be viewed as the equivalent of a state actor, and therefore restricted by the Constitution.

At the time of the framing of the Constitution, a far less intrusive invasion of privacy – namely, the warrantless search of private homes and desk drawers for seditious papers – was considered the paradigmatic case of an unreasonable and unconstitutional invasion of privacy. The fact that 24/7 ubiquitous surveillance may not violate the Constitution today suggests the challenge of translating the framers' values into a world in which Google and Facebook now have far more power over the privacy and free speech of most citizens than any King, president, or Supreme Court justice. In this essay, I will examine four different areas where the era of Facebook and Google will challenge our existing ideas about constitutional protections for free speech and privacy: ubiquitous surveillance with GPS devices and online surveillance cameras; airport body scanners; embarrassing Facebook photos and the problem of digital forgetting; and controversial YouTube videos. In each area, I will suggest, preserving constitutional values requires a different balance of legal and technological solutions, combined with political mobilization that leads to changes in social norms.

Let's start with Open Planet, and imagine sufficient government involvement to make the courts plausibly consider Facebook's program the equivalent of state action. Imagine also that the Supreme Court in 2025 were unsettled by Open Planet and inclined to strike it down. A series of other doctrines might bar judicial intervention. The Court has come close to saying that we have no legitimate expectations of privacy in public places, at least when the surveillance technologies in question are in general public use by ordinary members of the public.[1] As mobile camera technology becomes ubiquitous, the Court might hold that the government is entitled to have access to the same linked camera system that ordinary members of the public have become accustomed to browsing. Moreover, the Court has said that we have no expectation of privacy in data that we voluntarily surrender to third parties.[2] In cases where digital images are captured on cameras owned by third parties and stored in the digital cloud—that is, on distributed third party servers--we have less privacy than citizens took for granted at the time of the American founding. And although the founders expected a degree of anonymity in public, that expectation would be defeated by the possibility of 24/7 surveillance on Facebook.

The doctrinal seeds of a judicial response to Open Planet, however, do exist. A Supreme Court inclined to strike down ubiquitous surveillance might draw on recent cases involving decisions by the police to place a GPS tracking device on the car of a suspect without a warrant, tracking his movements 24/7. The Supreme Court has not yet decided whether prolonged surveillance, in the form of "dragnet-type law enforcement practices" violates the Constitution.[3] Three federal circuits have held that the use of a GPS tracking device to monitor someone's movements in a car over a prolonged period is not a search because we have no

[1] See *Florida v. Riley*, 488 U.S. 445 (1989) (O'Connor, J., concurring).
[2] See *United States v. Miller*, 425 U.S. 435 (1976).
[3] See *United States v. Knotts*, 460 U.S. 276, 283-4 (1983).

expectations of privacy in our public movements.[4] But in a visionary opinion in 2010, Judge Douglas Ginsburg of the U.S. Court of Appeals disagreed. Prolonged surveillance is a search, he recognized, because no reasonable person expects that his movements will be continuously monitored from door to door; all of us have a reasonable expectation of privacy in the "whole" of our movements in public. [5] Ginsburg and his colleagues struck down the warrantless GPS surveillance of a suspect that lasted 24 hours a day for nearly a month on the grounds that prolonged, ubiquitous tracking of citizen's movements in public is constitutionally unreasonable. "Unlike one's movements during a single journey, the whole of one's movements over the course of a month is not actually exposed to the public because the likelihood anyone will observe all those movements is effectively nil," Ginsburg wrote. Moreover, "That whole reveals more – sometimes a great deal more – than does the sum of its parts."[6] Like the "mosaic theory" invoked by the government in national security cases, Ginsburg concluded that "Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation."[7] Ginsburg understood that 24/7 ubiquitous surveillance differs from more limited tracking not just in degree but in kind – it looks more like virtual stalking than a legitimate investigation – and therefore is an unreasonable search of the person.

Because prolonged surveillance on "Open Planet" potentially reveals far more about each of us than 24/7 GPS tracking does, providing real time images of all our actions, rather than simply tracking the movements of our cars, it could also be struck down as an unreasonable search of our persons. And if the Supreme Court struck down Open Planet on Fourth Amendment grounds, it might be influenced by the state regulations of GPS surveillance that Ginsburg found persuasive, or by Congressional attempts to regulate Facebook or other forms of 24/7 surveillance, such as the Geolocational Privacy and Surveillance Act proposed by Sen. Ron Wyden (D-OR) that would require officers to get a warrant before electronically tracking cell phones or cars.[8]

The Supreme Court in 2025 might also conceivably choose to strike down Open Planet on more expansive grounds, relying not just on the Fourth Amendment, but on the right to autonomy recognized in cases like *Casey v. Planned Parenthood* and *Lawrence v. Texas*. The right to privacy cases, beginning with *Griswold v. Connecticut* and culminating in *Roe v. Wade* and *Lawrence*, are often viewed as cases about sexual autonomy, but in *Casey* and *Lawrence*, Justice Anthony Kennedy recognized

---

[4] See *United States v. Pineda-Morena*, 591 F.3d 1212 (9th Cir. 2010); *United States v. Garcia*, 474 F.3d 994 (7th Cir. 2007); *United States v. Marquez*, 605 F.3d 604 (8th Cir. 2010).

[5] See *United States v. Maynard*, 615 F.3d 544 (D.C. Cir 2010).

[6] 615 F.3d at 558.

[7] Id. at 562.

[8] See Declan McCullagh, "Senator Pushes for Mobile Privacy Reform," *CNet News*, March 22, 2011, available at http://m.news.com/2166-12_3-20045723-281.html

a far more sweeping principle of personal autonomy that might well protect individuals from totalizing forms of ubiquitous surveillance. Imagine an opinion written in 2025 by Justice Kennedy, still ruling the Court and the country at the age of 89. "In our tradition the State is not omnipresent in the home. And there are other spheres of our lives and existence, outside the home, where the State should not be a dominant presence," Kennedy wrote in *Lawrence*. "Freedom extends beyond spatial bounds. Liberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct."[9] Kennedy's vision of an "autonomy of self" that depends on preventing the state from becoming a "dominant presence" in public as well as private places might well be invoked to prevent the state from participating in a ubiquitous surveillance system that prevents citizens from defining themselves and expressing their individual identities. Just as citizens in the Soviet Union were inhibited from expressing and defining themselves by ubiquitous KGB surveillance, Kennedy might hold, the possibility of ubiquitous surveillance on "Open Planet" also violates the right to autonomy, even if the cameras in question are owned by the private sector, as well as the state, and a private corporation provides the platform for their monitoring. Nevertheless, the fact that the system is administered by Facebook, rather than the Government, might be an obstacle to a constitutional ruling along these lines. And if Kennedy (or his successor) struck down "Open Planet" with a sweeping vision of personal autonomy that didn't coincide with the actual values of a majority of citizens in 2025, the decision could be the *Roe* of virtual surveillance, provoking backlashes from those who don't want the Supreme Court imposing its values on a divided nation.

Would the Supreme Court, in fact, strike down "Open Planet" in 2025? If the past is any guide, the answer may depend on whether the public, in 2025, views 24/7 ubiquitous surveillance as invasive and unreasonable, or whether citizens have become so used to ubiquitous surveillance on and off the web, in virtual space and real space, that the public demands "Open Planet" rather than protesting against it. I don't mean to suggest that the Court actually reads the polls. But in the age of Google and Facebook, technologies that thoughtfully balance privacy with free expression and other values have tended to be adopted only when companies see their markets as demanding some kind of privacy protection, or when engaged constituencies have mobilized in protest against poorly designed architectures and demanded better ones, helping to create a social consensus that the invasive designs are unreasonable.

The paradigmatic case of the kind of political mobilization on behalf of constitutional values that I have in mind is presented by my second case: the choice between the naked machine and the blob machine in airport security screening. In 2002, officials at Orlando International airport first began testing the millimeter wave body scanners that are currently at the center of a national uproar. The designers of the scanners at Pacific Northwest Laboratories offered U.S.

[9] *Lawrence v. Texas*, 539 U.S. 558, 562 (2003).

officials a choice: naked machines or blob machines? The same researchers had developed both technologies, and both were equally effective at identifying contraband. But, as their nicknames suggest, the former displays graphic images of the human body, while the latter scrambles the images into a non-humiliating blob.[10]

Since both versions of the scanners promise the same degree of security, any sane attempt to balance privacy and safety would seem to favor the blob machines over the naked machines. And that's what European governments chose. Most European airport authorities have declined to adopt body scanners at all, because of persuasive evidence that they're not effective at detecting low-density contraband such as the chemical powder PETN that the trouser bomber concealed in his underwear on Christmas day, 2009. But the handful of European airports that have adopted body scanners, such as Schiphol airport in Amsterdam, have opted for a version of the blob machine. This is in part due to the efforts of European privacy commissioners, such as Germany's Peter Schaar, who have emphasized the importance of designing body scanners in ways that protect privacy.

The U.S. Department of Homeland Security made a very different choice. It deployed the naked body scanners without any opportunity for public comment—then appeared surprised by the backlash. Remarkably, however, the backlash was effective. After a nationwide protest inspired by the Patrick Henry of the anti-Naked Machines movement, a traveler who memorably exclaimed "Don't Touch my Junk," President Obama called on the TSA to go back to the drawing board. And a few months after authorizing the intrusive pat downs, in February 2011, the TSA announced that it would begin testing, on a pilot basis, versions of the very same blob machines that the agency had rejected nearly a decade earlier. According to the latest version, to be tested in Las Vegas and Washington, D.C, the TSA will install software filters on its body scanner machines that detects potential threat items and indicates their location on a generic, blob like outline of each passenger that will appear on a monitor attached to the machine. Passengers without suspicious items will be cleared as "OK," those with suspicious items will be taken aside for additional screening. The remote rooms in which TSA agents view images of the naked body will be eliminated. According to news reports, TSA began testing the filtering software in the fall of 2010 – precisely when the protests against the naked machines went viral. If the filtering software is implemented across the country, converting naked machines into blob machines, the political victory for privacy will be striking.

Of course, it's possible that courts might strike down the naked machines as unreasonable and unconstitutional, even without the political protests. In a 1983 opinion upholding searches by drug-sniffing dogs, Justice Sandra Day O'Connor recognized that a search is most likely to be considered constitutionally reasonable

[10] The discussion of the blob machines is adapted from "Nude Breach," *New Republic*, December 13, 2010.

if it is very effective at discovering contraband without revealing innocent but embarrassing information.[11] The backscatter machines seem, under O'Connor's view, to be the antithesis of a reasonable search: They reveal a great deal of innocent but embarrassing information and are remarkably ineffective at revealing low-density contraband.

It's true that the government gets great deference in airports and at the borders, where routine border searches don't require heightened suspicion. But the Court has held that non-routine border searches, such as body cavity or strip searches, do require a degree of individual suspicion. And although the Supreme Court hasn't evaluated airport screening technology, lower courts have emphasized, as the U.S. Court of Appeals for the 9th Circuit ruled in 2007, that "a particular airport security screening search is constitutionally reasonable provided that it 'is no more extensive nor intensive than necessary, in the light of current technology, to detect the presence of weapons or explosives.'"[12]

It's arguable that since the naked machines are neither effective nor minimally intrusive – that is, because they might be designed with blob machine like filters that promise just as much security while also protecting privacy – that courts might strike them down. As a practical matter, however, both lower courts and the Supreme Court seem far more likely to strike down strip searches that have inspired widespread public opposition – such as the strip search of a high school girl wrongly accused of carrying drugs, which the Supreme Court invalidated by a vote of 8-1,[13] then they are of searches that, despite the protests of a mobilized minority, the majority of the public appears to accept.

The tentative victory of the blob machines over the naked machines, if it materializes, provides a model for successful attempts to balance privacy and security: government can be pressured into striking a reasonable balance between privacy and security by a mobilized minority of the public when the privacy costs of a particular technology are dramatic, visible, widely distributed, and people experience the invasions personally as a kind of loss of control over the conditions of their own exposure.

But can we be mobilized to demand a similarly reasonable balance when the threats to privacy come not from the government but from private corporations and when those responsible for exposing too much personal information about us are none other than ourselves? When it comes to invasions of privacy by fellow citizens, rather than by the government, we are in the realm not of autonomy but of dignity and decency. (Autonomy preserves a sphere of immunity from government intrusion in our lives; dignity protects the norms of social respect that we accord to each other.) And since dignity is a socially constructed value, it's unlikely to be preserved by judges--or by private corporations--in the face of the expressed preferences of citizens who are less concerned about dignity than

[11] *United States v. Place*, 462 U.S. 696 (1983).
[12] *U.S. v. Davis*, 482 F.2d 893, 913 (9th Cir. 1973).
[13] *Safford Unified School District v. Redding*, 557 U.S. ___ (2009).

exposure.

This is the subject of our third case, which involves a challenge that, in big and small ways, is confronting millions of people around the globe: how best to live our lives in a world where the Internet records everything and forgets nothing—where every online photo, status update, Twitter post and blog entry by and about us can be stored forever.[14] Consider the case of Stacy Snyder. Four years ago, Snyder, then a 25-year-old teacher in training at Conestoga Valley High School in Lancaster, Pa., posted a photo on her MySpace page that showed her at a party wearing a pirate hat and drinking from a plastic cup, with the caption "Drunken Pirate." After discovering the page, her supervisor at the high school told her the photo was "unprofessional," and the dean of Millersville University School of Education, where Snyder was enrolled, said she was promoting drinking in virtual view of her under-age students. As a result, days before Snyder's scheduled graduation, the university denied her a teaching degree. Snyder sued, arguing that the university had violated her First Amendment rights by penalizing her for her (perfectly legal) after-hours behavior. But in 2008, a federal district judge rejected the claim, saying that because Snyder was a public employee whose photo didn't relate to matters of public concern, her "Drunken Pirate" post was not protected speech.[15]

When historians of the future look back on the perils of the early digital age, Stacy Snyder may well be an icon. With Web sites like LOL Facebook Moments, which collects and shares embarrassing personal revelations from Facebook users, ill-advised photos and online chatter are coming back to haunt people months or years after the fact.

Technological advances, of course, have often presented new threats to privacy. In 1890, in perhaps the most famous article on privacy ever written, Samuel Warren and Louis Brandeis complained that because of new technology — like the Kodak camera and the tabloid press — "gossip is no longer the resource of the idle and of the vicious but has become a trade."[16] But the mild society gossip of the Gilded Age pales before the volume of revelations contained in the photos, video and chatter on social-media sites and elsewhere across the Internet. Facebook, which surpassed MySpace in 2008 as the largest social-networking site, now has more than 500 million members, or 22 percent of all Internet users, who spend more than 500 billion minutes a month on the site. Facebook users share more than 25 billion pieces of content each month (including news stories, blog posts and photos), and the average user creates 70 pieces of content a month.

Today, as in Brandeis's day, the value threatened by gossip on the Internet – whether posted by us our by others – is dignity. (Brandeis called it an offense against honor.) But American law has never been good at regulating offenses

---

[14] The discussion of digital forgetting is adapted from "The End of Forgetting," *New York Times Magazine*, July 25, 2010.

[15] *Snyder v. Millersville University*, No. 07-1660 (E.D. Pa. Dec. 3, 2008).

[16] Brandeis and Warren, "The Right to Privacy," 4 Harv. L. Rev. 193 (1890).

against dignity – especially when regulations would clash with other values, such as protections for free speech. And indeed, the most ambitious proposals in Europe to create new legal rights to escape your past on the Internet are very hard to reconcile with the American free speech tradition.

The cautionary tale here is Argentina, which has dramatically expanded the liability of search engines like Google and Yahoo for offensive photographs that harm someone's reputation. Recently, an Argentinean judge held Google and Yahoo liable for causing "moral harm" and violating the privacy of Virginia Da Cunha, a pop star, by indexing pictures of her that were linked to erotic content. The ruling against Google and Yahoo was overturned on appeal in August, but there are at least 130 similar cases pending in Argentina to force search engines to remove or block offensive content. In the U.S., search engines are protected by the Communications Decency Act, which immunizes Internet service providers from hosting content posted by third parties. But as liability against search engines expands abroad, it will seriously curtain free speech: Yahoo says that the only way to comply with injunctions about is to block all sites that refer to a particular plaintiff.[17]

In Europe, recent proposals to create a legally enforceable right to escape your past have come from the French. The French data commissioner, Alex Turc, who has proposed a right to oblivion – namely a right to escape your past on the Internet. The details are fuzzy, but it appears that the proposal would rely on an international body – say a commission of forgetfulness – to evaluate particular take down requests and order Google and Facebook to remove content that, in the view of commissioners, violated an individuals' dignitary rights.

From an American perspective, the very intrusiveness of this proposal is enough to make it implausible: how could we rely on bureaucrats to protect our dignity in cases where we have failed to protect it on our own? Europeans, who have less of a free speech tradition and far more of a tradition of allowing people to remove photographs taken and posted against their will, will be more sympathetic to the proposal. But from the perspective of most American courts and companies, giving people the right selectively to delete their pasts from public discourse would pose unacceptably great threats to free speech.

A far more promising solution to the problem of forgetting on the Internet is technological. And there are already small-scale privacy apps that offer disappearing data. An app called TigerText allows text-message senders to set a time limit from one minute to 30 days, after which the text disappears from the company's servers, on which it is stored, and therefore, from the senders' and recipients' phones. (The founder of TigerText, Jeffrey Evans, has said he chose the name before the scandal involving Tiger Woods's supposed texts to a mistress.)[18]

---

[17] Vinod Sreeharsha, Google and Yahoo Win Appeal in Argentine Case, *N.Y. Times*, August 20, 2010, B4.

[18] See Belinda Luscombe, "Tiger Text: An iPhone App for Cheating Spouses?", *Time.com*, Feb. 26, 2010, available at http://www.time.com/time/business/article/0,8599,1968233,00.html

Expiration dates could be implemented more broadly in various ways. Researchers at the University of Washington, for example, are developing a technology called Vanish that makes electronic data "self-destruct" after a specified period of time. Instead of relying on Google, Facebook or Hotmail to delete the data that is stored "in the cloud" — in other words, on their distributed servers — Vanish encrypts the data and then "shatters" the encryption key. To read the data, your computer has to put the pieces of the key back together, but they "erode" or "rust" as time passes, and after a certain point the document can no longer be read. The technology doesn't promise perfect control — you can't stop someone from copying your photos or Facebook chats during the period in which they are not encrypted. But as Vanish improves, it could bring us much closer to a world where our data don't linger forever.

Facebook, if it wanted to, could implement expiration dates on its own platform, making our data disappear after, say, three days or three months unless a user specified that he wanted it to linger forever. It might be a more welcome option for Facebook to encourage the development of Vanish-style apps that would allow individual users who are concerned about privacy to make their own data disappear without imposing the default on all Facebook users.

So far, however, Zuckerberg, Facebook's C.E.O., has been moving in the opposite direction — toward transparency, rather than privacy. In defending Facebook's recent decision to make the default for profile information about friends and relationship status public, Zuckerberg told the founder of the publication TechCrunch that Facebook had an obligation to reflect "current social norms" that favored exposure over privacy. "People have really gotten comfortable not only sharing more information and different kinds but more openly and with more people, and that social norm is just something that has evolved over time," [19] he said.

It's true that a German company, X-Pire, recently announced the launch of a Facebook app that will allow users automatically to erase designated photos. Using electronic keys that expire after short periods of time, and obtained by solving a Captcha, or graphic that requires users to type in a fixed number combinations, the application ensures that once the time stamp on the photo has expired, the key disappears.[20] X-Pire is a model for a sensible, blob-machine-like solution to the problem of digital forgetting. But unless Facebook builds X-Pire-like apps into its platform – an unlikely outcome given its commercial interests – a majority of Facebook users are unlikely to seek out disappearing data options until it's too late. X-Pire, therefore, may remain for the foreseeable future a technological solution to a grave privacy problem—but a solution that doesn't have an obvious

[19]Marshall Kirkpatrick, "Facebook's Zuckerbeg Says the Age of Privacy Is Over," *ReadWriteWeb.com*, January 9, 2010, available at http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php

[20] Aemon Malone, "X-Pire Aims to Cut down on Photo D-Tagging on Facebook," *Digital Trends.com*, January 17, 2011, available at http://www.digitaltrends.com/social-media/x-pire-adds-expiration-date-to-digital-photos/

market.

The courts, in my view, are better equipped to regulate offenses against autonomy, such as 24/7 surveillance on Facebook, than offenses against dignity, such as drunken Facebook pictures that never go away. But that regulation in both cases will likely turn on evolving social norms whose contours in twenty years are hard to predict.

Finally, let's consider one last example of the challenge of preserving constitutional values in the age of Facebook and Google, an example that concerns not privacy but free speech.[21]

At the moment, the person who arguably has more power than any other to determine who may speak and who may be heard around the globe isn't a king, president or Supreme Court justice. She is Nicole Wong, the deputy general counsel of Google, and her colleagues call her "The Decider." It is Wong who decides what controversial user-generated content goes down or stays up on YouTube and other applications owned by Google, including Blogger, the blog site; Picasa, the photo-sharing site; and Orkut, the social networking site. Wong and her colleagues also oversee Google's search engine: they decide what controversial material does and doesn't appear on the local search engines that Google maintains in many countries in the world, as well as on Google.com. As a result, Wong and her colleagues arguably have more influence over the contours of online expression than anyone else on the planet.

At the moment, Wong seems to be exercising that responsibility with sensitivity to the values of free speech. Google and Yahoo can be held liable outside the United States for indexing or directing users to content after having been notified that it was illegal in a foreign country. In the United States, by contrast, Internet service providers are protected from most lawsuits involving having hosted or linked to illegal user-generated content. As a consequence of these differing standards, Google has considerably less flexibility overseas than it does in the United States about content on its sites, and its "information must be free" ethos is being tested abroad.

For example, on the German and French default Google search engines, Google.de and Google.fr, you can't find Holocaust-denial sites that can be found on Google.com, because Holocaust denial is illegal in Germany and France. Broadly, Google has decided to comply with governmental requests to take down links on its national search engines to material that clearly violates national laws. But not every overseas case presents a clear violation of national law. In 2006, for example, protesters at a Google office in India demanded the removal of content on Orkut, the social networking site, that criticized Shiv Sena, a hard-line Hindu political party popular in Mumbai. Wong eventually decided to take down an Orkut group dedicated to attacking Shivaji, revered as a deity by the Shiv Sena Party, because it violated Orkut terms of service by criticizing a religion, but she

[21] The discussion of free speech that follows is adapted from "Google's Gatekeepers," *New York Times Magazine*, November 30, 2008.

decided not to take down another group because it merely criticized a political party. "If stuff is clearly illegal, we take that down, but if it's on the edge, you might push a country a little bit," Wong told me. "Free-speech law is always built on the edge, and in each country, the question is: Can you define what the edge is?"

Over the past couple of years, Google and its various applications have been blocked, to different degrees, by 24 countries. Blogger is blocked in Pakistan, for example, and Orkut in Saudi Arabia. Meanwhile, governments are increasingly pressuring telecom companies like Comcast and Verizon to block controversial speech at the network level. Europe and the U.S. recently agreed to require Internet service providers to identify and block child pornography, and in Europe there are growing demands for network-wide blocking of terrorist-incitement videos. As a result, Wong and her colleagues worry that Google's ability to make case-by-case decisions about what links and videos are accessible through Google's sites may be slowly circumvented, as countries are requiring the companies that give us access to the Internet to build top-down censorship into the network pipes.

It is not only foreign countries that are eager to restrict speech on Google and YouTube. In May, 2006, Joseph Lieberman who has become the A. Mitchell Palmer of the digital age, had his staff contacted Google and demanded that the company remove from YouTube dozens of what he described as jihadist videos. After viewing the videos one by one, Wong and her colleagues removed some of the videos but refused to remove those that they decided didn't violate YouTube guidelines. Lieberman wasn't satisfied. In an angry follow-up letter to Eric Schmidt, the C.E.O. of Google, Lieberman demanded that all content he characterized as being "produced by Islamist terrorist organizations" be immediately removed from YouTube as a matter of corporate judgment — even videos that didn't feature hate speech or violent content or violate U.S. law. Wong and her colleagues responded by saying, "YouTube encourages free speech and defends everyone's right to express unpopular points of view." Recently, Google and YouTube announced new guidelines prohibiting videos "intended to incite violence."

That category scrupulously tracks the Supreme Court's rigorous First Amendment doctrine, which says that speech can be banned only when it poses an imminent threat of producing serious lawless action. Unfortunately, Wong and her colleagues recently retreated from that bright line under further pressure from Lieberman. In November, 2010, YouTube added a new category that viewers can click to flag videos for removal: "promotes terrorism." There are 24 hours of video uploaded on YouTube every minute, and a series of categories viewers can use to request removal, including "violent or repulsive content" or inappropriate sexual content. Although hailed by Senator Lieberman, the new "promotes terrorism category" is potentially troubling because it goes beyond the narrow test of incitement to violence that YouTube had previously used to flag terrorism related videos for removal. YouTube's capitulation to Lieberman shows that a user generated system for enforcing community standards will never protect speech as

scrupulously as unelected judges enforcing strict rules about when speech can be viewed as a form of dangerous conduct.

Google remains a better guardian for free speech than internet companies like Facebook and Twitter, which have refused to join the Global Network Initiative, an industry-wide coalition committed to upholding free speech and privacy. But the recent capitulation of YouTube shows that Google's "trust us" model may not be a stable way of protecting free speech in the twenty-first century, even though the alternatives to trusting Google – such as authorizing national regulatory bodies around the globe to request the removal of controversial videos – might protect less speech than Google's "Decider" model currently does.

I'd like to conclude by stressing the complexity of protecting constitutional values like privacy and free speech in the age of Google and Facebook, which are not formally constrained by the Constitution. In each of my examples – 24/7 Facebook surveillance, blob machines, escaping your Facebook past, and promoting free speech on YouTube and Google -- it's possible to imagine a rule or technology that would protect free speech and privacy, while also preserving security—a blob-machine like solution. But in some areas, those blob-machine-like solutions are more likely, in practice, to be adopted then others. Engaged minorities may demand blob machines when they personally experience their own privacy being violated; but they may be less likely to rise up against the slow expansion of surveillance cameras, which transform expectations of privacy in public. Judges in the American system may be more likely to resist ubiquitous surveillance in the name of *Roe v. Wade*-style autonomy than they are to create a legal right to allow people to edit their Internet pasts, which relies on ideas of dignity that in turn require a social consensus that in America, at least, does not exist. As for free speech, it is being anxiously guarded for the moment by Google, but the tremendous pressures, from consumers and government are already making it hard to hold the line at removing only speech that threatens imminent lawless action.

In translating constitutional values in light of new technologies, it's always useful to ask: What would Brandeis do? Brandeis would never have tolerated unpragmatic abstractions, which have the effect of giving citizens less privacy in the age of cloud computing than they had during the founding era. In translating the Constitution into the challenges of our time, Brandeis would have considered it a duty actively to engage in the project of constitutional translation in order to preserve the Framers' values in a startlingly different technological world. But the task of translating constitutional values can't be left to judges alone: it also falls to regulators, legislators, technologists, and, ultimately, to politically engaged citizens. As Brandeis put it, "If we would guide by the light of reason, we must let our minds be bold."

Jeffrey Rosen is a nonresident senior fellow at the Brookings Institution, where he explores issues involving the future of technology and the Constitution. He is also a professor of law at The George Washington University and the legal affairs editor of The New Republic. His most recent book is The Supreme Court: The Personalities and Rivalries that Defined America. He also is the author of The Most Democratic Branch, The Naked Crowd, and The Unwanted Gaze. Rosen is a graduate of Harvard College, summa cum laude; Oxford University, where he was a Marshall Scholar; and Yale Law School.

Professor Rosen's essays and commentaries have appeared in the New York Times Magazine, The Atlantic Monthly, on National Public Radio, and in The New Yorker, where he has been a staff writer. The Chicago Tribune named him one of the 10 best magazine journalists in America and the L.A. Times called him, "the nation's most widely read and influential legal commentator." Professor Rosen lives in Washington, D.C., with his wife Christine Rosen and two sons.

Governance Studies
The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
www.brookings.edu/governance.aspx

Editors
Jeffrey Rosen
Benjamin Wittes

Production & Layout
John S Seo

E-mail your comments to gscomments@brookings.edu