THE ROBERT L. LEVINE DISTINGUISHED LECTURE

THE DECIDERS: THE FUTURE OF PRIVACY AND FREE SPEECH IN THE AGE OF FACEBOOK AND GOOGLE

*Jeffrey Rosen**

I would like to begin with a hypothetical, which in a few years may not be a hypothetical after all. I was at a conference at Google in 2007 and Andrew McLaughlin, then the head of public policy, said he expected that before long, Google will be asked to post online live feeds to all the public and private surveillance cameras in the world. If the feeds were linked and archived, then it would be possible to click on an image of anyone in the world and ubiquitously track their movements forward and backward in time, 24/7, for months or years.

A ubiquitous surveillance system like this is hardly implausible: it is easy to imagine public and governmental demand for it over the next few years, due to a combination of interest in social networking, voyeurism, and demand from national security agencies that insist that a linked camera system is necessary to protect us against terrorism.

If Google succumbed to the strong public demand and implemented an open-circuit television system, would it violate the Constitution? You might say that surveillance on Google poses no constitutional issues at all. According to the Supreme Court, the Fourth Amendment, which protects us against unreasonable searches and seizures, and the First Amendment, which protects free speech, only regulate the state, and Google is a private corporation.

But maybe the state-action problem is not so simple. If the government used Open Planet to track citizens for national security purposes and the platform integrated both publicly and privately owned camera systems, then according to current doctrine, there might be enough of a hook to create a kind of state action and some sort of Fourth or First Amendment issue.

* Jeffrey Rosen is a professor of law at George Washington Law School. He is also legal affairs editor of *The New Republic* and a nonresident Senior Fellow at the Brookings Institution. He is a co-editor, most recently, of CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE (2011). His remarks, delivered on February 8, 2011, have been lightly edited and augmented in light of recent developments.

Let us imagine that the Supreme Court holds that police surveillance of random citizens on Google is, in fact, a search regulated by the Fourth Amendment. Would the Court require a warrant before the government can track someone's movements on Google for a month? This is precisely the issue raised by *United States v. Jones*,[1] the most important privacy case of the decade, which the Court recently decided. The question in that case was whether the police, without a valid warrant, could surreptitiously place a Global Positioning System (GPS) device on the bottom of someone's car and monitor his or her movements, 24/7, for a month.[2]

The Court had the discretion, within the contours of existing doctrine, to rule any way it liked. On the one hand, the Court could have agreed with the Obama Administration, which came close to arguing in *Jones* that we have no expectation of privacy in public places. Three federal circuit courts took a similar position, and upheld the use of GPS tracking devices to monitor a person's movement in a car, holding simplistically that such tracking is not a search because we have no expectation of privacy in our public movements.[3] Because any of our neighbors or any member of the public could put a tail on us without implicating our Fourth Amendment protections, these courts have held, then virtual cameras can put a dragnet tail on us and survey all of our movements.

But this seems counterintuitive. Is it really possible that 24/7 surveillance of the public raises no Fourth Amendment issues? At the time of the framing of the Constitution, a far smaller invasion was held to be the paradigmatic example of a Fourth Amendment search—namely, the decision by King George's henchmen to break into the houses of colonists in search of the author of a seditious pamphlet.[4] That inspired the Fourth Amendment principle that our "persons, houses, papers, and effects" that our personal papers should be immune from general fishing expeditions. The search of private desk drawers was a dramatic invasion of privacy, but surely the possibility of being tracked 24/7 from door to door is an even greater invasion.

Justice Louis Brandeis, when evaluating the constitutionality of wiretapping, recognized that the invasion committed by listening in on a telephone conversation was so much greater in degree than even the general warrants that the framers feared. The Constitution had to be understood to take account of this new technology, he insisted, or else citizens would have less privacy in the age of the wires than they did at the time of the framing.[5] Brandeis's challenge becomes even more urgent when we are faced with

1. 132 S. Ct. 945 (2012).

2. *Id.*

3. *See* United States v. Marquez, 605 F.3d 604, 609 (8th Cir. 2010); United States v. Pineda-Moreno, 571 F.3d 1212, 1214–15 (9th Cir. 2010), *vacated*, --- S. Ct. ----, No. 10-7515, 2012 WL 538278 (Feb. 21, 2012); United States v. Garcia, 474 F.3d 994, 997–98 (7th Cir. 2007).

4. *See generally* Entick v. Carrington, 95 Eng. Rep. 807 (K.B. 1765).

5. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

the possibility of ubiquitous surveillance of our public movements in cars or on Google.

In *Jones*, the majority opinion by Justice Antonin Scalia emphasized that the GPS surveillance was a search because the police had to trespass on Jones's property interests when they attached the GPS device to his car. In a path-breaking concurring opinion, Justice Samuel Alito emphasized that there is a difference between long-term virtual surveillance, which requires a warrant, and short-term surveillance, which does not. Alito seems to have been influenced by the visionary opinion of Judge Douglas Ginsburg, the D.C. federal court judge who ruled in *Jones* that the warrantless GPS surveillance was unconstitutional. Ginsburg properly rejected the implausible analogy between GPS surveillance and surveillance by neighbors by noting, "the likelihood anyone will observe" all of your movements over the course of a month is "effectively nil."[6] Ginsburg also emphasized 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."[7]

Let us now imagine that we are in the year 2025. It is possible that the Court might be more ambitious, striking down 24/7 Google surveillance not only as an unreasonable search but also as a violation of the right to personal autonomy recognized in cases like *Planned Parenthood of Southeastern Pennsylvania v. Casey*[8] and *Lawrence v. Texas*.[9] We think of the right-to-privacy cases, beginning with *Griswold v. Connecticut*,[10] and culminating in *Roe v. Wade*[11] and *Lawrence*, as cases about sexual autonomy. But in *Lawrence* and *Casey*, Justice Anthony Kennedy, the most enthusiastic proponent of expansive autonomy reasoning, recognized a far more sweeping principle of personal autonomy that might well protect individuals from totalizing forms of ubiquitous surveillance. As Kennedy wrote in *Lawrence*, "[F]reedom extends beyond spatial bounds. Liberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct."[12]

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 has been invoked recently to call into question not only ubiquitous surveillance but also the constitutionality of health care reform. As framed by libertarian strategists, the health care lawsuits purport to be about federalism—that is, the proper balance between state and federal power.

Libertarians believe that neither the states nor the federal government should be able to force people to buy things they do not want to buy—

6. United States v. Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 9545.
7. *Id.* at 562.
8. 505 U.S. 833 (1992).
9. 539 U.S. 558 (2003).
10. 381 U.S. 479 (1965).
11. 410 U.S. 113 (1973).
12. *Lawrence*, 539 U.S. at 562.

whether broccoli or Chevy Impalas or health care. But in pressing the broccoli objection,[13] libertarians are not really objecting that the health care mandate represents a federal intrusion on states' rights; instead, they are making an argument about individual liberty. Unlike Randy Barnett, for example, Richard Epstein has argued candidly that the health care mandate violates a sweeping libertarian right of freedom of contract that constrains not only Congress but the states as well. To uphold the mandate, he wrote,

> invites the government to force me to buy everything from exercise machines to bicycles, because there is always some good that the coercive use of state authority can advance. The ironic point is that this is not a commerce clause argument as such, for in my view any state statute would be subject to the same objection.[14]

There is, in fact, a line of Supreme Court cases that says that neither the states nor the federal government should be able to interfere with the "freedom of contract" or force people to engage in unwanted economic transactions. They are associated with *Lochner v. New York*,[15] which struck down a New York law setting maximum hours for bakers on the grounds that individuals should be able to arrange their economic affairs without becoming "wards of the State."[16] Conservative opponents of *Roe v. Wade* have denounced *Lochner* because they believe that resurrecting a right to freedom of contract would encourage judges to enforce other rights not listed in the text of the Constitution, such as the right to privacy recognized in *Roe*.

As a logical matter, it is possible to imagine a libertarian Justice like Anthony Kennedy striking down the health care mandate, warrantless GPS tracking, and even warrantless FBI surveillance on Open Planet in the name of the right to personal autonomy recognized in *Roe*, *Casey*, and *Lawrence*. Given his fervent beliefs about the need to protect the relationship between parents and children, as well as individual autonomy to make major life decisions, it is not hard to imagine him being sympathetic to the claim that the health care mandate violates the right of individuals to make basic health care decisions for themselves and their families. It is even possible to imagine Kennedy, in the same Supreme Court Term, voting to strike down the health care mandate and warrantless GPS tracking and to recognize a right to gay marriage, all on the same ground that the "liberty presumes an autonomy of self."[17] But no other conservative Justice would join him: John Roberts, Samuel Alito, Antonin Scalia, and Clarence Thomas have all staked their judicial philosophies on the wrongness of

13. *See* Randy Barnett, *If Obamacare's Mandate Is Approved, Congress Can Require Anything*, WASH. EXAMINER (June 6, 2011), http://washingtonexaminer.com/opinion/op-eds/2011/06/if-obamacares-mandate-approved-congress-can-require-anything/40085.

14. *See* Richard Epstein, *Obamacare Is Now on the Ropes*, RICOCHET (Dec. 13, 2011, 12:01 PM), http://ricochet.com/main-feed/ObamaCare-is-Now-on-the-Ropes.

15. 198 U.S. 45 (1905).

16. *Id.* at 57.

17. *Lawrence*, 539 U.S. at 562.

Lochner and *Roe*. "Who says *Roe* must say *Lochner* and *Scott*," Robert Bork wrote in *The Tempting of America*.[18]

A reluctance to create an amorphous new right of personal autonomy, in other words, may have persuaded Justice Scalia and the conservative justices who joined him to rule narrowly in the *Jones* case, rather than joining Justice Alito's broader prohibition on warrantless long term surveillance. All this suggests that whether the Supreme Court in 2012 or 2025 recognizes a right to privacy in public places narrowly or broadly depends less on the logic of the Fourth and Fourteenth Amendment arguments on behalf of privacy than on the composition of the Court and on public sentiment. If the past is any guide, the Court's answer will largely depend on whether the public 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 spaces and in real space, that the public *demands* 24/7 global camera feeds on Google rather than protesting against them.

This is the broad thesis that I want to try to persuade you of this evening. In the age of Google and Facebook, technologies that thoughtfully balance privacy with free expression and other values can be imagined. But they are only likely to be adopted when engaged minorities of citizens have protested against poorly designed architectures and demanded better ones, helping to create a social consensus that the invasive designs are unreasonable. To persuade you of that thesis—that it is possible to design good technologies, but you need a social consensus to implement them—I want to offer three other examples: first, the example of body-scanning machines at airports; second, the example of the internet that never forgets our drunken Facebook pictures; and third, the example of videos on YouTube that are being taken up and taken down, not on the order of courts, but on the order of Google executives, who exercise far more power over speech than does the Supreme Court.

First, consider the body scanners that proliferated at airports around the world after 9/11. As early as 2004, the U.S. government was confronted with a simple choice: naked machines or blob machines. The naked machines, as their name suggests, reveal not only contraband, metal, or plastics concealed under clothing, but also graphic images of the naked body. By contrast, the blob machines offered a sexless avatar, complete with an arrow pointing to any suspicious areas. From the perspective of privacy, the choice between the naked machines and the blob machine was, as they say, a no brainer: both offered identical amounts of security, while the naked machine threatened privacy and the blob machine preserved it. For this reason, the handful of European airports that adopted body scanners after 9/11 demanded versions of the blob machine rather than the naked machine. Most European airport authorities refused, after concluding

18. *See* ROBERT BORK, THE TEMPTING OF AMERICA 32 (1990).

that the machines were not effective in detecting low-density powders, such as those used by the 2009 Christmas trouser bomber.[19]

The U.S. Department of Homeland Security made a very different decision. It deployed the naked body scanners without any opportunity for public comment, releasing privacy impact statements that refused to demand the blob machine. Then the department appeared shocked—shocked!—by the backlash that ensued.

Remarkably, however, the backlash was effective. After a nationwide protest inspired by someone who should be considered the Patrick Henry of the anti-naked machines movement—the traveler who memorably exclaimed, "Don't touch my junk"[20]—President Obama called on the TSA to go back to the drawing board.

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 machine that the agency had rejected nearly a decade earlier.[21] It subsequently decided to install filtering software at the 41 airports that use millimeter wave technology, although the airports that use backscatter machines remain unfiltered for now.[22]

This is a case, in other words, where political protest had an effect. Of course, it was not just political protest that created this relatively happy outcome, which can be described as one of modified rapture; the threat of lawsuits also helped. The Electronic Privacy Information Center (EPIC), where I am proud to be on the advisory board, filed a lawsuit challenging the naked machines as unreasonable, and as unconstitutional.[23] I think there is a strong, although not decisive, argument under existing doctrine that EPIC should win. A 1983 opinion by the Supreme Court, written by Justice Sandra Day O'Connor, approved the use of drug-sniffing dogs.[24] O'Connor writes that a search is most likely to be considered constitutionally reasonable if it is very effective in discovering contraband without revealing any innocent but embarrassing information.[25] So a dog sniff is perfect in that regard. In that sense, the backscatter machines—the naked machines—are the antithesis of a perfect or reasonable search. They reveal a great deal of innocent but embarrassing information and are remarkably ineffective at revealing low-density contraband.

---

19. *See* Anahad O'Connor & Eric Schmitt, *U.S. Says Plane Passenger Tried to Detonate Device*, N.Y. TIMES, Dec. 26, 2009, at A1.

20. *See generally* Catherine Saillant, *Traveler who Resisted TSA Pat-Down Is Glad His Moment of Fame Is Nearly Over*, L.A. TIMES (Nov. 19, 2010), http://articles.latimes.com/2010/nov/19/local/la-me-screening-tyner-20101119.

21. *See* Ashley Halsey III, *TSA Debuts System for More Modest Scans*, WASH. POST, Feb. 2, 2011, at A2.

22. *See* Ashley Halsey III, *TSA to Roll Out Less Revealing Scanner*, BOSTON.COM (July 21, 2011), http://articles.boston.com/2011-07-21/business/29798553_1_scanners-john-s-pistole-tsa-administrator.

23. Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec., No. 09-2084 (D.D.C. filed Jan. 12, 2011).

24. United States v. Place, 462 U.S. 696 (1983).

25. *Id.* at 707.

Although the Supreme Court has not evaluated airport screening technology, lower courts have insisted that particular screening searches are reasonable if they are no more extensive or intrusive than necessary, in light of current technology, to detect the presence of weapons or explosives. Then-Judge Alito, in 2006, reiterated that screening technology has to be effective and minimally intrusive,[26] and by those standards, you could well say that the naked machines fail both tests.

But I am not betting on a broad victory for EPIC because, once again, the Court seems to follow social norms when it comes to the Fourth Amendment. It recently struck down strip searches of a high school girl, 8-to-1, because there was a national outcry against searching young girls in high school for drugs on very low degrees of suspicion.[27] But the public outcry against the naked machines, although significant, still represents the views of a mobilized minority.

I do think, though, that the tentative victory of the blob machines over the naked machines provides a model for other successful attempts to balance privacy and security. A mobilized public can pressure the government into striking a reasonable balance when the privacy costs of a particular technology are dramatic, visible, and widely distributed. And people have to experience the invasions personally, as a kind of loss of control over the conditions of their own exposure. There is something about the fact that all travelers experienced this invasion so viscerally that made the protests ultimately successful.

Can citizens mobilize to demand a similarly reasonable balance when the threats to privacy come not from government, but from private corporations, like Google and Facebook, and when the parties responsible for exposing too much personal information are not the government, but ourselves? Here I am less confident. 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 a different value of privacy—namely, dignity. Remember that autonomy preserves a sphere of immunity from government intrusion into our lives. Dignity, by contrast, protects the norms of social respect that we accord to each other. Dignity is a socially constructed value. It varies tremendously by country and by society and by epoch. In Germany, it is considered a violation of dignity and law to give someone the finger on the highway. It is an offense against honor. Imagine how citizens in California would fare under a regime like that. By contrast, the French are much more concerned than Americans about being asked about their salaries.

It is foolish to generalize about international norms when it comes to dignity because they vary so much. But precisely because dignity is a socially constructed value, it is very difficult to preserve by judges or by private corporations in the face of the express preferences of citizens who are in fact less concerned about dignity than exposure.

---

26. United States v. Hartwell, 436 F.3d 174, 179–80 (3d Cir. 2006).
27. Safford Unified Sch. Dist. No. 1 v. Redding, 557 U.S. 364 (2009).

That leads to my second example, the drunken Facebook picture and the right to be forgotten. We are all familiar by now of the perils of posting ill-advised photos, chats, and status updates on the Web that can come back to haunt us. The paradigmatic example is Stacy Snyder, the young teacher-in-training in Pennsylvania,[28] who made the mistake of posting on her MySpace page a picture of herself carrying a plastic cup, wearing a pirate's hat, and posting the caption "Drunken Pirate." Her employer, the public high school where she taught, decided that she was promoting underage drinking and fired her as a result.[29] Her university, the day before her graduation, denied her a teaching degree.[30]

She sued, arguing that her First Amendment rights had been violated, and a judge rejected the claim on the grounds that because she was a public employee, her speech was not a matter of public concern, and therefore was not protected by the First Amendment.[31] As a result, Snyder never became a teacher. She is now working in human resources. Her career was derailed because of this one unfortunate picture.

In America, it is hard to formulate a legal remedy for the injury that Stacy Snyder suffered: an inability to escape her internet past. In 1890, in the most famous article on the right to privacy ever written, Samuel Warren and Louis Brandeis warned that because of new technologies like the Kodak camera and the tabloid press, gossip is no longer the resource of the idle and the vicious, but has now become a trade.[32]

Although the volume of gossip on the internet today is vastly greater than the gossip of the Gilded Age tabloids that worried Brandeis, the threatened injury is the same: dignity. Brandeis, of course, struggled to articulate the value, because American law, as he recognized, has no vocabulary of protecting dignity. Unlike Roman law, said Brandeis, we do not make cognizable offenses against honor.[33] Instead, Brandeis tried to propose a whole new series of torts, which sound like a delicious dessert but are actually a frustrating series of civil causes of action to regulate offenses against dignity. Because of a lack of social consensus about how much privacy is reasonable to expect, those torts have failed to gain adherents in the U.S., despite finding support elsewhere; according to one law review article, the Brandeis torts are "alive and well" and living in France.[34] That is just about the only place where you can still sue photographers for taking pictures of celebrities.

---

28. *See* Brett Lovelace, *Web Photo Haunts Graduate; MU Sued for Denying Degree*, INTELLIGENCER J., Apr. 27, 2007, at A1.

29. *Id.*

30. *Id.*

31. Snyder v. Millersville Univ., No. 07-1660, 2008 WL 5093140, at *14–16 (E.D. Pa. Dec. 3, 2008).

32. *See* Warren & Brandeis, *supra* note 5, at 195–96 ("Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery.").

33. *Id.* at 198.

34. Jeanne M. Hauch, *Protecting Private Facts in France: The Warren & Brandeis Tort Is Alive and Well and Flourishing in Paris*, 68 TUL. L. REV. 1219 (1994).

In Europe, efforts to create legal remedies for the indignity of being tethered to your past on the internet are far more ambitious. An early proposal came from Alex Türk, the French data privacy commissioner, who endorsed the creation of a "right to oblivion."[35] You know this is coming from France. It is straight out of Sartre. Americans want to be famous while the French want to be forgotten. How exactly this was supposed to be administered is not clear. Türk proposed creating some kind of international body, perhaps an "international commission of forgetfulness," which would evaluate, on a case-by-case basis, whether or not a particular request to take down a particular picture should be granted as an offense against the dignitary or moral rights of the offended individual. But the details remain murky.

More recently, Viviane Reding, the EU Commissioner of Justice and Vice President of the European Commission, proposed to codify the "right to be forgotten." In a speech at the Second Annual Data Protection Conference in Brussels in December 2011, she declared:

> I also want to establish the famous right to be forgotten, which will build on existing rules to better cope with privacy risks online. I believe this right is very important in a world of increased connectivity and the unlimited search and storage. If users no longer want their data to be stored, and if there is no good reason to keep it online anymore, the data should be removed.[36]

If the right to be forgotten is nothing more ambitious than a right to demand deletion of personally identifiable stored data after a period of time, then it would clarify (and provide an enforcement mechanism) for a principle of "data economy" already implicit in the European privacy directive.[37]

As proposed, however, the right to be forgotten seems to create a legal entitlement for people to remove photos they have posted voluntarily, even after those photos have been widely shared.[38] In this sense, it clashes dramatically with American notions of free expression. We have examples of this broader conception of the right to be forgotten in a recent decision from Argentina, which dramatically expanded the liability of search engines like Google and Yahoo for offensive photographs.[39] Last year, an Argentine judge held that Google and Yahoo were liable for moral harm

---

35. *See* Jeffrey Rosen, *The End of Forgetting*, N.Y. TIMES, July 25, 2010, at MM30.

36. *See* Viviane Reding, Vice-President of the Eur. Comm'n, Speech at the Second Annual European Data Protection and Privacy Conference, The Future of Data Protection and Transatlantic Cooperation (Dec. 6, 2011), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/851&format=HTML&aged=0&language=EN&guiLanguage=en.

37. Axel Spies, *Analysis: Reform of the EU Data Protection Directive: 'Right to Be Forgotten'—What Should Be Forgotten and How?*, GLOBAL L. WATCH (Dec. 21, 2011), http://www.globallawwatch.com/2011/12/analysis-reform-of-the-eu-data-protection-directive-right-to-be-forgotten-what-should-be-forgotten-and-how/.

38. *See* Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88 (2012), http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten.

39. *See* Vinod Sreeharsha, *Google and Yahoo Win Appeal in Argentine Case*, N.Y. TIMES, Aug. 20, 2010, at B4.

and violating the privacy of Virginia da Cunha—a pop star who unwisely posed for some racy pictures, which got posted on the internet, and thought the better of it.[40] These were not pornographic or obscene, and they were voluntarily posted.[41] But she changed her mind. She said, in effect, "My dignitary rights are violated. Take down the pictures." The Argentine judge agreed and ordered Google and Yahoo to take the pictures down. Essentially, Yahoo's response was, "Technologically, it is so hard for us to do this. We cannot selectively just remove these pictures, which have been widely shared. Instead, we are going to have to remove all references to this person entirely." When Argentinian users plug da Cunha into Yahoo today, they see a blank page and a judicial order.

The potentials for abuse of this right to be forgotten are obvious. Pop stars who take racy pictures often have a habit of running for political office, especially in Italy. You could well imagine a candidate on the campaign trail, thinking better of those youthful pictures and trying to remove all references to herself in order to protect herself from embarrassment.

Enforcement is also difficult. Against whom is the right of action? Just Google and Yahoo? Against faithless friends who share the photographs? Under what circumstances should photographs be left up in the public interest? Do we want a "commission of forgetfulness" to be making case-by-case determinations of what is in the public's interest to demand?

As Peter Fleischer, the Global Privacy Counsel at Google, has noted, the right to be forgotten is a sweeping concept that can include a series of very different claims.[42] The least controversial is the right to delete something I post online on my own Facebook page or album—a service that most platforms already provide. But the right to delete becomes more controversial if I post something and someone else copies it onto another site—as in the case of the widely circulated photos of the Argentinian pop star. Surely, Fleischer suggests, internet platforms should not be asked to delete pictures of me from someone else's album without the owner's consent.[43] Even more difficult, he notes, is the question whether I should have the right to delete truthful but embarrassing information that someone else posts about me—a request that squarely pits values of privacy against free speech.[44] And the question how to enforce different national judgments makes the problem still harder, as Fleischer notes: if a German court decides that German murderers should be able to delete evidence of their conviction after a specified time has passed, should that deletion apply only in Germany or across the globe, and who should enforce it?[45]

---

40. *Id.*
41. *Id.*
42. Peter Fleischer, *Foggy Thinking About Right to Oblivion*, PETER FLEISCHER: PRIVACY . . . ? (Mar. 9, 2011, 8:59 AM), http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html.
43. *Id.*
44. *Id.*
45. *Id.*

Given the complexity of asking courts to balance clashing values of free speech and privacy in a world where there is no agreement about what privacy demands, my instinct is that technological solutions here are more promising than legal ones. There is, for example, a blob machine-like solution to the Stacy Snyder problem—namely, disappearing data. There are already small-scale apps that allow your data to disappear. There is one called TigerText that allows you to put expiration dates on your text messages.[46] They can disappear in three days or three months, as the user specifies.

More recently, a German company called X-Pire[47] 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, obtained by solving a CAPTCHA, one of those graphics that are impossible to read where you have to type in fixed-number combinations. The application ensures that once the timestamp on the photo has expired, the key disappears. X-Pire is a model for sensible blob machine-like solutions to the problem of digital forgetting. But unless Facebook builds X-Pire-like apps into its platform—in a sense, making it a default option that people can easily access—the chance of citizens opting in on a broad scale seem low, and therefore disappearing data will not, in practice, become a norm. And unfortunately, here is a case where Facebook's financial interests clash dramatically with the blob machine-like solution that could protect privacy. Facebook has been moving in the opposite direction, toward transparency rather than privacy. In defending Facebook's decision to make the default for profile information public rather than private, Mark Zuckerberg said that Facebook had an obligation to reflect current social norms that favor exposure over privacy.[48]

That seems like precisely the wrong approach to this complicated problem. As we saw in the case of the blob machine and Google 24/7 surveillance, social norms are not something that Facebook reflects. On the contrary, Google and Facebook have a crucial role in shaping those social norms. The decision to architect X-Pire-like technologies—to make it easy to delete data you have posted on your own site—will itself have a more dramatic impact on the scope of the right to oblivion than any series of decisions made by international courts and regulatory bodies. This confirms, once again, the difficulty of imposing contested social norms on a fractious globe.

---

46. *See* Belinda Luscombe, *TigerText: An iPhone App for Cheating Spouses?*, TIME (Feb. 26, 2010), http://www.time.com/time/business/article/0,8599,1968233,00.html.

47. *See* X-PIRE, http://www.x-pire.de/ (last visited Feb. 23, 2012).

48. *See* Marshall Kirkpatrick, *Facebook's Zuckerberg Says the Age of Privacy Is Over*, READWRITEWEB (Jan. 9, 2010, 9:25 PM), http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php (quoting Zuckerberg as saying, "We view it as our role in the system to constantly be innovating and be updating what our system is to reflect what the current social norms are."). *See generally* Jose Antonio Vargas, *The Face of Facebook: Mark Zuckerberg Opens Up*, NEW YORKER, Sept. 20 2010, at 54, 63–64.

My final example has to do with free speech and takes us to the case of Google. I have argued so far that courts may be better equipped to regulate offenses against autonomy by 24/7 surveillance and Facebook than offenses against dignity, such as drunken Facebook pictures that never go away. But the regulation in both cases will turn on evolving social norms whose contours in twenty years, let alone five years, are hard to predict.

Until recently, the person who had more power to determine who may speak and who may be heard around the world was not a president or king or Supreme Court Justice. She was Nicole Wong, who was deputy general counsel at Google until her recent resignation. Her colleagues called her "the Decider."[49] Nicole Wong was the Decider, who was awoken in the middle of the night to decide what content goes up or comes down, not only on Google.com, not only on each of the national Googles that are operated around the world, such as Google.fr, Google.de, but also what goes up or comes down on YouTube, which Google bought in 2006.[50]

You might be uncomfortable with the idea of allowing a single woman, a Decider, to make these incredibly contextual and difficult free speech decisions for the globe, but the truth is that this Decider model, as inadequate as it may be, may be better than the alternatives. At the moment, there is tremendous pressure from repressive countries around the world, and from Western democracies, for network-wide blocking of videos. Comcast and Verizon are pressured to block child pornography at the internet level. In Europe, there are growing demands for network-wide blocking of terrorist incitement videos.

As Evgeny Morozov demonstrates in his compelling new book, *The Net Delusion*, repressive governments such as Iran and even Egypt can use the internet to constrict freedom rather than to expand it.[51] Contrary to the meliorism of cyber-utopians, the revolution will not, Morozov argues, be tweeted.

Wong deserves the respect of libertarian conservatives and civil libertarian liberals, for she was essentially codifying, as a matter of policy, the firm protection for speech that the Supreme Court recognized in the 1969 *Brandenburg v. Ohio* case.[52] But unfortunately, Wong and her colleagues recently retreated from that bright line under further pressure from Senator Joe Lieberman. Recently, YouTube added a new category that viewers can click to flag videos for removal: "promoting terrorism."[53] This is troubling, because it sweeps more broadly than the Supreme Court standard for regulating speech that incites violence, and YouTube's capitulation to Lieberman shows that a user-generated system for enforcing

49. Jeffrey Rosen, *Google's Gatekeepers*, N.Y. TIMES, Nov. 30, 2008, at MM50.

50. Andrew Ross Sorkin, *Dot-Com Boom Echoed in Deal to Buy YouTube*, N.Y. TIMES, Oct. 10, 2006, at A1.

51. EVGENY MOROZOV, THE NET DELUSION 134 (2011).

52. 395 U.S. 444 (1969).

53. *See* Brian Bennett, *YouTube Is Letting Users Decide on Terrorism-Related Videos*, L.A. TIMES (Dec. 12, 2010), http://articles.latimes.com/2010/dec/12/nation/la-na-youtube-terror-20101213.

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, which has refused to join the Global Network Initiative, an industry-wide coalition committed to upholding free speech and privacy.[54] The critic Lee Siegel suggests that in fifty years we may look back on Google as we now do on the East India Company, and if so, it may be with nostalgia for a Decider model that, for all its flaws, protected speech better than the available alternatives.[55]

But the 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—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. And of course, whether the Decider model can survive the relentless commercial pressures to monetize journalism, so that the most prominently displayed stories and videos are the ones most likely to provide effective platforms for selling ads to targeted users, remains to be seen.

So let me sum up. I have tried to stress the complexity of protecting constitutional values like privacy and free speech in the age of Google and Facebook, entities which are not formally constrained by the Constitution. On the one hand, I am trying to offer an optimistic story in each of my examples—24/7 Google surveillance, blob machines, escaping your Facebook past, and promoting free speech on YouTube and Google. In each of these cases, it is possible to imagine a rule or technology that would protect values like free speech and privacy in a changing world. We can imagine a constitutional prohibition on ubiquitous surveillance, a preference for blob machines over naked machines, an expansion of disappearing data technologies, and an enlightened leadership at companies like Google and Twitter that protects free speech rather than suppressing it.

But whether these good rules or technologies will in fact be adopted depends crucially on what sort of rules and technologies the public demands. The majority opinion in the *Jones* case ultimately ruled against GPS surveillance narrowly rather than broadly, in part because of a reluctance to create amorphous new rights of personal autonomy such as the one recognized in *Roe v. Wade*. It took political protests—the "Don't touch my junk" movement—to persuade the Obama Administration to turn its naked machines into blob machines. Facebook has reluctantly made it easier to delete data in the face of user demand (and legal threats from Europe), although it is still betting that the demand for privacy will be outweighed by the demand for exposure. And Google, despite its

54. GLOBAL NETWORK INITIATIVE, http://www.globalnetworkinitiative.org (last visited Feb. 23, 2012).

55. Lee Siegel, *Twitter Can't Save You*, N.Y. TIMES, Feb. 6, 2011, at BR14.

commitment to free expression, chose not to resist political demands to expand its categories of prohibited speech on YouTube. Those categories, of course, are ultimately enforced by users and therefore reflect community standards rather than resisting them.

Will citizens around the globe demand laws and technology that protect liberty rather than threatening it? The choice is ours.