In 1787, the philosopher Jeremy Bentham proposed the construction of a “Panopticon,” a circular building with cells along the outer walls and, at the center, a watchtower or “inspector’s lodge” from which all the cells could be seen but no one would know, at any given moment, due to a system of blinds and partitions, whether he was actually being observed. Bentham thought this design would be particularly suited to prisons but suggested it could also be applied to factories, hospitals, mental asylums, and schools. Not only would prisoners, workers, the ill, the insane, and students be subject to observation, but also—if the person in charge of the facility visited the inspector’s area—the warders, supervisors, caregivers, and teachers. The gradual adoption of this “inspection principle,” would, Bentham predicted, create “a new scene of things,” transforming the world into a place with “morals reformed, health preserved, industry invigorated, instruction diffused, public burdens lightened.”

The modern Panopticon is not a physical building, and it doesn’t require the threat of an inspector’s presence to be effective. Technological breakthroughs have made it easy to collect, store, and disseminate data on individuals, corporations, and even the government. With surveillance technology like closed-circuit television cameras and digital cameras now linked to the Internet, we have the means to implement Bentham’s inspection principle on a much vaster scale. What’s more, we have helped construct this new Panopticon, voluntarily giving up troves of personal information. We blog, tweet, and post what we are doing, thinking, and feeling. We allow friends and contacts,
and even strangers, to know where we are at any time. We sign away our privacy in exchange for the conveniences of modern living, giving corporations access to information about our financial circumstances and our spending habits, which will then be used to target us for ads or to analyze our consumer habits.

Then there is the information collected without our consent. Since 2001, the number of U.S. government organizations involved in spying on our own citizens, both at home and abroad, has grown rapidly. Every day, the National Security Agency intercepts 1.7 billion emails, phone calls, instant messages, bulletin-board postings, and other communications. This system houses information on thousands of U.S. citizens, many of them not accused of any wrongdoing. Not long ago, when traffic police stopped a driver they had to radio the station and wait while someone checked records. Now, handheld devices instantly call up a person’s Social Security number and license status, records of outstanding warrants, and even mug shots. The FBI can also cross-check your fingerprints against its digital archive of 96 million sets.

Yet the guarded have also struck back, in a sense, against their guardians, using organizations like WikiLeaks, which, according to its founder Julian Assange, has released more classified documents than the rest of the world’s media combined, to keep tabs on governments and corporations. When Assange gave the Guardian 250,000 confidential cables, he did so on a USB drive the size of your little finger. Efforts to close down the WikiLeaks website have proven futile, because the files are mirrored on hundreds of other sites. And in any case, WikiLeaks isn’t the only site revealing private information. An array of groups are able to release information anonymously. Governments, corporations, and other organizations interested in protecting privacy will strive to increase security, but they will also have to reckon with the likelihood that such measures are sometimes going to fail.

New technology has made greater openness possible, but has this openness made us better off? For those who think privacy is an inalienable right, the modern surveillance culture is a means of controlling behavior and stifling dissent. But perhaps the inspection principle, universally applied, could also be the perfection of democracy, the device that allows us to know what our governments are really doing, that keeps tabs on corporate abuses, and that protects our individual freedoms just as it subjects our personal lives to public scrutiny. In other words, will this technology be a form of tyranny or will it free us from tyranny? Will it upend democracy or strengthen it?

The standards of what we want to keep private and what we want to make public are constantly evolving. Over the course of Western history, we’ve developed a desire for more privacy, quite possibly as a status symbol, since an impoverished peasant could not afford a house with separate rooms. Today’s affluent Americans display their status not only by having a bedroom for each member of the family, plus one for guests, but also by having a bathroom for every bedroom, plus one for visitors so that they do not have to see the family’s personal effects. It wasn’t always this way. A seventeenth-century Japanese shunga depicts a man making love with his wife while their daughter kneels on the floor nearby, practicing calligraphy. The people of Tikopia, a Pacific island inhabited by Polynesians, “find it good to sleep side by side crowding each other, next to their children or their parents or their brothers and sisters, mixing sexes and generations,” according to the anthropologist Dorothy Lee. “[A]nd if a widow finds herself alone in her...
one-room house, she may adopt a child or a brother to allay her intolerable privacy.” The Gebusi people in New Guinea live in communal longhouses and are said to “shun privacy,” even showing reluctance to look at photos in which they are on their own.

With some social standards, the more people do something, the less risky it becomes for each individual. The first women to wear dresses that did not reach their knees were no doubt looked upon with disapproval, and may have risked unwanted sexual attention; but once many women were revealing more of their legs, the risks dissipated. So too with privacy: when millions of people are prepared to post personal information, doing so becomes less risky for everyone. And those collective, large-scale forfeitures of personal privacy have other benefits as well, as tens of thousands of Egyptians showed when they openly became fans of the Facebook page “We are all Khaled Said,” named after a young man who was beaten to death by police in Alexandria. The page became the online hub for the protests that forced the ouster of President Hosni Mubarak.

Whether Facebook and similar sites are reflecting a change in social norms about privacy or are actually driving that change, that half a billion are now on Facebook suggests that people believe the benefits of connecting with others, sharing information, networking, self-promoting, flirting, and bragging outweigh breaches of privacy that accompany such behavior. 

More difficult questions arise when the loss of privacy is not in any sense a choice. Bentham’s Panopticon has become a symbol of totalitarian intrusion. Michel Foucault described it as “the perfection of power.” We all know that the police can obtain phone records when seeking evidence of involvement in a crime, but most of us would be surprised by the frequency of such requests. Verizon alone receives 90,000 demands for information from law-enforcement agencies annually. Abuses have undoubtedly accompanied the recent increase in government surveillance. One glaring example is the case of Brandon Mayfield, an Oregon attorney and convert to Islam who was jailed on suspicion of involvement in the 2004 Madrid train bombings. After his arrest, Mayfield sued the government and persuaded a federal judge to declare the provision of the Patriot Act that the FBI used in investigating him unconstitutional. But as with most excesses of state power, the cause is not so much the investigative authority of the state as the state’s erroneous interpretation of the information it uncovers and the unwarranted detentions that come about as a result. If those same powers were used to foil another 9/11, most Americans would likely applaud.

There is always a danger that the information collected will be misused—whether by regimes seeking to silence opposition or by corporations seeking to profit from more detailed knowledge of their potential customers. The scale and technological sophistication of this data-gathering enterprise allow the government to intercept and store far more information than was possible for secret police of even the most totalitarian states of an earlier era, and the large number of people who have access to sensitive information increases the potential for misuse. As with any large-scale human activity, if enough people are involved eventually someone will do something corrupt or malicious. That’s a drawback to having more data gathered, but one that may well be outweighed by the benefits. We don’t really know how many terrorist plots have been foiled because

1 Including those involved in international operations relating to homeland security and intelligence, 854,000 people currently hold top-secret security clearances, according to the Washington Post.
of all this data-gathering? We have even less idea how many innocent Americans were initially suspected of terrorism but not arrested because the enhanced data-gathering permitted under the Patriot Act convinced law-enforcement agents of their innocence.

The degree to which a government is repressive does not turn on the methods by which it acquires information about its citizens, or the amount of data it retains. When regimes want to harass their opponents or suppress opposition, they find ways to do it, with or without electronic data. Under President Nixon, the administration used tax audits to harass those on his “enemies list.” That was mild compared with how “enemies” were handled during the dirty wars in Argentina, Guatemala, and Chile, and by the Stasi in East Germany. These repressive governments “disappeared” tens of thousands of dissidents, and they targeted their political enemies with what now seem impossibly cumbersome methods of collecting, storing, and sorting data. If such forms of abuse are rare in the United States, it is not because we have prevented the state from gathering electronic data about us. The crucial step in preventing a repressive government from misusing information is to have alert and well-informed citizens with a strong sense of right and wrong who work to keep the government democratic, open, just, and under the rule of law. The technological innovations used by governments and corporations to monitor citizens must be harnessed to monitor those very governments and corporations.

One of the first victories for citizen surveillance came in 1991, when George Holliday videotaped Los Angeles police officers beating Rodney King. Without that video, yet another LAPD assault on a black man would have passed unnoticed. Instead, racism and violence in police departments became a national issue, two officers went to prison, and King received $3.8 million in civil damages. Since then, videos and photographs, many of them taken on mobile phones, have captured innumerable crimes and injustices. Inverse surveillance—what Steve Mann, professor of computer engineering and proponent of wearing imaging devices, terms “sousveillance”—has become an effective way of informing the world of abuses of power.

We have seen the usefulness of sousveillance again this year in the Middle East, where the disclosure of thousands of diplomatic cables by WikiLeaks helped encourage the Tunisian and Egyptian revolutions, as well as the protest movements that spread to neighboring countries. Yet most government officials vehemently condemned the disclosure of state secrets. Secretary of State Hillary Clinton claimed that WikiLeaks’ revelations “tear at the fabric of the proper function of responsible government.” In February of this year, at George Washington University, she went further, saying that WikiLeaks had endangered human rights activists who had been in contact with U.S. diplomats, and rejecting the view that governments should conduct their work in full view of their citizens. As a counterexample, she pointed to U.S. efforts to secure nuclear material in the former Soviet states. Here, she claimed, confidentiality was necessary in order to avoid making it easier for terrorists or criminals to find the materials and steal them.

Clinton is right that it is not a good idea to make public the location of insecurely stored nuclear materials, but how much of diplomacy is like that? There may be some justifiable state secrets, but they certainly are few. For nearly all other dealings between nations, openness should be the norm. In any case, Clinton’s claim that WikiLeaks releases documents “without regard for the consequences” is, if not deliberately misleading, woefully ignorant. Assange and his colleagues have consistently stated that they are motivated by a belief that a more transparent government will
bring better consequences for all, and that leaking information has an inherent tendency toward greater justice, a view Assange laid out on his blog in December 2006, the month in which WikiLeaks published its first document:

The more secretive or unjust an organization is, the more leaks induce fear and paranoia in its leadership and planning committees. Since unjust systems, by their nature induce opponents, and in many places barely have the upper hand, leaking leaves them exquisitely vulnerable to those who seek to replace them with more open forms of governance.1

Assange could now claim that WikiLeaks’ disclosures have confirmed his theory. For instance, in 2007, months before a national election, WikiLeaks posted a report on corruption commissioned but not released by the Kenyan government. According to Assange, a Kenyan intelligence official found that the leaked report changed the minds of 10 percent of Kenyan voters, enough to shift the outcome of the election.

Two years later, in the aftermath of the global financial crisis, WikiLeaks released documents on dealings by Iceland’s Kaupthing Bank, showing that the institution made multibillion-dollar loans, in some cases unsecured, to its major shareholders shortly before it collapsed. Kaupthing’s successor, then known as New Kaupthing, obtained an injunction to prevent Iceland’s national television network from reporting on the leaked documents but failed to prevent their dissemination. WikiLeaks’ revelations stirred an uproar in the Icelandic parliament, which then voted unanimously to strengthen free speech and establish an international prize for freedom of expression. Senior officials of the bank are now facing criminal charges.

And of course, in April 2010, WikiLeaks released thirty-eight minutes of classified cockpit-video footage of two U.S. Army helicopters over a Baghdad suburb. The video showed the helicopter crews engaging in an attack on civilians that killed eighteen people, including two Reuters journalists, and wounded two children. Ever since the attack took place, in 2007, Reuters had unsuccessfully sought a U.S. military inquiry into the deaths of its two employees, as well as access to the cockpit video under the Freedom of Information Act. The United States had claimed that the two journalists were killed during a firefight. Although no action has been taken against the soldiers involved, if the military is ever going to exercise greater restraint when civilian lives are at risk, it will have been compelled to do so through the release of material like this.

Months before the Arab Spring began, Assange was asked whether he would release the trove of secret diplomatic cables that he was rumored to have obtained. Assange said he would, and gave this reason: “These sort of things reveal what the true state of, say, Arab governments are like, the true human rights abuses in those governments.” As one young Tunisian wrote to the Guardian, his countrymen had known for many years that their leaders were corrupt, but that was not the same as reading the full details of particular incidents, rounded off with statements by American diplomats that corruption was keeping domestic investment low and unemployment high. The success of Tunisia’s revolution undoubtedly influenced the rest of the Arab world, putting U.S. diplomats in an uncomfortable predicament. A mere three months after condemning WikiLeaks for releasing stolen documents “without regard to the consequences,” Secretary Clinton found herself speaking warmly about one of those outcomes: the movement for reform in the Middle East.

WikiLeaks’ revelations have had profound ramifications, but as with any event of this scale, it is not
easy to judge whether those consequences are, on the whole, desirable. Assange himself admitted to the Guardian that as a result of the leaked corruption report in Kenya, and the violence that swept the country during its elections, 1,300 people were killed and 350,000 displaced; but, he added, 40,000 Kenyan children die every year from malaria, and these and many more are dying because of the role corruption plays in keeping Kenyans poor. The Kenyan people, Assange believes, had a right to the information in the leaked report because “decision-making that is based upon lies or ignorance can’t lead to a good conclusion.”

In making that claim, Assange aligned himself with a widely held view in democratic theory, and a standard argument for freedom of speech: elections can express the will of the people only if the people are reasonably well informed about the issues on which they base their votes. That does not mean that decision-making based on the truth always leads to better outcomes than decision-making based on ignorance. There is no reason for Assange to be committed to that claim, any more than a supporter of democracy must be committed to the claim that democratic forms of government always reach better decisions than authoritarian regimes. Nor does a belief in the benefits of transparency imply that people must know the truth about everything; but it does suggest that more information is generally better, and so provides grounds for a presumption against withholding the truth.

What of Clinton’s claims that the leaks have endangered human rights activists who gave information to American diplomats? When WikiLeaks released 70,000 documents about the war in Afghanistan, in July 2010, Admiral Mike Mullen, chairman of the Joint Chiefs of Staff, said that Assange had blood on his hands, yet no casualties resulting from the leaks have been reported—unless you count the ambassadors forced to step down due to embarrassing revelations. Four months after the documents were released, a senior NATO official told CNN that there had not been a single case of an Afghan needing protection because of the leaks. Of course, that may have been “just pure luck,” as Daniel Domscheit-Berg, a WikiLeaks defector, told the New York Times in February. Assange himself has admitted that he cannot guarantee that the leaks will not cost lives, but in his view the likelihood that they will save lives justifies the risk.

WikiLeaks has never released the kind of information that Clinton pointed to in defending the need for secrecy. Still, there are other groups out there, such as the Russian anti-corruption site Rospilinfo, the European Union site BrusselsLeaks, the Czech PirateLeaks, Anonymous, and so on, that release leaked materials with less scrupulousness. It is entirely possible that there will be leaks that everyone will regret. Yet given that the leaked materials on the wars in Afghanistan and Iraq show tens of thousands of civilian lives lost due to the needless, reckless, and even callous actions of members of the U.S. military, it is impossible to listen to U.S. leaders blame WikiLeaks for endangering innocent lives without hearing the tinkle of shattering glass houses.

In the Panopticon, of course, transparency would not be limited to governments. Animal rights advocates have long said that if slaughterhouses had glass walls, more people would become vegetarian, and seeing the factory farms in which most of the meat, eggs, and milk we consume are produced would be more shocking even than the slaughterhouses. And why should restaurant customers have to rely on occasional visits by health inspectors? Webcams in food-preparation areas could provide additional opportunities for checking on the sanitary conditions of the food we are about to eat.

Bentham may have been right when he suggested that if we all knew that we were, at any time, liable to be observed, our morals would be reformed. Melissa Batey and her colleagues at England’s Newcastle University tested this theory when they put a poster with a pair of eyes above a canteen honesty box. People taking a hot drink put almost three times as much money in the box with the eyes present as they did when the eyes were replaced by a poster of flowers. The mere suggestion that someone was watching encouraged greater honesty. (Assuming that the eyes did not lead people to overpay, the study also implies a disturbing level of routine dishonesty.)

We might also become more altruistic. Dale Miller, a professor of organizational behavior at Stanford University, has pointed out that Americans assume a “norm of self-interest” that makes acting altruistically seem odd or even irrational. Yet Americans perform altruistic acts all the time, and bringing those acts to light might break down the norm that curtails our generosity. Consistent with that hypothesis, researchers at the University of Pennsylvania found that people are likely to give more to listener-sponsored radio stations when they are told that other callers are giving above-average donations. Similarly, when utility companies send customers a comparison of their energy use with the average in their neighborhood, customers with above-average use reduce their consumption.

The world before WikiLeaks and Facebook may have seemed a more secure place, but to say whether it was a better world is much more difficult. Will fewer children ultimately die from poverty in Kenya because WikiLeaks released the report on corruption? Will life in the Middle East improve as a result of the revolutions to which WikiLeaks and social media contributed? As the Chinese communist leader Zhou Enlai responded when asked his opinion of the French Revolution of 1789, it is too soon to say. The way we answer the question will depend on whether we share Assange’s belief that decision-making leads to better outcomes when based on the truth than when based on lies and ignorance.