THE FIRST AMENDMENT IS AN INFORMATION POLICY

*Jack M. Balkin**

I. INFORMATION POLICY AND INFRASTRUCTURE

Inscribed on the main post office in New York City there is a famous motto: "Neither snow nor rain nor heat nor gloom of night stays these couriers from the swift completion of their appointed rounds."[1] It has become the unofficial slogan of the U.S. Post Office.[2] But the Post Office did not invent this famous saying. It is from the Greek historian Herodotus.[3] He was describing an elaborate system of horseback messengers created by the Persian monarchs to keep in touch with the reaches of their vast empire.[4] Herodotus reports that the great Persian King Xerxes used the couriers to report back to the capital that he had lost a major battle.[5]

Xerxes's system of couriers was an early form of what we might call a *knowledge and information policy*. Persian kings needed a reliable system for sending information securely across vast distances. So they created an ancient version of the Internet for their personal use.

All states throughout history have had knowledge and information policies. The earliest goals of these policies were to maintain state power, to execute military campaigns, to engage in surveillance and espionage, and to promote national security. Every nation-state in the

---

* Knight Professor of Constitutional Law and the First Amendment, Yale Law School. This Essay is based on remarks given at the 20th Annual Hugo L. Black Lecture on Freedom of Expression, at Wesleyan University on March 23, 2011. The lecture's title is a play on Alexander Meiklejohn's famous essay, "The First Amendment Is an Absolute." Alexander Meiklejohn, *The First Amendment Is an Absolute*, 1961 SUP. CT. REV. 245.

1. HISTORIAN, U.S. POSTAL SERV., POSTAL SERVICE MISSION AND "MOTTO" (1999), *available at* http://about.usps.com/who-we-are/postal-history/mission-motto.pdf.

2. *See id.*

3. *See* HERODOTUS, THE HISTORY 592 (David Grene trans., Univ. of Chicago Press 1987).

4. *See id.*

5. *See id.* at 591-92.

world today, whether democratic or authoritarian, has knowledge and information policies, even though the technologies have changed greatly from King Xerxes's day.

Most governments in the history of the world, like Xerxes's Persia, have been autocratic. Control over information, technologies of communication, even the education of the public, have been designed to serve the interests of the ruling classes.

The emergence of democracies changed the purpose of knowledge and information policy. In a democracy, sovereignty rests in the people. But if the people are the rulers, they need information in order to hold their representatives accountable. The public needs access to information about public issues, and about what government officials are doing in their name; it needs relatively inexpensive ways to communicate with other citizens, organize, discuss, protest, and form public opinion. In a democracy, political legitimacy necessarily depends on the free flow of information, and on the maintenance of a robust public sphere of discussion and opinion. In fact, the first democracy in Ancient Athens also pioneered techniques for spreading information among its citizens.[6]

The Framers of the U.S. Constitution were men of the Enlightenment. They assumed that representative government required people to be able to debate public issues; they believed that the growth and spread of science, art, and learning would benefit society and increase practical freedom. They understood that democratic self-government depends on a democratic knowledge and information policy.

Even before the First Amendment and the Bill of Rights were added in 1791, these Enlightenment ideas influenced the design of the 1787 Constitution. Article I, Section 8, gives Congress the power "[t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[7] The Progress Clause was designed to decentralize and democratize innovation and information production. Instead of relying on royal patronage to generate art and science, or tie up innovation through royal favoritism and crown monopolies, Congress wanted to use markets to create incentives for intellectual production and diffusion of knowledge. For the founders, the purpose of intellectual property was to serve democratic values and generate a truly democratic culture.[8]

---

6. *See* JOSIAH OBER, DEMOCRACY AND KNOWLEDGE: INNOVATION AND LEARNING IN CLASSICAL ATHENS 26-38 (2008) (explaining how Athenian democracy developed techniques for collecting and distributing valuable information and promoting social learning).

7. U.S. CONST. art. I, § 8, cl. 8.

8. *See* Neil Weinstock Netanel, *Copyright and a Democratic Civil Society*, 106 YALE L.J.

The 1787 Constitution also gives Congress the power "[t]o establish Post Offices and post Roads."[9] A democracy, especially one extending over such a large area, needed people to stay in touch with each other, not just with government officials. Good roads and a good mail system were essential to self-government in a large republic.

Two of the most important early decisions by the new national government involved knowledge and information policies. Anuj Desai has written about their history.[10] At the time of the founding, newspapers were often delivered by mail to different parts of the country. Congress created a special postal rate for newspapers to encourage the spread of news and opinion, educate the public, and promote communication of ideas and political cohesion throughout the republic. Congress imposed higher rates on business and personal correspondence to subsidize lower rates for newspaper delivery. A version of this cross-subsidy exists today, although it has largely outlived its usefulness because most people no longer get their newspapers delivered by mail.

The second major decision, also ratified in the 1792 Postal Service Act, was data security; when mail was delivered by the U.S. Postal Service, government officials could not look inside people's mail without a warrant.[11] Although the official English practice was that postal officers would not read private correspondence, it was not always followed, and during the Revolution people feared that insecure mail would lead to discovery that they were disloyal to the British crown.[12] European absolute monarchs probably felt even less compunction than British civil servants about opening and reading the correspondence of their subjects. By protecting informational privacy, this early policy also protected conscience and free expression. This principle is not recognized as a constitutional guarantee until many years later. It starts, however, as an information policy of the early American Republic that,

---

283, 289 (1996) ("In adopting the Constitution's Copyright Clause and enacting the first federal copyright statute, the Framers were animated by the belief that copyright's support for the diffusion of knowledge is 'essential to the preservation of a free Constitution.'" (footnote omitted)).

9. U.S. CONST. art. I, § 8, cl. 7.

10. *See generally* Anuj C. Desai, *The Transformation of Statutes into Constitutional Law: How Early Post Office Policy Shaped Modern First Amendment Doctrine*, 58 HASTINGS L.J. 671 (2007); Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 STAN. L. REV. 553 (2007) [hereinafter Desai, *Wiretapping*].

11. Desai, *Wiretapping*, *supra* note 10, at 566 ("When Congress passed its first comprehensive postal statute in 1792, the confidentiality of the contents of sealed correspondence was again written into law.").

12. *See id.* at 563-64 ("[B]y 1773, the Americans clearly worried, and had good reason to worry, that loyalist postmasters would intercept and read their letters, a frightening prospect when much of what they were doing likely constituted treason.").

together with postal subsidies and post roads, creates the beginnings of what I will call an *infrastructure of free expression*.[13]

II. DEMOCRATIC VERSUS AUTHORITARIAN INFORMATION POLICIES

It is not an exaggeration to say that modern states are *informational states*: states that recognize and solve problems of governance by collecting, analyzing, and distributing information. Knowledge and information policy is at the heart of government today.

Knowledge and information policy is about far more than the protection of free expression. Modern governments provide social services and benefits to their citizens, like social security, Medicare, and veterans' pensions. This requires vast data processing systems to compile statistics and distribute benefits. Modern citizenship requires data processing in order to distribute the benefits of citizenship, and this leads to the creation of vast government databases, which, in turn, creates the need for privacy regulation, another important information policy. Governments also invest heavily in public education because it is crucial to democratic citizenship. Governments subsidize the production of information, like agricultural and weather information, as well as geographical data. And, especially in the United States, governments subsidize most basic scientific research.

You might think that information states must tend toward democracy. But it is not so. East Germany had an enormous information collection apparatus—the Stasi—but it certainly was not democratic. Today, China's knowledge and information policies are designed to keep the Chinese Communist Party in power while growing China's economy.

The big choice we face today is between *democratic* information states and *authoritarian* information states.[14] Different countries lie on a spectrum between these two ideal types.

Authoritarian information states are information gluttons, information misers, and information monopolists. They try to collect as much information as they can, but they do not share it with their people. They try to monopolize control over information in order to serve the interests of those in power.

---

13. *See* Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1, 6, 51-55 (2004) (describing the infrastructure of free expression); Jack M. Balkin, *The Future of Free Expression in a Digital Age*, 36 PEPP. L. REV. 427, 432 (2009) [hereinafter Balkin, *Future*] ("A system of free speech depends not only on the mere absence of state censorship, but also on an infrastructure of free expression.").

14. Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 17-18 (2008) (distinguishing between democratic and authoritarian information states).

Democratic information states, by contrast, are information gourmets, information philanthropists, and information decentralizers. They collect only the information they need for governance, and they do not keep information secret any longer than necessary. They not only willingly share information with their citizens, they also create information and knowledge for their citizens to use and enjoy. Democratic information states try to ensure that their citizens have ample opportunities for education; they promote *access to knowledge and information* in order to form public opinion and to keep government officials in check. Democratic information states also *decentralize* the production of knowledge and information because this promotes democratic self-government.

Many people are optimistic that the Internet and the digital age will make authoritarian government increasingly difficult if not impossible. I am not so sure. In fact, as I will describe shortly, it is possible for authoritarian states to use the Internet and digital technologies to create digital versions of authoritarian information states. More troublingly, it is also possible that the Internet will tempt democracies like the United States to adopt increasingly authoritarian knowledge and information policies out of fear of terrorism and in order to protect interests in intellectual property.

Justice Hugo Black gave a pretty good account of a knowledge and information policy for a democracy. In a 1945 case called *Associated Press v. United States*,[15] he argued that "the widest possible dissemination of information from diverse and antagonistic sources is essential to the welfare of the public, [and] that a free press is a condition of a free society."[16] "Diverse" means that we should decentralize information production and information distribution. No one entity should control knowledge production, many people must participate in creating information, and it should be widely distributed. "Antagonistic" means that knowledge production should be structured to allow the clash of different viewpoints, and to encourage dissent and innovation. Therefore, governments should protect and foster institutions, like the press, universities, and scientific research, that can check facts, produce new forms of knowledge, and help guarantee the quality and salience of information.

Associated Press involved an agreement by newspapers to limit access to information to their members and create barriers to entry by

15. 326 U.S. 1 (1945).
16. *Id.* at 20.

other news organizations.[17] The members of the Associated Press argued that as members of the media, they had a First Amendment right to do so.[18]

Justice Black disagreed. The Associated Press was using its monopoly power to stifle competition in the gathering and dissemination of news. Justice Black argued that the same values that prevented the government from restricting the flow of information also gave it the right to regulate powerful private interests when they interfered with "the widest possible dissemination of information from diverse and antagonistic sources."[19] As Justice Black put it, "[i]t would be strange indeed . . . if the grave concern for freedom of the press which prompted adoption of the First Amendment should be read as a command that the government was without power to protect that freedom."[20] Justice Black explained:

> Surely a command that the government itself shall not impede the free flow of ideas does not afford non-governmental combinations a refuge if they impose restraints upon that constitutionally guaranteed freedom. Freedom to publish means freedom for all and not for some. Freedom to publish is guaranteed by the Constitution, but freedom to combine to keep others from publishing is not.[21]

Today we live in a world of large and powerful corporations that shape and control the production and flow of knowledge. Many of these players now use the First Amendment to challenge regulation of their business models and to limit competition in the marketplace of ideas. Justice Black's opinion in *Associated Press* reminds us that the First Amendment protects speech, not incumbent business models. Government regulation that decentralizes control over innovation and knowledge production does not necessarily violate the First Amendment and may even be required to promote its central values. As Justice Black put it, "Freedom of the press from governmental interference under the First Amendment does not sanction repression of that freedom by private interests."[22]

---

17. *Id.* at 4.
18. *See id.* at 19.
19. *Id.* at 20.
20. *Id.*
21. *Id.*
22. *Id.*

III. TWO BIG IDEAS

There are two big ideas that I want you to take away from this Essay. The first is that it is important to think in terms of *knowledge and information policy*.[23] Think about our valued individual liberties of freedom of speech, press, and assembly not in isolation, but in the larger context of policies for the spread and growth of knowledge and information.

We usually talk about the First Amendment not as a policy but as an individual right. But I also want you to see it as an integral part of knowledge and information policy. Why? Because many parts of information policy cannot easily be cashed out in terms of individual rights. You do not have an individual right to have the government create public libraries. The Constitution did not require the early Congress to subsidize newspaper delivery. You do not have an individual right to government decisions about how much to invest in science in fiscal year 2011. You do not have an individual right to have fiber optic cable brought to your neighborhood, or to have particular frequencies of the electromagnetic spectrum sold at auction, handed out in the form of licenses, or made into a commons for spread-spectrum technologies. These are policy choices. They are decisions about institutions and technological design. And they are crucial to your practical ability to speak in a digital world.

The second big idea is that individual freedoms of speech, press, and assembly require *an infrastructure of free expression*.[24] That infrastructure includes technologies of communication, policies that promote innovation and diffusion of knowledge, the institutions of civil society that create knowledge and help ensure its quality, and government and private investments in science, education, and communications technology.

I began this Essay with the example of an infrastructure built by a Persian monarch. These days, however, the infrastructure of free expression is not primarily controlled by kings and dictators. Increasingly it is in the hands of powerful private corporations like Facebook, Google, Yahoo, Verizon, Comcast, and Cisco; they create and

---

23. Balkin, *Future*, *supra* note 13, at 428 ("In the twenty-first century . . . the future of the system of free expression will require other sources of assistance. . . . [T]he values of freedom of expression will become subsumed under an even larger set of concerns that I call knowledge and information policy.").

24. *See id.* at 432.

maintain the architectures, networks, and platforms through which everyone else communicates.

In fact, governments often work in cooperation with the companies that control digital content and digital telecommunications networks. Knowledge and information policy—and power over knowledge and information—is increasingly the product of coordination between state power and private power.

How are these two ideas—information policy and infrastructure—related? Think about the title of this Essay: *The First Amendment Is an Information Policy*. What I mean is this: The First Amendment is a crucial information policy in a democracy, but it is also only one information policy among many others. Constitutional guarantees of free expression are a necessary part of knowledge and information policy for a democratic information state, but they are not sufficient. To understand free expression in the digital age, we must grasp this central truth. Good policy and good design promote democracy and a democratic culture; bad policy and bad design foster oligarchy, aristocracy, and even totalitarianism.

I want to offer two examples of how the infrastructure of free expression is crucial to democracy in the Internet age. Both of them take place outside of the United States. Both of them show the powerful role of infrastructure in a networked world. And both of them serve as lessons for why we must keep our own infrastructure of expression free and open in this country.

IV. THE INFRASTRUCTURE OF DEMOCRATIC PROTESTS

My first example takes place where King Xerxes implemented his information policy thousands of years ago: in the Middle East, including King Xerxes's own kingdom of Persia, which is now called Iran.

In 2009 following a disputed election, Iranian citizens took to the streets in massive protests, which took months for the government to subdue. The unrest is sometimes called the "Twitter Revolution," because social media like Twitter, Facebook, and YouTube played a prominent role. In late 2010, massive protests began in Tunisia, and in late January 2011, protests broke out in Egypt, and spread to about a dozen countries around the Middle East, including Iran.

The infrastructure of free expression—in this case, digital networks and software platforms—played an important role in these uprisings; so much so that Egypt shut down access to the Internet and cell phones for about five days. By that point in the uprising, however, it was too late. Reporters were already in Egypt, mass-media coverage by Al Jazeera

and other broadcasters continued, and a few Egyptians still found ways to communicate with the outside world.

If anything, the protests merely got worse after the government tried to flip the Internet kill switch. Egyptians were outraged by the loss of communications. Business interests objected vehemently, and access was soon restored. Egypt's long-time strong man, Hosni Mubarak, was forced out of office, and the Egyptian military took control of a caretaker government.

We do not yet know whether the January 2011 revolution will lead to real democracy in Egypt. Nor do we know what will happen in the various other Middle Eastern countries where protests have sprung up. What we can ask is what role the infrastructure of free expression, and control over that infrastructure, have played.

People tend to think of democracy as a single thing, but it is actually a set of interconnected activities: deliberating, debating, spreading information, organizing like-minded individuals, forming and maintaining political parties and civil society organizations, protesting, petitioning, picketing, voting in elections, and governing. Changes in technology and infrastructure make some of these activities of democracy harder or easier, more expensive or less expensive, easier to control or harder to control. To understand how the Internet affects democracy, always ask: How does technology affect specific or particular activities of democracy? Does it make them more prominent or less prominent, easier or harder, less costly or more costly, less vulnerable, or more vulnerable to centralized control?

Since the 2009 Twitter Revolution there has been almost continuous debate about whether the Internet or digital technologies "caused" the uprisings in the Middle East.[25] It is unhelpful to debate the question in these terms. At the risk of oversimplification, there are two basic ingredients to democratic revolutions: grievances and courage. First, people must have a felt sense that the regime has treated its citizens badly, and second, people must be willing to stand up to the regime and risk ostracism or punishment. These two factors interact. The grievances

25. For a sampling of different views on this question, see, e.g., Sarah Joseph, *Social Media, Political Change, and Human Rights*, 35 B.C. INT'L & COMP. L. REV. 145 (2012); Malcolm Gladwell, *Small Change: Why the Revolution Will Not Be Tweeted*, NEW YORKER, Oct. 4, 2010, at 42; C.W. Anderson, *Tech and Social Movements: Beyond 'Did Twitter Cause the Tunisian Uprising?,'* ATLANTIC (Jan. 14, 2011, 4:17 PM), http://www.theatlantic.com/technology/archive/2011/01/tech-and-social-movements-beyond-did-twitter-cause-the-tunisian-uprising/69616/; Tom Chatfield, *The Net Delusion: How Not to Liberate the World by Evgeny Morozov–Review*, OBSERVER (Jan. 8, 2011), http://www.guardian.co.uk/books/2011/jan/09/net-delusion-morozov-review; Clay Shirky, *The Political Power of Social Media*, FOREIGN AFFAIRS (Jan./Feb. 2011), http://www.foreignaffairs.com/articles/67038/clay-shirky/the-political-power-of-social-media.

have to be bad enough that people feel it is worth taking action; courage is necessary because protests pose a problem of collective action. One lonely protester, or a small number of protesters will easily be crushed: they will quickly be arrested, severely punished, or never heard from again. People are more likely to take to the streets if they believe that others will do so as well. They are more likely to take risks if there is strength in numbers. Hence democratic protests, especially in unjust regimes, present a problem of collective action that needs to be solved.

These basic issues are as relevant to the uprising of 1776 as the uprisings of 2011. We should ask how digital technology affected the formation and the experience of grievance and courage, how it helped solve problems of collective action, how it could be employed in organizing and conveying information about popular uprisings, and, equally important, how governments in the future will likely react to these changes.

I just compared the problems faced by Egyptian protestors today with the problems faced by the colonists in 1776. But there is an important difference. In 1776, American colonists were armed with weapons almost as powerful as the government's. They could form citizen militias. That's not true today in most autocratic states. Often citizens can easily be plowed down by government troops if the rulers are truly determined to restore order. In fact, often what differentiates successful from unsuccessful protests is whether the protesters can manage to get the army or the police force on their side, or at least persuade the government not to use force against them. If the government is sufficiently ruthless, however, and believes that the outside world is not paying attention or does not care, then the protests will probably be crushed. To succeed, lots of people must know about the protests, and it is even better if there are pictures or video, making it difficult for the government to attack and suppress protestors. This is the media strategy of Mahatma Gandhi and Martin Luther King, Jr.

Mass-media coverage, especially visual coverage, is crucial to the success of this strategy. If the government overreacts, media will broadcast the events around the country and around the world. The ultimate goal is to use the power of social norms and public opinion to put the army in a position where it will refuse to attack the citizens, so that the regime loses power. This is a dangerous strategy and not always successful. This is more or less what happened in Egypt in 2011, but it did not happen in China during the Tiananmen Square Massacre in 1989, and it did not happen in the recent protests in several of the other Middle Eastern states.

How do the Internet and social media affect these considerations? How do they affect people's framing of their grievances, and their courage? How do they solve collective action problems and publicize government misconduct and overreaction? The answer requires us to look at the entire media ecology: not just Facebook and Twitter and YouTube, which anyone can participate in, but also more traditional types of journalistic organizations like CNN and Al Jazeera.

First, grievance requires *knowledge* plus *framing*: Problems must be articulated in a way that people can understand and that motivate them to act. It is not enough that bad things happen and that people recognize them as bad. People must also see these things as related to what the government is doing or failing to do. Access to the Internet allows political entrepreneurs to frame the situation; it also creates awareness of freer conditions elsewhere. This helps produce both grievance and envy.

Second, social media lower the costs of informing and organizing people quickly. Collective action requires trust—especially collective action that might be punished. I will not protest unless I know that other people will, too. Social media allow political entrepreneurs to convey the message that many people feel upset at the government, and this helps create the belief that if ordinary citizens act, others will, too.

Third, social media allow individuals to report quickly and easily if government overreacts to protests or otherwise misbehaves. This provides additional sources of grievance and additional motivation. Protests of previous government actions—often at funerals and memorials—can become important drivers of continuing protest. Conversely, reports that the government has been unable to stop protests have a snowball effect; they bolster trust and courage and the belief that joining in is worth the effort and the risk.

Fourth, social media and broadcast media are directed both to fellow citizens and to the world in general. They help people recognize that protests are possible, they lower the costs of collective action, and they create a model for others to follow. Social media can inspire copycat behavior in other regions of the country and in other countries.

Fifth, one of the most important functions of media in protest movements is to express emotion. Facebook and Twitter are well-designed to convey short, emotionally charged messages. Like broadcast television, YouTube is particularly important, because it allows sound and video. This makes experiences vivid, emotional, and more present. It personalizes story telling. It makes violence and tragedy seem more real than mere textual depictions, no matter how eloquent or elaborate.

Sixth, in contrast to traditional broadcasters, digital networks are decentralized media. Decentralization means that it is more difficult for

the government to control what citizens hear or see. A single state-operated broadcasting network can easily be co-opted or controlled. International coverage complicates matters, but a determined state can keep most reporters out of the country. But if media is truly decentralized, then everyone in the country is a reporter. Cell phone cameras and cheap video cameras become part of the infrastructure of free expression.

Moreover, decentralized media supplement what centralized media can do. You do not need Al Jazeera or CNN to cover your protest to get other people to see it. You can put it on YouTube. Traditional broadcast media like the BBC and CNN can repeat these broadcasts, reinforcing the work of participatory social media.

There was no YouTube during the civil rights protests of the 1950s and 1960s in the United States. Civil rights protesters depended heavily on national mass media to describe what was happening in the South. Without extensive coverage by sympathetic media organizations, they would probably have been crushed. Instead, mass media made Rosa Parks and Martin Luther King, Jr. into national (and international) icons. The civil rights movement succeeded in part because protestors were able to obtain widespread national and international sympathy after Southern law enforcement and defenders of Jim Crow overreacted: Two famous examples are Sheriff Bull Connor's decision to set fire hoses and attack dogs on civil rights protestors, and the police riot on the Edmund Pettus Bridge that led to the passage of the 1965 Voting Rights Act.

Seventh, Egypt's closing down of the Internet delegitimated the government. The reasons why are complicated:

(1) When Internet access becomes sufficiently widespread in a country, it becomes a commonplace utility, like electricity. Perhaps more interestingly, it is increasingly understood as akin to a human right. In this way the infrastructure becomes part of background assumptions about what it means to be free.

(2) Internet access is a sign of a civilized, developed nation even if it is secretly filtered. Countries sign human rights treaties even if they violate human rights, because it signifies that they are civilized nations. Internet access has the same symbolic meaning. Cutting off Internet access completely has the opposite effect; it makes a country a pariah.

(3) Shutting down the Internet disrupts commerce. Even though Egypt kept access open for certain institutions like banks and stock exchanges, a wide range of other commerce—including tourism—was halted. This delegitimates the nation in the eyes of other countries and businesses that operate in many countries.

So far, I have described how digital infrastructure lowered the costs of the democratic activities of organization, spreading information, dissent, and protest. That is only half the story, however. Having foreseen the potential of social networks, authoritarian states will surely redesign their telecommunications facilities to head off future protest, facilitate surveillance, and promote propaganda and misinformation. Most autocratic governments are not stupid; they will respond to the strategic challenges generated by new information technology in much the same way that they respond to changes in military technology. And not only autocratic governments. As I will describe later on in this Essay, our own country is facing pressures to subtly reshape our information infrastructures out of fear of future cyberattacks and terrorist plots, and out of pressure by the content industries to prevent the unauthorized use of intellectual property.

Here is the basic idea: governments and protesters are in an arms race or an innovation cycle. New innovations in using digital technologies for protest lead to new government innovations designed to deter protest in advance and prevent future uprisings.

Because successful protest requires trust and overcoming the costs of organization, authoritarian governments can use the Internet to destroy trust and make organization more costly. They can block access to certain sites or platforms. They can track and spy on protesters. They can seek to undermine trust and sow fear and social discord through surveillance, propaganda, and misinformation. They can seek to discredit their political opponents through faked videos and false rumors. They can hinder—or even launch cyberattacks—against outside organizations that are trying to help protesters. Finally, governments can use the same social media as the protestors to organize their own allies. They can send pro-government thugs into the public square to attack demonstrators and create civil unrest; then governments can justify the use of military force as necessary to stop the rioting and restore order.

Each new innovation that protesters develop with digital technologies prompts governments to consider it in advance and check what protesters might do. China designed the Internet to make censorship easier and less obtrusive. Put differently, China got into the game of digital censorship much earlier and more pervasively than Egypt did.

If you design your telecommunications systems in advance to facilitate an authoritarian information state, you do not need to close them down and lose legitimacy. You can keep the Internet operating, spread misinformation, engage in surveillance, and block or filter dissenting voices. Control over conduits is built into Internet access in

those states that have the most successful censorship regimes. All other things being equal, the earlier you begin to design the conduits to serve state functions, the more effective you can be. Later technological advances can allow you to layer new surveillance and filtering technologies over old ones. But some decisions are best made at the beginning, for example, ensuring that only a small number of telecommunications providers control access into the country. That way the government has very few points of control that it has to worry about.

Egypt tried to shut down the Internet; China built its Internet so it does not have to shut it down. China regulated at the hardware, protocol, application, and social levels. It limited permissible telecommunications access into the country. It built devices for surveillance and blocking at the hardware levels. It has put pressure on the operators of search engines to block sites and share data about users. It monitors cybercafés.

The Chinese government cannot prevent all disfavored information from leaking into or out of the country. But it does not have to. It only has to shape access for the vast majority of its population, so that only a relatively few elites and very technically proficient members of society can get information that the government wants to block.

V. WIKILEAKS

My second example concerns WikiLeaks. I am less interested in the individual personality of Julian Assange than in the larger phenomenon that WikiLeaks represents. WikiLeaks symbolizes a new way of doing investigative journalism, which cooperates with traditional media organizations but is also independent of them.

Neither traditional media organizations nor nation states—including the United States—are particularly happy about these developments. Nation states do not like WikiLeaks because they cannot control or co-opt it as they have learned to do with more traditional forms of journalism, including, I am sad to say, American journalism. Traditional media organizations do not like WikiLeaks because it challenges and competes with their professional vision of how to do journalism. Equally important, WikiLeaks significantly undermines traditional organizations' carefully calibrated long-term relationships with (or less charitably, their co-optation by) powerful nation-states like the U.S. government and powerful business organizations.

WikiLeaks began in 2006, obtaining its domain name in October of that year, and releasing the first set of documents it received from

anonymous sources that December.[26] WikiLeaks acted as a conduit or publisher for other leakers; it did not obtain the documents on its own. It did not pick targets based on what we in America think of as benefitting the left or the right; rather, it was an equal opportunity annoyer and provocateur. Its early releases included information about assassination plots by a Somali rebel leader, revelations about corrupt government and business practices in various countries, a manual describing operating procedures at Guantanamo Bay, Cuba, documents describing assassinations and disappearances in Kenya, an early draft of an international treaty on intellectual property issues, hacked e-mails from Sarah Palin's Yahoo account, the membership list of the far right British National Party, and e-mails from climate scientists that encouraged right-wing critics of global warming.[27]

By 2009, WikiLeaks had a global reputation as a muckraking institution that exposed corruption or misconduct by governments and by powerful business organizations. Accordingly, it won an award from Amnesty International in 2009 and received the Freedom of Expression Award from *Index of Censorship*, a British Magazine.[28]

WikiLeaks's reputation, at least in the United States, changed dramatically in 2010 when it released four sets of documents about American foreign policy. It released a video clip of two American Apache attack helicopters firing on people in Iraq, killing twelve people, including a Reuters photographer and a driver.[29] In July 2010, WikiLeaks released war logs from Afghanistan; they showed, among other things, how the Afghan War looked on the ground and that the United States was targeting Taliban leaders for assassination.[30] None of the information was unknown, but it gave a much richer picture of the war.[31]

Importantly, WikiLeaks worked with traditional news organizations: the *New York Times*, the *Guardian*, and *Der Spiegel*.[32] Each organization was provided the documents in advance and given time to verify, analyze, and prepare them for release; all of the documents were released by the four organizations on the same day.[33]

---

26. *See* Yochai Benkler, *A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate*, 46 HARV. C.R.-C.L. L. REV. 311, 315-30 (2011) (describing WikiLeaks's history in detail).

27. *Id.* at 315-17.

28. *Id.* at 316.

29. *Id.* at 321.

30. *Id.* at 323-24.

31. *See id.* at 325.

32. *Id.* at 323.

33. *Id.*

The first batch included about 77,000 documents, and later WikiLeaks released another 15,000 documents after redacting them to remove "names of people who might be put in danger."[34] In October, WikiLeaks followed up with 400,000 field reports from Iraq that were heavily censored and redacted, again working with media organizations.[35]

Then, at the end of November 2010, WikiLeaks announced that it had a cache of over 250,000 diplomatic cables that it would begin releasing in small amounts.[36] The first 220 documents were published on November 28th; WikiLeaks worked with *El País* (Spain), *Le Monde* (France), *Der Spiegel* (Germany), the *Guardian* (United Kingdom), and the *New York Times* (United States) (which obtained the documents from the *Guardian*), and sought guidance from the U.S. State Department to decide which cables to release and what portions to redact.[37] Each news organization published stories contemporaneous with important releases. WikiLeaks estimates that some 130,000 of the 250,000 documents are "unclassified," some 100,000 are labeled "confidential," about 15,000 are classified as "secret," and none are classified as "top secret."[38]

Under the original plan, around 80 to 100 cables would be released each day. However, in September 2011, WikiLeaks released the remainder of the documents.[39] It noted that the password that encrypted the files had been distributed in a book published by the *Guardian* in February 2011; hence anyone could get access to the entire cache.[40]

The irony of this negligence is that it confirmed people's worst fears about WikiLeaks. Yochai Benkler at Harvard Law School did a study showing that media repeatedly reported that all 250,000 diplomatic cables had been dumped onto the Internet at once in November 2010.[41] Media reports generally failed to mention the process of selection and

---

34. *Id.* at 324.

35. *Id.* at 325.

36. *Id.* at 326.

37. *Id.*; Scott Shane & Andrew W. Lehren, *Leaked Cables Offer a Raw Look Inside U.S. Diplomacy*, N.Y. TIMES, Nov. 29, 2010, at A1.

38. Päivikki Karhula, *What Is the Effect of WikiLeaks for Freedom of Information*, Int'l Fed'n Libr. Ass'ns & Insts. (Jan. 19, 2011), http://www.ifla.org/files/assets/faife/publications/spotlights/wikileaks-karhula.pdf.

39. Benkler, *supra* note 26, at 326.

40. Robert Mackey et al., *All Leaked U.S. Cables Were Made Available Online as WikiLeaks Splintered*, N.Y. TIMES: THE LEDE (Sept. 1, 2011), http://thelede.blogs.nytimes.com/2011/09/01/all-leaked-u-s-cables-were-made-available-online-as-WikiLeaks-splintered/; Mark Seibel, *WikiLeaks Makes All Its U.S. Diplomatic Cables Public*, MCCLATCHEY (Sept. 2, 2011), http://www.mcclatchydc.com/2011/09/02/122923/WikiLeaks-makes-all-its-us-diplomatic.html; Christian Stöcker, *A Dispatch Disaster in Six Acts*, SPIEGEL INT'L (Sept. 1, 2011), http://www.spiegel.de/international/world/leak-at-WikiLeaks-a-dispatch-disaster-in-six-acts-a-783778.html.

41. Benkler, *supra* note 26, at 333-35.

redaction by WikiLeaks and mainstream media organizations, or stated the facts in a way that the reader would assume that all the cables were released at once.[42] Pundits and politicians naturally repeated these stories, often downplaying or ignoring the coordination between WikiLeaks and major journalistic organizations.[43] But nine months later, once it became known that the password to the entire cache had become freely available by accident, WikiLeaks actually did publish the remainder of the cables un-redacted.

Given the media presentation of the facts, much of the rhetoric about WikiLeaks has been hyperbolic. On December 19, 2010, Vice President Joe Biden compared Julian Assange to a "hi-tech terrorist."[44] Various politicians and pundits, striving to outdo each other, called for Assange to be kidnapped, assassinated, or treated as a terrorist or enemy combatant; some called for him to be tried for treason, even though he is not an American citizen.[45]

Senator Dianne Feinstein, Chairman of the Senate Intelligence Committee, called for Assange to be prosecuted under the Espionage Act of 1917,[46] and the Justice Department quietly began an investigation.[47]

---

42. *See id.* at 333-36.

43. *See id.* at 331-36.

44. Ewen MacAskill, *WikiLeaks Founder Is a Hi-Tech Terrorist, Says Biden*, GUARDIAN, Dec. 19, 2010, at 11.

45. *See, e.g.*, Eric Kleefeld, *Newt Gingrich: Julian Assange Is an Enemy Combatant*, TALKING POINTS MEMO (Dec. 1, 2010, 11:04 AM), http://tpmdc.talkingpointsmemo.com/2010/12/gingrich-julian-assange-is-an-enemy-combatant-video.php (quoting former House Speaker Newt Gingrich as saying, "we should treat [Assange] as an enemy combatant, and as an absolute enemy of the United States"); William Kristol, *Whack WikiLeaks: And There's a Role for Congress.*, WEEKLY STANDARD (Nov. 30, 2010, 8:25 AM), http://www.weeklystandard.com/blogs/whack-WikiLeaks_520462.html ("Why can't we act forcefully against WikiLeaks? Why can't we use our various assets to harass, snatch or neutralize Julian Assange and his collaborators, wherever they are?"); Doug Mataconis, *Treason and the Wikileaks Case*, OUTSIDE BELTWAY (Dec. 10, 2010), http://www.outsidethebeltway.com/treason-and-the-WikiLeaks-case/ (quoting Senator Joe Lieberman, in response to a Fox News inquiry, wondering why Assange had not yet been charged with treason); Michael O'Brien, *Republican Wants WikiLeaks Labeled as Terrorist Group*, HILL'S BLOG BRIEFING ROOM (Nov. 29, 2010, 8:38 AM), http://thehill.com/blogs/blog-briefing-room/news/130863-top-republican-designate-WikiLeaks-as-a-terrorist-org (quoting Rep. Peter King, the then-incoming chairman of the House Homeland Security Committee, who called on Secretary of State Hillary Clinton "to declare WikiLeaks a foreign terrorist organization"); Sarah Palin, *Serious Questions About the Obama Administration's Incompetence in the WikiLeaks Fiasco*, FACEBOOK (Nov. 29, 2010, 12:17 PM), http://www.facebook.com/note.php?note_id=465212788434 (calling Assange "an anti-American operative with blood on his hands," and asking, "Why was [Assange] not pursued with the same urgency we pursue al Qaeda and Taliban leaders?"); Marc A. Thiessen, *WikiLeaks Must Be Stopped*, WASH. POST (Aug. 3, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/08/02/AR2010080202627.html ("WikiLeaks is not a news organization; it is a criminal enterprise. [The government] can employ not only law enforcement but also intelligence and military assets to bring Assange to justice and put his criminal syndicate out of business.").

46. Dianne Feinstein, Editorial, *Prosecute Assange Under the Espionage Act*, WALL ST. J.,

The Espionage Act, passed during the Wilson Administration, was employed repeatedly to silence opposition to World War I, and was even used to imprison Eugene V. Debs, the Socialist Party candidate for President, who received almost a million votes while in prison during the 1920 elections.[48] President Harding later commuted his sentence.[49]

It is worth noting that the Espionage Act has not been used to prosecute a media defendant since World War II. The very fact that the Justice Department considered prosecution suggests that it does not think of WikiLeaks as a media organization engaged in journalism, but rather has framed the situation as one of hacking or sabotage, which, of course raises the question of how one should characterize WikiLeaks's partners: the *New York Times*, the *Guardian*, *Le Monde*, *Der Spiegel*, and *El Pais*.

My major focus here, however, is on infrastructure. One of the most interesting elements of the WikiLeaks story is how private power was used to hinder WikiLeaks, and how governments encouraged the private parties who control important features of the digital infrastructure to assist in censoring WikiLeaks. In other words, this is a story about the subtle and not-so-subtle relationships between public and private power in the digital age.

After a series of cyberattacks on its website, WikiLeaks moved its operations to Amazon's hosting services.[50] Senator Joseph Lieberman of the Senate's Homeland Security Committee criticized companies for doing business with WikiLeaks: "No responsible company—whether American or foreign—should assist WikiLeaks in its efforts to disseminate these stolen materials."[51] Amazon then booted WikiLeaks off its site on December 1st.[52] On December 4th, PayPal cut off the account that WikiLeaks used to collect donations.[53] On December 6th, MasterCard stopped making payments to WikiLeaks, followed by Visa on December 7th.[54] In each case, WikiLeaks scrambled to find new

---

Dec. 7, 2010, at A19.

47. *See* Charlie Savage, *Building Case for Conspiracy by WikiLeaks*, N.Y. TIMES, Dec. 16, 2010, at A1.

48. On the use of Espionage Act during World War I, see GEOFFREY R. STONE, PERILOUS TIMES: FREE SPEECH IN WARTIME FROM THE SEDITION ACT OF 1789 TO THE WAR ON TERRORISM 146-75 (2004).

49. *See id.* at 196-98, 232.

50. Benkler, *supra* note 26, at 338-39.

51. Charles Arthur, *WikiLeaks Under Attack: The Definitive Timeline*, GUARDIAN (Jan. 8, 2010, 11:39 AM), http://www.guardian.co.uk/media/2010/dec/07/wikileaks-under-attack-definitive-timeline.

52. Ewen MacAskill, *Amazon Pulls Plug on WikiLeaks*, GUARDIAN, Dec. 2, 2010, at 11; Arthur, *supra*, note 51.

53. Arthur, *supra* note 51.

54. *Id.*

facilities for hosting, domain name access, and financial payment systems.[55] It had to: these online facilities are crucial parts of the infrastructure that make WikiLeaks's model of journalism possible.

The Obama Administration ordered WikiLeaks blocked on federal computers. It forbade government employees from even visiting the site, leading to the interesting result that people who dealt with the government were more informed about WikiLeaks and what it had disclosed than government officials themselves.[56] The *Washington Post*, no doubt reflecting the views of government officials, wrote a story suggesting that even accessing the site or sites that discussed the cables could be hazardous for a security clearance or for the possibility of future government employment.[57]

All of this played out just before Secretary of State Hillary Clinton gave a well-publicized lecture in January 2010 celebrating Internet freedom, the freedom to connect, and the importance of digital technologies in making information available in countries that had blocked their citizens' access to vital information about the way that their governments worked. "[D]espite an intense campaign of government intimidation," Clinton noted, without a hint of irony:

> brave citizen journalists in Iran continue using technology to show the world and their fellow citizens what is happening inside their country. In speaking out on behalf of their own human rights, the Iranian people have inspired the world. And their courage is redefining how technology is used to spread truth and expose injustice.[58]

When it came to WikiLeaks exposing embarrassing facts about the American government, however, Secretary Clinton was far less enthusiastic about Internet freedom; indeed she argued in November 2010 that the disclosure of the diplomatic cables "is not just an attack on America—it's an attack on the international community."[59]

---

55. Benkler, *supra* note 26, at 347-48.

56. *See* David de Sola, *U.S. Agencies Warn Unauthorized Employees Not to Look at WikiLeaks*, CNN (Dec. 3, 2010, 10:05 PM), http://www.cnn.com/2010/US/12/03/wikileaks.access.warning/index.html.

57. Derrick T. Dortch, *Job Hunters Should Steer Clear of WikiLeaks Site*, WASH. POST, Dec. 9, 2010, at B3.

58. Hillary Rodham Clinton, Sec'y of State, U.S. Dep't of State, Remarks on Internet Freedom at The Newseum (Jan. 21, 2010), *available at* http://www.state.gov/secretary/rm/2010/01/135519.htm.

59. Scott Neuman, *Clinton: WikiLeaks 'Tear at Fabric' of Government*, NPR (Nov. 29, 2010), http://www.npr.org/2010/11/29/131668950/white-house-aims-to-limit-WikiLeaks-damage.

VI. PROSECUTING WIKILEAKS

I will return to the relationship between public power and private intermediaries in a moment. But before I do, you may be wondering whether the government can prosecute Assange and WikiLeaks consistent with the First Amendment.

In the Pentagon Papers case, *New York Times v. United States*,[60] the Supreme Court Justices agreed that the government could not halt the publication of the Pentagon Papers.[61] These documents described how the United States got involved in the Vietnam War, and contained a lot of embarrassing materials that probably undermined U.S. diplomatic efforts. Daniel Ellsberg, a government contractor who worked for the RAND Corporation, had leaked the papers to the *New York Times* and (later) the *Washington Post*. The Supreme Court refused to enjoin publication, applying a version of the old "clear and present danger" test that goes back to the beginning of the twentieth century. Justice Potter Stewart's concurrence explained that the test was whether "disclosure of [the papers] will surely result in direct, immediate, and irreparable damage to our Nation or its people."[62]

Justice Black connected the dots between the purposes of the First Amendment and the goals of information policy, arguing that the First Amendment is an information policy for democracy:

> The press was to serve the governed, not the governors. The Government's power to censor the press was abolished so that the press would remain forever free to censure the Government. The press was protected so that it could bare the secrets of government and inform the people. Only a free and unrestrained press can effectively expose deception in government. And paramount among the responsibilities of a free press is the duty to prevent any part of the government from deceiving the people and sending them off to distant lands to die of foreign fevers and foreign shot and shell.[63]

In this case Justice Black was pretty clearly talking about the Vietnam War, but one could easily apply the same logic to more recent events in the past, including our country's response to the 9/11 attacks and the decision to go to war in Iraq.

I have no idea what Justice Black would have thought of WikiLeaks. I think, however, that he would find the government's response, and especially Senator Lieberman's call for private parties to

60. 403 U.S. 713 (1971).
61. *See id.* at 714 (per curiam).
62. *Id.* at 730 (Stewart, J., concurring).
63. *Id.* at 717 (Black, J., concurring).

try to silence WikiLeaks, to be constitutionally troublesome. Remember that in *Associated Press*, Justice Black argued that although "[f]reedom to publish is guaranteed by the Constitution, . . . freedom to combine to keep others from publishing is not."[64]

The Pentagon Papers case is different from the WikiLeaks case in several important respects, however. First, unlike the *New York Times*, Assange acted outside the United States, and it is not clear if he could be extradited. Second, it's not clear how American criminal law applies extraterritorially.

Third, and most important for our purposes, in the Pentagon Papers case, President Richard Nixon sought an injunction to prevent further publication, and the Court rejected the request on the grounds that the injunction would act as an unconstitutional prior restraint on the press.[65] However, several of the Justices noted that various federal statutes, including the 1917 Espionage Act, were available for a criminal prosecution after the fact.[66]

Perhaps, then, the constitutional standard for a criminal prosecution following publication might be lower. But it is likely that some version of the "clear and present danger" test applies even to a subsequent criminal prosecution. As the Court explained in *Bartnicki v. Vopper*,[67] a recent case involving a taped conversation leaked to a radio program, "if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need . . . of the highest order."[68]

The government can prosecute government employees or contractors who leak information to the press, but the government cannot punish the press if it obtained the information lawfully and merely published what was leaked unless there would almost certainly be very serious harm to the nation. In this case, there has been no showing yet that the WikiLeaks revelations meet that standard. In fact, then-Secretary of Defense Robert Gates had more or less admitted that although the revelations in the cables are embarrassing, they were not life threatening and did not seriously harm national security. As Gates put it, "Is this embarrassing? Yes. Is it awkward? Yes. Consequences for U.S. foreign policy? I think fairly modest."[69]

---

64. Associated Press v. United States, 326 U.S. 1, 20 (1945).

65. *New York Times*, 403 U.S. at 714 (per curiam); *id.* at 717 (Black, J., concurring); *id.* at 730-31 (White, J., concurring).

66. *New York Times*, 403 U.S. at 730 (Stewart, J., concurring); *id.* at 733-40, (White, J., concurring); *id.* at 745 (Marshall, J., concurring).

67. 532 U.S. 514 (2001).

68. *Id.* at 528 (alteration in original) (internal quotation marks omitted).

69. *See* Elisabeth Bumiller, *Gates on Leaks, Wiki and Otherwise*, N.Y. TIMES: THE CAUCUS

Compare the WikiLeaks disclosures to the *New York Times*'s 2005 disclosure of the Bush Administration's secret domestic surveillance program (which, in my opinion, almost certainly violated federal law). The Bush Administration and its allies insisted that the story would seriously jeopardize our intelligence gathering operations and damage our efforts in the war on terror. Yet the Bush Administration never tried to prosecute the *New York Times* for the disclosures. Indeed, the Nixon Administration never sought to prosecute either the *New York Times* or the *Washington Post* after the release of the Pentagon Papers.

Is there anything that distinguishes Assange from the *New York Times* and the *Washington Post*? He is not an employee of a traditional professional journalistic organization. But the doctrine of clear and present danger does not turn on that distinction. Moreover, it is worth noting that Assange has been working with the *New York Times*, the *Guardian*, and other European newspapers. It's hard to justify prosecuting Assange if you are not going to prosecute the newspapers he has been working with.

To be sure, the government can prosecute the original leaker. We believe that the leaker was Private Bradley Manning, and the government has gone after Manning with a vengeance. For months it kept him in solitary confinement in a military prison in Quantico, Virginia, in harsh conditions well calculated to drive an ordinary person insane.[70]

Manning has been deliberately punished well before he is ever convicted of a crime, and he has been subjected to extremely harsh conditions that are not necessary to prevent his escape. Indeed, after a State Department official, P.J. Crowley, remarked that the treatment of Manning was "ridiculous and counterproductive and stupid," he was forced to resign because his remarks required President Obama to publicly defend the Pentagon's actions.[71]

(Nov. 30, 2010, 7:30 PM), http://thecaucus.blogs.nytimes.com/2010/11/30/gates-on-leaks-wiki-and-otherwise/.

70. *See* Ed Pilkington, *Bradley Manning's Lawyers Seek to Show Torturous Holding Conditions*, GUARDIAN (July 29, 2012, 3:47 PM), http://www.guardian.co.uk/world/2012/jul/29/bradley-manning-torturous-holding-conditions; Matt Williams, *Bradley Manning Treatment in 'Flagrant Violation' of Military Code–Lawyer*, GUARDIAN (Aug. 10, 2012, 3:19 PM), http://www.guardian.co.uk/world/2012/aug/10/bradley-manning-military-code-lawyer; Kim Zetter, *Three-Star General Was Behind Harsh Treatment of Bradley Manning, Defense Alleges*, WIRED (Aug. 10, 2012, 6:26 PM), http://www.wired.com/threatlevel/2012/08/general-manning-jail-treatment.

71. *See* Mike Allen & Josh Gerstein, *P.J. Crowley Resigns over Manning Remark*, POLITICO (Mar. 13, 2011, 1:17 PM), http://www.politico.com/news/stories/0311/51197.html.

What is going on? Two things. First, the government cannot prosecute WikiLeaks constitutionally if WikiLeaks merely received Manning's leaks. But it might be a different story if WikiLeaks conspired with Manning to leak the materials. So one possible reason for the harsh treatment of Manning is to get him to tell the government that WikiLeaks conspired with him.

There are two problems with this approach. First, if Manning does tell the government that there was a conspiracy, the question would then naturally arise whether his confession was legitimate or was the result of coercion and inhumane treatment.

Second, the conspiracy theory is very difficult to distinguish from what professional journalists do. Professional journalists work with whistleblowing sources to get them to release leaks, often coaxing them and offering to help them over extended periods of time. It may be hard to distinguish the government's theory from what Bob Woodward and Carl Bernstein did for Deep Throat in their coverage of the Watergate scandal, or indeed, what a wide range of investigative journalists do in coaxing information from disgruntled sources who provide leaks of sensitive government information.

A second possible reason for Manning's harsh treatment is more likely, but also more troubling. The government may realize that it cannot prosecute non-government employees once sensitive information is leaked to them. Instead, they must simply redouble their efforts to ensure that leaks do not occur. (This is Justice Stewart's point in the Pentagon Papers case.)[72] If that is so, then the harsh treatment visited on Manning before conviction is a message to all other government employees. Mess with us, the government is saying, and we will most assuredly mess with you, and we will not even have to convict you of a crime to do it. Rather, we will throw you into a dark cell in solitary confinement and slowly drive you mad.

None of this is to underestimate the seriousness of what Manning has been accused of. If he is found guilty, he should be punished. The point is that he should not be singled out as an example and punished before he is convicted.

VII. THE DIFFERENCE INFRASTRUCTURE MAKES

The story of WikiLeaks, like the story of the Egyptian protests, is about the infrastructure of free expression and how it helps or hinders the activities of democracy.

---

72. *See* New York Times Co. v. United States, 403 U.S. 713, 728-30 (1971) (Stewart, J., concurring) ("The responsibility must be where the power is.").

The government did not seek an injunction against WikiLeaks largely because the digital infrastructure makes it futile. Assange did not have to rely on the facilities of a major newspaper to publish his revelations. He created mirror sites in multiple countries around the world that made it impossible to block all of his copies. He worked with newspapers for a different reason: to give himself political cover.

Yochai Benkler has pointed out another important feature of the new digital infrastructure: Once the leaker (we assume Private Manning) uploaded the materials on the WikiLeaks website, Assange could not be co-opted in the same way that traditional media organizations could.[73] Assange picked newspapers in different countries and promised them a scoop in their countries in return for helping him sort through the materials. Because the papers knew that someone else in their country would get the scoop if they refused, they had incentives to cooperate. And because Assange worked with multiple newspapers in different countries, his disclosures would not be prevented if one or two of them were co-opted by their governments.

Compare this with the *New York Times*'s revelation of the Bush Administration's secret domestic surveillance program. It is likely that President Bush and his associates had violated the law; at the very least, there is a strong argument that they had improperly gone around the Foreign Intelligence Surveillance Act.[74] Nevertheless, the Bush Administration convinced the *Times* to delay publication until well after the 2004 election, possibly helping George W. Bush win a second term as President.[75] Why did the *Times* agree to delay publication? It was probably a complicated set of reasons: a personal request from the President, a sense of patriotism, and a desire to maintain the access and contacts with government that contemporary journalists crave. Today, major news organizations depend on a series of leaks and background information from government officials, and they do not want to bite the hand that feeds them too often or too hard.

---

73. *See* YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM ch. 7 (2006).

74. For a useful introduction to the legal problems with the program, see David Cole et al., *On NSA Spying: A Letter to Congress*, N.Y. REV. BOOKS, Feb. 9, 2006, at 42, 42-44 (discussing the statutory and constitutional issues raised by the Bush Administration's warrantless surveillance program).

75. *See* Byron Calame, Op-Ed., *Behind the Eavesdropping Story, a Loud Silence*, N.Y. TIMES, Jan. 1, 2006, at C8; Byron Calame, Op-Ed., *Eavesdropping and the Election: An Answer on the Question of Timing*, N.Y. TIMES, Aug. 13, 2006, at C10; *Context of 'Early November 2004: New York Times Agrees to Delay Publication of Wiretapping Story Until After Elections*,*'* HISTORY COMMONS, http://www.historycommons.org/context.jsp?item=a0904calumenyt (last visited Dec. 10, 2012).

The Obama Administration had no such leverage over Assange and WikiLeaks. Even if the Administration co-opted the *Times*, there were plenty of other papers to take its place, and Assange could publish the materials himself without anyone's permission. Indeed, the Obama Administration refused to deal with Assange directly, although it was apparently willing to talk to its acquaintances at traditional papers like the *Times*.

Daniel Ellsberg, the leaker in the Pentagon Papers case, faced a very different infrastructure of free expression in 1971. The key technological innovation in his day was the copying machine. Ellsberg made his copies using a Xerox copier in an advertising agency.[76] This was a long and cumbersome process, and Ellsberg later remarked that if he had today's technology, he would have simply published the copies on the Internet.[77]

Ellsberg first tried to get the Pentagon Papers read on the Senate floor, where they would be protected by the Constitution's Speech or Debate Clause.[78] When that failed he went to the *New York Times*. After a federal district court issued an injunction against the *New York Times*, he sent copies to the *Washington Post* and then to several other papers, which began publishing the papers one after the other.[79]

This was actually an early version of WikiLeaks' strategy. Each newspaper had incentives to participate because each circulated in a different geographical area. Ellsberg hoped that the Nixon Administration would not or could not go after all of the country's major newspapers at once.

Even so, it was a dangerous game in the pre-Internet world. First, all of the newspapers were located in one country. If the Supreme Court ruled against any one paper, that was the end of the game. Second, there were a finite number of copies, and making new ones—and distributing them to new locations—took time. If the government could enjoin the papers and round the copies up quickly enough, Ellsberg might not be able to create more and place them in secure locations. Third, unlike Assange, the publisher in the WikiLeaks case, Ellsberg did not own his

---

76. DANIEL ELLSBERG, SECRETS: A MEMOIR OF VIETNAM AND THE PENTAGON PAPERS 299-302 (2002).

77. MICAH L. SIFRY, WIKILEAKS AND THE AGE OF TRANSPARENCY 28 (2011); Noam Cohen, *What Would Daniel Ellsberg Do with the Pentagon Papers Today?*, N.Y. TIMES, Apr. 19, 2010, at B3.

78. ELLSBERG, *supra* note 76, at 356-61, 367; *see also* Gravel v. United States, 408 U.S. 606, 615-16 (1972) (describing as "incontrovertible" the claim that the Speech or Debate Clause protects a Senator from criminal or civil liability for reading the Pentagon Papers into the public record at a subcommittee hearing).

79. *See* SIFRY, *supra* note 77, at 28.

own newspaper or broadcasting facility. He relied on the mass-media distribution of newspapers.

WikiLeaks is the beginning of a new model of journalism that uses digital networks to obtain sensitive information anonymously, secure it in multiple sites, and publish it in defiance of territorial governments. Although WikiLeaks itself may not survive in its current form, similar organizations have sprung up around the Internet, and more are likely to follow. Later innovators will no doubt improve on the techniques pioneered by WikiLeaks and attempt to learn from its mistakes.

Traditional media organizations will eventually join this trend: They will create and install their own anonymous file depositories and form cooperatives with other newspapers around the world. Conversely, NGOs (non-governmental organizations) like the American Civil Liberties Union will do an increasing amount of what is now called investigative journalism: obtaining documents, processing them, and releasing them to the press. In the twentieth century, professional journalists, NGOs, and ordinary citizens had different and clearly demarcated functions and activities; that is giving way to a new decentralized system in which other actors become more like traditional journalism organizations and traditional journalism organizations become more like WikiLeaks and NGOs. As this happens, professional identities and professional norms will change.

Monroe Price has pointed out that most countries not only have internal policies for regulating their own media, they also have policies for regulating the media of other countries.[80] Countries want to affect the knowledge and information circulating in other nations.[81] During the Cold War, for example, the United States invested in Radio Free Europe, Radio Liberty, and Radio Marti to influence Eastern Europe, Central Asia, the Middle East, and Cuba. Secretary of State Hillary Clinton's speech on global Internet policy shows that the United States believes that it is in our interest to promote Internet freedom and the dissemination of information in other countries, especially countries which the United States disagrees with.[82]

Taking Price's insight one step further, we might say that the Internet allows each individual, or each NGO, to have its own media policy, giving people in other countries information that their

80. MONROE E. PRICE, MEDIA AND SOVEREIGNTY: THE GLOBAL INFORMATION REVOLUTION AND ITS CHALLENGE TO STATE POWER 3, 6-11 (2002).

81. *See id.* at 6-11, 19 (emphasizing "the effort by a state (or states) to influence or alter media space and media structures outside its own borders").

82. *See id.* at 19.

governments do not want them to have. That includes the United States. The United States, naturally, does not like it one bit.

In discussing the Middle East protests, I noted that governments and protestors are in an arms race or an innovation cycle. Just as China has worked to design its infrastructure to undermine protest, governments will seek to find new ways to undermine WikiLeaks and its successors.

Divide these techniques into "old school" and "new school" forms of censorship. "Old school" censorship means enjoining publications, taking control of newspapers and television stations, and rounding people up, either to prevent them from speaking, or to teach others a lesson that the government is not to be messed with. As I said, I think this is what the U.S. government is doing in the case of Bradley Manning.

"New school" censorship tries to control the digital infrastructure of free expression; it leverages privately owned networks and employs public-private cooperation. It may prove just as effective in the long run.

First, states can use their power over information infrastructure to insert government controls and surveillance technologies into the infrastructure. They can order businesses who control elements of the infrastructure to hinder, delay, block or censor content and speakers. These parties include the owners of telecommunications facilities like Verizon, technology companies like Cisco, domain name registrars like GoDaddy, website hosting services like Amazon, institutions of electronic commerce like MasterCard and PayPal, platform owners like Blogger, Facebook, or Twitter, and search engines like Google. These are all potential private censors, and thus they are all potential targets of government control.

Second, instead of direct orders, the government can coax, persuade, or signal to private owners of the information infrastructure to hinder or block offending publications and speakers. This allows the government to assert that private parties are doing the censoring, not the state itself. And because it is private censorship, we should respect it, first because the market will check any abuses, and second, because corporations have free speech rights to own and control the infrastructure.

What is new here is the use of the various elements of the digital infrastructure—telecommunications conduits, servers, domain name registrars, and payment systems—to censor. The strategy of government officials coaxing or signaling private parties to censor, by contrast, is not new at all. It was used, for example, during the McCarthy period, when

private parties blacklisted people for fear of being thought communist sympathizers.

Both direct control of infrastructure and public-private cooperation were used in the Middle East and in China. Both are fully available to the United States, and, moreover, the United States is currently employing them. The strategies of the new digital censorship in other parts of the world are not as dissimilar from what we do in the United States as you might think. The greatest threat to freedom of speech today is not simply that of public power or private power. It is their potent combination.

The Hugo Black of the *Associated Press* case in 1941—who was worried about the power of private combinations to suppress speech—turns out to be just as important to understanding free speech on the Internet today as the Hugo Black of the Pentagon Papers case in 1971, who was worried about government prosecution.

We criticize Yahoo when it capitulates to China. We should also criticize Amazon and PayPal when they capitulate to Joe Lieberman, just as we should criticize Senator Lieberman himself for making appeals that he would never direct at the *New York Times*, the *Guardian*, or *Der Spiegel*. If Senator Lieberman had suggested that MasterCard stop processing the *New York Times*'s subscriptions or that Amazon stop hosting its content on its servers, people would have thought he was a lunatic.

Despite the pressure, however, WikiLeaks was able to find new intermediaries to work with. The resilience of WikiLeaks suggests how crucial certain features of digital infrastructure can be to freedom of speech. The network as currently organized does not respect national boundaries. It is decentralized, redundant, flexible, plastic, and allows for many competitors and services. But that free speech-friendly design is not guaranteed in the future.

VIII. CONCLUSION

Right now there is enormous pressure in the United States to build back doors to allow surveillance on Internet networks and digital platforms in the United States, and to implement technologies that will make it easy for governments and corporations to filter content and block access to disfavored content.[83]

---

83. The most recent example was the political fight over the proposed Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011), and the PROTECT IP Act of 2011, S. 968, 112th Cong. (2011). These bills, promoted by the content industries, were ultimately shelved after opposition by other technology organizations and a wave of popular protests. Eric Goldman, *Celebrating (?) the Six-*

The pressure on the United States to do these things is not coming from authoritarian strongmen in the Middle East. It is not coming from the People's Republic of China. It is coming from our government and from the content industry. The government is worried about potential criminal activities and terrorist networks that use Skype, Facebook, and Gmail. The content industry is worried about file sharing and intellectual property. Meanwhile, telecommunications and broadband companies, which oppose some of these proposals, have their own shopping list: they want to protect the right to block and filter traffic that interferes with their business models or to favor traffic by their business partners. That is why the industry vigorously opposes network neutrality.

The danger in these proposals is that, however well-intentioned, they may also threaten the American infrastructure of free expression. Building networks that allow you to filter for intellectual property also allows you to filter for anticompetitive reasons, or even for ideological reasons. Implementing broadband technologies to slow and block traffic that your business partners do not like allows slowing and blocking traffic for other reasons as well.

Moreover, building a back door into everyday online communications means building a surveillance system into every aspect of our lives that uses digital communications systems, ranging from e-mail to Facebook to gaming software to Google Docs. If the government required that building contractors install bugs and hidden cameras in every home or apartment, people would object strenuously even if the government assured them that the bugs and cameras would only be turned on when the government had very good reasons.

Building a backdoor greatly lowers the costs of routine surveillance. In the pre-digital world the government had to decide whether the cost of a wiretap or a surveillance stakeout was worth the manpower and the expense. When government builds surveillance into digital communications systems, the cost of surveillance, including unnecessary surveillance, declines rapidly, so it is reasonable to expect that there will be more of it. And if there will be more of it, it is imperative to design systems to help ensure that surveillance is not abused.

The same is true of proposals to require that broadband providers install filtering systems or deep packet inspection systems to look for contraband intellectual property. Once these facilities are built into a

---

Month Anniversary of SOPA's Demise, FORBES (July 18, 2012, 1:20 PM), http://www.forbes.com/sites/ericgoldman/2012/07/18/celebrating-the-six-month-anniversary-of-sopas-demise; Amy Goodman, *The SOPA Blackout Protest Makes History*, GUARDIAN (Jan. 18, 2012, 6:51 PM), http://www.guardian.co.uk/commentisfree/cifamerica/2012/jan/18/sopa-blackout-protest-makes-history.

system, they greatly reduce the costs of blocking, filtering, and censoring. Designing an infrastructure in this way shifts the cost of surveillance and censorship away from government and onto citizens.

The First Amendment is an information policy for democracy, but it is only one information policy among many. It needs the assistance of an infrastructure of free expression to make good on its promises. The fight over free speech today, around the world, is a fight over how that infrastructure will be designed and implemented. If we want to preserve a free Internet, we must have networks that cannot easily be abused in the future. We must design democratic values into the infrastructure of free expression if we want an infrastructure that protects democracy.