The Fourth Quadrant

THE FOURTH QUADRANT

*Jonathan Zittrain**

INTRODUCTION

In the late 1990s, Larry Lessig suggested a way to systematize the study of cyberlaw. He started with a blank PowerPoint slide and placed a red dot at its center. The dot represented you: an individual buffeted by extrinsic forces. The forces take up the rest of the slide, each pushing the dot one way or another. They are laws, norms, code, and market. Lessig's insight was that these forces are each a form of control, and thus a form of law. To study cyberlaw by studying only that which is formally labeled law—that which emanates from sovereigns—was to miss the influences exerted through other means and by other parties. Moreover, since the government can create laws to influence norms, markets, and code, there are many paths for regulators to push around the poor embattled individual, more subtle and perhaps more difficult to resist than direct regulation.[1]

Lessig's structure inspired people to think more about just how constructed their environments were, and to appreciate a much broader range of levers of control. It was a call to action directed at the red dot.

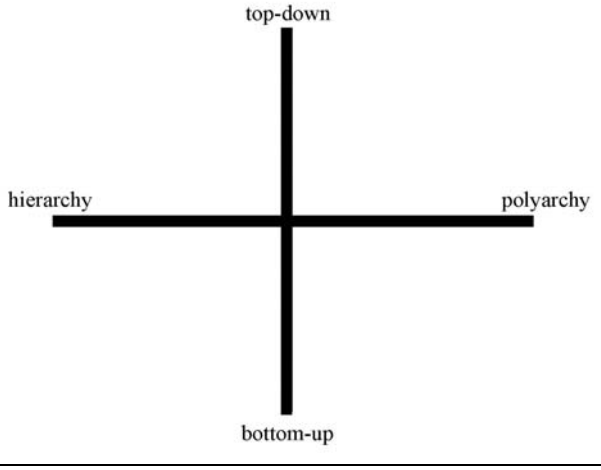
Nearly fifteen years later, the libertarian mindset in part captured by Lessig's existential dot has been complemented by an increasingly communitarian sensibility online. The intervening years have seen the rise of enterprises that weave individual actions into a collective whole. Web 1.0 might be represented by the home page and Web 2.0 by the blog, including others' comments. Web 3.0 is activity under a common umbrella, a centripetal recentralizing of user effort—but not by the state. Wikipedia, Couchsurfing, Facebook, Twitter—each is a platform accumulating users' work into a whole greater than a sum of parts. Twitter isn't just a convenient microblog for a particular user; it's an echo chamber of tweets and retweets that cultivates and accelerates popular memes with simple clicks by its users.

* Professor of Law, Harvard Law School and Harvard Kennedy School of Government; Professor of Computer Science, Harvard School of Engineering and Applied Sciences; Co-founder, Berkman Center for Internet & Society. The author wishes to acknowledge the contributions of Tim Berners-Lee in the development of this essay, in particular in originating the mirror-as-you-link idea, and participants in the Fordham symposium that inspired the piece. The author also thanks Heather Casteel for excellent assistance in research and in drawing from talks at Columbia and Duke Universities for this essay.

1. *See* LAWRENCE LESSIG, CODE: VERSION 2.0 (2006).

I want to suggest an additional framework for thinking about these phenomena, and for thinking about the Internet as a whole. The core idea is that an undertaking can be understood along two surprisingly independent dimensions. The first is how "generative" it is—in essence, whether it is meaningfully open to contributions from outsiders, where the line between insiders and outsiders is blurred or nonexistent. The second is how singular it is—whether it is one of a kind for those affected by it, or one of many. Charting these two fundamental characteristics for an activity can help us understand the problems that are likely to develop—and the options for solving them.

Envision a four quadrant chart with two axes. The X-axis runs between what I call hierarchy on one end and polyarchy on the other. These may not be the perfect words, but I use them with a particular meaning in mind. The term "hierarchy" on the left side connotes a system for which there is no alternative, either because it does not exist, because it would be too costly, or because law precludes it. For these or any other reasons, those subject to the system do not have a lot of choice. The right side is labeled "polyarchy." Polyarchy is defined by choice. The more choice an actor has, the further to the right side of the chart the actor exists. In this context, choice is the ability to choose among various regimes or systems in which you might exist. The second axis, positioned somewhat counterintuitively at right angles to the first, divides "top-down" and "bottom-up."[2] Position on this axis is determined by the extent to which those empowered to shape the system—to make its rules and enforce them—share an identity with the people of the system. To the extent that there is a separation between those who make the rules and those who live under them, the system is closer to the top of the axis. To the extent that there is no separation, that the rules or constraints emanate as readily from one person as another within the system, it is closer to the bottom.



2. This chart is adapted from prior scholarship, in which the Y-axis represented the division between "sterile" and "generative." *See generally* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT (2008).

I. PLOTTING IN THE FOUR QUADRANTS

A. *Governments and Systems*

At the risk of a little imprecision, even butchery, of political science terminology, we can plot some examples of governance systems on the chart. In the upper left might be something like an authoritarian regime. In an authoritarian system, the rules are fairly clear, and there are a lot of them. They are enforced upon the citizens, who do not get to make them, which positions it high on the chart. Generally citizens do not get to leave, which is how the regime is able to enforce unpleasant rules. If it were easy to get out of the system, everyone would flee. That places it leftward on the chart.

A little bit further down, or potentially much further down but still north of the horizontal axis, would be an indirect representative system such as in the United States. Democracies are going to be more responsive to those who are regulated because there are regular elections. Citizens do not make rules directly, but they can always throw the bums who do out of office. This popular control mechanism is an indirect ongoing dialogue, a rather crude method of feedback between those who regulate and those who are regulated. Every so often, the citizens, like the lowly spy in the game Stratego who yet gets to kill the general, determine the professional fate of those who make the rules.

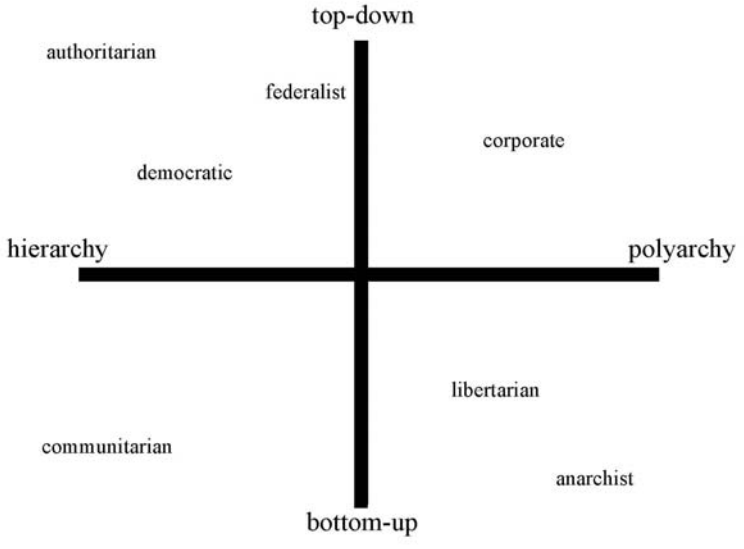
Federalism is further to the right, towards polyarchy. These systems may still not include the people very much, except via elections, but the point of the federalist system, in theory, is choice. Within the United States, the theory goes, no one has to live in one state because it is possible to pick up stakes and move. There is a high transaction cost in moving, but less and less over time. This is what I mean by polyarchy: the idea that the availability of many systems provokes a certain kind of competition.

Speaking of competition, on the very far right we might place corporatism. By this I am referring to the classical understanding of markets. If the markets are dominated by large firms with various barriers to entry for smaller players, the position is up as well as right. Imagine there is a product you want, and the corporations that make that product or who choose to enter that market are desperate for you to buy it. They want to make the price as low as they can get away with if it means more sales. They want to shape their products to your desires. In that sense, there is the same kind of feedback between those who buy the products and those who make them as there is between those who pass the laws and those who live under them. Still, we would not mistake the entities that make the products for the people who buy them. An individual does not get a vote in making the product; in particular, an individual does not get to walk into the building and start making his own products. There is still a difference between those who create and those who buy.

Down in the lower right corner one might put anarchists, in the sense of those who want no government at all. Anarchists believe that the more people are able to do whatever they wish, the happier they will be. The source of constraint is as likely to be the person next to you as it is those bureaucrats in government. Under anarchy, the regulation or constraint upon a person could come from anywhere, just as that person could enforce a constraint upon anyone else.

Slightly above anarchy one might place libertarianism, at least that strain of libertarianism that is highly skeptical of government in general and believes that the best means to security is a shotgun. Under this sense of the word, libertarians want a system where you rely on yourself, your neighbors, your family, or your friends for protection and for constraint.

In the bottom left might belong something like communitarianism. This embodies the idea that there are times when the needs of the whole may outweigh the desires of one particular member—indeed, where individual identity can only be understood through membership in a group. Perhaps what the people want is supposed to somehow emanate from such a low point within the community that the format for decision making really is the town hall meeting. This system can still bind people to any given decision who do not agree with it; in that sense it is hierarchy. In the communitarian conception, if one person does not like some decision, it is not so clear that he gets to leave. He owes something to the community, including a duty to stay even when things do not go his way. The communitarian system is supposed to embody participation in a much richer way than by merely casting a vote, the way some of the systems in the upper left work.



B. *Movement and Evolution in the Four Quadrants*

These four quadrants are useful for more than merely plotting static objects. We can add verbs to the picture and begin to tell stories about political, corporate, and technological change by tracking the migration of various actors across the chart. For instance, most people are familiar with the antiglobalization story. According to some, globalization is a problem. Part of the complaint of, say, G-20 protestors is that corporations used to exist on the right side of the chart, in polyarchy, where they competed with each other. Recently, however, these corporations either got together in a smoke-filled room and cut deals, or just got so big that no meaningful competition remains. As a result, many of these corporations exist closer to hierarchy. We, the citizens of the corporate system, do not even have the chance to throw these bums out the way we might an unpopular politician. Corporations are only responsive to us as consumers, and too many groups of consumers are not in the market for a particular product but are still affected by its producer's so-called externalities.

Another story we could tell might be the race to the bottom. A government begins on the left, in hierarchy, but because capital and people flow so easily from one place to another, it might slide towards polyarchy. Eventually it ends up on the far right, just as if it were another corporation.[3] When this happens, any hope of regulating in a positive sense is greatly thinned out. If one entity pushes too hard, its citizen-customers leave and go somewhere else. Depending on your normative prior commitments, this is either a serious problem or the race to the top. Some might view this as the ideal system, where usurious taxes get forced down through competition because businesses will flow to the places that offer them the best package.[4]

II. THE INTERNET AND THE FOUR QUADRANTS

A. *Online Enforcement*

Consider mapping a story about the Internet and the process of online control and regulation.[5] Governments, for the most part, still occupy the upper left corner of the chart. People occupy the lower right. Governments have the power to act directly on their citizens, to make laws about what the people are allowed to see, or know, or say. Governments can regulate sedition, copyright infringement, or anything else. Defamation, for instance, is triggered by fellow people but mediated by the government.

---

3. This problem was beautifully envisioned by Neal Stephenson in SNOW CRASH (1992).

4. *See, e.g.*, Posting of Matthew Shaer to Horizons, http://www.csmonitor.com/Innovation/Horizons/2010/0302/Welcome-to-Google-the-new-capital-of-Kansas (Mar. 2, 2010) (describing Topeka's effort to entice Google to select Topeka as the test market for its ultra-high-speed broadband by renaming the city "Google" for a month).

5. For a general overview of the development and governance of the Internet, see DAVID G. POST, IN SEARCH OF JEFFERSON'S MOOSE: NOTES ON THE STATE OF CYBERSPACE (2009).

The law deals with the individual directly and what he or she is allowed to utter, whether or not it is laundered through another platform, such as the Internet. These are forms of regulation designed to keep you in line, for better or for worse.

In the online context, however, there is another approach to enforcement: the terms of service violation. There is no need to involve the authorities; a user can try to get AOL or another online service provider to protect her by kicking off a subscriber. Again, Larry Lessig had a very powerful insight about this dynamic, which he described as an implication of "Code is Law."[6] The environment itself can control a person just as readily as the government's naked exercise of regulatory power. In turn, the government can tell these online intermediaries how they must shape their service. There are rules about e-mail retention, and if the government wants to identify any particular user, the intermediary can be forced to disclose that information, as long as it has the credit card records.

Lessig's claim was that this path of regulation, in part because of its indirect nature, is the more effective and therefore more worrisome path. When the government comes after individuals, we tend to be suspicious. When the government comes after people through brands, individuals tend not to notice that it is government regulation affecting their lives.

This story is evident throughout the development of the Internet. The Internet came about in the lower part of the chart in the sense that it was built by people with no particular profit motive, who were not looking exclusively to compete against anything. The Internet does not have a CEO. It has a group of people who decide to collaborate and experiment with networking. As the Internet starts to get more popular, however, there came to be a business component to it. The first Internet access came through proprietary services, such as AOL and Prodigy, that began popping up to offer Internet service to people who otherwise were not a part of the founding clique. Back around 1990, these companies controlled most people's access to and experience of the Internet. Eventually, however, people moved away from these original access points; they began signing up for direct Internet service. As this took place, the Internet became more and more influential, even if you were not yourself a part of it. It is now a firmly entrenched hierarchy; there is no direct competition for the Internet. It became such a gathering place that the original players essentially died off. Their names still exist, but they were just rebranded as little areas on the new Internet.

We then end up in a configuration where anything can be built on top of the Internet. Consider, for example, Friendster.[7] There was a time when Friendster seemed important. It turned out that Friendster was not as fun as we thought it would be, but other options came along. As more and more applications come about, the realm of competition is no longer among the

6. *See* LESSIG, *supra* note 1, at 5, 88–94.

7. Friendster, http://www.friendster.com (last visited Apr. 7, 2010).

original gated proprietary services, but among different applications, built by companies that all run according to Internet protocol. By 2008, all of these applications and online services shaped what their subscribers saw and experienced, just as those intermediaries in last generation's corporations did. Under the new system, you can still try and reach people over the Net who do bad things. It may be a bit more difficult, because we lack the built-in authentication and identification that the old proprietary services offered. For the most part, however, it is usually possible to catch or at least identify bad actors online.

The modalities of regulation remain the same today as in 1990. The government can still intervene if there is a problem online. If someone e-mails a threat to the President, the government will do what it takes to find out the identity of that person, either by looking at clues in the threat itself, such as the text of the e-mail, or through the Lessig move of demanding information from the ISP. Alternatively, you see governments starting to impose regulations and shaping the services that Internet companies offer. The configuration of control has remained the same, just with a different set of players, themselves mediated through the Internet.

B. *Censorship*

This picture becomes a bit more troubling when one realizes that among the governments engaging in this regulation are regimes like that of China. It was originally thought that this new system would cause problems for China, that the Chinese government would face the problem of regulating its own people because of the difficulties of regulating the Internet.[8] However, the Chinese government can still lean on plenty of intermediaries to control its citizens' access to the Internet. In fact, we are seeing a shakeout in recent times of an increasing handful of intermediaries without whom you would truly feel that your Internet experience was incomplete: think of Google, or even Facebook. If someone took away your top five most visited sites, you would feel yourself to be missing a lot. For this reason, maybe the polyarchy is not as "poly" as we think; some of these intermediaries and companies are starting to slide towards hierarchy. As they do so, the opportunities for top-down regulation are multiplying, whether or not you think the source of the regulation is legitimate. This is the blowback story of the modern Internet, which gives cause for concern even as we know that the average person's access to information—to material his government does not want him to see—is greater today than it was yesterday, and will continue to improve.

The incentives for government control of information are not new, but the Internet poses a greater threat for widespread public dissemination of undesirable information. A few years ago, there was one particular science

8. *See generally* James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177 (1997) (describing the inadequacies of the theory of "digital libertarianism").

paper that showed how easy it would be to poison the milk supply.[9] Terrorists have yet to target milk, but the academic paper said they could. It is unclear what the proper government response is in this situation, if any. Some might argue that the benefit of the paper was not worth the risk of exposing this information to hostile parties; if so, it becomes tempting to suppress risky information.[10]

The same thing happened with the EPA's luridly titled "Worst-Case Scenarios." In 1998, the EPA asked various chemical plants and factories to imagine the worst thing that could happen, the event that could hurt as many people as possible, involving their instrumentality. They compiled a database of these worst-case scenarios for the purpose of informing nearby people. The FBI strongly resisted posting this information online; it seemed too tempting for aspiring terrorists.[11] The compromises attempted with respect to the information seem quaint now. The EPA established government reading rooms, which anyone could enter but in which recording devices were banned.[12] One could, in the privacy of his or her own mind, read the worst-case scenario and leave. Terrorists would have to remember everything on their own. It was a totally well-meaning compromise, but one with an element of comicality to it. It is unclear that it was worth the EPA's effort to produce those particular facts in the first place.

More recently, Internet-based corporations are beginning to run up against the preferences of various governments.[13] Google, beginning with Google.cn in 2006, agreed to self-censor under threats from the Chinese government, though Google has since ceased such self-censorship on Google.cn and moved its Chinese search services to the Hong Kong-based Google.com.hk.[14] Microsoft has also had to grapple with these issues; if someone attempts to title a Microsoft-platform blog with any prohibited words—free speech, democracy, human rights, and so forth—an error message will pop up.[15] The user will have to choose a different title.[16]

---

9. Lawrence M. Wein & Yifan Liu, *Analyzing a Bioterror Attack on the Food Supply: The Case of Botulinum Toxin in Milk*, 102 PROC. NAT'L ACAD. SCIS. U.S. 9984 (2005).

10. This pressure to suppress can result in what is now commonly known as the "Streisand Effect," in which efforts to censor information can result in its greater popularity and dissemination. *See* Wikipedia, Streisand Effect, http://en.wikipedia.org/wiki/Streisand_effect (last visited Apr. 7, 2010).

11. *See* Courtney Macavinta, *Battle over Worst-Case EPA Data Online*, CNET NEWS, July 10, 1998, http://news.cnet.com/Battle-over-worst-case-EPA-data-online/2100-1023_3-213186.html.

12. *See* Kerry E. Rodgers, *The Limits of Collaborative Governance: Homeland Security and Environmental Protection at U.S. Ports*, 25 VA. ENVTL. L.J. 157, 223–24 (2007).

13. *See* POST, *supra* note 5, at 164–69.

14. Posting of David Drummond to The Official Google Blog, A New Approach to China: An Update, http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html (Mar. 22, 2010, 12:03 PST).

15. *See Microsoft Censors Chinese Blogs*, BBC NEWS, June 14, 2005, http://news.bbc.co.uk/2/hi/technology/4088702.stm.

16. Interestingly, this censorship extends only to the name for the blog, not for individual entries, from which one may infer an attempt to trumpet compliance with

C. *The Historical Record*

For years, businesses ended up with paper records that turned out to have a certain Newtonian momentum to them. A business had to affirmatively shred documents it wished to keep undiscovered. More recently, services have developed that promise to turn the Newtonian momentum into Aristotelian motion, where the transmission of information stops unless its owner keeps pushing it forward. An example of this is a company that used to be called Disappearing Inc., later called Omniva.[17] Their business plan is based on what they portray as the "problem" with e-mail: that it is easy to distribute and nearly impossible to erase. Their solution entails requiring a proprietary client to read every e-mail you send. E-mails can only be read and displayed using keys. These keys are time based; they are set to expire after some fixed period, perhaps a year. After that time period expires, the keys are destroyed. Once this happens, all the copies out there that require that key for decryption are no longer accessible. This flips the paradigm: no longer does information exist until you destroy it; rather, it does not exist unless you affirmatively find a way to save it.

Similar problems of information permanence arise in other contexts. For instance, should the Google Books system succeed, it would make no sense for a library to store thousands of physical books in its basement. Rather, under the Google Books plan, there is one master copy of the book in Google's possession.[18] The library partners display it and access it according to particular privileges. A user can access it from anywhere. This raises a huge problem, what can be thought of as the Fort Knox problem.[19] If one book in the system contains infringing material, the rights-holder can get a court order requiring the infringing pages of the book to be deleted from the Google server. Google has no choice but to comply, at least as long as it continues to be headquartered in the United States. This order affects every book that is distributed through the Google platform. Anyone who does not own a physical copy of the book will now lack access to that section of the book—or the entire thing. Add in defamation or any other cause of action, and holes begin to appear in the historical record in a way they did not before.

Once this threat is pointed out, there is a tendency to think of it as important but not urgent. People seem to assume that we can deal with it

---

censorship demands without true obedience to a politically problematic doctrine. *See* RConversation, Microsoft Takes Down Chinese Blogger, http://rconversation.blogs.com/rconversation/2006/01/microsoft_takes.html (Jan. 3, 2006, 11:06 EST).

17. Omniva was later acquired by Liquid Machines, which continues to offer similar data management plans. *See* Press Release, Liquid Machines, Liquid Machines Acquires Omniva Policy Systems (Sept. 20, 2004), http://www.liquidmachines.com/content511.html.

18. *See generally* Google Books Settlement Agreement, http://books.google.com/googlebooks/agreement/ (last visited Apr. 7, 2010).

19. The "Fort Knox problem" arises when information is stored and controlled in a single centralized location. Anyone with access to that location could tamper with or remove information from circulation entirely; libraries and others would have no recourse as there exist few or no other ready copies of the material to which they might refer.

later, even though the systems are being designed and implemented right now. One helpful catalyst was an incident that could not have been invented better than it happened in reality. Somebody offers, through Amazon, a Kindle version of *1984* by George Orwell.[20] People buy it. Later, Amazon has reason to think there is a copyright issue that was not cleared by the source who put it on Amazon. Amazon panics and sends a signal that actually deletes *1984* off of all the Kindles. It is as if the user never bought *1984*. That is terrifying. That is the Fort Knox problem. It is not literally cloud computing; for the period of time the user possesses *1984*, it technically resided physically on his or her Kindle. But because it is not the user's to copy or to process, and it is Amazon's to reach in and revise or manipulate, it is as good as the Google Books configuration—or, in this case, as bad.

III. THE CYBERSECURITY PROBLEM

Most frightening are the implications of the Fort Knox problem for cybersecurity. There is not yet consensus within the relevant communities about how bad the cybersecurity problem actually is, certainly not what to do about it, but there is rising panic over the situation. As long ago as 2003, the U.S. Cybersecurity Advisor produced *The National Strategy To Secure Cyberspace*.[21] The first half comprised dire predictions, imagining a digital Pearl Harbor and sending a clear message to the public: be afraid, be very afraid. The second half's recommendations, which called for such things as public-private partnerships, seemed insignificant given the gravity of the threat.

Last year the FBI said that "[c]yber attacks pose the greatest threat to the United States after nuclear war and weapons of mass destruction."[22] One article described how "US experts warn of 'cybergeddon', in which an advanced economy—where almost everything of importance is linked to . . . computers—falls prey to hackers, with catastrophic results."[23] This the FBI believes, and I believe.[24] Many sectors of our government are terrified of a somewhat amorphous, but multifaceted, cybersecurity threat. Other people are also out there beating the drum of fear about cybersecurity, insisting we worry about it.[25] This runs up against the crowd

20. *See* Brad Stone, *Amazon Erases Two Classics from Kindle. (One Is '1984.')*, N.Y. TIMES, July 18, 2009, at B1.

21. U.S. COMPUTER EMERGENCY READINESS TEAM, U.S. DEP'T OF HOMELAND SEC., THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2003), *available at* http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.

22. Sebastian Smith, *FBI Warns of Cyber Attack Threat*, SYDNEY MORNING HERALD, Jan. 7, 2009, http://news.smh.com.au/world/fbi-warns-of-cyber-attack-threat-20090107-7bot.html.

23. *Id.*

24. *See, e.g.*, Ellen Nakashima, *FBI Director Warns of 'Rapidly Expanding' Cyberterrorism Threat*, WASH. POST, Mar. 4, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/04/AR2010030405066.html.

25. Posting of Kim Zetter to Threat Level, http://www.wired.com/threatlevel/2010/01/csis-report-on-cybersecurity/ (Jan. 28, 2010, 14:30 PST).

of Internet nerds, who park themselves in the bottom right corner of the chart, smug in their own technological defense abilities, and who firmly resist all efforts at regulation. This tension is part of what makes cybersecurity such a difficult problem.

It was not that long ago when many sovereigns actually came down on the other side of the cybersecurity ledger, and many may still remain there. There is a member of the German government who has suggested that the country resort to denial-of-service attacks in order to take down neo-Nazi websites.[26] In other words, if Google does not improve their neo-Nazi filtering in Germany or, maybe, the entire world, Germany might just take matters into its own hands. Certainly any government, including the United States, holds the double-edged official policy that it should be impervious to cyberattack but, at the same time, possess a cyberattack capability—that its networks should be invulnerable even though it should be able to bring down any computer or system anywhere.

IV. SOLUTIONS

To pull together the threads of cybersecurity regulation now on the table, let us return to the chart and, in particular, to the fourth quadrant, the one on the lower left. Right now, when problems arise, people tend to turn first to the governmental or corporate quadrants. Solutions originating there might help, but they also carry costs—costs that are magnified when the problems happen in the bottom quadrants. For example, when a cyberattack happens, victims look for help from Symantec and other digital Pinkertons who exist in the top right, akin to hiring bodyguards and escorts to assist in transport along a dangerous highway. Those victims who are unwilling or unable to write the big check that corporate help requires are left with whatever free solutions and government assistance are available. Possibly, however, there are some solutions that can come from the quadrant on the lower left, the sector that otherwise might not seem as intuitive or common as the others. These solutions are on the left side of the diagram because they will bind people even if everyone does not agree. But at the same time, these are solutions built of the Internet among its participants, rather than answers sent down from government actors; they properly belong at the bottom of the chart.[27] They have their own drawbacks, but because we rarely look here for solutions, there may be opportunities that are less well known than the well-worn formats of government and corporate intervention.

The basic idea is built upon a commitment to solving the Fort Knox problem by eliminating, or at least backing up, any monopolistic repository

26. Steve Kettmann, *Nebraska Neo-Nazi Irks German Pol*, WIRED, Jan. 10, 2002, http://www.wired.com/politics/law/news/2002/01/49566 ("[German Interior Minister Otto Schily] suggested that the German government itself might engage in denial-of-service attacks—in effect, hacking—to shut down some sites based in the United States.").

27. *See generally* Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998) (discussing rules created by nongovernmental actors for digital networks).

of information. Libraries are a step ahead in this area; there is an initiative called LOCKSS—Lots of Copies Keeps Stuff Safe—based at Stanford.[28] LOCKSS envisions a role for libraries to play that is also emerging as an answer to the problem of the Google Books (or even Kindle) situation. Google Books provides a great example: let Google do exactly what it is doing, but make sure participating trusted libraries each get their own master copy of what Google has. The libraries put it under their own lock and key. Every so often, they check their master copy against the copies held by other libraries and the Google master copy to make sure the book has not changed. If there is a change, it is clear that somebody has had a hand in the cookie jar, and the libraries can start to talk about what happens next. Rather than just having one place to serve process and send a national security letter or court order demanding redaction or alteration, now any disgruntled party has to engage with dozens or hundreds of public-minded organizations to see whether they are all ready to turn that key together and decree that the past shall be changed. This creates a useful friction in the system, while still preserving opportunity for removing material so truly damaging that it belongs down the Memory Hole.

It is even possible to imagine inverting the Disappearing Inc./Omniva paradigm of Aristotelian informational momentum.[29] Instead of having digital archives of classified and government information that automatically delete themselves after a period of time, why not encrypt them with keys that after 30, 40, or 50 years go public one day at a time? Only if the government takes the initiative to go back and redesignate something as private will it stay out of the public eye. Decryption keys could be put in the hands of the libraries or in some other escrow; the vaults of government data and reports would open only at the proper time.

As a concrete example of a solution originating in a bottom-up fashion, though from the right side of the chart rather than the left, consider the Internet Archive's Wayback Machine.[30] This was designed by just one person—Brewster Kahle—who happened to decide that somebody ought to keep a copy of the Web.[31] In what was probably the largest copyright infringement ever, he copied everything online and put it into a database. This is a wonderful library of information, and Brewster is a hero. But Brewster is still one guy, and Internet Archive is only one address on which to serve process. The company has not yet been sued out of existence in part because it is so accommodating. Anyone can request that their material

28. LOCKSS, Home Page, http://lockss.stanford.edu/lockss/Home (last visited Apr. 7, 2010). Its icon is a tortoise, both because the tortoise lives so long and because it is so boring that no one notices it. LOCKSS, About Us, http://lockss.stanford.edu/lockss/About_LOCKSS (last visited Apr. 7, 2010).

29. *See supra* note 17 and accompanying text.

30. Internet Archive, http://www.archive.org/ (last visited Apr. 7, 2010).

31. *See* Heather Green, *A Library as Big as the World*, BUSINESSWEEK, Feb. 28, 2002, http://www.businessweek.com/technology/content/feb2002/tc20020228_1080.htm.

be excluded from the project, and Internet Archive will comply.[32] They do keep a copy of the data, mindful of its value into the future, but it is no longer publicly accessible.

The principle of distribution rather than centralization is really one of mutual aid, and it can be extended to the cybersecurity problem. Imagine a user attempting to follow some link to a particular site, but the site has been brought down by a denial-of-service attack, by a government order, or anything else. That site was, in a way, a miniature Fort Knox; the user has no alternative route to access its contents. She sees the link, but the link does not persist. To Web engineers (and to the site owner), this is a real problem. Uniform resource locators are meant to be uniform, not just across place but across time. What could we do that does not involve the creation of a centralized Fort Knox solution like the Internet Archive to prevent this from happening?

It is time for a metaphorical NATO for the Internet, not among states but among Internet participants, something built into its fabric through Web servers and clients. There is strength in numbers, and we can draw upon those principles of mutual aid that built the Internet to begin with in order to gather otherwise powerless individual entities together into a stronger force. The heart of the proposal is simple: mirror as you link.[33] As one website is rendering the page of links in response to a user's request, it actually goes and fetches the contents of those links. The website stores not just its own information but everything it links to as well. If one site later fails or is blocked, the user can request a copy of it from the server that linked him there.[34] This system can be made "opt-in" in the sense that before one site copies the content from another, it checks for consent, which mitigates the potential copyright issues. Each participating site embodies the principle of mutual aid: if one site goes down, others will duplicate and disseminate its information. In exchange, that one site promises to do the same for those sites to whom it links.

This extremely simple configuration is implementable with just a few tweaks to the two major Web servers in the world: Apache and Microsoft. It would transform the nature of information retention, and it would support the construction of a historical record that now contains so much information that is born and remains digital rather than being archived and catalogued through traditional means. As an added bonus, if information is unreachable not because of an attack on the server but because of filtering imposed somewhere in the network, by the ISP or by a government, the

32. *See* Internet Archive, Frequently Asked Questions, http://www.archive.org/about/faqs.php (last visited Apr. 7, 2010).

33. Again, I am grateful to Tim Berners-Lee for several discussions that refined some complicated implementations into this more elegant formulation.

34. A group of academics in the Netherlands has previously suggested a similar protocol-based solution. *See* Globule: An Open-Source Content Distribution Network, http://www.globule.org/ (last visited Apr. 7, 2010).

system still works flawlessly. Essentially, the system functions as a supply-side circumvention tool.[35]

In addition, the system removes the question of individual liability. No single website need worry about disobeying the filtering orders of the Chinese government; they are all merely participating in a Web robustness scheme that also happens to deal with censorship as well as cybersecurity attacks. All thanks to the characteristics of this fourth quadrant.

The power and potential of the fourth quadrant has already been well illustrated by, among others, Wikipedia. Wikipedia began as the ultimate bottom-up hallucination: a reliable, multimillion-article, global encyclopedia built on the backs of volunteer editors. Wikipedia has worked so well that it has migrated further and further to the left of the chart—so far, now, that if Wikipedia says something bad about a person, that person cannot solve the problem by declining to use Wikipedia. Nor does Wikipedia represent a single point of access for that person to contact and complain. Instead, problems have to be solved collectively; revisions cannot be imposed from above.

The benefits of this collective effort reveal themselves in surprising places: for instance, the unexpectedly famous, or perhaps infamous, Canadian student known as "Star Wars Kid." In 2002, this student taped himself swinging a golf ball retriever around and pretending it was a light saber. He then returned the video recorder to the school with this film still on it. Somehow, someone else found the footage and put it on the Internet, where it became incredibly popular, much to the student's great dismay. The phenomenon got a large amount of media attention, a lot of which included the student's name. But if you look at the Wikipedia entry for Star Wars Kid,[36] which is very informative, his name is not mentioned anywhere.[37] Why not? It turns out that the Wikipedia editors who worked on this page carried on an extensive discussion, found on the discussion page that corresponds to the article, about whether the article ought to include the student's name.[38] Some argued that Wikipedia stands for truth and openness, so his name ought to go in for the sake of complete disclosure.[39] Others argued that the student wanted privacy, and his name was not material to the cultural significance of the phenomenon. The second group won, and the student's name has stayed off the page. The dozens, perhaps hundreds, of volunteer editors who worked on this page

35. By building the system into the fabric of the two major servers, it can reach and assist a much greater audience than the currently available, often technologically daunting, circumvention approaches such as Tor. *See* Tor: Anonymity Online, http://www.torproject.org (last visited Apr. 7, 2010).

36. Wikipedia, Star Wars Kid, http://en.wikipedia.org/wiki/Star_Wars_Kid (last visited Apr. 7, 2010).

37. *See* Jonathan Zittrain, *A Simple Way To Avoid Being the Next Star Wars Kid*, SUNDAY TIMES (London), May 4, 2008, § 4, at 8.

38. *See* Wikipedia, Star Wars Kid Discussion Page, http://en.wikipedia.org/wiki/Talk:Star_Wars_Kid (last visited Apr. 7, 2010).

39. *See id.*

turned out to have greater discretion and respect for privacy than the mainstream media.

So this example begins to demonstrate the influence and respect that Wikipedia has attained among its editors and users. Once the losers of a Wikipedia editorial argument agree that the mob has spoken and reached an alternate conclusion, they will then enthusiastically enforce the outcome they argued so strongly against. There is real power in the fourth quadrant. And as long as there are more right people than wrong people, the fourth quadrant actually provides a means of policing so many of those online areas that cry out for policing.

There are, of course, some potential excesses and problems with the fourth quadrant. For instance, during the 1990s, there were two competing private solutions to the growing spam problem: the Mail Abuse Prevention System (MAPS), founded by Paul Vixie, and the Open Relay Behavior Modification System (ORBS). MAPS functioned as a mutual aid treaty of sorts—people would report to the organization with the IP addresses of spammers they had encountered. MAPS would keep a running list, and mail servers could sign up to subscribe to the list and block the specified IP addresses. Of course, it was hard for anyone on the blacklist to get off of it, since their e-mails asking for a second chance never got through. ORBS, on the other hand, used robots to send test e-mails. The system then condemned any mail server that let its test messages back through to itself, on the principle that those mail servers were obviously not vigilant enough. Each organization, frustrated by the other's divergent approach, blacklisted the other.[40]

CONCLUSION

In short, the fourth quadrant is not a cure-all. In fact, all four zones have their drawbacks. Nonetheless, the fourth quadrant, at this point, holds the most promising and underexplored solutions. The key is to draw directly upon the netizens, the Web servers, the Wikipedians, those who operate in good faith, to try to make the Internet a better place. Any Internet user can ask for help from the lower-right quadrant, or even initiate a project like mirror-as-you-link by simply starting it off and seeing what happens. Then, if it gathers enough momentum, it ends up in the fourth quadrant. A successful project just becomes the fabric of the web, moving from polyarchy to hierarchy just as the Web itself did. In many circumstances, this form of group self-help, empowered through technological protocols, can make progress on real problems without having to invoke the sometimes-effective but also structurally worrisome machinery of government regulation or corporate intervention.

40. *See* Kieren McCarthy, *The ORBS/MAPS Anti-spam Battle Revisited*, REGISTER, July 20, 2000, http://www.theregister.co.uk/2000/07/20/the_orbs_maps_antispam_battle/.