Code 2.0

Four Puzzles From Cyberspace

Everyone who is reading this book has used the Internet. Some have been in "cyberspace." The Internet is that medium through which your e-mail is delivered and web pages get published. It's what you use to order books on Amazon or to check the times for local movies at Fandango. Google is on the Internet, as are Microsoft "help pages."

But "cyberspace" is something more. Though built on top of the Internet, cyberspace is a richer experience. Cyberspace is something you get pulled "into," perhaps by the intimacy of instant message chat or the intricacy of "massively multiple online games" ("MMOGs" for short, or if the game is a role-playing game, then "MMORPGs"). Some in cyberspace believe they're in a community; some confuse their lives with their cyberspace existence. Of course, no sharp line divides cyberspace from the Internet. But there is an important difference in experience between the two. Those who see the Internet simply as a kind of Yellow-Pages-on-steroids won't recognize what citizens of cyberspace speak of. For them, "cyberspace" is simply obscure.

Some of this difference is generational. For most of us over the age of 40, there is no "cyberspace," even if there is an Internet. Most of us don't live a life online that would qualify as a life in "cyberspace." But for our kids, cyberspace is increasingly their second life. There are millions who spend hundreds of hours a month in the alternative worlds of cyberspace—later on we will focus on one of these worlds, a game called "Second Life."1 And thus while you may think to yourself, this alien space is nothing I need worry about because it's nowhere I'll ever be, if you care to understand anything about the world the next generation will inhabit, you should spend some time understanding "cyberspace."

That is the aim of two of the stories that follow. These two describe cyberspace. The other two describe aspects of the Internet more generally. My aim through these four very different stories is to orient by sometimes disorienting. My hope is that you 'll come to understand four themes that will recur throughout this book. At the end of this chapter, I come clean about the themes and provide a map. For now, just focus on the stories.

Borders

It was a very ordinary dispute, this argument between Martha Jones and her neighbors. 2 It was the sort of dispute that people have had since the start of neighborhoods. It didn't begin in anger. It began with a misunderstanding. In this world, misunderstandings like this are far too common. Martha thought about that as she wondered whether she should stay; there were other places she could go. Leaving would mean abandoning what she had built, but frustrations like this were beginning to get to her. Maybe, she thought, it was time to move on.

The argument was about borders—about where her land stopped. It seemed like a simple idea, one you would have thought the powers-that-be would have worked out many years before. But here they were, her neighbor Dank and she, still fighting about borders. Or rather, about something fuzzy at the borders—about something of Martha's that spilled over into the land of others. This was the fight, and it all related to what Martha did.

Martha grew flowers. Not just any flowers, but flowers with an odd sort of power. They were beautiful flowers, and their scent entranced. But, however beautiful, these flowers were also poisonous. This was Martha's weird idea: to make flowers of extraordinary beauty which, if touched, would kill. Strange no doubt, but no one said that Martha wasn't strange. She was unusual, as was this neighborhood. But sadly, disputes like this were not.

The start of the argument was predictable enough. Martha's neighbor, Dank, had a dog. Dank's dog died. The dog died because it had eaten a petal from one of Martha's flowers. A beautiful petal, and now a dead dog. Dank had his own ideas about these flowers, and about this neighbor, and he expressed those ideas—perhaps with a bit too much anger, or perhaps with anger appropriate to the situation.

“There is no reason to grow deadly flowers,” Dank yelled across the fence. “There’s no reason to get so upset about a few dead dogs,” Martha replied. “A dog can always be replaced. And anyway, why have a dog that suffers when dying? Get yourself a pain-free-death dog, and my petals will cause no harm.”

I came into the argument at about this time. I was walking by, in the way one walks in this space. (At first I had teleported to get near, but we needn’t complicate the story with jargon. Let’s just say I was walking.) I saw the two neighbors becoming increasingly angry with each other. I had heard about the disputed flowers—about how their petals carried poison. It seemed to me a simple problem to solve, but I guess it’s simple only if you understand how problems like this are created.

Dank and Martha were angry because in a sense they were stuck. Both had built a life in the neighborhood; they had invested many hours there. But both were coming to understand its limits. This is a common condition: We all build our lives in places with limits. We are all disappointed at times. What was different about Dank and Martha?

One difference was the nature of the space, or context, where their argument was happening. This was not “real space” but virtual space. It was part of what I call “cyberspace.” The environment was a “massively multiple online game” (“MMOG”), and MMOG space is quite different from the space we call real.

Real space is the place where you are right now: your office, your den, maybe by a pool. It’s a world defined by both laws that are man-made and others that are not. “Limited liability” for corporations is a man-made law. It means that the directors of a corporation (usually) cannot be held personally liable for the sins of the company. Limited life for humans is not a man-made law: That we all will die is not the result of a decision that Congress made. In real space, our lives are subject to both sorts of law, though in principle we could change one sort.

But there are other sorts of laws in real space as well. You bought this book, I trust, or you borrowed it from someone who did. If you stole it, you are a thief, whether you are caught or not. Our language is a norm; norms are collectively determined. As our norms have been determined, your “stealing” makes you a thief, and not just because you took it. There are plenty of ways to take something but not be thought of as a thief. If you came across a dollar blowing in the wind, taking the money will not make you a thief; indeed, not taking the money makes you a chump. But stealing this book from the bookstore (even when there are so many left for others) marks you as a thief. Social norms make it so, and we live life subject to these norms.

Some of these norms can be changed collectively, if not individually. I can choose to burn my draft card, but I cannot choose whether doing so will make me a hero or a traitor. I can refuse an invitation to lunch, but I cannot choose whether doing so will make me rude. I have choices in real life, but escaping the consequences of the choices I make is not one of them. Norms in this sense constrain us in ways that are so familiar as to be all but invisible.

MMOG space is different. It is, first of all, a virtual space—like a cartoon on a television screen, sometimes rendered to look three-dimensional. But unlike a cartoon, MMOG space enables you to control the characters on the screen in real time. At least, you control your character—one among many characters controlled by many others in this space. One builds the world one will inhabit here. As a child, you grew up learning the physics that governed the world of Road Runner and Wile E. Coyote (violent but forgiving); your children will grow up making the world of Road Runner and Wile E. Coyote (still violent, but maybe not so forgiving). They will define the space and then live out the story. Their choices will make the laws of that space real.

This is not to say that MMOG space is unreal. There is real life in MMOG space, constituted by how people interact. The “space” describes where people interact—much as they interact in real space no doubt, but with some important differences. In MMOG space the interaction is in a virtual medium. This interaction is “in” cyberspace. In 1990s terms, people “jack” into these virtual spaces, and they do things there. And “they” turns out to be many many people. As Edward Castronova estimates, “an absolute minimum figure would be 10 million [but my] guess is that it is perhaps 20 to 30 million ” participating in these virtual worlds.3 The “[t]ypical user spends 20–30 hours per week inside the

fantasy. Power users spend every available moment."4 As one essay estimates, "assuming just average contact time among these 9.4 million people, subscribers to virtual worlds could be devoting over 213 million hours per week to build their virtual lives. "5

The things people do there are highly varied. Some play role-playing games: working within a guild of other players to advance in status and power to some ultimate end. Some simply get together and gab: They appear (in a form they select, with qualities they choose and biographies they have written) in a virtual room and type messages to each other. Or they walk around (again, the ambiguity is not a slight one) and talk to people. My friend Rick does this as a cat —a male cat, he insists. As a male cat, Rick parades around this space and talks to anyone who 's interested. He aims to flush out the cat-loving sorts. The rest, he reports, he punishes.

Others do much more than gab. Some, for example, homestead. Depending on the world and its laws, citizens are given or buy plots of undeveloped land, which they then develop. People spend extraordinary amounts of time building a life on these plots. (Isn 't it incredible the way these people waste time? While you and I spend up to seventy hours a week working for firms we don 't own and building futures we're not sure we'll enjoy, these people are designing and building things and making a life, even if only a virtual one. Scandalous!) They build houses —by designing and then constructing them—have family or friends move in, and pursue hobbies or raise pets. They may grow trees or odd plants—like Martha's.

MMOG space grew out of "MUD" or "MOO" space.6 MUDs and MOOs are virtual worlds, too, but they are text-based virtual worlds. There are no real graphics in a MUD or MOO, just text, reporting what someone says and does. You can construct objects in MOO space and then have them do things. But the objects act only through the mediation of text. (Their actions are generally quite simple, but even simple can be funny. One year, in a MUD that was part of a cyberlaw class, someone built a character named JPosner. If you poked JPosner, he muttered, "Poking is inefficient." Another character was FEasterbrook. Stand in a room with FEasterbrook and use the word "fair," and FEasterbrook would repeat what you said, substituting the word "efficient." "It's not fair" became "You mean, it's not efficient.")

Although it was easy for people who liked texts or who wrote well to understand the attraction of these text-based realities, it was not so easy for the many who didn 't have that same fondness. MMOG space lifts that limit just a bit. It is the movie version of a cyberspace novel. You build things here, and they survive your leaving. You can build a house, and people walking down the street see it. You can let them come in, and in coming into your house, they see things about you. They can see how you construct your world. If a particular MMOG space permits it, they might even see how you 've changed the laws of the real world. In real space, for instance, people "slip and fall" on wet floors. In the MMOG space you've built, that "law" may not exist. Instead, in your world, wet floors may make people "slip and dance."

The best example of this space today is the extraordinary community of Second Life. In it, people create both things and community, the avatars are amazingly well crafted, and their owners spend hundreds of thousands of hours building things in this space that others see, and some enjoy. Some make clothes or hair styles, some make machines that make music. Whatever object or service the programming language allows, creators in Second Life are creating it. There are more than 100,000 residents of Second Life at the time of this writing. They occupy close to 2,000 servers housed in downtown San Francisco, and suck 250 kilowatts of electricity just to run the computers —about the equivalent of 160 homes.

But here we get back to Martha and Dank. In their exchange—when Martha blamed Dank for having a dog that died with pain—they revealed what was most amazing about that particular MMOG. Martha's remarks ("Why do you have a dog that suffers when dying? Get yourself a pain-free-death dog, and my petals will cause no harm ") should have struck you as odd. You may have thought, "How weird that someone would think that the fault lay not in the poisonous petals but in a dog that died with pain. " But in this space, Dank did have a choice about how his dog would die. Maybe not a choice about whether "poison" would "kill" a dog, but a choice about whether the dog would "suffer" when it "died." He also had a choice about whether a copy of the dog could be made, so that if it died it could be

“revived.” In MMOG space, these possibilities are not given by God. Or rather, if they are defined by God, then the players share the power of God. For the possibilities in MMOG space are determined by the code —the software, or architecture, that makes the MMOG space what it is. “What happens when” is a statement of logic; it asserts a relationship that is manifested in code. In real space we don ’t have much control over that code. In MMOG space we do.

So, when Martha said what she said about the dog, Dank made what seemed to me an obvious response. “Why do your flowers have to stay poisonous once they leave your land? Why not make the petals poisonous only when on your land? When they leave your land —when, for example, they are blown onto my land—why not make them harmless?”

It was an idea. But it didn’t really help. For Martha made her living selling these poisonous plants. Others (ok not many, but some) also liked the idea of this art tied to death. So it was no solution to make poisonous plants that were poisonous only on Martha ’s property, unless Martha was also interested in collecting a lot of very weird people on her land.

But the idea did suggest another. “Okay,” said Dank, “why not make the petals poisonous only when in the possession of someone who has ‘purchased’ them? If they are stolen, or if they blow away, then let the petals lose their poison. But when kept by the owner of the plant, the petals keep their poison. Isn ’t that a solution to the problem that both of us face?”

The idea was ingenious. Not only did it help Dank, it helped Martha as well. As the code existed, it allowed theft. 7 (People want reality in that virtual space; there will be time enough for heaven when heaven comes.) But if Martha could modify the code slightly so that theft 8 removed a plant’s poison, then “theft” would also remove the plant’s value. That change would protect the profit in her plants as well as protect Dank ’s dogs. Here was a solution that made both neighbors better off—what economists call a pareto superior move. And it was a solution that was as possible as any other. All it required was a change of code.

Think for a second about what’s involved here. “Theft” entails (at minimum) a change in possession. But in MMOG space “possession” is just a relation defined by the software that defines the space. That same code must also define the properties that possession yields. It might, like real space, distinguish between having a cake and eating it. Or it might erase that distinction, meaning you can “eat” your cake, but once it’s “eaten,” it magically reappears. In MMOG space you can feed a crowd with five loaves and two fishes, and it isn ’t even a miracle.9

So why not craft the same solution to Martha and Dank’s problem? Why not define ownership to include the quality of poisonousness, and possession without ownership to be possession without poison? If the world is designed this way, then it could resolve the dispute between Martha and Dank, not by making one of them change his or her behavior, but by changing the laws of nature to eliminate the conflict altogether.

We’re a short way into this not so short book, though what I’m about to say may make it a very short book indeed (for you at least). This book is all about the question raised by this simple story, and about any simplicity in this apparently simple answer. This is not a book about MMOG space or avatars. The story about Martha and Dank is the first and last example that will include avatars. But it is a book about cyberspace. My claim is that both “on the Internet” and “in cyberspace,” we will confront precisely the questions that Martha and Dank faced, as well as the questions that their solution raised. Both “on the Internet” and “in cyberspace,” technology constitutes the environment of the space, and it will give us a much wider range of control over how interactions work in that space than in real space. Problems can be programmed or “coded” into the story, and they can be “coded” away. And while the experience with gamers so far is that they don’t want virtual worlds to deviate too far from the real, the important point for now is that there is the capacity to make these worlds different. It is this capacity that raises the question that is at the core of this book: What does it mean to live in a world where problems can be coded away? And when, in that world, should we code problems away, rather than learn to work them out, or punish those who cause them?

It is not MMOG space that makes these questions interesting problems for law; the very same problems will arise outside of MMOG space, and outside MUDs and MOOs. The problems of these

spaces are problems of the Internet in general. And as more of our life becomes wired (and weird), in the sense that more of our life moves online, these questions will become more pressing.

But I have learned enough in this business to know that I can't convince you of this with an argument. (I've spent the last 12 years talking about this subject; at least I know what doesn 't work.) If you see the point, good for you. If you don't, I must show you. So my method for readers of the second sort must be more indirect. Proof, for them, will come in a string of stories, which aim to introduce and disorient. That, again, is the purpose of this chapter.

Let me describe a few other places and the oddities that inhabit them.

Governors

A state—call it "Boral"—doesn't like its citizens gambling, even if many of its citizens do like gambling. But the state is the boss; the people have voted; the law is as it is. Gambling in the state of Boral is illegal.

Then along comes the Internet. With the Net streaming into their homes through phones or cable lines, some citizens of Boral decide that Internet gambling is the next "killer app." A citizen of Boral sets up a "server" (a computer that is accessible on the Internet) that provides access to online gambling. The state doesn 't like it. It tells this citizen, "Shut down your server or we will lock you up."

Wise, if evasive, the gambling Boralian agrees to shut his server down—at least in the state of Boral. But he doesn't choose to leave the gambling business. Instead, he rents space on a server in an "offshore haven." This offshore web server hums away, once again making gambling available on the Net and accessible to the people of Boral via the Internet. Here 's the important point: Given the architecture of the Internet (at least as it was circa 1999), it doesn 't really matter where in real space the server is. Access doesn't depend on geography. Nor, depending on how clever the gambling sorts are, does access require that the user know anything about who owns, or runs, the real server. The user 's access can be passed through anonymizing sites that make it practically impossible in the end to know what went on where and with whom.

The Boral attorney general thus now faces a difficult problem. She may have moved the server out of her state, but she hasn 't succeeded in reducing Boralian gambling. Before the Net, she would have had a group of people she could punish —those running gambling sites, and those who give those places custom. Now, the Net has made them potentially free from punishment —at the least because it is more difficult to know who is running the server or who is gambling. The world for this attorney general has changed. By going online, the gamblers moved into a world where this behavior is no longer regulable.

By "regulable" I mean simply that a certain behavior is capable of regulation. The term is comparative, not absolute —in some place, at some time, a certain behavior will be more regulable than at another place and in another time. My claim about Boral is simply that the Net makes gambling less regulable there than it was before the Net. Or at least, in a sense that will become clearer as the story continues, with the architecture of the Net as it originally was, life on the Net is less regulable than life off the Net.

Jake's Communities

If you had met Jake at a party in Ann Arbor (were Jake at a party in Ann Arbor), you would have forgotten him. 10 If you didn't forget him, you might have thought, here's another quiet, dweeby University of Michigan undergraduate, terrified of the world, or, at least, of the people in the world.

You wouldn't have figured Jake for an author—indeed, quite a famous short-story author, at least within his circles. In fact, Jake is not just a famous author, he was also a character in his own stories. But who he was in his stories was quite different from who he was in "real" life—if, that is, after reading his stories you still thought this distinction between "real life" and "not real life" made much sense.

Jake wrote stories about violence—about sex as well, but mainly about violence. They seethed with hatred, especially of women. It wasn 't enough to rape a woman, she had to be killed. And it wasn't

enough that she was killed, she had to be killed in a particularly painful and tortured way. This is, however unfortunate, a genre of writing. Jake was a master of this genre.

In real space Jake had quite successfully hidden this propensity. He was one of a million boys: unremarkable, indistinguishable, harmless. Yet however inoffensive in real space, the harmfulness he penned in cyberspace was increasingly well known. His stories were published in USENET, in a group called alt.sex.stories.

USENET isn't itself a network, except in the sense that the personal ads of a national newspaper are part of a network. Strictly speaking, USENET is the product of a protocol —a set of rules named the network news transfer protocol (NNTP)—for exchanging messages intended for public viewing. These messages are organized into "newsgroups," and the newsgroups are organized into subjects. Most of the subjects are quite technical, many are related to hobbies, and some are related to sex. Some messages newsgroups come with pictures or movies, but some, like Jake 's, are simply stories.

There are thousands of newsgroups, each carrying hundreds of messages at any one time. Anyone with access to a USENET server can get access to the messages (or at least to the ones his administrator wants him to read), and anyone with access can post a message or respond to one already posted. Imagine a public bulletin board on which people post questions or comments. Anyone can read the board and add his or her own thoughts. Now imagine 15,000 boards, each with hundreds of "threads" (strings of arguments, each tied to the next). That, in any one place, is USENET. Now imagine these 15,000 boards, with hundreds of threads each, on millions of computers across the world. Post a message in one group, and it is added to that group 's board everywhere. That, for the world, is USENET.

Jake, as I said, posted to a group called alt.sex.stories. "Alt" in that name refers to the hierarchy that the group sits within. Initially, there were seven primary hierarchies. 11 "Alt" was created in reaction to this initial seven: Groups are added to the seven through a formal voting process among participants in the groups. But groups are added to "alt" based solely on whether administrators choose to carry them, and, generally, administrators will carry them if they are popular, as long as their popularity is not controversial.

Among these groups that are carried only on demand, alt.sex.stories is quite popular. As with any writing space, if stories are "good" by the standards of the space—if they are stories that users of the space demand—they are followed and their authors become well known.

Jake's stuff was very valuable in just this sense. His stories, about kidnapping, torturing, raping, and killing women, were as graphic and repulsive as any such story could be —which is why Jake was so famous among like-minded sorts. He was a supplier to these people, a constant and consistent fix. They needed these accounts of innocent women being violated, and Jake supplied them for free.

One night in Moscow, a sixteen-year-old girl read a story by Jake. She showed it to her father, who showed it in turn to Richard DuVal, a Michigan alum. DuVal was shocked at the story, and angry that it bore the tag "umich.edu" on the story's header. He called his alma mater and complained. They took the complaint seriously. 12

The university contacted the police; the police contacted Jake—with handcuffs and a jail cell. A slew of doctors examined him. Some concluded that he was a threat. The local prosecutors agreed with these doctors, especially after his computer was seized and e-mails were discovered between Jake and a Canadian fan who was planning to re-enact in real space one of the stories Jake published in cyberspace. At least, that 's what the e-mails said. No one could tell for certain what the two men really intended. Jake said it was all pure fiction, and indeed, there was no evidence to prove otherwise.

Nonetheless, federal charges were brought against Jake for the transmission of a threat. Jake said that his stories were only words, protected by the First Amendment to the U.S. Constitution. A month and a half later, a court agreed. The charges were dropped, 13 and Jake returned to the special kind of obscurity that had defined his life before.

I don't care so much just now about whether Jake Baker's words should have been protected by the

Constitution. My concern is Jake Baker himself, a person normed into apparent harmlessness in real space, but set free in cyberspace to become the author of this violence. People said Jake was brave, but he wasn't "brave" in real space. He didn't express his hatred in classes, among friends, or in the school newspaper. He slithered away to cyberspace, and only there did his deviancy flourish.

He did this because of something about him and something about cyberspace. Jake was the sort who wanted to spread stories of violence, at least if he could do so without public account. Cyberspace gave Jake this power. Jake was in effect an author and publisher in one. He wrote stories, and as quickly as he finished them he published them —to some thirty million computers across the world within a few days. His potential audience was larger than twice that for the top fifteen best-selling novels combined, and though he made nothing from his work, the demand for it was high. Jake had discovered a way to mainline his depravity into the veins of a public for whom this stuff was otherwise quite difficult to find. (Even Hustler wouldn't publish the likes of this.)

Of course, there were other ways Jake could have published. He could have offered his work to Hustler, or worse. But no real-world publication would have given Jake a comparable audience. Jake 's readership was potentially millions, stretching across country and continent, across culture and taste.

This reach was made possible by the power in the network: Anyone anywhere could publish to everyone everywhere. The network allowed publication without filtering, editing, or, perhaps most importantly, responsibility. One could write what one wanted, sign it or not, post it to machines across the world, and within hours the words would be everywhere. The network removed the most important constraint on speech in real space —the separation of publisher from author. There is vanity publishing in real space, but only the rich can use it to reach a broad audience. For the rest of us, real space affords only the access that the publishers want to give us.

Thus cyberspace is different because of the reach it allows. But it is also different because of the relative anonymity it permits. Cyberspace permitted Jake to escape the constraints of real space. He didn't "go to" cyberspace when he wrote his stories, in the sense that he didn't "leave" Ann Arbor. But when he was "in" cyberspace, it allowed him to escape the norms of Ann Arbor. He was free of real-life constraints, of the norms and understandings that had successfully formed him into a member of a college community. Maybe he wasn't perfectly at home; maybe he wasn't the happiest. But the world of the University of Michigan had succeeded in steering him away from the life of a psychopath — except when it gave him access to the Net. On the Net he was someone else.

As the Internet has grown, it has produced many more opportunities for Jake-like characters — characters that do things in the virtual world that they would never do in the real world. One of the most popular MMOGs is a game called "Grand Theft Auto." In this game, one practices committing crimes. And one of the most troubling uses of video chat is the practice of virtual-prostitution by children. As the New York Times recently reported, thousands of children spend hundreds of hours prostituting themselves online. Sitting in the "privacy" of their own bedroom, using the iSight camera their parents gave them for Christmas, a 13-year-old girl or boy enacts the sexual behavior demanded by the audience. The audience gets their fix of sexual perversion. The kid gets money, and whatever psychological baggage this behavior creates. 14

It is impossibly difficult to look across this range of Jake-like characters and not think that, at some point, the virtual has crossed over into something real. Or, at least, the virtual has real effects —either on those who live it, or on those who live with them.15 When Jake was prosecuted, many First Amendment defenders argued his words, however vivid, never crossed into reality. And no doubt, there is a difference between writing about rape and raping, just as there is a difference between an actor enacting rape and actually raping someone. But I take it that all concede a line is crossed somewhere as we move across this range of Jake-like characters. If a parent was untroubled by the virtual prostitution of her son in his bedroom, we would not understand that to be principled free speech activism, even if the only "prostitution" was the son describing in text how he was molested by those in the chat.

But my point is not to draw lines between the acceptable virtual dual-lives and the unacceptable. It is

instead to remark that this space enables more of this duality. And though part of this duality is always "only virtual," and sometimes "only words," real-space regulators (whether parents or governments) will feel compelled to react. The Net enables lives that were previously impossible, or inconvenient, or uncommon. At least some of those virtual lives will have effects on non-virtual lives —both the lives of the people living in the virtual space, and the lives of those around them.

Worms That Sniff

A "worm" is a bit of computer code that is spit out on the Net and works its way into the systems of vulnerable computers. It is not a "virus" because it doesn't attach itself to other programs and interfere with their operation. It is just a bit of extra code that does what the code writer says. The code could be harmless and simply sit on someone 's machine. Or it could be harmful and corrupt files or do other damage that its author commands.

Imagine a worm designed to do good (at least in the minds of some). Imagine that the code writer is the FBI and that the FBI is looking for a particular document belonging to the National Security Agency (NSA). Suppose that this document is classified and illegal to possess without the proper clearance. Imagine that the worm propagates itself on the Net, finding its way onto hard disks wherever it can. Once on a computer 's hard disk, it scans the entire disk. If it finds the NSA document, it sends a message back to the FBI saying as much. If it doesn't, it erases itself. Finally, assume that it can do all this without "interfering" with the operation of the machine. No one would know it was there; it would report back nothing except that the NSA document was on the hard disk.

Is this an unconstitutional worm? This is a hard question that at first seems to have an easy answer. The worm is engaging in a government-initiated search of citizens ' disks. There is no reasonable suspicion (as the law ordinarily requires) that the disk holds the document for which the government is searching. It is a generalized, suspicionless search of private spaces by the government.

From the standpoint of the Constitution—the Fourth Amendment in particular—you don't get any worse than that. The Fourth Amendment was written against the background of just this sort of abuse. Kings George II and George III would give officers a "general warrant" authorizing them to search through private homes looking for evidence of a crime. 16 No suspicion was needed before the officer ransacked your house, but because he had a warrant, you were not able to sue the officer for trespass. The aim of the Fourth Amendment was to require at least suspicion, so that the burden of the search fell on a reasonably chosen class. 17

But is the worm really the same as the King's general search? One important difference is this: Unlike the victims of the general searches that the Framers of our Constitution were concerned about, the computer user never knows that his or her disk is being searched by the worm. With the general search, the police were breaking into a house and rummaging through private stuff. With the worm, it is a bit of computer code that does the breaking, and (I've assumed) it can "see" only one thing. And perhaps more importantly, unlike the general search, the worm learns little and leaves no damage after it 's finished: The code can't read private letters; it doesn't break down doors; it doesn't interfere with ordinary life. And the innocent have nothing to fear.

The worm is silent in a way that King George's troops were not. It searches perfectly and invisibly, discovering only the guilty. It does not burden the innocent; it does not trouble the ordinary citizen; it captures only what is outside the protection of the law.

This difference complicates the constitutional question. The worm's behavior is like a generalized search in that it is a search without suspicion. But it is unlike the historical generalized search in that it creates no disruption of ordinary life and "discovers" only contraband. In this way, the worm is like a dog sniff—which at least at airports is constitutionally permissible without probable cause 18—but better. Unlike the dog sniff, the worm doesn't even let the computer user know when there is a search (and hence the user suffers no particularized anxiety).

Is the worm, then, constitutional? That depends on your conception of what the Fourth Amendment protects. In one view, the amendment protects against suspicionless governmental invasions, whether

those invasions are burdensome or not. In a second view, the amendment protects against invasions that are burdensome, allowing only those for which there is adequate suspicion that guilt will be uncovered. The paradigm case that motivated the framers does not distinguish between these two very different types of protections, because the technology of the time wouldn't distinguish either. You couldn't—technically—have a perfectly burdenless generalized search in 1791. So they didn't—technically—express a view about whether such a search should be constitutionally proscribed. It is instead we who must choose what the amendment is to mean.

Let's take the example one step further. Imagine that the worm does not search every machine it encounters, but instead can be put on a machine only with judicial authorization —say, a warrant. Now the suspicionless-search part of the problem has been removed. But now imagine a second part to this rule: The government requires that networks be constructed so that a worm, with judicial authorization, could be placed on any machine. Machines in this regime, in other words, must be made worm-ready, even though worms will be deployed only with judicial warrant.

Is there any constitutional problem with this? I explore this question in much greater detail in Chapter 11, but for now, notice its salient feature. In both cases, we are describing a regime that allows the government to collect data about us in a highly efficient manner —inexpensively, that is, for both the government and the innocent. This efficiency is made possible by technology, which permits searches that before would have been far too burdensome and invasive. In both cases, then, the question comes to this: When the ability to search without burden increases, does the government 's power to search increase as well? Or, more darkly, as James Boyle puts it: "Is freedom inversely related to the efficiency of the available means of surveillance? " For if it is, as Boyle puts it, then "we have much to fear."19

This question, of course, is not limited to the government. One of the defining features of modern life is the emergence of technologies that make data collection and processing extraordinarily efficient. Most of what we do —hence, most of what we are—is recorded outside our homes. When you make telephone calls, data are recorded about whom you called, when, how long you spoke, and how frequently you made such calls. 20 When you use your credit cards, data are recorded about when, where, what, and from whom you made purchases. When you take a flight, your itinerary is recorded and possibly profiled by the government to determine whether you are likely to be a terrorist. 21 If you drive a car in London, cameras record your license plate to determine whether you 've paid the proper "congestion tax." No doubt Hollywood's image of counter-terrorist units—where one person sitting behind a terminal instantly tracks the life of another—is wrong. But it need not be terribly wrong for much longer. It may not be easy to imagine systems that follow an individual wherever he goes, but it is easy to imagine technologies that gather an extraordinary amount of data about everything we do and make those data accessible to those with the proper authorization. The intrusiveness would be slight, and the payoff could be great.

Both private and public monitoring in the digital age, then, have the same salient feature: monitoring, or searching, can increase without increasing the burden on the individual searched. Both present a similar question: How should we think about this change? How should the protection the framers gave us be applied to a world the framers couldn't even imagine?

Themes

Four stories, four themes, each a window into one aspect of cyberspace that will be central in all that follows. My aim in the balance of this book is to work through the issues raised by these four themes. I thus end this chapter with a map of the four, laid out in the order they will appear in the balance of the book. That order begins with story number two.

Regulability

"Regulability" is the capacity of a government to regulate behavior within its proper reach. In the context of the Internet, that means the ability of the government to regulate the behavior of (at least) its citizens while on the Net. The story about Boral was thus a story about regulability, or more

specifically, about the changes in regulability that cyberspace brings. Before the Internet, it was relatively easy for the attorney general of Boral to control commercial gambling within her jurisdiction; after the Internet, when the servers moved outside of Boral, regulation became much more difficult.

For the regulator, this is just a particular instance of a much more general story. To regulate well, you need to know (1) who someone is, (2) where they are, and (3) what they ’re doing. But because of the way the Internet was originally designed (and more on this below), there was no simple way to know (1) who someone is, (2) where they are, and (3) what they ’re doing. Thus, as life moved onto (this version of) the Internet, the regulability of that life decreased. The architecture of the space —at least as it was—rendered life in this space less regulable.

The balance of Part I is about regulability. Can we imagine a more regulable cyberspace? Is this the cyberspace we are coming to know?

Regulation by Code

The story about Martha and Dank is a clue to answering this question about regulability. If in MMOG space we can change the laws of nature —make possible what before was impossible, or make impossible what before was possible —why can’t we change regulability in cyberspace? Why can’t we imagine an Internet or a cyberspace where behavior can be controlled because code now enables that control?

For this, importantly, is just what MMOG space is. MMOG space is “regulated,” though the regulation is special. In MMOG space regulation comes through code. Important rules are imposed, not through social sanctions, and not by the state, but by the very architecture of the particular space. A rule is defined, not through a statute, but through the code that governs the space.

This is the second theme of this book: There is regulation of behavior on the Internet and in cyberspace, but that regulation is imposed primarily through code. The differences in the regulations effected through code distinguish different parts of the Internet and cyberspace. In some places, life is fairly free; in other places, it is more controlled. And the difference between these spaces is simply a difference in the architectures of control —that is, a difference in code.

If we combine the first two themes, then, we come to a central argument of the book: The regulability described in the first theme depends on the code described in the second. Some architectures of cyberspace are more regulable than others; some architectures enable better control than others. Therefore, whether a part of cyberspace —or the Internet generally—can be regulated turns on the nature of its code. Its architecture will affect whether behavior can be controlled. To follow Mitch Kapor, its architecture is its politics. 22

And from this a further point follows: If some architectures are more regulable than others —if some give governments more control than others—then governments will favor some architectures more than others. Favor, in turn, can translate into action, either by governments, or for governments. Either way, the architectures that render space less regulable can themselves be changed to make the space more regulable. (By whom, and why, is a matter we take up later.)

This fact about regulability is a threat to those who worry about governmental power; it is a reality for those who depend upon governmental power. Some designs enable government more than others; some designs enable government differently; some designs should be chosen over others, depending upon the values at stake.

Latent Ambiguity

The worm tells a different story still. Though it is a technology for searching, the worm ’s function differs from “searching” in real space. In real space, a search carries costs: the burdens of the search, the insecurities it might create, the exposure it might make possible to invasions beyond a legitimate reach. 23 The worm erases those costs: The burden is gone, the search is (practically) invisible, and the searching technology is programmed to find only what is illegal. This raises a question about how

such a search should, under the Constitution, be understood.

A fair view of the Constitution's protections could go in either of two ways. It may be that we see the worm's invasion as inconsistent with the dignity that the amendment was written to protect, 24 or it may be that we see the invasion of the worm as so unobtrusive as to be reasonable. The answer could be either, which means that the change reveals what I will call "a latent ambiguity" in the original constitutional rule. In the original context, the rule was clear (no generalized search), but in the current context, the rule depends upon which value the Constitution was meant to protect. The question is now ambiguous between (at least) two different answers. Either answer is possible, depending upon the value, so now we must choose one or the other.

You may not buy my story about the worm. You may think it is pure science fiction. But by the end of the book, I will convince you that there are any number of cases in which a similar ambiguity troubles our constitutional past. In many of them our Constitution yields no answer to the question of how it should be applied, because at least two answers are possible —in light of the choices that the framers actually made and given the technologies of today.

For Americans, this ambiguity creates a problem. If we lived in an era when courts felt entitled to select the value that produced an answer that made the most sense in the context, there would be no problem. Latent ambiguities would be answered by choices made by judges —the framers could have gone either way, but our judges choose to go this way.

But we don't live in such an era, and so we don't have a way for courts to resolve these ambiguities. As a result, we must rely on other institutions. My claim is a dark one: We have no such institutions. If our ways don 't change, our constitution in cyberspace will be a thinner and thinner regime.

Cyberspace will present us with ambiguities over and over again. It will press this question of how best to go on. We have tools from real space that will help resolve the interpretive questions by pointing us in one direction or another, at least some of the time. But in the end the tools will guide us even less than they do in real space and time. When the gap between their guidance and what we do becomes obvious, we will be forced to do something we 're not very good at doing—deciding what we want, and what is right.

Competing Sovereigns

But regulation by whom? For the rules are different in one place versus another.

This was one important issue raised by Jake Baker. Jake lived in Ann Arbor, Michigan. His life there was subject to the norms of Ann Arbor, and he apparently adapted to these norms reasonably well. The authority of that space governed Jake, and, as far as anyone knew, it appeared to govern him exclusively.

But in cyberspace, Jake's behavior changed, in part because the norms of the space were different. That created the problem. For when Jake "went to" cyberspace, he didn't leave real space. In particular, he never left Ann Arbor. While sitting in a dorm at the University of Michigan, he was able to teleport himself —in the only normatively significant sense—to a different world where the norms of civility and decency that governed outside his dorm room did not reign. Cyberspace gave Jake the chance to escape Ann Arbor norms and to live according to the norms of another place. It created a competing authority for Jake and gave him the chance to select between these competing authorities merely by switching his computer on or off.

Again, my point is not that no similar possibility exists in real space—it plainly does. There is no doubt a Jake living in Hackensack, New Jersey (a suburban town with suburban values), who drives every night into lower Manhattan and live s for a few hours according to the "rules" of lower Manhattan. Those rules are not the rules of Hackensack; that life is different. Like Ann Arbor Jake, the Hackensack Jake lives under competing authorities. But between the lives of these two Jakes, there is a difference in degree that ripens into a difference in kind: It is at least conceivable that the Ann Arbor Jake raises a more significant problem for Ann Arbor than the Hackensack Jake raises for Hackensack. The differences could well be greater, and the effect more pervasive.

Nor should we think too narrowly about the competing normative communities into which a Jake might move. “Escape” here can be good or bad. It is escape when a gay teen in an intolerant small town can leave the norms of that town through a gay chat room on America Online; 25 it is escape when a child predator escapes the norms of ordinary society and engages a child in online sex. 26 Both escapes are enabled by the architecture of cyberspace as we now know it. Our attitudes about each, however, are very different. I call the first escape liberating and the second criminal. There are some who would call both escapes criminal, and some who would call both liberating. But the question isn ’t about name-calling, it’s about the consequences of living in a world where we can occupy both sorts of space at the same time. When 50 people from 25 jurisdictions around the world spend 2,000 hours building a virtual community in Second Life that is housed on servers in San Francisco, what claim should real world jurisdictions have over that activity? Which of the 25 jurisdictions matters most? Which sovereign should govern?

These four themes frame everything that follows. They also map the understanding that I want this book to provide. Regulation in cyberspace can help us see something important about how all regulation works. That’s the lesson of the first theme, “regulability.” It will also introduce a regulator (“code”) whose significance we don’t yet fully understand. That’s the second theme, “Regulation by Code.” That regulation will render ambiguous certain values that are fundamental to our tradition. Thus, the third theme, “latent ambiguity.” That ambiguity will require us, the United States, to make a choice. But this choice is just one among many that many sovereigns will have to make. In the end the hardest problem will be to reckon these “competing sovereigns,” as they each act to mark this space with their own distinctive values.

I explore these four themes against a background that, as I said at the start, has changed significantly since the first edition of this book. When I first wrote the book, two ideas seemed to dominate debate about the Net: first, that the government could never regulate the Net, and second, that this was a good thing. Today, attitudes are different. There is still the commonplace that government can ’t regulate, but in a world drowning in spam, computer viruses, identity theft, copyright “piracy,” and the sexual exploitation of children, the resolve against regulation has weakened. We all love the Net. But if some government could really deliver on the promise to erase all the bads of this space, most of us would gladly sign up.

Yet while attitudes about the Net have progressed, my own views have not. I still believe the Net can be regulated. I still believe that the obvious consequence of obvious influences will be to radically increase the ability of governments to regulate this Net. I also still believe that, in principle, this is not a bad thing. I am not against regulation, properly done. I believe regulation is essential to preserving and defending certain fundamental liberties. But I also still believe that we are far from a time when our government in particular can properly regulate in this context. This is both because of a general skepticism about government —grounded in a disgust about the particular form of corruption that defines how our government functions —and a particular skepticism about government—that it has not yet fully recognized just how regulation in the digital age works.

No doubt this particular mix of views will continue to puzzle some. How can I believe in regulation and yet be so skeptical about government? But it doesn’t take much imagination to understand how these apparently conflicting views can go together. I take it we all believe in the potential of medicine. But imagine your attitude if you were confronted with a “doctor” carrying a vial of leeches. There’s much we could do in this context, or at least, that is my view. But there’s a very good reason not to want to do anything with this particular doctor.

Chapter Two Notes Edit

1. Second Life--"What is Second Life?", available at link #3. The currently leading game, World of Warcraft, claims more than five million alone. Availab link #4.
    - Link 3: http://secondlife.com/whatis/ [cached]
2. Link 4: http://www.blizzard.com/press/051219.shtml [cached]
3. It is also hypothetical. I have constructed this story in light of what could be, and in places is. I'm a law

professor; I make up hypotheticals for a living.

4. Edward Castronova, *Synthetic Worlds: The Business and Culture of Online Games* (Chicago: University of Chicago Press, 2005), 55.
5. Ibid., 2.
6. John Crowley and Viktor Mayer-Schoenberger, "Napster's Second Life?--The Regulatory Challenges of Virtual Worlds" (Kennedy School of Government, Working Paper No. RWP05?052, 2005), 8.
7. "MUD" has had a number of meanings, originally Multi-User Dungeon, or Multi-User Domain. A MOO is a "MUD, object-oriented." Sherry Turkle's analysis of life in a MUD or MOO, *Life on the Screen: Identity in the Age of the Internet* (New York: Simon and Schuster, 1995), is still a classic. See also Elizabeth Reid, "Hierarchy and Power: Social Control in Cyberspace," in *Communities in Cyberspace,* edited by Marc A. Smith and Peter Kollock (New York: Routledge, 1999), 107. The father--or god--of a MUD named LambdaMOO is Pavel Curtis. See his account in "Mudding: Social Phenomena in Text-Based Virtual Realities," in Stefik, *Internet Dreams,* 265?92. For two magical pages of links about the history of MUDs, see Lauren P. Burka, "The MUDline," available at link #5; and Lauren P. Burka, "The MUDdex," available at link #6.
    - Link 5: http://www.linnaean.org/~lpb/muddex/mudline.html [cached]
8. Link 6: http://www.linnaean.org/~lpb/muddex/ [cached]
9. This is not a rare feature of these spaces. It is indeed quite common, at least within role playing games. Julian Dibbell described to me a "parable" he recognized within Ultima Online: As he calls it, the "case of the stolen Bone Crusher." "I got two offers for a Bone Crusher, which is a powerful sort of mace for bopping monsters over the head. I started dealing with both of them. At a certain point I was informed by one of them that the Bone Crusher had been stolen. So I said, `I'll go buy it from the other guy. But, by the way, who was it that stole the Bone Crusher, do you know?' He said the name of the other guy. I was faced with this dilemma of was I going to serve as a fence for this other guy knowingly. And so, I turned to my mentor in this business, the guy who had been doing this for years and makes six figures a year on it, and, you know, I thought of him as an honest guy. So I sort of thought and maybe even hoped that he would just say just walk away. We don't do these kinds of deals in our business. We don't need that, you know, blah, blah, blah. But he said, `Well, you know, thieving is built into the game. It is a skill that you can do. So fair is fair.' It is in the code that you can go into somebody's house and practice your thieving skills and steal something from them. And so, I went ahead and did the deal but there was this lingering sense of, `Wow, in a way that is completely arbitrary that this ability is in the code here whereas, you know, if it wasn't built into the code it would be another story; they would have stolen it in another way.' . . ." "But in Ultima Online, it is very explicitly understood that the code allows you to steal and the rules allow you to steal. For me what was interesting was that there remains this gray area. It made it an interesting game, that you were allowed to do something that was actually morally shady and you might have to decide for yourself. I'm not sure that now, going back to the deal, I would have taken the fenced item. I've been stolen from in the game, according to the rules, and it feels like shit." Audio Tape: Interview with Julian Dibbell (1/6/06) (on file with author).
10. And only theft. If you transferred the property for a different purpose--say, sold the property--then the feature wouldn't change.
11. Compare Susan Brenner, "The Privacy Privilege: Law Enforcement, Technology and the Constitution," *Journal of Technology Law and Policy* 7 (2002): 123, 160. ("Pool tables in cyberspace do not require legs in this place where gravity does not exist"), citing Neal Stephenson, *Snow Crash* (New York: Bantam, 1992), 50 (in the Metaverse, tables only have tops, not legs).
12. Jake Baker's given name was Abraham Jacob Alkhabaz, but he changed his name after his parents' divorce. See Peter H. Lewis, "Writer Arrested After Sending Violent Fiction Over Internet," *New York Times,* February 11, 1995, 10.
13. The seven are comp, misc, news, rec, sci, soc, and talk. See Henry Edward Hardy, "The History of the Net, v8.5," September 28, 1993, available at link #7.
    - Link 7: http://www.eff.org/Net_culture/net.history.txt [cached]
14. I have drawn from Jonathan Wallace and Mark Mangan's vivid account in *Sex, Laws, and Cyberspace* (New York: M&T Books, 1996), 63?81, though more interesting variations on this story circulate on the Net (I'm playing it safe).
15. See *United States v. Baker,* 890 FSupp 1375, 1390 (EDMich 1995); see also Wallace and Mangan, *Sex, Laws, and Cyberspace,* 69?78.
16. See Kurt Eichenwald, "Through His Webcam, a Bot Joins a Sordid Online World," *New York Times* ,

December 19, 2005, A1.

17. See C. Anderson and B. Bushman, "Effects of Violent Video Games on Aggressive Behavior, Aggressive Cognition, Aggressive Affect, Physiological Arousal, and Prosocial Behavior: A Meta-Analytic Review of the Scientific Literature," *Psychological Science* 12(5) (2001): 353?359, available at link #8; Jonathan L. Freedman, *Media Violence and Its Effect on Aggression* (Toronto: Toronto University Press, 2002).
    - Link 8: http://www.psychology.iastate.edu/faculty/caa/abstracts/2000-2004/01AB.pdf [cached]

18. See William J. Stuntz, "The Substantive Origins of Criminal Procedure," *Yale Law Journal* 105 (1995): 393, 406?7.

19. See, for example, Thomas K. Clancy, "The Role of Individualized Suspicion in Assess ing the Reasonableness of Searches and Seizures," *University of Memphis Law Review* 25 (1995): 483, 632. "Individualized suspicion . . . has served as a bedrock protection against unjustified and arbitrary police actions."

20. See *United States v. Place,* 462 US 696, 707 (1983).

21. James Boyle, *Shamans, Software, and Spleens: Law and the Construction of the Information Society* (Cambridge, Mass.: Harvard University Press, 1996), 4.

22. See Susan Freiwald, "Uncertain Privacy: Communication Attributes After the Digital Telephony Act," *Southern California Law Review* 69 (1996): 949, 951, 954.

23. Cf. John Rogers, "Bombs, Borders, and Boarding: Combatting International Terrorism at United States Airports and the Fourth Amendment," *Suffolk Transnational Law Review* 20 (1997): 501, n.201.

24. See Mitchell Kapor, "The Software DesignManifesto," available at link #9; David Farber, "A Note on the Politics of Privacy and Infrastructure," November 20, 1993, available at link #10; "Quotations," available at link #11; see also Pamela Samuelson et al., "A Manifesto Concerning the Legal Protection of Computer Programs," *Columbia Law Review* 94 (1994): 2308. Steven Johnson powerfully makes a similar point: "All works of architecture imply a worldview, which means that all architecture is in some deeper sense political"; see *Interface Culture: How New Technology Transforms the Way We Create and Communicate* (San Francisco: Harper Edge, 1997), 44. The Electronic Frontier Foundation, originally cofounded by Mitch Kapor and John Perry Barlow, has updated Kapor's slogan "architecture is politics" to "architecture is policy." I prefer the original.
    - Link 9: http://hci.stanford.edu/bds/1-kapor.html [cached]

25. Link 10: http://www.interesting-people.org/archives/interesting-people/199311/msg00088.html [cached]

26. Link 11: http://www.cs.arizona.edu/icon/oddsends/farber.htm [cached]

27. Jed Rubenfeld has developed most extensively an interpretive theory that grounds meaning in a practice of reading across time, founded on paradigm cases; see "Reading the Constitution as Spoken," *Yale Law Journal* 104 (1995): 1119, 1122; and "On Fidelity in Constitutional Law," *Fordham Law Review* 65 (1997): 1469. See also Jed Rubenfeld, *Freedom and Time: A Theory of Constitutional Government* (New Haven: Yale University Press, 2001).

28. See *Minnesota v. Dickerson,* 508 US 366, 380 (1993) (Justice Antonin Scalia concurring: "I frankly doubt . . . whether the fiercely proud men who adopted our Fourth Amendment would have allowed themselves to be subjected, on mere suspicion of being armed and dangerous, to such indignity. . . .").

29. See Steve Silberman, "We're Teen, We're Queer, and We've Got E-Mail," *Wired* (Novem ber 1994): 76, 78, 80, reprinted in *Composing Cyberspace: Identity, Community, and Knowledge in the Electronic Age,* edited by Richard Holeton (Boston: McGraw-Hill, 1998), 116.

30. Cf. *United States v. Lamb,* 945 F.Supp 441 (NDNY 1996). (Congress's intent in passing the Child Protection Act was to regulate child pornography via computer transmission, an interest legitimately related to stemming the flow of child pornography.)