FINN BRUNTON

Constitutive Interference: Spam and Online Communities

Introduction: "Spam," "Community," and Other Places

"COMMUNITY" AND "SPAM" ARE BOTH difficult to talk clearly about, outstanding examples of words as places rather than fixed objects, zones where we can meet and negotiate. These words act as open space for the movements of great powers and agendas, as well as for small roving groups of actors. "Community" enables conversations. For early sociologists like Ferdinand Tönnies and Emile Durkheim, "community" (along with the similarly spacious "society") makes room for describing the condition of people together after the advent of industrial modernity—indeed, for drawing opposing conclusions about that condition. For Jean Lave and Etienne Wenger, "communities of practice" are areas for theorizing learning and, later, knowledge management. For the Chicago School of sociology—and Marshall McLuhan, and those in his aphoristic wake—"community," among other meanings, frames the conversation around theories of media, like the visionary "Great Community" whose possibility John Dewey discerns in the artful adoption of "the physical machinery of transmission and circulation."[1]

Two qualities unite these disparate uses of "community." First, deep uncertainties about properties and edges: Is community about location and face-to-face proximity, or does it consist of affective bonds that can be established by a text message just as well as an embrace? Does it encompass huge swathes of human experience, or is it at best a way to outline a formal arrangement of shared interests? Where is the lower boundary—when does a group of atomized individuals, a scattered and manifold accumulation of people and groups (to take some of the common adjectives drawn on for the pre- or anticommunal state) transform into a community? Where is the

ABSTRACT This paper examines the large and strange domain of spam and the role of spamming in the development of virtual communities and Internet governance. It contends that spamming operates by exploiting the tension between communities and the technological infrastructure that underlies them, and that these exploits illuminate both the complex relationship between virtual communities and the governments within which they operate and the changing politics of attention online. REPRESENTATIONS 117. Winter 2012 ISSN 0734-6018, electronic ISSN 1533-855X, pages 30–58. DOI: 10.1525/rep.2012.117.1.30.

upper boundary: when does a sufficiently large or sufficiently self-reflective community become a "society," a "public," a citizenry, or another communal apotheosis? (And when does a community become a crowd, a mob?) The second quality that binds all these diverse applications of "community" lies in how very nearly impossible it is to use the word negatively, with its many connotations of affection, solidarity, interdependence, mutual aid, consensus, and so on. As Lori Kendall succinctly says, it "carries significant emotional baggage"; Raymond Williams summarizes the baggage as its "warmly persuasive" tone—"It seems never to be used unfavourably."[2]

Williams also notes that "community" seems "never to be given any positive opposing or distinguishing term," though there are many negatives, with new ones being added with each transformation of the word. A whole family of negatives developed when "community" appeared in yet another guise, as the integument of the "virtual village" produced by "webs of personal relationships in cyberspace," in the words of Howard Rheingold.[3] The atmosphere of free expression online, Rheingold went on (after quoting Tönnies by way of Durkheim, positioning his argument in the lineage of grand modal transitions, agricultural to industrial to informational), emphasizes the "fragility of communities and their susceptibility to disruption."[4] So susceptible and fragile, in fact, that "community management" for online groups is a paying occupation with its own evolving best practices and theories, in a cluster of related occupations such as moderator, community advocate, evangelist, and social network facilitator. This latest, and in some ways strangest, application of the community concept draws on its history and "warmly persuasive" prestige to manage user behavior and activity on behalf of a given site's objectives, whether that means keeping things on-topic, maintaining a civil tone, or strengthening the "brand community" for the sake of marketing—online community, these days, being more often than not a business proposition. "Is it going to have a social layer?" is an entirely reasonable question to ask of a company seeking venture capital. (In the 1998 revision to his landmark 1992 essay "Cyberspace Innkeeping: Building Online Community," John Coate, employee number two on the early social network the WELL, captured the change in the word's use and value from the perspective of the old order: "Assigning the mantle of 'community' to one's enterprise before the fact as a marketing hook just serves to cheapen the term.")[5] The disruptions a community manager works against, the points of fragility and vulnerability, capture the specific complexities of the idea of community as expressed over infrastructure and code, much as issues like class struggle, anomie, and urban tumult offered points of departure for previous conversations. These are phenomena like "flamewars" (ferocious and rapidly escalating arguments), "trolling" (strategic provocation and harassment for maximum chaos), "sockpuppetry" (a person using multiple pseudonymous

accounts to create the illusion of support or bully others into submission)—and, of course, "spam."

"Spam's" etymology is a story of transitive and mutable meanings that mirrors, in negative form, that of "community," pejorative where the latter is persuasive, sharply exploitative rather than vaguely beneficial. It starts with a 1970 Monty Python sketch—Vikings chanting "spam, spam, spam," overwhelming conversation in a restaurant—that was reenacted endlessly on the forums of the early Internet, not least because it was well-suited to automatic duplication and a good way to annoy others by driving the rest of the conversation up off the screen with your text.[6] It came to cover many forms of unwanted activity on the network, from the accidental material generated by a malfunctioning algorithm to the excessive posting of another user; from the mere introduction of commercialism into a notionally civil society to the domination of online discourse by machine output. The term passed easily across very different modes and scales of activity. When the network architect Jon Postel wrote the Request for Comment (RFC) 706 in 1975, "On the Junk Mail Problem," he was referring to the "misbehaving or . . . simply annoying" material being sent by a malfunctioning program on the network, a purely mechanical failure among a very small group of hosts; when a programming accident in 1993 hit a Usenet discussion with hundreds of copies of a recursively growing message it was entered in the historical record of the Jargon File, a collection of the network's neologisms and slang, as having "proceeded to spam."[7] Yet human speech could also be so dubbed: "spam," writes Elizabeth Hess in an overview of the early collaborative text world LambdaMOO, "refers to generating so much text that its sheer quantity is offensive regardless of its content."[8] In the application for the expulsion of a user from LambdaMOO in 1994, reference is made to "a long history of vindictiveness, paranoia, slander, harassment, lying, and cheating; but especially her compulsive spam"—which is not commercial speech, but "long, semicoherent screeds," that is, unwanted speech.[9] These uncertainties enter legal discourse as well, as in the opinion on *CompuServe, Inc. v. Cyber Promotions, Inc.*: "Defendants refer to this as 'bulk e-mail,' while plaintiff refers to it as 'junk e-mail.' In the vernacular of the Internet, unsolicited e-mail advertising is sometimes referred to pejoratively as 'spam.'"[10]

"Bulk," "junk," "screeds," "annoyance," "offensive" in content or quantity: "spam" is very nearly the perfect obverse of "community," a negative term in both colloquial and specialized technical use that remains expansive and vague, covering a vast range of technical and social practices, with varying motives, incentives, actors, and targets. Both words have a productive blurriness that turns them into platforms for development and delineation—for individuals or collectives, markets or nonmarket values, appropriate and just ways to live. Where "community" stands in for our capacity to

join one another, share our efforts, sympathize, and so on, "spam" acts as an ever-growing monument to the most mundane human failings: gullibility, technical incompetence, lust (and the sad anxieties of male potency), vanity, and greed for the pettiest stakes. We go to community to discuss how people are generous, empathetic, and gregarious—and to spam to discuss them as suckers, criminals, and morons.

Spam is the shadow history, the negative space, of the concept of community online, and also a significant force in that history as a limit test, a provocation to new developments, a form of failure that helped to define the meaning of success. Germinating in its many different forms wherever the attention of a group is gathered—whether as a discussion board, a blog's comment thread, a Usenet group, or more diffuse areas of collective attention like the results aggregated by Google's PageRank algorithm or the space of personal e-mail addresses—spam magnifies the contradictions that lie within communities online. With such diverse expressions and agendas carried in one capacious sack, the virtual community demands conversation, debate, and clarification, concerning both the new order produced by its operation, and the old order it interferes with or obsolesces, and so does spam, interfering with the interference and exposing contradictions within it. In Alexander Galloway's phrase, the rise of the mediating network and its communities obliges us to find a "new logic of organization"—because if we do not, the shear between our old models and the new forms will become steadily greater and harder to bear.[11] This shear is easily seen in most of the domains shaped by information scarcity or secrecy, from journalism, book and music publishing, and international diplomacy to the quotidian selective privacy that Helen Nissenbaum terms "contextual integrity," where our friends, family, and professional life operated in distinct partitions.[12] Spam presents us with a vital and current—if negative—case of this new logic of organization in action, and it redefines our understanding of "community" online: how it works, and the paradoxes of that work.

The cardinal problem within the virtual community, the problem that spam exploits and aggravates, is the tension between infrastructure and expression, or capacities and desires. One manifestation of tension—one specific to an unusual group, and distinct from the more generic "community," but a readily intelligible example—is what Christopher Kelty terms "recursive publics," a public "vitally concerned with the material and practical maintenance and modification of the technical, legal, practical, and conceptual means of its own existence as a public," whose existence "is only possible through discursive and technical reference to the means of creating this public."[13] What makes this example somewhat unusual is that Kelty is describing the culture of open source programmers, which is to say, people for whom how they talk and collaborate is something they can easily modify

and transform, and this transformation is, in fact, a major part of their discourse. They operate, first and foremost, from a position of reflexive self-awareness of the means and purposes through and for which they work; many of the examples of spam's provocation show us groups of people who have recursion thrust upon them. Like Dewey's model of the "public," which is called "into existence having a common interest"—with its existence consisting primarily in the ability to "locate and identify" itself and to cohere and amass attention, votes, and money against a perceived negative consequence—spam provides us with reactive publics.[14] Obliged, suddenly, to be aware of the means of their own existence and to create deliberate mechanisms that blur distinctions among technical, social, political, and legal, these reactive publics must manage themselves as infrastructure, answering major questions on the way: In whose name? By whose standards? By what methods?

Yes, you may have a "community," with all the emotional baggage that term entails in its dense interlace of shared interest and solidarity—but your community is also a particular arrangement of hardware and software. Your community needs electricity. It is rack-mounted servers, Apache, and forum software, perhaps funded by advertising revenue, volunteers, or corporate largesse. Your community may be someone else's property and subject to someone else's laws. (To simply name only the most recent and prominent expressions of this tension in various domains, consider Google and China, social media and Iran, Facebook and privacy, or the question, "Can you copyright a tweet?")[15] Perhaps, like GeoCities—or Imeem, Lively, AOL Hometown, OiNK, and so on in the necrology—your community will one day disappear with little or no warning, user-generated content and all. Until it evaporates like a mirage due to a change in business plan, how is your community to police and maintain itself, and how are the rules to be decided? Internet governance is the space of the *really different* (as Lee A. Bygrave and Jon Bing perfectly put it in *Internet Governance*), where the properties of the network dramatically change what is transacted on it.[16]

These properties themselves can change as well, at different scales and populations of machines and users—spam's appearance often demands responses on behalf of "us," where "us" can be anything from "a few hundred people on the network" to a vague polity of users on systems hosting millions of people around the world, to "Internet-using citizens of the United States." These different scales create different possibilities for organization, complaint, redress, and the persuasive invocation of "community." Looking at the history suggests a physical comparison: we can draw distinctions between the quantum scale, the atomic scale, and the galactic scale, because they function under very different types of laws—the elegant simplicity of Newtonian physics breaks down at the edge of the atomic and

subatomic, where the strangeness of quantum mechanics takes over, and it is subsumed at the upper limit by the still-greater elegance of the cosmic scale, where we can set aside things like chemistry and electromagnetism, and work from gravity and mass alone. The uneasy balance between the group, and the means of their existence as a group, obtains at every scale we will see through the network's history, but this balance and its modification take very different forms on small professional networks and massive public systems and within and across the borders of countries.

Spammers, in their crude way, articulate this swaying balance between infrastructure and the concept of a community by exploiting it relentlessly, working in the space where we are obliged to reflect on our technologies because they at once underlie and diverge from our understanding and use of them. This tension is spam's native environment. It is what distinguishes it from other forms of computer crime and why it is of particular relevance to thinking about communities virtual and actual: spammers take the infrastructure of the "good things" and push them to extremes. Spamming is the hypertrophied form of the very technologies and practices that enable the virtual communities that loathe and fight it. This is why it is so hard define, so hard to stop, and so valuable to our understanding of networked digital media and the gatherings they support. It is this fact about spam that makes it really different.

To illustrate this, consider the case of affiliate advertising as practiced on "spam blogs" and "spam pages." Google, as representative a company of our era as Ford was of the 1910s, is not in the business of search but the business of advertising—its ad services provide 97 percent of its revenue.[17] These ads take the form of little squibs of text or images, often in response to particular search keywords. If a site's owner puts some of these ads on their page, they can receive some amount of revenue, generally very small, on a per-impression basis (that is, every time a page with the ad is loaded in a browser) or per-click basis (a viewer actually clicking on the ad to visit the advertiser's page). Google gets a cut of this revenue as well, and all those ads on blogs and Web pages, sponsored links in search results, and ads accompanying the conversations in Google's e-mail service, accumulate into the company's income, and this pays for nearly everything else—including the oceans of free content whose hosting is paid for out of an individual's share of this money. Which begs the question: if ads are the business, and content merely the enticement, the ornament on the engine, why not optimize for advertising? The spam blogs ("splogs") and spam sites consist of post after post and page after page of text, automatically gathered and generated to best fit Google's search engine algorithms and filled to the last pixel with advertising, so that every pageview and click-through is maximized as a source of revenue. The ads on a spam page may be entirely served through Google's

affiliate advertising program—in other words, they can be a significant source of revenue for Google. What this means is that search-engine spammers running their vast stables of spam blogs and sites are not anomalous. They are making the greatest possible use of the technologies and economies available, constructing a system in which all the extraneous matter of people and conversation has been pruned away in favor of the automation of content production, search results, clicks, and ads served. (The "Enterprise" package of one of the many businesses in this field will mass produce up to a thousand blogs for the subscriber, turning out ten thousand posts a day with automatic text built around the 150 keywords of the subscriber's choice—a daily volume of text that quantitatively dwarfs that of entire literate cultures and historical epochs.)[18] This in turn puts Google in the contradictory position of having to analyze and expel many of their most dedicated customers, those who overexploit, and overexpose, the financial and attention economies and technologies that underlie the contemporary Web.[19]

Still more problematic ambiguities exist—consider the "content farm." Demand Media, an exemplary case, commissions content from human writers (willing to meet very low standards for very little money) on the basis of an algorithm that determines ad revenue over the lifetime of any given article; it then posts this content through several domains like eHow.com. Generating, at peak, thousands of articles a day, Demand Media can create a simulacrum of knowledge convincing enough to attract both search engine returns and the clicks of actual humans (despite producing a kind of nonsensical poetry of uselessness, the correlative of spam's machine-mangled posthuman semantics, with articles like "How to Wear a Sweater Vest" and lengthy reviews of deodorant containers). As C. W. Anderson has observed, content farms are engaged in the attraction and manipulation of a "quantified audience," a strategy that marks a nebulous border space between more reputable and legitimate media production and spam as such—after all, these are very precisely targeted articles written by people for people; at what point do they cross over from the space of a merely frivolous or attention-grabbing article a newspaper would run to sell ads against and into the domain of network misbehavior?[20] When does algorithmic quantification part ways with the canny editor who knows that sex, serial killers, and how-to stories sell?

As Google refines their strategy for blocking and removing the more overt of the ad spammers, the spammers work with persistence and alacrity to reverse-engineer the refinements and find ways around the new developments in a mutually coconstitutive relationship, or an arms race, that has obtained throughout the history of spammers and their targets.[21] This dynamic can be seen quite early in the history of the Internet. At every point spammers bring contradictions to light by exploiting them and force

questions that could otherwise go unasked—particularly as to who and what belongs in the conversation on the network and where the edges, in practice, are drawn. Spam begs the question and demands answers, turning users into publics and forcing inclusive "communities" to articulate and specify themselves. Spammers and their tools play a major and under-thought role in the transformations of the groups—from communities to publics to citizens—using these new technologies, in the constant redefinition of their terms of existence, and in the relationship they have with those prior orders of power and control that are not so amenable to the new logics of organization.

The Coevolution of Spam, Community, and Governance, 1971–2010

The history that follows will be extremely synoptic. My hope is to provide a high-altitude overview of the complex shared life of "spam" and "community," and the governance practices that evolved between them, as a foundation for further studies of spam. Any one of the events alluded to in this history would make a rewarding study in itself as an instance in the tangled evolution of our networked society, revealing global events, fortunes made and lost, inventions, anti-inventions, and anti-anti-inventions. Collectively, these events build a history in which spam is always part of a conversation about "community," its meanings and its edges.

It starts off simply, long before the Internet, at Massachusetts Institute of Technology (MIT) in 1971. The school was the hub of the Compatible Time-Sharing System for remote computer access (CTSS). Multiple users on distant terminals—about a thousand in all, both at MIT and at other institutions—could access a mainframe computer and use it to run programs; due to the work of Tom Van Vleck and Noel Morris, two MIT programmers, users could also use a form of messaging, a system for forwarding files to particular users, that predated e-mail.[22] Typing "MAIL F1 F2 M1416 2962" would send a message to Van Vleck, and "MAIL F1 F2 M1416 *" would send a message to everyone on a given project team (in this case, the CTSS programming project itself). For structural reasons, those in the CTSS programming team had a unique privilege: they could type "MAIL F1 F2 * *" and send a message to everyone using the CTSS system at all locations. "I was mighty displeased one day, probably about 1971," writes Van Vleck, "to discover that one of my team [a sysadmin named Peter Bos] had abused his privilege to send a long anti-war message to every user of CTSS that began THERE IS NO WAY TO PEACE. PEACE IS THE WAY." Van Vleck "pointed out to [Bos] that this was inappropriate and possibly unwelcome, and he said, 'but this is important!'" "There is no way to peace" is a quote from A. J. Muste, the Christian pacifist and dedicated anti–Vietnam

War activist; 1971, of course, a period of protests over university-military engagement, two years after the formation of the Union of Concerned Scientists at MIT. Bos used his privilege as a systems administrator to turn this theoretically telephonic one-to-one or one-to-many medium into a broadcast system, one-to-all, and to transform this group of people using a mainframe into a politically engaged community of the like-minded. Van Vleck and Morris had created an elegant hack for the addressing of files in a set of time-sharing computer accounts, but they had also created an audience heavily weighted toward exactly the group—engineers on defense contracts—that a morally passionate antiwar programmer would want to reach and convince.

This story should be more complex: a new means of communication, a high-minded endeavor, a chilling effect. But the administrator's position over the system, with mastery of the code and the knowledge and the access privileges to change it, is that of the lawmaker, creating and banning users and altering the capacities and structure of the network. Of course, these sovereigns are in turn subjected to the authority of the universities, corporations, and governments that employ them, often an uneasy balance of power. Take the case of the next protospam message, sent to addresses on ARPANET on May Day of 1978, that provoked a conversation whose implications continue to resonate, a family dispute among the Olympians that starts to explain why we are at war on the plains of Troy today. Olympians: the list of 593 addresses for this advertising message included ENGELBART@SRI-KL, Douglas Engelbart, co-inventor of the computer mouse and key figure in human-computer interaction; POSTEL@USC-ISIB, Jon Postel, one of the Internet's architects and at one time the authority in assigning IP numbers; FEINLER@SRI-KL, Elizabeth "Jake" Feinler, who ran the organizational Network Information Center (NIC) and, with an executive decision, created the domain name structure of ".com," ".org," and the rest.[23] The message was an ad for the new computers being released by the Digital Equipment Corporation: "DIGITAL WILL BE GIVING A PRODUCT PRESENTATION OF THE NEWEST MEMBERS OF THE DECSYSTEM-20 FAMILY"[24] The DECSYSTEM-20 series computers were the first to ship with built-in support for ARPANET connections; clearly this would be significant to the users of ARPANET. They were exactly the people who would want to know.

This message exposed the rift within the concept of "community" on the network, the split that Kendall captures between community as "communication and shared interests"—the community that in its most facile form exists as a market, the target of products, an institutional structure with its sociological roots in the *Gesellschaft*—and the community of "relationships and values," "deeper human values," of *Gemeinschaft* (with all the baggage those two categories in turn bring with them).[25] The former articulation of

community, a "family" of users to mirror the DECSYSTEM-20 FAMILY of machines, had its defender in the reply to the DECSYSTEM advertising message from Maj. Raymond Czahor: "THIS WAS A FLAGRANT VIOLATION OF THE USE OF ARPANET AS THE NETWORK IS TO BE USED FOR OFFICIAL U.S. GOVERNMENT BUSINESS ONLY." It is a contractual and industrial arrangement, based on the complementarity of work. ARPANET is not to be used for outside advertising, because its attention, bandwidth, and hardware are the property of the institutions that created it, for their communication and shared interests.

A more nuanced position, with the possibility of shared values as well as interests, came from within the user base with Elizabeth Feinler's May 7 message following Czahor's official statement. She started framing the discussion in her opening disclaimer: "The comments are my own. They do not represent any official message from Defense Communication Agency or the NIC." If the network was in fact strictly for government business, everyone involved would simply write from their official position, but there are two networks, and she—a critical administrator for the official network of machines and standards overseen by the Department of Defense—is speaking as a person in the unofficial network, the graph of the people using the machines, whose shared mores made room for private correspondence, playing text adventures, announcing marriages and births, and holding a long-running conversation on science fiction. "The official message sent out," Feinler wrote, "asked us ('us' being network users) to address the issue ourselves. I personally think this is reasonable and think we should lend our support or otherwise be saddled with controls that will be a nuisance to everyone involved." The "official message," which Feinler had distributed on Czahor's behalf, is distinct from the group, "ourselves," the "us ('us' being network users)" to which she also belongs. Her import is clear: let's come to an agreement and handle this ourselves, so we can keep our side of the network relatively free of "controls that will be a nuisance." Do the users really want to invite outside authorities in? To take a term from Julian Dibbell's typology of responses to online misbehavior, Feinler's was a parliamentarian position, generating an internal rule structure to mediate between "us" and what she calls "the powers-that-be"—to govern ourselves in a compromise with our larger context and prevent further incursions into our space.[26]

This position's character as a compromise was amplified by the response from no less a figure than Richard Stallman, RMS@MIT-AI, arguably the most important person in the creation of the open source software movement: "It has just been suggested that we impose someone's standards on us because otherwise he MIGHT do so. . . . I doubt that anyone can successfully force a site from outside to impose censorship, if the people there don't fundamentally agree with the desirability of it." Stallman makes the most basic

form of the anarchist argument—"anarchist" as Dibbell means it: not a stand for advertising, spam, or a laissez-faire attitude as such, but for self-regulated standards and values that emerge from the network and are enforced there by the "network users" rather than being imported, imposed, or in dialog with the network's context. This is anarchism in the Kropotkinist mode, where the "customary law," our standards, the laws that develop among "the members of the tribe or community" keeps "cordial relations" operating smoothly and functioning best without outside intervention of any kind.[27]

Which raises the question of "what ought to be included in the 'self' of self-regulation"—solely the body of individual users, or Internet service providers (ISPs), interested private companies, and national governments?[28] Spammers, reliable as rain finding holes in a leaky roof, enter these definitionally problematic spaces when there's attention to capture, operating in the corners created by regulatory arguments where liberty, trust in users, and regulatory domains transect unprecedentedly powerful reproduction and transmission technologies. The antispammers gather to meet them there.

A dramatic change in scale begins at this point—from a network that can be diagrammed on a single sheet of paper, where most of the users know each other personally, to an international mesh of thousands of host machines and millions of users.[29] Almost ten years to the day after Feinler's message, on 27 May 1988, in response to a Usenet protospam message sent by "Jay-Jay"/"J J," a user posted a draft of a letter to the US postal authorities and added a comment: "I am concerned, though, whether [sending this letter] is opening up a bigger and possibly more dangerous can of worms than it is worth."[30] Though strongly contested, there was still a sense that the self that regulated should be that of organized network users as a coherent and self-declared community, and not their putative governments. "J J," the pseudonym used for a small-time charity scam by a grifter named Rob Noha, had rendered this more complex. In prior cases of misbehavior, those offended could simply turn to the sovereign power of the relevant sysadmin at the offender's school or business. The administrator could assess the situation, and give the malefactor a lecture or just kick them off the network. Noha, as he posted his begging letter across Usenet ("Poor College Student needs Your Help!! :-("), operated under the e-mail address J J@cup.portal.com. Portal.com, the Portal Information Network, was one of the first private companies to offer Internet access to customers as a subscription business, rather than providing free access to students or employees, breaking a key element of the tacit social agreement. Noha's action was in all respects disturbingly connected to the extranetwork context of postal systems, currency, and business: did the sysadmins owe their loyalty to the rough consensus of "a bottom-up democracy," or to the business that employed

them—itself beholden to shareholders and customers?[31] Usenet was the site of a raging debate over freedom of speech that made this question of governance still more charged: was this a worthy form of speech to defend?[32]

The parliamentarian reaction to Noha faced some of the very real questions of governance and community raised earlier: who wants to bring in the territorial government? Is there a way we can regulate ourselves—and who will be in charge of those decisions and their enforcement? ("Actually, more to the point, does anyone want the FCC or the U.S. Mail snooping around Usenet trying to figure out how to use his postings in court and incidently [*sic*] whether they shouldn't be exercising more visable [*sic*] control over such a visable [*sic*] underground communications system as Usenet?")[33] To again take Dibbell's coinage, there was a "technolibertarian" wing that advocated setting aside all this messy social stuff in favor of the "timely deployment of defensive software tools"—you didn't need the Department of Justice or some kind of Usenet star chamber if you had well-developed "killfiling" technology to keep you from seeing the messages you didn't want.[34] Many advocated making things so unpleasant for the administrators of Portal.com that they would take the appropriate sovereign action. Which, wilting under all the flames, they did, but in an unprecedented manner: "We have received a number of inquiries about J J. . . . If you view these questions as the burning issues of our time, you might wish to call J J yourself. You can reach him as: Rob Noha (aka J J) 402/488-2586."[35] If you want a well-regulated Internet, do it yourselves.

This was a prophetic act, particularly in what it provoked. The antispam social enforcement that began in earnest with Portal's posting seems like a vigilante movement in many respects: self-organized by volunteers, at times acting in defiance of the law, with the explicit goal of punishing bad actors about whom "there was nothing [the authorities] could do" (to quote Portal's official communication with law enforcement).[36] "Vigilante" is a bad analogical fit in one respect, however, because they never moved to outright violence. Their methods were prankish, noisy, mocking: collect calls at all hours, "black faxes," ordering pizzas for collect-on-delivery payment, sending postage-due mailings and masses of furious, profane, and abusive e-mail, illegal computer exploits, and harassment of parents, coworkers, and friends of the malefactor. Alleged spammers were surrounded by a constant swarm of threats, trolling, name-calling, and other abuse—almost the mirror image of their violation of the social mores with technically enabled rudeness. Such a response to spam is much closer to the symbolic and communal form of vigilantism called the charivari.

"A married couple who had not had a pregnancy after a certain period of time," writes Natalie Zemon Davis in *The Return of Martin Guerre*, "was a perfect target for a charivari. . . . The young men who fenced and boxed

with Martin must have darkened their faces, put on women's clothes, and assembled in front of the Guerre house, beating on wine vats, ringing bells, and rattling swords."[37] The practice was turned against anything the community found unnatural, including marriages between the young and old, widows remarrying during the mourning period, adulteries, and excessive spousal abuse. "With kettles, fire shovels, and tongs," goes a description of a Dutch variant, "the mob hurries towards the culprit's house, before whose door soon resounds a music whose echoes a lifetime does not shake off."[38] "[She] was disturbed by a hubbub in the distance," writes Thomas Hardy, describing a Dorset variation on the charivari, "The numerous lights round the two effigies threw them up into lurid distinctness; it was impossible to mistake the pair for other than the intended victims. . . . The rude music . . . [and] roars of sarcastic laughter went off in ripples, and the trampling died out like the rustle of a spent wind."[39] The "rude music" of banging pots and pans and yelling voices ("discordant voices" is the contemporary meaning of "charivari" in legal parlance) and the march around the house, the sarcastic laughter, the intensely public humiliation and harassment—so the charivari works in the present case: "Rob Noha / 8511 Sunbeam Lane / Lincoln, NE 68505 / (402) 488-2586 / Phone books are such wonderful things," wrote a user two days after Portal posted Noha's name and number. "Can someone in Lincoln drive by and get the license numbers at his address?" Just as suddenly, the pack disperses, "like the rustle of a spent wind": the charivari is reactive, offering no constructive plan beyond humiliating and shaming the offender, and dies away as quickly as it flares up.[40] Faced with a more confident antagonist, with the audacious shamelessness of chutzpah, the charivari quickly exhausts its repertoire.

Six years after Noha, on April 12, 1994, Usenet—whose population of users had again multiplied dramatically—hosted the first message to be called "spam," which included something truly disturbing from the charivari perspective: legitimate contact information. Noha had used a pseudonym and a post office box; proper contact information implied legitimacy—this was marketing, so of course they wanted clients to be able to reach them. Lawrence Canter and Martha Siegel were a pair of immigration lawyers hoping to cash in by misrepresenting the work required to enter the United State's lottery for green cards, and they felt no need to hide—quite the opposite. "Freedom of speech has become a cause for us," Siegel said in an interview with the *New York Times*. "I continue to be personally appalled at the disrespect for freedom of speech by this handful of individuals who would take over the net if they could."[41] Note the shift of scale—the vocal anger with advertising could be recast as the province of a "handful" of users, presented as extremists in a commercial and constitutional environment of "the net" now alien to them. The fundamental covert misrepresentation of

the lawyers' project—no immigrant needed their help with the "paperwork" (a postcard) to enter the green card lottery—was occluded by their capacity for publicity: yes, what they had done was advertising, and they got a book deal, a marketing company, and, so they claimed, a hundred thousand dollars' worth of new clients for their firm. While they spoke to the *Times* and made their case in their book: "The only point on which both sides in the Internet ad wars agree is that there is no law against advertising on Usenet. . . . Left without any legitimate basis for objecting to what we have done, most of our critics have decided that what we have done is 'rude.'" Usenet's population fell back on torrents of hate mail, phone phreak prank calls, letters to the Board of Professional Responsibility, and arguing their options on news.admin.policy.[42]

Canter and Siegel eventually paid a professional price for their vanguard spamming, but by then the practice was already exploding. One of first things spammers commonly sold were the tools and materials, the text files and software, that had helped them become spammers—today, some of the money in the business of running the vast networks of compromised spam-generating computers called botnets is in the sale of the software one uses to build the botnet, as in the 2010 "Mariposa" case, where the three people running the system had quite limited programming skills.[43] This business model created a kind of dark mirror of the General Public License (GPL), the landmark open source software license that requires a program using open source code to be open source itself: spammers financing their initial stake by enabling other spammers—like gold rush entrepreneurs striking it rich by selling shovels and sieves to others hoping to strike it rich. Mass-mailing programs, special "bulletproof" hosting contracts, instructional guides, databases of e-mail addresses were the business then (the complete AOL address database, 37 million people, went for $52,000, providing its owner with both a terrific target for spamming and a product with very high resale value), to which can now be added automated blog hosting and text generation services, hosted e-mail account production, a variety of ad fraud packages, ready-to-run malware systems, subscription services to break the anti-automation CAPTCHA protections, and so on.[44]

At every point, the constitutive tension: as spamming spread by the combination of skill sharing and the rapid expansion of audiences and technical capacities, so did antispam efforts. In 1996, by a vote of 451 to 28, the forum news.admin.net-abuse.email (NANAE) was created for people to discuss "possible abuses of e-mail . . . mailbombing, denial-of-service attacks, 'listserv bombs,' unsolicited and/or unwanted mail, email address lists, mailing list abuse, large-scale mailings in general," and so on down the growing list of malfeasances.[45] The NANAE forum combined the dossiers and how-tos of the charivari's researcher/pranksters, the legal methods for complaint and

recourse developed by the parliamentarian wing, proposals for technical solutions from the technolibertarians (turn e-mail into a metered service, develop better filtering software), and conversations between knowledgeable sysadmins and the spam-maddened average users of e-mail and Usenet. After Canter and Siegel, a press release had been drafted and redrafted on news.admin.misc that tried to describe the "implicit social contract" online that the spammers were violating; NANAE made that contract explicit, contested, and vital, a matter of immediate defense by a skill-sharing volunteer crew.[46] They wrote up step-by-step examples to teach the tools—commands like "whois" and "traceroute" and the art of extracting the pertinent traces from data-laden e-mail headers used to track down and expose the spammers—as well as longer documents like the 24,000-word "alt.spam FAQ," which are monuments to the project of finding enforcement methods.[47]

Through it all ran a profound uncertainty about governance—for whom, and by whom? Spam campaigns like Noha's and Canter and Siegel's had provoked statements on behalf of "users of the Internet"—but who now in 1996 could be confident of their univocity? Did they speak on behalf of the users and shareholders of AOL? Or the interests represented by President Clinton's science adviser Ira Magaziner, who made it quite clear to Jon Postel that the Internet was owned by the US government and was to be an engine of commerce?[48] Or did they speak solely for the people whom Martha Siegel mocked as "the wild-eyed zealots who view the Internet as their home"?[49] Even as the antispam contingent gathered governmental tools for the fight against spam, they debated serious questions of the efficacy and validity of national governments online, particularly the much-derided CAN-SPAM bill in the United States.[50] Advertisers could afford lobbyists to draft bills to turn the Internet into a space friendly to them; by allying with the state, volunteer groups like NANAE might win the battle but lose the war—aiding in the creation of a network where the low-rent spammers were gone because the powerful ones had seized a monopoly on attention akin to the Weberian monopoly on violence.[51]

In fact, territorial governments notwithstanding, NANAE remained for a long time the central court of complaint and appeal in the spam world. The period of spam from 1994 to 2003 can roughly be described as the local phase, when spammers and antispammers knew one another and for all their subterfuge were relatively easily accessible, especially to the diligent digital gleaners of NANAE; many spammers were still attempting to give their business a faint air of legitimacy and remained in a kind of duplicitous communication with the antispam world. When proposed antispam legislation and legal texts became available, many spammers incorporated the text into their messages to suggest that they were in compliance and within their rights. (At one point David Sorkin, who ran spamlaws.com, was obliged to explain that

he was not responsible for the many disclaimers linking to his site that had begun to appear in spam messages.)[52] Sanford Wallace, the spammer behind Cyber Promotions, Inc., issued a public apology to NANAE in 1998 in one of his attempts to leave the business ("You folks are WINNING the war against spam. My fight is over")—contrite language directed not to a judge or a reporter, but to the people most in a position to exert pressure on the spammer and his business, as well as the only people besides other spammers to really understand it in detail.[53] Spam could be a lonely way to make money, and it was soon to get lonelier.

Another relatively small set of loosely affiliated groups had begun antispam work from an antisocial perspective, focusing on a technical and infrastructural fix. The interventions of governments were doomed to be on the side of the media incumbents, and the handicraft process of tracking and attacking spammers in NANAE was unable to keep up with the onslaught. Technolibertarians looking for software tools to break the spamming model found an answer in Bayesian filtering systems. Sparked by Paul Graham's 2002 essay "A Plan for Spam," a wave of significantly improved spam filters rolled out that took text as their subject, in the form of the statistical likeliness of words to appear in a spam or not-spam message.[54] Spammers were already adept at sending messages from misleading addresses, and avoiding the various telltale paratextual signs of a spam message—but their language, the language of the sales pitch and the begging letter, could be turned against them. Words like "though," "tonight," and "apparently" were highly reliable signs of legitimate mail, and "madam," "guarantee," and "republic" indicative of spam: on these distinctions you could build powerful blocking systems. In combination with new laws that demanded the use of regular language, like disclaimers and legal notices, in legitimated "Internet marketing" mass mail, the adoption of Bayesian filters changed the economics of spam. The conversion rates on spam messages had always been abysmally low; having the vast majority of the spam messages blocked before even reaching human eyes pushed the problem into the absurd. Those spammers that remained in the e-mail business rather than moving into some easier domain, like AdSense-harvesting Web pages, began to operate as outright criminals without the pretense of the legitimate advertising business: they needed to produce messages at a far higher volume than before, with characteristics more likely to evade filtering, and with any successful message producing more revenue than a simple sale of, say, herbal diet pills.

From the need to pass filters sprang one of the strangest chapters in spam's history. Literary spam messages incorporated language scraped from public domain texts in hopes of throwing off the probabilistic analysis of words, producing an onslaught of machine-generated cut-up modernism that

would not have looked out of place coming from Tristan Tzara or Louis Zukofsky. The somewhat less public and more esoteric world of search spamming—using Web pages and, later, user-generated content tools like blogs, comments, and wikis to create the illusion of popularity and relevance and thus alter search engine results to the spammer's benefit—had already introduced what I call the "biface text," a Web page designed to read one way to a human and a very different way to a search engine's ranking algorithm. Litspam pushed this dual legibility, with a protective husk of statistically unlikely literature around the payload of a link or an attachment to attract the curious human click.

What answered that click spoke to the other two needs of the new spam—for far greater message volume and return on investment.[55] When the credulous recipient opened the Web page in his or her browser or downloaded the attachment, a malware attack quietly began on their computer, an exploit that put their machine under the control of a remote user, joining ranks of other machines in a "botnet." Even as the nominal owner of a computer on the botnet used it to make a spreadsheet or check a Web page, it was receiving instructions and sending out waves of spam—including self-propagation spam, messages to everyone in the computer's address book, sent with a malware attachment to link their machines into the botnet as well. Analysis of the Storm botnet reveals something akin to a language factory, complete with queuing systems for distributing workload across the available bots, template spam messages and systems for filter-beating language variation, feedback mechanisms to remove dead addresses from the master list, and a production rate averaging 152 messages a minute per computer, hour after hour, day after day, with a network that may include thousands or even millions of compromised computers.[56] (Furthermore, any computer infected with one bit of malware is likely to be hosting several, coexisting uneasily or trying to eliminate one another. A new worm, taking over a new machine, will include an antimalware kit to clean its competitors off. Everything in spam has competitors, imitators, duplicates, and rip-offs, even at this level of intricacy and sophistication.) Because they can only send spam when their host computers are turned on, botnets can have a global pulse that reflects the Earth's rotation. The beginning and end of the workday, the sun's rise and fall, create spam's planetary circadian clock.[57]

This excess capacity of compromised computers has produced its own follow-on effects: when you have a system like that, you can do a lot more than send spam and scrub host machines for passwords and credit card numbers. You can turn some of the accumulated processing power to cracking passwords and protection schemes, and use the massed number of the computers to request a particular Web site rapidly and repeatedly, overwhelming the server's bandwidth and driving the site offline for other users—a

"distributed denial of service" (DDOS) attack, with which you can extort money from site owners and temporarily silence critics.

The threat of botnets has been met by a similarly global and infrastructurally sophisticated system of resistance. Consider the case of McColo, a Web hosting service in Colorado, notorious as a haven for the "command-and-control" systems necessary to run botnets: when it was shut down in the fall of 2008, the global volume of spam fell by more than half, albeit temporarily, while the botnet owners found new providers from which to reinstate control. The forces involved in the shutdown included journalists, security analysts, and the administrators of the major hubs that provided McColo's connectivity.[58] (Its shutdown left a strange dead zone in the Internet's address space: the block of addresses allocated to McColo had ended up on enough blacklists for their bad activity to render others leery of taking them over, like potential tenants shunning a house known for its suicides.)[59] An international collection of security specialists from different organizations formed the Mariposa Working Group, collaborating with the United States' FBI and Spain's Guardia Civil to arrest the controllers of Mariposa, a major botnet, in March of 2010. As Bygrave and Bing suggest, the very concept of Internet governance is presently "diffuse," and so is the enforcement, with loose working groups that overlap jurisdictions and expertise, odd bedfellows in some cases—like the Finnish security specialists, NATO and US observers, and Estonian ISPs brought together by the DDOS attacks on Estonia in 2007—that form in relation to the diffusion of the problem.[60]

Though we seem to have come a very long way from Peter Bos's message of conscience to the terminals supported by MIT, this history can also be read as a kind of interregnum, a transit from one period of overt control by systems administrators to another. The sysadmins of the early years of the network, Gandalfian figures maintaining order in their domains according to their lights, have become what Alan Liu terms "a priesthood of backend and middleware coders," as well as a small expert elite of security analysts, state agents, and ISPs.[61] Users can take refuge within the relatively spam-free zones the developers build, like Gmail and Facebook, with robust filtering and community management, paying with advertising and user information—that is, with their attention, a topic to which we will return. (In this respect, spam plays a significant role in the monopolistic drift that Tim Wu has identified: spam's irksomeness drives users into the proprietary spaces that can employ security specialists and pool vast quantities of user data to train the spam filters.)

Spam remains relentlessly diverse, thriving in the interstices of technical architectures and business plans. Even as e-mail spam is dominated by a small family of botnet titans, warring with each other for market share on a global scale, low-end practices germinate inside the new centrally administered

social spaces like Facebook, Twitter, and various hosted e-mail services. These range from the simple act of convincing the naive to click a link, or using Twitter bots to auto-retweet posts from certain users to make their material appear more popular and important than it really is, to the lightweight identity theft of assuming another person's public account, developing a plausibly panicky message, and cadging emergency money transfers from his or her family and friends.[62] This survey has not even mentioned the thriving and complex world of "419" or advance fee fraud messages that promise a huge return in concealed assets from a small investment, creating narratives of chaos from Accra and Lagos to Rotterdam (and a cinematic subgenre in Nollywood, the Nigerian film industry). We have passed very briefly over the underground advertising world of "black hat" search engine optimization, which binds Chinese stone quarries to spam entries on unsecured academic wikis in Europe. There is a book to be written that follows the epic struggle between the public classified ad site Craigslist and its spammers, who have turned random ringtone-seeking mobile phone owners into a distributed army to subvert voice authentication. For now, this brief history suggests the outlines of the event of spam and its simultaneously exploitative and constitutive relationship with concepts of community, governance, and collective experience online.

Conclusion: Thinking Spam and Communities Together

Walking in the hills above Sausalito in the early 1990s, Howard Rheingold and John Coate discussed all the ways a virtual community could sour, schism, and crash. "A core of people must flat-out believe in the possibility of community," they concluded—echoing, if inadvertently, the Deweyan vision of a community as "an object of desire," a belief in the existence of a domain where competing publics can find equilibrium.[63] (Online community, read this way, can be seen to "boot up," a term that derives from the impossible strange loop of someone pulling themselves off the ground by their own bootstraps: a complex system that seemingly calls itself into being, as a powered-off computer needs software to start running, and it needs to be running to launch the software. A community of people believes themselves to be "a community," and therefore they begin to become one.) But how was that belief to manifest? How do you manage the day-to-day business of turning a desire, a beautiful prospect, into something that can manage the many immediate points of failure? You do it through "norms, folklore, ways of acceptable behavior that are widely modeled, taught, and valued," Rheingold summarized.[64] These ways, these norms, carried out day-to-day, plus the belief in the possibility of its existence, constitute the

"community" part of the virtual community, a self-sustaining act of attention, under constant definitional pressure from forces internal and external—a form of what Randall Collins, in his analysis of the social history of philosophy, has termed "attention space," the link graph of people agreeing to listen to each other, to argue together. "Why would anyone listen to anyone else?" Collins asks, questioning why some schools of thought, some conversations, flourish—and he continues: "What strategy will get the most listeners?"[65] The first question is at the heart of community, and the second at the heart of spam. It is difficult to answer the first question without making some kind of warmly persuasive statement about the value of discourse between people, learning from others, sharing, finding common ground—the emotionally powerful rhetorical possibility of community. Answering the second is easy, if you do not ask too much of the concept of a "listener": use attention-grabbing tactics, automate production, rely on economies of scale, and cast a wide net. Yet the two questions are intimately related—the answer to one defines the other in negative.

Which brings us to the "virtual" part of virtual community, that is, hardware and code and infrastructure, the enabling stuff of our screen-based online experience and discourse. Throughout the history of spammers and their work, we have seen community—norms, folklore, and acceptable behavior plus laws, interested and contesting publics, acts of self-definition, and reflexivity—come into being, obliged to make qualitative arguments and normative claims about quantitative misuse. You have already joined me in a strange perspectival act, seeing the history of networked computation with the phenomenon of spam at the center rather than the edges; let us extend this contrarian project with a closing exercise in the technological sublime, as has become almost traditional in histories of the Internet—but with spam providing the sublimity, and suggesting precisely why it is so productive of community statements. What if spam were not the antithesis of the systems of the Internet, but rather those systems used maximally and most efficiently—for a certain value of "use"?

Consider e-mail spam, all those millions of messages cranked out by thousands of computers around the world in hopes that a vanishingly small amount will get through to the eyes of that percent of a percent of people who will actually respond to them (and get their credit card information stolen): yes, it is prodigiously wasteful, waste on an epic scale, day after day and month after month, a waste of time and bandwidth and disk storage space for all those spam folders. Spammers will fill every available channel to capacity, use every exploitable resource—all the squandered central processing unit cycles as a computer sits on a desk while its owner is at lunch, or toiling over some Word document, can now be put to use sending polymorphic spam messages, hundreds a minute and each one unique. So many neglected blogs

and wikis and other social spaces: automatic bot-posted spam comments, one after another, will fill the limits of their server space, like barnacles and zebra mussels growing on an abandoned ship until their weight sinks it. Servers do what they're supposed to under DDOS attacks: serve Web pages so rapidly and in such quantity that they can no longer provide them to anyone else. Spammers adopt micropayment labor systems like Amazon's Mechanical Turk, and search engine spam content creation services like Textbroker, to use the distributed production of scattered workers to achieve their ends.[66] Elements central to our understanding of digital media, from most any theoretical perspective, are adopted and pushed to an extreme by spammers: the capacity for automation, algorithmic manipulation, and scripting; the leveraging of network effects and vast economies of scale; distributed connectivity and free or very low-cost participation. The machines are being maxed out, and the humans, whose attention is the ultimate thing to be captured, the sole scarce resource in the whole arrangement, are a tedious and problematic element, so likely to flag a spam page, block a comment, or delete an e-mail—an unavoidable but annoying factor, like aerodynamic drag. This is a grand and global machine built in answer to the question of how one dominates the attention space and gets "the most listeners."

This is obviously ludicrous, a panegyric of pure function, while still being true. So on what basis do we stop spam? In framing the software and the laws and the communal rules, we must draw on the messy, fragile, emotionally laden and contingent language of community, the largely rhetorical realm that Manovich terms the "cultural layer"—or, as a network engineer once described it to me: "the top of the protocol stack—that is, people."[67] There is a parallel but separate meaning for "spam" in the world of video games, in terms like "grenade spamming" and "ship spamming," that exemplifies these distinctions. "Grenade spamming" is an optimally effective but fundamentally crude and unimaginative strategy: rather than do something clever, thrilling, or dangerous, you simply pitch wave after wave of grenades at your enemies. You may win the battle or game, but in doing so you miss the point. "The point" being a particularly human division—any serious player is going to draw to some degree on similar techniques for optimizing their character's actions, and spamming in the game is simply a more extreme case of optimization. It is the far end of a spectrum, past some vague and personal edge of the concept of "fun," into a zone in which winning in the most efficient, direct, easiest fashion is enough. At some point in this process, for most gamers, there is an aesthetic turn away from this total efficiency, a sense invoked by "grenade spamming" that there is something wrong with this wholly functional approach, and there is a superior purpose to be defended in the deliberate challenges of play and fun. ("Play" and "fun," of course, being terms nearly as vexed and complex as "community.")

Spam makes us find the point of play, and argue for it, and determine what use of the machinery is appropriate to our understanding of community; it puts the same burden on our digital gatherings as they have placed on so many of the analog world's arrangements. Digital media and computer software have acted as the flashpoint in enormous and significant debates about copyright and intellectual property—the means by which our culture is reproduced and transmitted. The infrastructure of anonymous submission and distributed publication has delivered grave questions about secrets, whistleblowing, and the relation of a state to its citizens. Encryption and online commerce regularly threaten to throw taxation into chaos; enormously complex computational modeling and risk analysis in finance has already delivered its share of mayhem. This list could go on—and at every turn questions are raised, arguments are made: for what can be done, what could, and what should. Privacy, social relationships, economics, politics, how we learn, how we write and make art: what remains that has not been brought to crisis by our devices and capabilities?

So does spam function, a perennial provocation of constraint from capability, with those constraints having much to teach us about what has been threatened. Trailing its constitutive interference helps us understand what it attacks, whether in Charles Stivale's work on the "escalating mores" of early spamming (a movement from "playful" to "ambiguous" to "pernicious" that we can see in contemporary developments in trolling practices), or Jenna Burrell's ethnography of deliberate manipulation of media stereotypes by West African 419 spammers, or the studies collected by Jussi Parikka and Tony Sampson, which make a case for the abandonment of analytic categories of normal and anomalous in the face of a radically imperfect network.[68] Two concluding thoughts follow from the shadowing of spam we have done here.

Peter Sloterdijk writes about the military use of chlorine gas at Ypres in 1915 as producing, among other things, an "explication" of the air, suddenly putting the atmosphere into relief and into question as something fragile (what Latour, commenting on the event, calls a "matter of concern"): "The fact of the living organism's immersion in a breathable milieu arrives at the level of formal representation, bringing the climatic and atmospheric conditions pertaining to human life to a new level of explication."[69] The history of just war theory includes the "inimici," figures like pirates, native peoples, and anarchists, stateless forces without senate or treasury, with whom we cannot draw up treaties. Permanent enemies of commerce, they lie outside the state and define one of its edges, where "extraordinary expenditure" is set aside to fight the "enemies of all" who are so alien to our logic of operation.[70] Spammers combine the abstract forms of these two events: The moment when we abruptly become aware of the spheres in which we live, the life-support systems on which we rely,

and the recognition of our edges and the extraordinary forces we must manage to make it clear who we are, and how we conceive of ourselves. What spammers render explicit is not the Earth's atmosphere or the border of the state but the technical reality of the network, and the space of our attention—the milieu of our time online (machines and protocols, which can be exploited) and how we constitute ourselves there. "Community" online is free of accidents of proximity and geography; what spammers make maddeningly clear is that it is constructed from time, our human time—our attention. That community of time and attention extends all the way from J. C. R. Licklider at the very beginnings of networked computing ("I was one of the very few people, at that time, who had been sitting at a computer console four or five hours a day")[71] through people on MOOs and Usenet complaining about bandwidth waste and reading through unwanted and duplicate text; to sites looking to catch your eye on the first page of search returns; and e-mails speaking in the provocative language of disastrous news, sudden boons, or a friend in trouble. It may seem drastic to associate thinking about spam with the history of chemical weaponry and extra-state warfare, but spam touches on a similar existential point, though of course quotidian and without martial gravity: Our attention is our lives, the finite hours and days of waking experience, and out of it, however unaware, we construct community and culture online as acts of concentration—clicking, reading, and writing. Spammers explicate these everyday acts of attention by treating them as a resource to be captured.

The spammers are far from alone in this project. The many different arms of the antispam movement all worried about bringing the territorial government into the conversation, because the government might successfully shut down the independent spammers while permitting more powerful and established interests to engage in legitimated "Internet marketing"—the state monopoly on attention, sold to those interests that could afford good lobbyists. Now, spammy techniques migrate over to more legitimate projects, like content farming, looking to increase pageviews, and into the lexicon that describes people as "personality spammers," a bit too happy to promote themselves or see their own words. So much of the history of spamming consists in laughably crude projects to get clicks and eyeballs, with the classic come-on tactics of the huckster and the con artist that, in their crudity, have a salutary visibility, explicating milieu and constitution alike. Much online social and communal experience now takes place in environments far more subtly tailored for attentional capture, with all the machinery of "community management" and "gamification" and "stickiness" and precise metrics (the "quantified audience") and churn-reduction strategies at work to keep us online and interacting on their platform, with our minutes of wakeful focus, and hence revenue, coming in—with moderation and flagging systems, of course, to keep spam at bay, as a

neighborhood controlled by organized crime is free of mere bandits and small-time muggers. We are beginning a fundamentally political struggle in the twenty-first century over attention, over what is available, what we notice, to whom we listen, and the formation and direction of our awareness by our systems of technical mediation. Spammers, ridiculous, ingenious, desperate and shameless, were onto this early—the wildcatters and rogue prospectors of the great aggregation of available human attention, before the heavy industry moved in. The history of dealing with them is not solely that of "community" articulating itself, but the beginnings of a politics of attention online.

Notes

This project was researched and written with funding from Air Force Office of Scientific Research: Multidisciplinary University Research Initiative (ONR BAA 10-002), National Science Foundation: Privacy, Obligations, and Rights in Technologies of Information Assessment (ITR-0331542), and National Science Foundation: Cyber Trust-Medium (CNS-0831124) grants; I am grateful for their support. The article was enormously improved through the conversation and inspiration of Gabriella Coleman, Erica Robles, and Alexander Galloway and by the very thorough and helpful comments on earlier drafts by the editors of *Representations*. I would also like to thank Helen Nissenbaum and Mario Biagioli, without whose consistent help, encouragement, and exemplary guidance this article would not have been possible.

1. John Dewey, *The Public and Its Problems* (Denver, 1954), 184.
2. Lori Kendall, "Community and the Internet," in *The Handbook of Internet Studies*, ed. Robert Burnett, Mia Consalvo, and Charles Ess (Singapore, 2010), 309–25, 309. Raymond Williams, *Keywords: A Vocabulary of Culture and Society* (Oxford, 1983), 76. For an overview of the complex and contradictory ideas around "community," especially as it enters the virtual, see Allison Cavanagh, *Sociology in the Age of the Internet* (Maidenhead, UK, 2007), 102–19.
3. Howard Rheingold, *The Virtual Community* (London, 1994), 5.
4. Ibid., 64.
5. John Coate, "Cyberspace Innkeeping: Building Online Community," 1998. Revision available from author at http://cervisa.com/innkeeping.html.
6. "In those days," begins one of the many folk etymologies of the early chat systems, "a lot of people who didn't have a clue what to do to create conversation would just type in their favorite song lyrics, or in the case of people at tech schools like [Rensselaer Polytechnic Institute], recite entire Monty Python routines verbatim. A particular favorite was the 'spam, spam, spam, spammity spam' one because people could just type it once and just use the up-arrow key to repeat it. Hence, 'spamming' was flooding a chat room with that sort of clutter." James Parry, message in discussion "Totally Spam? It's Lubricated" on

alt.religion.kibology, September 2, 2003, http://groups.google.com/group/alt.religion.kibology/msg/a89af63f065a35da?hl=en&dmode=source&pli=1.

7. Jon Postel, Request For Comments: 706: "On the Junk Mail Problem," Nov. 1975, http://www.ietf.org/rfc/rfc706.txt; for the self-replicating message, see Eric Raymond, "ARMM," in the Jargon File (no date, but see nomination and proposed text by Joel Furr posted in discussion "ARMM: ARMM: >>>>Ad Infinitum" on news.admin.policy on March 31, 1993: http://groups.google.com/group/news.admin.policy/msg/dc98a1f9c6a59477?hl=en), http://www.eps.mcgill.ca/jargon/jargon.html#ARMM.
8. Elizabeth Hess, *Yib's Guide to MOOing: Getting the Most from Virtual Communities on the Internet* (Victoria, BC, 2003), 29.
9. Lee-Ellen Marvin, "Spoof, Spam, Lurk and Lag: the Aesthetics of Text-Based Virtual Realities," *Journal of Computer-Mediated Communication* 1, no. 2 (1995), http://jcmc.indiana.edu/vol1/issue2/marvin.html; Julian Dibbell, *My Tiny Life* (New York, 1998), 100.
10. Compuserve v. Cyber Promotions, Inc., 962 F.Supp. 1015 (S.D. Ohio 1997). In a moment of high legal surrealism the opinion includes the footnote "This term is derived from a skit performed on the British television show *Monty Python's Flying Circus*, in which the word 'spam' is repeated to the point of absurdity in a restaurant menu."
11. Alexander R. Galloway, "Position Paper," *Exploring New Configurations of Network Politics*, 2010, http://www.networkpolitics.org/request-for-comments/alexander-r-galloways-position-paper.
12. Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford, 2010), passim.
13. Christopher M. Kelty, *Two Bits: The Cultural Significance of Free Software* (Durham, NC, 2008), 3, 30.
14. Dewey, *The Public and Its Problems* ("into existence": 126; "locate and identify": 141).
15. On new media and Iran, see Annabelle Sreberny, "Thirty years on: The Iranian Summer of Discontent," *Social Text* (2009), http://www.socialtextjournal.org/periscope/2009/11/thirty-years-on-the-iranian-summer-of-discontent.php; on Facebook and privacy, see James Grimmelman, "Saving Facebook," *Iowa Law Review* 94 (2009): 1137–1206; on Twitter and intellectual property, see Brock Shinen, "Twitterlogical: The Misunderstandings of Ownership," 2009, http://www.canyoucopyrightatweet.com/.
16. Lee A. Bygrave and Jon Bing, *Internet Governance: Infrastructure and Institutions* (Oxford, 2009), 50. Or, as Bryan Pfaffenberger puts it in the case of free speech on Usenet, "The notion of free speech that we find in Usenet today cannot be fully understood by likening it to traditions of free speech developed in nontechnological settings; like Usenet itself, it's an artifact that took shape as competing groups struggled in a new technological arena"; Bryan Pfaffenberger, "'If I Want It, It's Okay': Usenet and the (Outer) Limits of Free Speech," *Information Society* 12, no. 4 (1996), http://www.ingentaconnect.com/content/routledg/utis/1996/00000012/00000004/art00002.
17. Google Inc., Securities Exchange Commission Form 10-Q, November 4, 2009, 23, http://investor.google.com/documents/20090930_google_10Q.html.
18. See DataPresser, http://www.datapresser.com.
19. "Google only pays you adsense revenue because they are making money," writes "The Junk Man," a manipulator of AdSense revenue, "and all they care about is

keeping their customers happy. If your content is pin point and you are capturing the proper audience you are doing google's advertisers a favor. . . . That is what googles [*sic*] business revolves around!" thejunkman, "MNS: Bury the Hatchet," February 14, 2010, http://www.blackhatworld.com/blackhat-seo/adsense/171744-mns-bury-hatchet.html.

20. C. W. Anderson, "Deliberative, Agonistic, and Algorithmic Audiences: Journalism's Vision of Its Public in an Age of Audience Transparency," *International Journal of Communication* 5 (2011), http://ijoc.org/ojs/index.php/ijoc/article/view/884.
21. See, for example, the presentation of the Google algorithm partially as a method for preventing gaming of the system: "Automated search engines that rely on keyword matching usually return too many low quality matches. To make matters worse, some advertisers attempt to gain people's attention by taking measures meant to mislead automated search engines. . . . 'Junk results' often wash out any results that a user is interested in"; Sergey Brin and Lawrence Page, "The Anatomy of a Large-Scale Hypertextual Web Search Engine," *Computer Networks & ISDN Systems* 30, no. 1–7 (1998): 107–17. Or the closely related paper on Web link analysis from the following year, in which we can see "spam" replacing "junk" in the lexicon: "Linkage on the Web represents an implicit endorsement of the document pointed to . . . several systems—e.g., HITS, Google, and Clever—recognize and exploit this fact for Web search. Several major portals also apparently use linkage statics [*sic*] in their ranking functions because, unlike text-only ranking functions, linkage statistics are relatively harder to 'spam'"; Ravi Kumar et al., "Trawling the Web for Emerging Cyber-Communities," *Computer Networks: The International Journal of Computer and Telecommunications Networking* 31, no.11–16 (1999): 1481–93.
22. Tom Van Vleck, "The History of Electronic Mail," 2008, http://www.multicians.org/thvv/mail-history.html. The documentary filmmaker and essayist Errol Morris conducted several fascinating interviews with Van Vleck and others connected with the history of time-sharing and e-mail: Errol Morris, "Did My Brother Invent E-Mail with Tom Van Vleck?" parts 1–5, *New York Times*, June 19, 2011, http://opinionator.blogs.nytimes.com/2011/06/19/did-my-brother-invent-e-mail-with-tom-van-vleck-part-one/.
23. Many of those on the list never received the message due to technical incompetence on the part of the senders.
24. Brad Templeton, "Reaction to the DEC Spam of 1978" (no date), http://www.templetons.com/brad/spamreact.html.
25. Kendall, "Community and the Internet," 310.
26. Julian Dibbell, "A Rape in Cyberspace: How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society," *Village Voice*, December 23, 1993.
27. Peter Kropotkin, "Law and Authority: An Anarchist Essay," in *Anarchism: A Collection of Revolutionary Writings* (Mineola, NY, 2002), 202.
28. Monroe E. Price and Stefaan G. Verhulst, *Self-Regulation and the Internet* (The Hague, 2005), 14.
29. For a fascinating overview of the early evolution of Usenet, including questions of social constraint (flaming) and the infrastructural/social problems involved with profiting from it, see Henry Edward Hardy, "The Usenet System," *ITCA* [International Teleconferencing Association] *Yearbook, 1993* (McClean, VA, 1993), 140–51; available online at http://internet.eserver.org/Hardy-Usenet-System.txt.

30. Matthew P. Wiener, message posted in discussion "Nebraska Letter" on news.misc on May 27, 1988, http://groups.google.com/group/news.misc/browse_thread/thread/c7b4c158caa1f579/b13590445e1fba94.
31. Pfaffenberger, "'If I Want It, It's Okay.'"
32. For an extensive analysis of the politics and technologies of free speech on Usenet, including the role of sysadmins and the problem of spam, see ibid.
33. Bob Webber, message posted in discussion "FCC? U.S.Mail.? (Re: JJ's Revenge—Part II)" on news.admin, June 1, 1988, http://groups.google.com/group/news.admin/msg/a702f4908ded4c89?hl=en.
34. Dibbell, "A Rape in Cyberspace."
35. Customer Service at Portal Communications, message posted in discussion "JJ's posting" on news.sysadmin, May 27, 1988, http://groups.google.com/group/news.sysadmin/msg/d8aed91249879fcf?hl=en.
36. Customer Service at Portal Communications, message posted in discussion "A Note From Portal Regarding the 'JJ' Incident" on misc.misc, June 1, 1988, http://groups.google.com/group/misc.misc/msg/b44db800c9cc7d0a?hl=en.
37. Natalie Zemon Davis, *The Return of Martin Guerre* (Boston, 1983), 21.
38. Bryan D. Palmer, "Discordant Music: Charivaris and Whitecapping in Nineteenth-Century North America," *Labour/Le Travail* 3 (1978): 5–62.
39. Thomas Hardy, *The Mayor of Casterbridge* (London, 1887), 366–69.
40. For other projects that violate privacy and collectively produce public shame online, with varying approaches, goals, and histories, see Dongxiao Liu, "Human Flesh Search Engine: Is It a Next Generation Search Engine?" 3rd Communication Policy Research, South Conference, Beijing, China, 2008, http://ssrn.com/abstract=1555438, as well as Gabriella Coleman, "Old and New Net Wars over Free Speech, Freedom and Secrecy; or How to Understand the Hacker and Lulz Battle Against the Church of Scientology," lecture, Goldsmiths College, University of London, March 16, 2010, Internet Archive, "Community Audio," 58:39, http://www.archive.org/details/coleman-scientology_versus_the_internet.
41. Laurie Flynn, "'Spamming' on the Internet," *New York Times*, October 16, 1994.
42. Lawrence Canter and Martha Siegel, *How to Make a Fortune on the Information Superhighway: Everyone's Guerrilla Guide to Marketing on the Internet and Other On-Line Services* (New York, 1994), 85.
43. On the sale of spamming materials, software, and expertise to other spammers, see, for instance, the work of the spammer Davis Hawke as reported by Brian McWilliams, *Spam Kings: The Real Story Behind the High-Rolling Hucksters Pushing Porn, Pills, and %*@)# Enlargements* (Sebastopol, CA, 2005), 89 and 180. On the lack of expertise among the Mariposa botnet programmers, see BBC News, "Spanish Police Arrest Masterminds of 'Massive' Botnet," March 3, 2010, http://news.bbc.co.uk/2/hi/technology/8547453.stm.
44. On the AOL address sale, see McWilliams, *Spam Kings*, 223. The world of ancillary products for the spam business is vast; the curious reader can begin with Captcha King, http://www.captchaking.com/; the software cracking request team at Rent-a-Cracker, http://www.rentacracker.com/ (note how many of their cracked wares are for spam); and ListGrabber and AutoMail, http://www.egrabber.com/listgrabberstandard/automail.html.
45. Jani Patokallio, message posted in discussion "Result: News.admin.net-abuse Reorganization All Groups Pass," news.announce.newgroups, November 9, 1996,

http://groups.google.com/group/news.announce.newgroups/msg/2f658897021a0a89?dmode=source.

46. "Sine Nomine," message posted in discussion "Proposed Press Release, 2nd draft," news.admin.misc, June 6, 1994, http://groups.google.com/group/news.admin.misc/msg/f4d20bfe170f5edd?hl=en.
47. Ken Hollis, "Alt.spam FAQ" (created 1995), http://gandalf.home.digital.net/spamfaq.html.
48. Jack L. Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford, 2006), 46.
49. Flynn, "'Spamming' on the Internet."
50. "You should also read Title 47 of the United States Code, Section 227. There is a FAQ at cornell.law.edu for the text of the law. . . . Sylfest tells us Norwegians should report these via email to the national taskforce on economical crime, the KOKRIM"; Hollis, "Alt.spam FAQ." Note that this document includes both guidance in the use of the legal system and reporting to authorities, as well as significant critique of the problems of proposed and existing antispam legislation.
51. The programmer Paul Graham captures the essential concern in one of his essays on spam filtering: "It's hard to pass effective laws against spam now, because there is a continuum of spammers, ranging from (ahem) 'permission-based email marketers' like Virtumundo that send unsolicited email to addresses they buy from sites with unscrupulous privacy policies, to bottom-feeders like Alan Ralsky who send unsolicited email to addresses culled from web pages, chat rooms, and newsgroups. . . . The companies at the more legitimate end of the spectrum lobby for loopholes that allow the bottom-feeders to slip through too"; Paul Graham, "So Far, So Good," August 2003, http://www.paulgraham.com/sofar.html.
52. McWilliams, *Spam Kings*, 139.
53. As cited by Jeffery J. Leader and others in discussion "I'm Out!" on news.admin.net-abuse.email, April 11, 1998, http://groups.google.com/group/news.admin.net-abuse.email/browse_thread/thread/db1ce802d66ec505/.
54. Paul Graham, "A Plan for Spam," 2002, http://www.paulgraham.com/spam.html.
55. To be clear, a number of the malware technologies described here predate their use by spammers—the literature on worms and distributed computing, for example, goes back to 1982—but their adoption at this point reflects a deep change in how e-mail spam is practiced.
56. Christian Kreibich et al., "On the Spam Campaign Trail," *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats* (LEET '08), 2008, http://www.usenix.org/event/leet08/tech/full_papers/kreibich/kreibich_html/.
57. David Dagon et al., "Modeling Botnet Propagation Using Time Zones," *Proceedings of the 13th Annual Network and Distributed System Security Symposium* (NDSS '06), 2006, http://www.isoc.org/isoc/conferences/ndss/06/proceedings/papers/modeling_botnet_propagation.pdf.
58. Brian Krebs, "Host of Internet Spam Groups Is Cut Off," *Washington Post*, November 12, 2008. For the gradual resumption of spam e-mail, see Brad Stone, "Spam Back to 94% of All E-Mail," *New York Times*, March 31, 2009, http://bits.blogs.nytimes.com/2009/03/31/spam-back-to-94-of-all-e-mail/.

59. Brian Krebs, "A Year Later: A Look Back at McColo," *Washington Post*, November 11, 2009, http://voices.washingtonpost.com/securityfix/2009/11/a_year_later_a_look_back_at_mc.html.
60. Bygrave and Bing, *Internet Governance*, 2. Estonia's "Internet war" was a complex event whose detailed history remains to be written; for an overview see Gadi Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts During the Internet War," *Georgetown Journal of International Affairs* (Winter/Spring 2008): 121–26.
61. Geert Lovink, "Interview with Alan Liu," networkcultures.org, February 28, 2006, http://networkcultures.org/wpmu/geert/interview-with-alan-liu/.
62. On auto-retweeting in Twitter: Andrei Boutyline, personal communication. (Note that this automation is distinct from the human-based retweeting practices examined by danah boyd, Scott Golder, and Gilad Lotan, "Tweet, Tweet, Retweet: Conversational Aspects of Retweeting on Twitter," Proceedings of the 43rd Hawaii International Conference on Social Systems (HICSS 43), 2010, http://www.danah.org/papers/TweetTweetRetweet.pdf. On social network scams, a representative instance is that of Rakesh Agwaral as discussed by Graham Cluley, "See a Facebook Scam in Action," sophos4.com, January 22, 2009, http://www.sophos4.com/blogs/gc/g/2009/01/22/facebook-scam-actio/.
63. Rheingold, *Virtual Community*, 42. Dewey, *The Public and Its Problems*, 151.
64. Rheingold, *Virtual Community*, 54.
65. Randall Collins, *The Sociology of Philosophies: A Global Theory of Intellectual Change* (Cambridge, MA, 2000), 38.
66. Matt Haughey, "Does Amazon Enable Comment Spam?" wholelottanothing.org, February 22, 2010, http://a.wholelottanothing.org/2010/02/does-amazon-enable-comment-spam.html. For Textbroker, see http://www.textbroker.com.
67. Lev Manovich, *The Language of New Media* (Cambridge, MA, 2001), 46.
68. Charles J. Stivale, "Spam: Heteroglossia and Harassment in Cyberspace," in *Internet Culture*, ed. David Porter (New York, 1997), 133–44, 136. Jenna Burrell, "Problematic Empowerment: West African Internet Scams as Strategic Misrepresentation," *Information Technology and International Development* 4, no. 4 (2008): 15–30. Jussi Parikka and Tony D. Sampson, *The Spam Book: On Viruses, Porn, and Other Anomalies from the Dark Side of Digital Culture* (Cresskill, NJ, 2009).
69. Peter Sloterdijk, *Terror from the Air* (Los Angeles, 2009), 23.
70. Ian Baucom, "Financing Enlightenment, Part Two: Extraordinary Expenditure," in *This Is Enlightenment*, ed. Clifford Siskin and William Warner (Chicago, 2010), 350.
71. J. C. R. Licklider, "Some Reflections on Early History," in *A History of Personal Workstations*, ed. A. Goldberg (New York, 1988), 115–40.