

Bugs: Rethinking the History of Computing

Cait McKinney & Dylan Mulvin

Communication, Culture & Critique (In press; pre-print)

Abstract

This paper argues that scholars of computing, networks, and infrastructures must reckon with the inseparability of “viral” discourses in the 1990s. This co-assembled history documents the reliance on viral analogies and explanations honed in the HIV/AIDS crisis and its massive loss of life, widespread institutional neglect, and comprehensive technological failures. As the 1990s mark a period of intense domestication of computing technologies in the global north, we document how public figures, computer experts, activists, academics, and artists used the intertwined discourses surrounding HIV and new computer technologies to explicate the risks of vulnerability in complex, networked systems. The efficacy of HIV-as-analogy is visible in the circulation of viral concepts, fears surrounding interdependence, and emergent descriptions of precarity in the face of a widespread “infrastructure crisis.” Through an analysis of this decade we show how HIV/AIDS discourses indelibly marked the domestication of computing, computer networks, and nested, digitized infrastructures.

Keywords: Computer history; HIV/AIDS; Infrastructure; Networks; Viruses; History of communication; Crisis

Acknowledgments: We would like to thank Marc Aidinoff, Bart Cammaerts, Marika Cifor, Devin Kennedy, Sharif Mowlabocus, Gili Vidan, two anonymous and generous reviewers, and the Social Media Collective at Microsoft Research New England for their assistance in thinking through and revising this work.

Introduction

Imagine a user of a PC running MS-DOS in 1990 who has recently added a modem to their hardware set-up, which they use to communicate with a global network of likeminded individuals; they send and receive floppy disks in the mail, each loaded with a new program; it's all very new and exciting. Then one day their computer is overtaken, and they are left with the following message:

ATTENTION:

I have been elected to inform you that throughout your process of collecting and executing files, you have accidentally ¶[HÜçKΣ]► yourself over; again, that's PHUCKED yourself over. No, it cannot be; YES, it CAN be, a √itûs [virus] has infected your system. Now what do you have to say about that? HAHAAHAHAHA. Have ¶[HÜÑ [phun] with this one and remember, there is NO cure for AIDS. [Figure 1]

Their computer has been infected with “AIDS,” a computer virus.¹ Its origins are unclear: possibly it came through the network, or maybe through a disk. The user's friend has a supposedly immune Apple computer, but it is soon infected with “CyberAIDS,” a separate virus that targets Mac systems.²

These viruses were acute, material examples of a wider equation between computing and HIV/AIDS. In 1989, U.S. Representative Wally Herger spoke to the U.S. House Judiciary Committee while they considered computer virus legislation: “the problem of computer viruses and their cousins, the computer worm and the trojan horse, has become one of the primary topics of conversation within the computer industry....Some have even called [an attack on the ARPANET] the AIDS of the computer world” (“Committee on the Judiciary,” 1989). Soon after, in 1991, the National Research Council (NRC) published *Computers at Risk: Safe Computing in the Information Age*, a report cautioning that risk was multiplied in a network structure: “The most damaging change in the operating assumptions underlying the PC was the advent of network attachment” (p. 12). In 1999, the NRC published a follow-up report, *Trust in Cyberspace*, in which they promoted institutional and personal responsibility for protecting networks. While reaching for a useful analogy, William Flanagan, a co-author of the report, likened the sharing of data through “open networking environments” to the “spread of AIDS, noting new concerns about the trustworthiness of the people who

constitute one's social network and the dire consequences that could result from the indiscriminate expansion of one's contacts" (p. 187).



Figure 1 - Virus screen for the "AIDS" computer virus

These episodes frame a story about computing in this period: using a computer is risky, being connected to other humans is risky, and the more we rely on computers—and in particular, networked computers—the more we put ourselves at risk. There is also another familiar story about this period. When we reach for analogies to explain the risk involved in trusting our networked connections, we often light upon the language of sex, the technical *and* biological dangers of infections, and our fears of vulnerability.

Throughout the 1990s, the dangers of networked connection structured how many seemingly disparate kinds of social relations were described—including networks of sexual partners and networks of computers. In the lead-up to the year 2000, under the headline “The Y2K Disease,” the British software CEO Karl Feilder wrote,

We are exchanging digital fluids with each other every day as we experience the bump and grind of unlimited Internet access. We're hooked on our daily cyber orgasms. But are we practicing safe computing? Are we wearing virtual condoms?

Writing in the same year in the digital media studies journal *CTheory*, Jennifer Ruth Fosket and Jennifer Fishman (1999) describe anxieties about the Y2K bug as situated within larger fears of the “network society.” They argue,

the Y2K problem indicates the complexity of issues of trust and uncertainty within a networked society, where it is no longer enough simply to trust an organization, but *one must also trust all of those organizations with which the first organization is connected.*

Relying on an understanding of networked contagions, this language reflects what Cindy Patton (1996) calls the “National Pedagogy” of Safe Sex Education that had developed in response to the HIV/AIDS epidemic. As expressed by some gay men early in the crisis, and widely promoted by American health institutions, the national pedagogy presented monogamy and abstinence as the only solutions to the vulnerability of humans who are connected with other humans; [See figures 2 – 3] the national pedagogy cautioned that an individual, to be certain of preventing transmission, ought to disengage from participation in ambiguous sexual networks occupied by intravenous drug users, communities of color, and gay men, who were all stigmatized and blamed for the North American AIDS crisis. Perhaps most famously, the threat of networked contagions was frequently used by the Reagan-era Surgeon General, C. Everett Koop, as the U.S. government’s official standpoint on HIV. From a 1988 description of Koop’s response to the HIV crisis and the government’s pedagogical approach:

[Koop stated that] the only certain protection against AIDS “is not to have sex at all.” That idea drew laughs and even a few hoots. Koop did not crack a smile. “The next best thing is to find the one right person . . . what we call monogamy. *When you have sex with someone, you are having sex with everyone that he or she has had sex with in the past.*” (Fisher 1988, p. C1)

Understanding AIDS

A Message From The Surgeon General


This brochure has been sent to you by the Government of the United States. In preparing it, we have consulted with the top health experts in the country.

I feel it is important that you have the best information now available for fighting the AIDS virus, a health problem that the President has called "Public Enemy Number One."

Stopping AIDS is up to you, your family and your loved ones.

Some of the issues involved in this brochure may not be things you are used to discussing openly. I can easily understand that. But now you must discuss them. We all must know about AIDS. Read this brochure and talk about it with those you love. Get involved. Many schools, churches, synagogues, and community groups offer AIDS education activities.

I encourage you to practice responsible behavior based on understanding and strong personal values. This is what you can do to stop AIDS.



C. Everett Koop, M.D., Sc.D.
Surgeon General

Este folleto sobre el SIDA se publica en Español.
Para solicitar una copia, llame al 1-800-344-SIDA.

Figure 2 – Cover of an eight-page pamphlet distributed by the U.S. Department of Health and Human Services, c. 1988

<h2 style="text-align: center;">What Behavior Puts You At Risk?</h2> <p>You are at risk of being infected with the AIDS virus if you have sex with someone who is infected, or if you share drug needles and syringes with someone who is infected.</p> <p>Since you can't be sure who is infected, your chances of coming into contact with the virus increase with the number of sex partners you have. Any exchange of infected blood, semen or vaginal fluids can spread the virus and place you at great risk.</p> <p><i>The following behaviors are risky when performed with an infected person. You can't tell by looking if a person is infected.</i></p>	<p style="text-align: center;">RISKY BEHAVIOR</p> <p>Sharing drug needles and syringes.</p> <p>Anal sex, with or without a condom.</p> <p>Vaginal or oral sex with someone who shoots drugs or engages in anal sex.</p> <p>Sex with someone you don't know well (a pickup or prostitute) or with someone you know has several sex partners.</p> <p>Unprotected sex (without a condom) with an infected person.</p> <p style="text-align: center;">SAFE BEHAVIOR</p> <p>Not having sex.</p> <p>Sex with one mutually faithful, uninfected partner.</p> <p>Not shooting drugs.</p>
--	--

AMERICA RESPONDS TO AIDS

3

Figure 3 – Excerpt from the HHS pamphlet c. 1988 (from page 3)

Koop's dictum ("When you have sex... with everyone that he or she has had sex with") is echoed almost verbatim ten years later in the Fosket & Fishman discourse analysis of the Y2K crisis ("one must trust all of those organizations with which the first organization is connected").

Our focus in this article is the handiness and pervasiveness of this conspicuous network analogy and how it travelled across HIV and computing discourses. Our history builds on earlier work that was attuned to the inseparability of sex and technology in the 1990s. In her crucial study of the early consumer web, Wendy Chun argued that "sex and sexuality dominate descriptions and negotiations of the thrills and dangers of networked contact" (2006, p. 12). Likewise, Andrew Ross (1991) and Stefan Helmreich (2000) were early in identifying many of the ways that AIDS was being used as a heuristic for networked dangers. One of Helmreich's informants, a computer security professional, told him, "We tried to use the analogy of AIDS and its impact on sexual practices as an analogy to viruses and their impact on 'safe computing'" (p. 476). Extending beyond the realm of computing to other media, Douglas Rushkoff's *Media Virus* (1996) — itself a watershed document in the popularization of "viral" concepts — also connects tactics practiced by the AIDS activist group ACT UP to the origins of memetics and viral media.

From our retrospective vantage point, we argue that to understand the emergence of the network society scholars must grapple with the fact that HIV/AIDS offered a convincing template for explaining the dangers of interdependence in networked relationships. To a lesser extent, networked computing provided a powerful way to

understand HIV/AIDS, especially the ways networks of human connection could bond disparate populations and provide a potential structure for survival. In researching this project we have come to a surprising and potentially discomfiting conclusion: to write the history of computing in the global north it is necessary to understand the ways experts and non-experts alike used HIV to explain the threats of networked connection.

This is a historical project that seeks to intervene in the historiography of the network society of the 1980s and 1990s. While HIV/AIDS is still widely ignored in much of the historiography of this period (Brier 2009), it undeniably transformed the politics of the late twentieth century. We argue that HIV – its biological mechanisms, its epidemiological spread, and its aftermath – also marked technological discourses and the ways networked computing was explained. We do so by documenting key examples of network homologies as well as the ways AIDS activists objected to tidy attempts to pathologize networked computing through the lens of HIV. Which is to say: while computing discourses drew heavily upon HIV as a model virus and model crisis of trust, AIDS activists and people living with HIV had to adapt to computing as a means of survival. This article departs from existing literature by documenting this asymmetrical response to emerging computing technologies through the scant remnants of a material record.

This article is organized around three frameworks contemporary with the cusp, middle, and end of the 1990s:

In part one, “**the virus,**” we examine the year 1989 through the early 1990s, when the overlap of the HIV/AIDS epidemic and emerging computing technologies was largely confined to explicating risk: the portrayal of HIV as a high tech alien invader, the mixing of biological and technical meanings of virus, and fears around sharing either digital information or bodily fluids with a potentially endless network of anonymous others.

In part two, “**the network,**” we examine how HIV and computing were refracted through each other during a period of rapid adoption in the mid-1990s. Many people in the global north were experiencing a commercialized internet for the first time and some people living with HIV/AIDS accessed new pharmaceuticals that allowed them to live with the disease as a chronic illness. Here, the homology serves to explain systemic interdependence within the emerging everyday-ness of networked computing and health management.

In part three, “**the infrastructure,**” we examine the end of the decade when the “Y2K crisis” took on prominence as a subject of fear and outrage. In this period, we see AIDS activists and those living with the virus respond to the crisis as experts in surviving institutional failure; if the fear of contracting HIV compelled a crisis of trust (of sexual partners, state actors, technoscientific expertise, and networks of survival) in the 1980s,

an almost identical set of concerns were articulated in the 1990s as the Y2K crisis tested a complex society built on computerized infrastructure.

Because vulnerability to technological failure and to HIV/AIDS is unevenly distributed, risk is not felt to be shared nor experienced by the politically powerful. Vulnerable groups manage their risk within systems of necessary interdependence, including dependence on technological systems, through social movements, and grassroots organizing (Hamraie, 2017; Nakamura, 2015). In some cases, occupying a particular subject position towards vulnerability is the organizing principle around which new activists can self-organize and mutually recognize each other. Our history of HIV and computing shows how diverse actors develop understandings of vulnerability through differential access to information, treatment, technological remediation, and a basic exposure to risk.

Methods and Terminology

Our method draws on the cultural history of technology and textual analysis to ask what purpose HIV serves to understanding the computer world and what purpose the computer world serves in understanding how communities of struggle responded to HIV as yet another potential failure of infrastructure. To answer this question, we have assembled a collection of documents drawn from the popular and grey literatures of computing and AIDS activism: policy reports, trade publications, marketing materials, newsletters, blog posts, and mainstream cinema. These materials speak across our individual projects, each of which engage deeply with archival methods, and an interest in uncovering the histories of infrastructures. Cait McKinney is researching how AIDS activists used early computer networks to circulate health information in the late 1980s and 1990s, toward a queer history of early internet use. Dylan Mulvin is undertaking a history of the Y2K crisis as a significant and overlooked moment of technological repair, and a key episode in educating and training individuals and organizations to manage the unforeseen, and potentially devastating effects of old computer code on people's lives.

We came to this collaborative work because these literatures kept creeping across our individual projects—not all of the time, but too often to disregard as incidental. It is impossible to quantify the influence HIV had on computing, and so, our method attends to subtlety and saturation over scale. Our sample is necessarily interpretive rather than systematic, because it looks for sexuality in the background of scenes where it is not supposed to be. Our project shares with sexuality studies a commitment to taking

seriously the speculative, shadowy ways sex infiltrates public life. One conclusion we are able to make about scale with certainty is that the homology between computing and HIV is asymmetrical. Examples of HIV used in computer network discourse are abundant, while we found only a small set of examples of AIDS activists responding to or refracting this metaphor. To refine our analysis in light of this smaller sample, we look more broadly to the ways that AIDS activists used new computer networks, and to how HIV/AIDS scholarship and public health materials described networked vulnerabilities.

Metaphors and analogies do cultural work, explicating a complex idea, communicating an underestimated problem's severity, building empathy, or assigning stigma by articulating something new to a more familiar object. Susan Sontag's "AIDS and Its Metaphors" (1989) argues that metaphors about HIV/AIDS – including those used for computer viruses – rationalized the uneven distribution of vulnerability to the illness and positioned HIV/AIDS as a larger infrastructure problem. More recently, Lauren Berlant (2016) builds on Susan Leigh Star's (1999) work to explore infrastructure itself as a kind of metaphor for understanding difference, differential vulnerability, and the heterogeneity of systems. Working through these critical approaches to infrastructure and communication, we approach the metaphorical work in our cases as strategies for giving new users something to grasp as they struggled to understand their places in networks, while imagining a future defined by interdependence.

One difficulty of doing this project are our actors' terms as they move frequently between categories and registers: computing, communication, networks, infrastructures, information systems and even technology are often interchangeably used. It's no surprise, given the plasticity of these terms, that we see HIV used as a clarifying metaphor for computing's many apparent dangers and crises. Where we can, we use our actors' terms. When we need to be more abstract, we have settled on "networked connection" to describe the kinds of homomorphic structures invoked in this decade. A secondary contribution of this project is to expand the historical context for this key term in digital studies: by networked connection we mean the ways that humans are simultaneously joined with a potentially endless number of others through social interaction and the exchange of substances that can carry the network's traces – data, information, money, blood, semen and breast milk, to name a few.

Part 1

1989 – "The virus"

In December 1989, thousands of individuals and AIDS service organizations received a floppy disk in the mail labeled “AIDS Information — an Introductory Diskette Version 2.0.” Drawn from misappropriated mailing lists, recipients included HIV/AIDS researchers, who had attended a 1988 World Health Organization conference on AIDS, subscribers to *P.C. Business World*, members of the financial services industry, and the United States’ National Institutes for Health (“AIDS Information 2.0,” 1990; “Computer Alert,” 1990; Clough & Mungo, 1992). A fictitious organization called “PC Cyborg Corp” made the AIDS Information Diskette, though we now know that the disk was produced and distributed by a single individual, Joseph Popp, an anthropologist with a doctorate from Harvard who had been denied a position at the World Health Organization. Popp had idiosyncratic, hateful views about HIV. The disk was sent to organizations in the UK, Scandinavia, Africa, Australia, and the United States, and caused major data losses in many cases in which it was used.

The Diskette included two programs, INSTALL.EXE and AIDS.EXE. Users had to run the “INSTALL” program before they could access AIDS.EXE, an “interactive program for health education on the disease called AIDS” that promised “up-to-date information about how you can reduce the risk of future infection, based on details of your own lifestyle and history” (Clough & Mungo, 1992). When running AIDS.EXE a user would answer thirty-eight questions about their medical history and sexual behavior since 1980 (Kerr, 2016). In response to their answers, users received tailored (though cynical) advice, “Buy condoms today when you leave your office” or “Danger: Reduce the number of your sex partners now!” This advice was especially useless for HIV/AIDS experts, who might have wondered at the disk’s true purpose. These users did not know that the disk installed a second, hidden layer of software that we would now recognize as a Trojan horse and a form of malware. The diskette is recognized as the first piece of ransomware—a form of software that extorts unwitting users by seizing their computer hard drives until they pay a fee.

If the survey was the reason for running the disk, its true purpose was actually hidden in the INSTALL program, which clandestinely installed software on the user’s C: drive. After roughly ninety system reboots the program took the computer hostage (Bates, 1990). Users locked out of their machines confronted one of several error messages. These included: “You are advised to stop using this computer. The software lease has expired.” To renew the software lease, users needed to send payment to a Panama City post office box: either \$189 for 365 further uses of their computer, or \$389 for the lifetime of their hard disk (p. 5).

The AIDS information diskette yoked multiple understandings of viruses. The disk provided software *about* a virus (HIV) that infected computers with the kind of malware

often lumped into the category of “computer virus.” This coupling was instrumental in the way the attack worked. To circumvent any existing defenses, the disk traded in the user’s trust of computer software and desire for information about the spread of HIV. Recipients had few reasons to assume that the disk’s contents were nefarious, especially given that this event came while the antivirus industry was still in its nascence.³ For AIDS researchers and AIDS service organizations, the disk promised timely, useful information they were encouraged to share: “The health information provided could save your life.... Please share this program diskette with other people so that they can benefit from it too.” (Clough & Mungo, 1992, p. 139). Users who spread this information also unwittingly transmitted malware.

Soon after the disk’s arrival, the editors of *PC Business World* were alerted to the surreptitious use of their mailing list and they hired a virus expert, Jim Bates. Bates reverse-engineered the AIDS disk to create an “antidote” for infected computers, which he named AIDSOUT.COM. A second tool, called AIDSCLEAR, could de-encrypt files claimed by the software (“AIDS Information 2.0,” 1990). These ready-to-hand cures for AIDS.EXE stood in stark contrast to the lack of effective, coordinated response to the actual HIV. The episode, and its retelling in the history of computer viruses, speak directly to the entwinement of the AIDS crisis and computers. In their history of early computer viruses, Clough and Mungo (1992) outline the superficial similarities between these two “viruses.” They write,

It was curious, [Bates] thought, that the damned thing had been written to behave almost like the real AIDS virus.⁴ The technological bug was opportunistic, just like its biological counterpart. Both slowly, insidiously, infected the victim’s immune systems; both were patient; both were ultimately fatal to their hosts. (p. 139)

It requires a particularly distanced squint to see the diskette and its malware as homologous with HIV; yet, embedding malware within a pedagogical tool for virus education makes the comparison all but unavoidable. The virus metaphor’s wide adoption over alternatives— “worm” or “rogue program”—relied on wide media coverage of AIDS to explain how computer “viruses” could “spread” and “infect” whole systems (Gozzi, 1990; Parikka, 2007; Noble, 2018). Unlike the other pieces of metaphor-driven malware that were merely called “AIDS,” this disk’s content was also *about* HIV/AIDS, and targeted AIDS activists and researchers.

The burgeoning anti-virus community celebrated Bates’s speedy response to the AIDS diskette, including the editors of *The Virus Bulletin* (“AIDS Information 2.0,”

1990), who describe a series of lessons learned from the disk. They too tied together AIDS, risk, and computer use:

Some salutary lessons have been learned. Unsolicited software will, in the future, be treated with extreme caution by many. It is extraordinary that controls to prevent use of these rogue disks failed, or never existed, in so many businesses. It is also worth pointing out that virus specific software is useless for tackling unknown threats ... companies should take note that they are vulnerable to the misuse of their mailing lists... (p. 2)

If a mailing list can become a route of infection, then the contributors to *The Virus Bulletin* located responsibility for prevention squarely in the hands of computer users and business owners. Like “good” monogamous or abstinent citizens, these users were urged to act responsibly to shore up their own vulnerability, and that of their communities. These networked communities included AIDS activist networks, who circulated news of AIDS.EXE through text-based online Bulletin Board Systems (BBS) and mailing lists. The disk threatened to impede grassroots use of computer networks to circulate health information. In response, Philadelphia’s Critical Path AIDS Project, a BBS service and HIV-focused community internet service provider, published information about the diskette in its monthly newsletter.⁵ Critical Path warned readers that the virus specifically targeted organizations serving people living with HIV. The activist organization distributed the AIDSOUT remedy and offered free, 24-hour tech support over the phone to those whose computers were affected (“Computer Alert,” 1990). Critical Path’s rapid, community-focused response showed how users living with HIV relied on nascent computer networks to share up-to-date information that was otherwise hard to access within conditions of censorship and stigma. Here the strong interdependent networks built by AIDS activists are not a source of exposure, but rather a strength, and facilitated an effective response.

The episode surrounding the AIDS disk is a bizarre event, but it is not at all isolated. Throughout the 1990s, new and would-be computer users often confronted explanations of their vulnerability to technological systems through the heuristics of HIV/AIDS. Computers and trustworthy knowledge about transmission and treatment were both difficult to understand (Patton, 1996; Epstein, 1996). As the AIDS diskette showed, one could readily (if misleadingly) be used to explain the other. The editors of *The Virus Bulletin* could admonish companies that lacked protocols for protecting themselves from “rogue disks” just as “low risk behavior” within sexual networks was becoming a

requirement for both HIV-positive and negative people to demonstrate personal responsibility and “good” citizenship (Patton, 1996).

In this context, *The Virus Bulletin's* advice appears consistent with state responses to viral epidemics. The overlap of AIDS and computing does not end with the network metaphors used to explain personal responsibility and the viral prophylaxes that were emergent in computing cultures in the early 1990s. This period also includes a rich and under-explored history of computing by AIDS activists, who imagined how networked computing might support survival for people with HIV and responded with expertise to the prevalence of fear and panic surrounding new computing practices (McKinney, 2018).

Part 2

1995 – “The Network”

The 1990s represent a key transitional period in both networked computing and the North American AIDS crisis. Between 1990 and 1996, as more effective combination antiretrovirals reached market, AIDS-related deaths declined in the U.S. for the first time (Centers for Disease Control and Prevention, 1997). The widespread use of these drugs led to regular viral load testing as a health maintenance practice, and a growing sense of responsibility for managing one’s own health data. During the same years, increasing amounts of data about individuals moved into networked computing environments, including social security, banking, human resources, and electronic medical records (Berner, Detmer & Simborg, 2005; NRC, 1999; NRC, 1991); accordingly, these data were at risk to widespread network and security failures. Explicating this risk was a challenge for experts, journalists, and other cultural intermediaries.

During this transitional period, risk, data, infrastructure, and computerized information needed to be explained and widely discussed by a public that was newly engaged with the idea of pervasive and personal computing, and the possibility that human lives were already caught up in various databases. It’s during this period, for instance, that the National Research Council published several reports compelling policy makers and industry actors to responsibly manage the transition to networked infrastructures. The NRC cites the AIDS Diskette as a key example in a list of “Evidence of Inadequate Trustworthiness” (1991, p. 9). In the United Kingdom, during a debate of the 1990 Computer Misuse Act, Member of Parliament Emma Nicholson highlighted the danger of digitized medical files for people living with HIV/AIDS, hypothesizing, “AIDS victims can be identified through their blood details and then they can be blackmailed” (House of Commons, 1990).

Beneath this policy level, personal computer users and office workers became more aware of their data's imbrication in computer networks: "networking was in the air" (Cambell-Kelly & Aspray, 2004, p. 252). Office workers, who encountered the personal computer in the 1980s as a device for carrying out their own clerical tasks, would now encounter each machine as a node within a larger network of interdependent technologies. The growth of Local Area Networks (LAN) eliminated the need for some workers to perform their own backup routines, transferring the responsibility for data management to the network itself (and the network administrators responsible for maintenance) (Ceruzzi, 2003). By the mid-1990s, people with access to Netscape Navigator, Internet Explorer, and other interfaces could explore the wider internet beyond closed environments like CompuServ and America Online. In their public representation, computers transitioned from isolated devices used for word-processing, bookkeeping, and local databasing, to interconnected machines for communication and data management (Cambell-Kelly & Aspray, 2004).

The potential portability of network metaphors to HIV was of no interest to AIDS activists; however, their work also emphasized the importance of information and systematic understandings of interdependence. Beginning in the early 1980s, activists created and circulated their own information about HIV transmission and sex, working against the climate of abstinence, sex-negativity, and personal responsibility that characterize the National Pedagogy. Activists also engaged critically with data produced by medical industries to shape research to their needs, advocating for faster clinical trials that included women, people of color, and drug users (Epstein, 1996). AIDS information activism also mobilized computer networks. Activists built community-based ISPs and BBS networks in the 1980s and 90s to circulate grassroots health information within precarious conditions. Other sites of internet activism by AIDS activists include the "ACT UP Network," which acted as a communications infrastructure linking ACT UP chapters across the United States, Canada, and Europe, using conference calling, fax, BBS, and email (ACT UP New York, n.d.). Activists in New York State also consulted Silicon Valley encryption experts to advocate for anonymous electronic records of T-cell count data (Shapiro, 2004). These activists wanted to build internet-based resources for people with HIV by drawing on the potential of interdependence, as a source of networked *solidarity*, which Deborah Gould defines as affinities and reciprocities that bridge difference (2009, p. 329). [Figure 4]

Despite these activists' work, in the 1990s self-regulation and personal responsibility governed both mainstream public pedagogies around HIV and user responsibility in computing (and continue to do so today). The computer industries were tasked with building comfort and trust in the idea that people's lives could be managed

through databases and mediated through computer interfaces. Kevin Driscoll (2012) argues that this pedagogical framing of databases advocated “a kind of rugged individualism in which users must acquire and deploy technical knowledge defensively in order to avoid exploitation” (p. 4–5). As part of this moment, anti-virus software, couched in the language of personal responsibility for mitigating risk, was marketed to personal computer users. When Symantec launched Norton AntiVirus in 1991, advertisements featured a picture of Peter Norton wearing a medical mask, arms crossed in front of his chest: “Warning. Peter Norton has determined that PC viruses can be hazardous to your data... If your PC is unprotected, do the right thing: Pick up a copy of Norton AntiVirus.” [Figure 5] It’s through such discourses that responsibility and bodily autonomy became equated with protecting one’s data.

Next time your word processor is out sick, call someone with AIDS.

When you need word processing, duplicating, mailing services or database management, do the right thing: call a person with AIDS. The highly-trained staff at Multitasking Systems will pick up your work, complete it quickly, accurately and economically, and drop it off. In return, you'll be giving people with AIDS the best contribution of all: work. Work that will give them the financial and emotional support they need.

Next time you need to get the job done, call MTS at 727-9210.

We're more than up to the task.



- I want to give MTS my business. Please call me.
- I want to hire a worker with AIDS.
- I want to learn more about MTS.

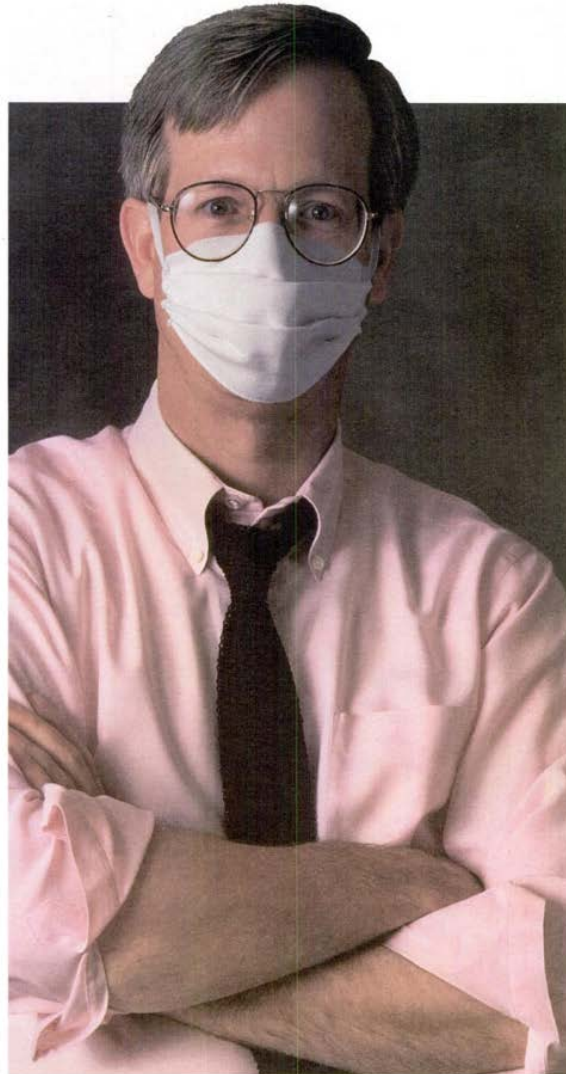
Name _____
Company _____
Address _____
Telephone _____

Please return to: Multitasking Systems of N.Y., Inc.
636 Sixth Ave., Suite 3D
New York, NY 10011

Figure 4 - MTS ad

— Detects over 540 viruses.* —

PETER NORTON NOW CURES VIRUSES.



Warning, Peter Norton has determined that PC viruses can be hazardous to your data. So to combat the threat, he's developed the Norton AntiVirus™, the only comprehensive virus protection, detection and elimination software for DOS.



The Norton AntiVirus stops viruses dead in their tracks before they infect your system. It also exterminates viruses already living on your hard disk or floppies. And it operates invisibly in the background, alerting you only when a virus is detected.

For protection against new viral strains, just call the 24-hour Virus Newsline. It's a free service that provides new virus information and easy instructions to keep your virus protection up to date, without the need to upgrade your software.

The Norton AntiVirus is 100% compatible with PC networks like Novell® and 3Com®. MIS managers can configure and password protect the Norton AntiVirus to meet their corporate needs.

And of course, it's Windows® compatible.

All this protection is yours for only \$129* with a 60 day money-back guarantee.

Take it from Peter Norton. If your PC is unprotected, do the right thing: Pick up a copy of the Norton AntiVirus. Call for more information.

1-800-343-4714, Ext. 711 0

SYMANTEC.

*Suggested retail price. © 1991 Symantec Corporation. The Norton AntiVirus is a trademark of Symantec Corporation. All other brand or product names mentioned are trademarks or registered trademarks of their respective holders. *Certified by NCSA, February 1991.

Copyrighted material

Figure 5 - Norton Antivirus advertisement from 1991. Taken from Infoworld (April 15, 1991), p. 33.

HIV's metaphorical utility for explaining risks associated with digitized and networked data is conspicuously represented in *The Net* (1995), a Hollywood action-thriller that introduced mainstream audiences to the Internet's transformative but also catastrophic potential. Chun (2006) lists this film as a key text that "revealed the dangers of living in cyberspace" (p. 37). Just as the NRC (1991) and the British parliament highlighted the threat of networked databases to individual medical records, *The Net's* opening scene shows a U.S. Under-Secretary of Defense receiving a positive HIV diagnosis and promptly committing suicide. As we learn, his electronic medical records had been hacked. [Figure 6]

The film is full of recurring plot devices that rely on the apparent plasticity and leakiness of data, and the dangers of networked connection. *The Net's* protagonist Angela Bennett (Sandra Bullock) has her identity "erased" and her Social Security Number reassigned to another name, all through the manipulation of online databases. The film also repeatedly refers to the ways emergent computing technologies might transform sex and sexuality. "IceMan," one of Bennett's chatroom correspondents, evokes national AIDS pedagogy when he writes, "No one leaves the house anymore. No one has sex. The Net is the ultimate condom." [Figure 7] To cement the imbrication of computing and HIV, the film's climax shows Bennett escaping from a hit-man hired by a tech company, by blending in with an ACT UP demonstration. [Figure 8] Part rally, part vigil, this protest is art-directed to look eerily like real ACT UP protests, minus the anger. As the protest passes by the Macworld expo at San Francisco's Moscone Center Bennett sprints out of the trade show. The crowd provides Bennett with cover so she can slip away.

While *The Net* was a significant part of 1995's "bumper crop of movies about computers, the Internet, and cyberspace" (Faden, 2001, p. 78), the prevalence of HIV-related imagery in the film passed unnoted in reviews. Faden goes as far as to state that "*The Net's* depiction of social unrest, while subtle, remains narratively inexplicable" (p. 89 n9). The depiction of unrest in the film *is* explicable if we acknowledge that HIV and computing discourses were fully entwined in the early 1990s; and that the stigma surrounding a positive HIV diagnosis could be used as a film's MacGuffin speaks to the twin fears of infection and data leakage.

If a health diagnosis is a gathering of data points, it can become an instrument of stigma, managed increasingly within imperfect computer systems. *The Net*, in both form and function, embodies the prevalent fear that you are at risk while using a computer—that you might "contract" a disease through mis-diagnosis or mis-categorization, via malevolent or careless computer use. But if the film begins with the presumed stigma of a positive HIV diagnosis—which is treated as a *de facto* death sentence—its protest scene also portrays the collective action and interdependence of AIDS activists as a safe refuge

against the violence of weaponized data. These are infrastructures in which vulnerability is collectively held through solidarity.

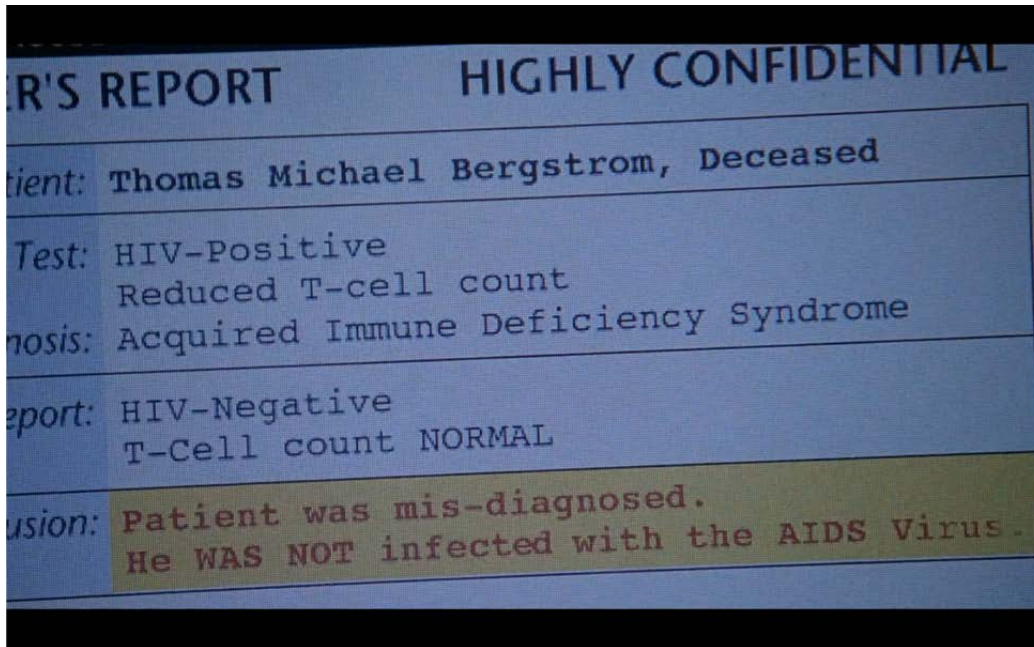


Figure 6 - Evidence of an edited electronic medical file that had falsely diagnosed an Under Secretary of Defense as being HIV positive. (From: The Net)

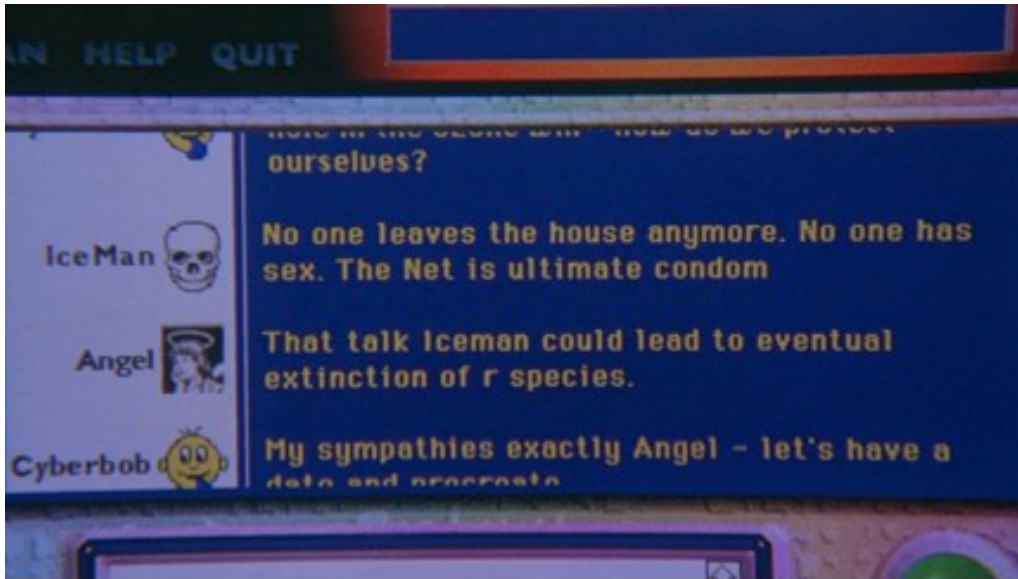


Figure 7 - Online chat dialogue. (From: The Net)



Figure 8 - As an ACT UP vigil passes in front of San Francisco's Moscone Center, Angela Bennett uses the crowd to escape her would-be assassins. (From: The Net)

Part 3

1999 – “The Infrastructure”

The year 2000 problem continues to behave like AIDS. It is a difficult concept to communicate to a wide audience. What's worse, most of us are PC HIV positive and we don't want to know it - and we're certainly not going to tell others. And, just like AIDS, not all of us will develop the full-blown virus at exactly the same time. (Feilder, 2000)

The term “infrastructure crisis” first appears with its contemporary valence beginning in the early 1980s (Brown, 1985; Sanders, 1993). It quickly became a common refrain of American political discourse and a bi-partisan watchword. The threat of the crisis holds that society’s material foundations are crumbling and putting everyone at risk. The crisis’ lasting power is attributable to its metonymical claim: as goes the material environment, so go the lives lived in those conditions. Such a crisis is different from isolated problems that only threaten at-risk populations, and also contrasts with “foreign” problems like nuclear apocalypse or war. Like HIV/AIDS, this crisis is structural, deeply embedded, and home-born of mismanagement. It also surfaces an endemic relationship of vulnerability to technologies that are meant to make life smooth: highways, bridges, tunnels, electricity, and communication networks. Hence, “infrastructure crisis” came to describe a kind of systemic fragility and gave a name to a new kind of rot at the base of development in the global north of the late 20th century.

In this era of apparent infrastructural breakdown, the Y2K bug represented a new kind of threat. In the lead-up to the year 2000, hundreds of billions of dollars were spent by governments, corporations, and smaller organizations to fix flawed computer code and prepare the general population for the possibility of widespread computer failure. Though it is popularly remembered now as a punchline to the 20th century, the bug was a non-trivial and potentially devastating threat to complex information networks. The main concern with the Y2K Bug was the fact that dates were stored in six digits instead of eight, with only two digits used for the year (e.g., DD/MM/YY vs. DD/MM/YYYY). Fear turned on the unanswerable question of how computer systems would interpret a century date written as two zeros. While many people, including members of the press, speculated that planes might fall from the sky and nuclear reactors might melt down, there were less spectacular (though no less existential) threats to welfare systems, credit cards, heating and ventilation systems, and waste treatment facilities. These were real-life versions of

the dystopian collapses pictured in *The Net*. Though the bug's risks were spectacular, the sites of greatest danger were often emphatically ordinary.

The Y2K crisis also presented an opportunity for refracting HIV as a continuing crisis; another "Millennium Bug" still threatening public health infrastructures. A person's survival relies on their access to care; it can also rely on their ability to use basic financial services, receive benefits checks, or cash in food stamps, processes dependent on functioning institutional databases. These threats are more practically felt for a person living with chronic illness than the state's capacity to keep planes afloat and nuclear missiles grounded. For Paul Edwards (1998), the Y2K crisis exposed the ways that computing (in particular, software) had become infrastructural: "Computers have become, as it were, the infrastructure of our infrastructures. . . [they operate] at the meta-level that we have learned to call *internetwork*" (p. 11, original emphasis). Edwards argues that the integration of otherwise unarticulated systems enabled new kinds of interdependence. His work modelled the scale of risk that Y2K posed through the concept of infrastructure breakdown; Y2K exposed several decades worth of legacy code that had silently become the foundation of everyday life.

By elevating computing as a form of meta-infrastructure, the late 1990s saw the fusing of network and infrastructural thinking. As a model for thinking about risk and vulnerability, this meant that infrastructural collapse now carried the danger of reverberating through systems of networked connection. We could now better understand state welfare systems, institutions of disease control, and non-governmental development work, as playing a vital role in the maintenance of ever-more precarious infrastructures. Moreover, we could understand the collapse of such institutions as threatening globally interdependent populations.

Manuel Castells opens *End of Millennium* (the final book [1998] of his three-volume series *The Information Age*) with a nod to these millenarian fears. Supporting his initial observation in the second edition (2010), he remarks that the Y2K crisis was, indeed, anti-climactic. Despite the book's title, and its subject matter, this is the only mention of Y2K. Instead, Castells frequently leverages the HIV/AIDS epidemic as a pivotal example, using it as a metaphor for communication, linkage, and the spatial organization and distribution of his understanding of the network. Castells's model of the network had given scholars, policy makers, and lay publics a new tool for imagining complex social arrangements at a global scale, during a period when the efficacy of drug treatments in the U.S. re-located AIDS elsewhere in the geographic imagination (specifically, to the global south). As is typical for the entanglement of HIV and computing, Castells concludes with a reminder of humanity's interdependence, vis-a-vis AIDS in Africa:

If Africa's plight is ignored or played down, it is unlikely to remain confined within its geographical boundaries. Both humankind and our sense of humanity will be threatened. Global apartheid is a cynic's illusion in the Information Age. (2010[1998], p. 122)

In many ways, this framework is a logical extension of the preceding use of HIV as an illustrative analogy. Whereas previous writers used the dangers of networked connection to compel prophylactic measures, Castells is arguing that harm in the network *anywhere* is harm *everywhere* – an argument that unites infrastructure collapse with the endemic risks of networked connection, through the threat of AIDS.

For a majority of the population, the Y2K crisis was not connected to the AIDS crisis in any material way. But discourses of stigma, vitality, and vulnerability connect the two crises. In focusing on the figure of infrastructure, we can see three trajectories converge in 1) the co-development of a widespread infrastructure crisis; 2) the integration of computers and infrastructure through the Y2K crisis; and 3) the equation of infrastructure with the underpinning of society. This convergence led to a terrifying conclusion: if the collapse of vital computer systems could lead to widespread infrastructure collapse, it could also entail the collapse of advanced society. This crisis language obscures the ways people working to survive know first-hand that infrastructural abandonment is already a standard operating condition.

In direct response to this disparity, people living with HIV addressed others living with the virus about the disparate implications of the Y2K bug and HIV. Ronald Russo published, "Y2K: Prepare, Don't Panic" (April 1999) in *The Body* — a significant website for people living with HIV/AIDS. Russo interviewed people living with HIV on their outlook and preparations for Y2K. The article outlines emergency preparedness tips including to stock up on medication and expect delays in disability benefit checks. Those interviewed for the article describe communities affected by HIV as uniquely suited to dealing with infrastructure failure, because they had already been doing so for nearly twenty years. Gould's formulation of solidarity says that communities drew strength from interdependence in the face of HIV/AIDS, as "both an affective state—an inclination toward, and perhaps identification with—along with a set of practices of mutual assistance and support, of having one another's back" (2009, pg. 329). In mainstream Y2K discourse, interdependence threatens exposure and vulnerability. In HIV/AIDS activist contexts, interdependence is a source of resilience that enables survival.

While Russo's article strikes a balance between preparedness and skepticism about the true threats of Y2K, another article published by the AIDS Survival Project (and hosted on *The Body's* web site) refuses the premise. Near the end of 1999, under the title "The Other Millennium Bug" David Salyer begins by stating, "I don't care about the so-

called Y2K problem. I'm supposed to care.” He itemizes all of Y2K’s potential minor inconveniences compared to living with HIV/AIDS. Salyer decries a lack of continued attention to AIDS, resulting from the relative success of combination antiretrovirals, the news media’s fatigue with covering the virus, activist burnout, and a shift away from visible impact on privileged, white lives:

[...] By January 1, 2000, we'll know what the Y2K bug can do. Experts tell us it can be fixed or eliminated. Y2K may cause minor inconvenience, they say. The other big millennium bug, HIV, will continue to defy eradication for the time being, creeping into the next century, invading bodies all over the world, wreaking havoc on lives. No matter what you may have heard, AIDS isn't over. (Salyer, 1999)

Salyer was correct about the disproportionate attention paid to the Y2K crisis compared to the ongoing HIV/AIDS epidemic. To put a fine point on it: while we have yet to identify a single death attributable to the Y2K crisis, it nonetheless compelled hundreds of billions of dollars of spending on preparedness efforts. In contrast, by 1999, an estimated 33.6 million individuals had contracted HIV and at least 2.6 million people had died from AIDS-related illnesses worldwide (“The HIV/AIDS Epidemic,” 1999). And by the end of the decade in the U.S., people of color far exceeded the number of white Americans who met the AIDS-case definition, signaling disparate access to health care (CDC, 2001).

Within these conditions of disparity, AIDS activists, service organizations, and people living with HIV brought their own expertise to thinking about the representation of crises, the risks of infrastructural collapse, and the vulnerability of data in networked systems. Because of stigma, people living with HIV were already advocates for their own data-management autonomy, in particular concerning access to information and electronic health records. Vulnerable populations build interdependencies in response to potential infrastructure failures – like activist responses to imagining how computing failures would affect a chronically ill person’s drug prescriptions or disability benefit checks. As a chapter in an ongoing reckoning with the precarity of infrastructure, the Y2K bug exposed and aggravated the knowledge that we all make do and make a living in structures not of our own design (Berlant, 2016). Self-policing one’s data or body presented a wholly inadequate response to this infrastructural precarity, while HIV/AIDS-informed expertise about the power of interdependence offered other models for living with systemic vulnerability.

Conclusion

In the global north, the 1990s marked a period of heightened flexibility in the interpretation of what computing meant and would come to mean. With every new promise of what a networked computer could do came corresponding fears and threats. Analogies and metaphors are instrumental in simplifying and stabilizing the meaning of new technologies and the practices surrounding them. HIV/AIDS provided a ready template for interpreting the future of computing's domestication. We can see this in the circulation of viral metaphors, fears surrounding interdependence, and a sense of precarity in the face of a widespread "infrastructure crisis." Likewise, emergent understandings of information technologies, the leakiness of data, and the endemic vulnerabilities of networked connection were instrumental in the public pedagogy surrounding HIV. The virus's "high tech" discourse was key to portraying the epidemic as a threat to complex information societies.

We write this project in the midst of a new crisis of networked publics. A widespread collapse of trust in institutions, democratic politics, and entrenched media are being blamed on polarization, filter bubbles, the virality of misinformation, and the interdependence of world-wide information networks. Amid larger controversies surrounding the acceptable limits of "content moderation," YouTube must decide how to handle popular and often "viral" videos promoting AIDS-denialism (Schulson, 2018; Gillespie, 2018). These incidents restage a classic problem around the quality of health information: the first discussion of HIV in *Wired Magazine* is a short review, in 1994, of the AIDS-denialist text *Rethinking AIDS*, by Robert Root-Bernstein (Coupland, 1994). The review appears in the second year of the magazine's run, yet the disease appears frequently in the margins of this key Silicon Valley artifact and the magazine's premier issue includes a full-page ad for an AIDS service organization ("Visual AID") local to San Francisco. None of this should be surprising, as the rise of Silicon Valley in the 1980s and 1990s shared a time and geography with one of the United States' most visible responses to HIV. How these communities may have been entangled escapes consideration in existing industry histories, presenting an area for future research.

For historians of this period, and for readers who care about the discursive construction of crises and new technologies, we believe that the relationship between HIV and computing must be taken seriously. More than a trifling coincidence, we have come to believe that computer history must reckon with its reliance on viral metaphors honed in the AIDS crisis' massive loss of life, total disenfranchisement, and comprehensive technological failures, all of which have an exaggerated impact on the most marginalized and resource-poor. We have only been able to offer a small sample of our assembled research and we would welcome more additions to this historical work, and to our shared understandings of the cultural milieu in which common sense forms.

Networked connections always carry the risk that a failure in one place may reverberate and cause harm across the entire system. Fears of bugs, viruses, and harm hone the ways in which our imbrication in these systems is understood and felt (Mulvin, 2018). Communities of struggle know that today's networked crises are not new and they are not simply the result of novel technologies. As our history shows, we may also want to know how our own fears of contagion, sense of vulnerability, and awareness of our interdependence shape and distort the ways we understand and talk about our own unfolding crises.

Notes

- 1 Detailed information about the AIDS computer virus is sketchy. We excerpted this text from watching an Australian person self-infect their hard-drive on YouTube. "AIDS MS-DOS Virus" posted by Ripspawnguild:

<https://www.youtube.com/watch?v=G252lZkydbQ>

- 2 CyberAIDS was one of the first viruses to infect Apple computers, beginning in the mid-1980s, and is discussed at length in Usenet groups for Apple users. See:

<https://groups.google.com/forum/#!topic/comp.sys.apple/OfoeMIQwjPQ>

- 3 John McAfee's antivirus company was founded in 1987, while "computer viruses" were the cover story of the September 26, 1988 issue of *Time*.

- 4 AIDS is, of course, not a virus. Though much of the primary source material for our research does not disambiguate HIV and AIDS.

5 Community Internet Service Providers offer free or low-cost online access supported by training programs geared towards political or service-oriented goals.

Bibliography

- ACT UP New York Records. Box 11, Folders 1–3; Box 233, Folders 2–3. *New York Public Library Manuscripts and Archives Division*.
- AIDSInformation 2.0. (January, 1990). *Virus Bulletin*, 2.
- Bates, J. (January, 1990). Trojan horse: AIDS information introductory diskette version 2.0. *Virus Bulletin*, 3–6.
- Berlant, L. (2016). The commons: Infrastructures for troubling times. *Environment and Planning D: Society and Space*, 34(3), 393–419.
- Berner, E. S., Detmer, D. E., & Simborg, D. (2005). Will the wave finally break? A brief view of the adoption of electronic medical records in the United States. *Journal of the American Medical Informatics Association*, 12(1), 3–7.
- Brier, J. (2009). *Infectious ideas: US political responses to the AIDS crisis*. Chapel Hill: University of North Carolina Press.
- Brown, R. W. (Oct 27, 1985). Long Island Opinion; We Must Rebuild Island's Roads. *New York Times*, p. LI11.
- Campbell-Kelly, M., & Aspray, W. (2004). *Computer: a history of the information machine*. Boulder: Westview Press.
- Castells, M. (2010[1998]). *End of millennium*. Oxford; Malden, MA: Blackwell Publishers.
- Centers for Disease Control and Prevention. (1997). *Update: Trends in AIDS Incidence, Deaths, and Prevalence – United States, 1996*. Retrieved from <https://www.cdc.gov/mmwr/preview/mmwrhtml/00046531.htm>
- Centers for Disease Control and Prevention. (2001). *HIV and AIDS — United States, 1981–2000*. Retrieved from <https://www.cdc.gov/mmwr/preview/mmwrhtml/00046531.htm>

- Ceruzzi, P. E. (2003). *A history of modern computing*. Cambridge, MA: MIT Press.
- Chun, W. H. K. (2006). *Control and freedom: power and paranoia in the age of fiber optics*. Cambridge, MA: MIT Press.
- Clough, B., & Mungo, P. (1992). *Approaching Zero: Data Crime and the Computer Underworld*. London: Faber & Faber.
- Computer Alert: 'Trojan Horse' AIDS Diskette. (1990). *Critical Path AIDS Project Newsletter*, 1(3), 8–9.
- Committee on the Judiciary, House of Representatives. (1990). *Computer virus legislation*. Hearing before the Subcommittee on Criminal Justice of the Committee on the Judiciary, House of Representatives, 101st Congress. *Computer Virus Eradication Act of 1989*. Washington, DC: U.S. Government Printing Office.
- Coupland, K. (1994). AIDS: Not what you think it is? *Wired* 2(3), 114.
- Driscoll, K. (2012). From Punched Cards to "Big Data": A Social History of Database Populism. *Communication +1*, 1(1), 1–33.
- Edwards, P. N. (1998). Y2K: Millennial reflections on computers as infrastructure. *History and Technology*, 15(1–2), 7–29.
- Epstein, S. (1996). *Impure Science: AIDS, Activism, and the Politics of Knowledge*. Berkeley: University of California Press.
- Faden, E. S. (2001). The cyberfilm: Hollywood and computer technology. *Strategies: journal of theory, culture & politics*, 14(1), 77–90.
- Feilder, K. (February 17, 2000). The Y2K disease. *IT Web*. Retrieved from http://v2.itweb.co.za/index.php?option=com_content&view=article&id=107520
- Fisher, M. (1988, February 26). Surgeon General Minces No Words on AIDS. *Washington Post*, p. C1.
- Fosket, J. R., & Fishman, J. (1999). *Constructing The Millennium Bug: Trust, Risk, And Technological Uncertainty*. *CTheory*.

Retrieved from

<https://journals.uvic.ca/index.php/ctheory/article/view/14743/5613>

- Gillespie, T. (2018). *Custodians of the Internet*. New Haven, CT: Yale University Press.
- Gould, D. (2009). *Moving Politics; Emotion and ACT UP's Fight Against AIDS*. Chicago: University of Chicago Press.
- Gozzi, R. (1990). The Computer "Virus" as Metaphor. *ETC: A Review of General Semantics*, 177–180.
- Hamraie, A. (2017). *Building access: universal design and the politics of disability*. Minneapolis: University of Minnesota Press.
- Helmreich, S. (2000). Flexible infections: computer viruses, human bodies, nation-states, evolutionary capitalism. *Science, Technology, & Human Values*, 25(4), 472-491.
- The HIV/AIDS Epidemic at the End of 1999. (1999). *Population and Development Review*, 25(4), 827–829.
- House of Commons. (1990). *February 9 Debate (col 1153)*. Retrieved from <https://publications.parliament.uk/pa/cm198990/cmhansrd/1990-02-09/Debate-1.html>
- Kerr, T. (2016). AIDS 1969: HIV, History, and Race. *Drain*, 13(2).
- McKinney, C. (2018). Printing the network: AIDS activism and online access in the 1980s, *Continuum* 32(1), 7–17.
- Mulvin, D. (2018). Media Prophylaxis: Night Modes and the Politics of Preventing Technological Harm. *Information & Culture: a Journal of History*, 53(2), 175–202.
- Nakamura, L. (2015). The unwanted labour of social media: Women of colour call out culture as venture community management. *New Formations*(86), 106-112.
- National Research Council. (1991). *Computers at risk: safe computing in the information age*. Washington, DC: National Academy Press.

- National Research Council. (1999). *Trust in Cyberspace*. Washington, DC: National Academies Press.
- Noble, S. (2018). *Epidemiology of Algorithms*. Paper presented at the Society for Cinema and Media Studies.
- Parikka, J. (2007). *Digital Contagions*. New York: Peter Lang.
- Patton, C. (1996). *Fatal Advice: How Safe-Sex Education Went Wrong*. Durham, NC: Duke University Press.
- Rushkoff, D. (1994) *Media Virus! Hidden Agendas in Popular Culture*. New York: Ballantine.
- Russo, R. (April, 1999). Y2K: Prepare, Don't Panic. *Body Positive*, 12(4), 16–23. Retrieved from <http://www.thebody.com/content/art31239.html>
- Salyer, D. The Other Millennium Bug. *The AIDS Survival Project*, (November/December, 1999). Retrieved from <http://www.thebody.com/content/art32264.html>
- Sanders, H. T. (1993). What Infrastructure Crisis? *Public Interest* (110), 3–18.
- Schulson, M. Are Google and Facebook Responsible for the Medical Quackery They Host? *Undark*. Retrieved from <https://undark.org/article/aids-denialism-quackery-facebook-youtube/>
- Shapiro, S. (October 23, 2004) ACT UP Oral History Project/Interviewer: S. Shulman & J. Hubbard.
- Sontag, S. (1989). *AIDS and Its Metaphors*. New York: Farrar, Straus and Giroux.
- Star, S. L. (1999). The Ethnography of Infrastructure. *American Behavioral Scientist* (43), 377–91.