Jonathan Zittrain, *The Future of the Internet—And How to Stop It*
Allen Lane: London 2008, £20, hardback
342 pp, 978 1 846 14014 3

Daniel Miller

STERILIZING CYBERSPACE

When theorists and artists first started exploring the internet in the early nineties, one of the most popular metaphors deployed was that of the rhizome, drawing an analogy between the web's proliferating pathways and the underground root system of plants. More recently, the allegory of choice has shifted one stage along, and the rhizome has been supplanted by the figure of the feed. With the internet's increasing commercialization, web content has come to be aggregated and distributed in the form of RSS, video and html-embedded feeds; the lateral spread of vegetable life has given way to the means of digesting it, and in place of the hackers and cyberpunks who once dominated the public imaginary, there are now user-consumers chewing digital cud. The utopian future that the early net seemed to promise, meanwhile, has been thoroughly broken down by its passage through the system.

Jonathan Zittrain's lucid new book traces this movement and puts it in context. Zittrain is—astonishingly—the professor of Internet Governance and Regulation at Oxford; one of a burgeoning number of legal scholars who have recently trained their attention on cyberspace. *The Future of the Internet* opens by contrasting two different tendencies that run through the history of information technology. In the red corner, there is the tinkerer–hobbyist model, best represented by flexible, re-programmable personal computers like the 1977 Apple II. In the blue, there is the new leading edge of consumerist–technological development, embodied by the same company's iPhone, launched in 2007. 'The Apple II was quintessentially *generative* technology', Zittrain stresses, while 'the iPhone is the opposite. It is sterile. Rather than a platform that invites innovation, the iPhone comes pre-programmed: you are not allowed to tinker with the all-in-one device

that Steve Jobs sells you.' According to Zittrain, the post-1970 phase of the history of computing produced a double victory for generativity. Firstly, the spread of the hobbyists' personal computer into the mainstream in the mid-80s, which effectively destroyed the previously existing IBM business model of powerful general-purpose machines, maintained exclusively by the vendor. Windows PCs, like their Mac OS and Linux counterparts, were designed to run code from any source: even Bill Gates, as Zittrain points out, did not aim at a world in which PCs *only* ran Microsoft software, but one in which *all* ran it. Secondly, the revolutionary expansion of the internet from the mid-90s, after the development of dial-up software—Winsock was coded by an employee of the Tasmanian University Psychology Department in 1994, and bundled by Microsoft in Windows 95—sidelined proprietary, centrally controlled networks like Compuserve and AOL in favour of the college-born World Wide Web, with its absence of paying subscribers or private capital.

This double triumph opened the way to a surge of creative endeavour, in which the grid's generativity was a boon not only to code-writing but to a much wider range of artistic and cultural ventures, including 'those that benefit from the ability of near-strangers to encounter each other on the basis of mutual interest, form groups, and then collaborate smoothly enough that actual works can be generated' (Zittrain's prose occasionally reflects his geek-at-law-school formation). Hotmail took off in 1996; Google was incorporated in 1998; Wikipedia launched in 2001. In the early 2000s, collective tinkering played a key role in generating the social-network applications of Web 2.0 platforms (MySpace in 2003, Facebook in 2004), video-sharing (YouTube was launched by three ex-PayPal employees in 2005) and experimental mash-ups, integrating data from different sources (notably the reworking of Google Maps). The great virtue of PCs and the internet to date, Zittrain suggests, has been their capacity to produce 'unanticipated change' by dint of 'unfiltered contributions from broad and varied audiences'—an input that far exceeds that of the best-funded R&D department.

But this fragile ecology is now under threat as the proprietary model, once championed by IBM, stages a Thermidorian comeback. The central argument of *The Future of the Internet* is that the open, generative technology upon which the internet was first built has left it fatally vulnerable to invasion by the free market's evil twin, organized crime. By 2006, 80 per cent of the world's total emails were spam, with nearly half of this originating in the US. Hostile software code is used to capture networked PCs, creating 'botnets' of zombie computers which can be turned into automated password-cracking 'phish' farms, virus incubators or spam servers, spewing out millions of messages unbeknown to their users, to email addresses gleaned from the internet or from the invaded PCs themselves. The earliest viruses were limited in their effects by transient dial-up connections; more

importantly, they were mainly motivated by mischief or curiosity rather than profit. The first is said to be a programme sent out by a Cornell graduate student in 1988 to count how many computers were using the internet; it turned out to be buggy and temporarily took over the PCs it was supposed to count, before their users united to stop it. But from around 1997, according to statistics compiled by the anti-virus centre CERT/CC, there has been a geometric increase in the number of 'security incidents'; by 2003, they had become too numerous to count.

With the expansion of the net and the advent of permanent broadband connections, viral invasion was developed as a business model. Even if only 0.001 per cent of email recipients take up the offer of fake watches, cheap software, designer replicas, anti-depressants, penile enlargement or university diplomas, dollars will be made. These commercial viruses are not destructive: 'those who hack for profit have no interest in destroying their hosts or drawing attention to themselves'; but they are increasing exponentially, their numbers doubling each year since 2003. The going rate for good spam code is now around $50,000. The scale is dizzying: a 2007 report estimated that the number of PCs belonging to botnets ranged from '100 to 150 million, or a quarter of all the computers on the internet'; around 1 million new bots were emerging each month. Spyware can be installed along with free downloads on unwitting users' PCs. Skype internet telephony software generates network traffic even when it is not being used; if it were to be reverse engineered by hostile software code, it could create 'the biggest botnet ever'. A single advertisement, contaminated with bad code and flashed from, say, the NYT website by a third-party advertiser, 'can instantly be circulated to the browsing tens of thousands', and thence to many more. It is a myth, Zittrain argues, that Macs and Linux, or Firefox and Opera browsers, are intrinsically better protected than Microsoft products: the scale of attacks only reflects Microsoft's market share and switching will simply make the other platforms more attractive as targets.

It is this low-level but high-volume exploitation of generativity that is rendering the status quo unsustainable, Zittrain argues. Though he conjures the spectre of an electronic apocalypse—a 'worm' spreading throughout the internet that eventually instructs infected machines 'to erase their own hard drives at the stroke of midnight'—he thinks the greater likelihood is a gathering stampede of frustrated users away from generative platforms and into the arms of a revamped IBM model: a network based on locked-down appliances, which 'incorporates some of the web's most powerful features while limiting innovative capacity and heightening regulatability'. The PC will lose its place at 'the centre of the information technology ecosystem' as people turn instead to the seemingly more secure patterns of access provided by sterile appliances and restrictive computing environments, such

as those found in libraries and schools. Zittrain's fear is that a 'lockdown on PCs and a corresponding rise of tethered appliances will eliminate what today we take for granted: a world where mainstream technology can be influenced, even revolutionized, out of left field'.

The trend away from generativity has been powerfully reinforced by the latest generation of non-modifiable appliances, such as the iPhone: elegant, multi-functional but, in Zittrain's terms, totally sterile. Other crucial devices here are the TiVo digital video recorder, the Blackberry wireless handheld device, the Amazon Kindle (a.k.a. 'swindle') e-book device and Microsoft's Xbox 360 games console. Although each of these systems is predicated on the advances of generative computing power—the TiVo, for instance, is run on the open-source Linux operating system—each of them also denies its users the possibility of additional generativity. In the case of the iPhone itself—a device which consumers technically do not own, but lease—Apple has clamped down on users who modify their machines by transmitting electronic kill-signals direct from Apple HQ, turning their phones into non-functioning iBricks. The Kindle is arguably still more restrictive: not only does it lock users into dependence on Amazon's own system for distributing e-books, it also proposes to end the archaic custom of lending books to others; those who purchase 'Kindle' e-books are contractually prohibited from sharing them or transferring them to another device.

But as Zittrain warns, 'on the internet, channels of communication are also channels of control', and tethered appliances can more easily be turned to purposes beyond the purely commercial. Already GPS—'sat-nav'—systems can be remotely programmed to eavesdrop on their users, and mobile phones turned into roving microphones or radar-transmission devices. TiVo knows what TV channel you are watching. A networked PC's microphone and video camera can be activated remotely, and its files searched and shared. In Zittrain's view, the growing trend towards sterile, proprietary devices only widens the scope for such surveillance, laying the foundations for the lockdown of internet space. Clearly, this is more than a merely technological issue: it raises the question of how the changing nature of the internet is transforming the way in which the world itself may be influenced.

The theme of convergence arguably provides a better focus for tracing the history of computing than Zittrain's opposition between generativity and sterility. In its conventional usage, convergence refers to the merging of different streams of media into a single, integrated system: in the living room, for example, the internet, telephone, digital video recording and television are blending into a single interface, accessed by a single controller. There are implications here for the still-further colonization of leisure time, as Gates was happy to admit with regard to the Xbox: 'It was about strategically being in the living room.'

Yet there is another sense to the term: namely, the increasing convergence between digital media and everyday life, as computing and networking power have accelerated into the social and commercial mainstream, dissolving earlier boundaries. Zittrain adverts to this in his discussion of surveillance, drawing a distinction between the 'post-Watergate' model of privacy and what he calls 'Privacy 2.0'. The former turned on the dangers of centralized entities and their plain-clothed agents amassing data and abusing it. By contrast, in the age of Privacy 2.0 the advent of cheap processors, networks and sensors means that governments or corporations may not be the agents of surveillance: 'peer-to-peer technologies can eliminate points of control and gate-keeping from the transfer of personal data and information just as they can for movies and music.' Hence civil-rights questions about, for example, police monitoring of public demonstrations are blind-sided when armies of amateur cameramen can assemble all the information law-enforcement professionals need, and then place it on Flickr for easy mobile browsing. Zittrain cites a 2006 pilot programme in Texas, where the state authorities set up eight webcams along the Mexican border whose feeds were published on a website which invited the public to alert the police if they thought they saw 'suspicious activity'. Similarly,

> With image-recognition technology mash-ups, photos taken as people enter [abortion] clinics or participate in protests can be instantly cross-referenced with their names. One can easily pair this type of data with Google Maps to provide fine-grained satellite imagery of the homes and neighbourhoods of these individuals, similar to the 'subversive books' maps created by computer consultant and tinkerer Tom Owad, tracking wish lists on Amazon.

As Zittrain himself appreciates, these developments stem from the consequences of generativity, rather than the effects of tethered sterility. In his view the general problem posed here is that, whether deployed by the state, corporations or private groups of activists, 'peer-leveraging technologies are overstepping the boundaries that laws and norms have defined as public and private, even as they are also facilitating beneficial innovation.' *The Future of the Internet* approaches its topic from a classically liberal perspective, and Zittrain's principal suggestion is that Madison's mechanisms of due process and separation of powers, to help 'substitute the rule of law for plain virtue', need to be translated into a compact for online communities. In the idiom of political philosophy, Zittrain's opposition between generativity and sterility appears to be a reformulation of that between liberty and security. Yet since Locke, liberalism has depended on the assertion of a clear separation between public and private spheres that here, it seems, is dissolving under the digital onslaught; how liberalism itself attempts to resolve this contradiction remains to be seen.

The main concern of *The Future of the Internet*, however, is to safeguard the generative creativity of PCs and the internet, both from the torrent of spam and viruses that threatens to render the web unusable within the next few years and from the neutering effects of sterile appliances and the IBM model. Blanket regulatory intervention is both too crude—preventing experimentation—and ineffective: spammers will remain in hiding. Instead, Zittrain outlines a series of measures which he hopes may plug the breach before it becomes critical—a multi-tiered digital-health programme, designed to make generative ecology safe for ordinary computer users. Wikipedia's consensus-based, self-governing procedure and communitarian ethos supply the normative model. The ultimate aim is to mobilize the wiki process of user participation not just at the content level, but at that of code: the PC–internet security space needs to explore ways of pooling the power of its millions of users—to 'empower rank-and-file users, rather than imposing security models'. Above all, 'we need to develop tools and practices that will enable people to help secure the net themselves, instead of waiting for someone else to do it'.

One step towards this is an information clearing-house to provide 'reliable, objective information about downloadable applications in order to help consumers to make better choices about what they download onto their computers.' Zittrain has already launched such a project, the unattractively named StopBadware.org, run in partnership with Google. The main weapon in this task is a piece of software called Herdict—'the verdict of the herd'—which assembles signs like the number of pop-up windows or crashes per hour, and makes the information available to other users for collective evaluation. PCs themselves might also be made more secure if the Wikipedia 'content recovery' safety nets could be applied at the level of code to create 'system restore' features in case of crashes. A PC could be split into two 'virtual computers': its 'Green' PC would house reliable software and important data—'tax returns, term papers, business documents'—while the 'Red' PC could be used for experimentation. PCs could also be built to provide better information on data going in and out, 'on the model of a speedometer or fuel gauge'.

Zittrain proposes a series of modest legal reforms to increase protection against corporate overreach. Discussing the issue of data storage on tethered products such as iPhones, he invites us to 'imagine cameras that effectively made [personal] photos property of Kodak, usable only in certain ways that the company dictated from one moment to the next'. Zittrain argues that users' rights to data portability need to be codified, to ensure that material is readily extractable in a standardized form should the user wish to change appliances—a move that would help to keep traffic open between generative and sterile technologies. Similarly, in instances where internet services such as Google Maps and Facebook encourage users to add their own customized

inlays and gizmos to the standard site template—adding value to the commercial enterprise by increasing participation—Zittrain contends that 'those who attempt to harness the generative cycle ought to remain application-neutral after their efforts have succeeded, so all those who have built on top of their interfaces can continue to do so on equal terms.'

Much more controversially, Zittrain proposes to encourage Internet Service Providers to detect and quarantine zombified PCs on their networks, instituting filters and gateways on the web. Such a move would fly in the face of the 'end-to-end neutrality' principle on which the internet has always been based. Zittrain endorses it somewhat sheepishly, arguing that it would buy time in which to develop a more educated user community, and permit generative technologies to remain sufficiently central within the digital ecosystem so as to be able to produce the next round of innovations.

Does it matter? Arguably, hobbyists will continue to tinker regardless of what gadgets go on sale, and the Gateses and Jobses will continue to harvest and exploit their inventions. Most PC and internet users are blithely unaware of the generative powers beneath their fingertips. But Zittrain provides a useful model for thinking about the relations between the internet's social and technological functions. He describes a series of layers: first, a physical layer—the wires or airwaves over which the information is sent; a protocol layer, establishing the addresses and codes through which the data can flow; an applications layer, at which tasks are performed; a content layer; and a social layer, comprising the interactions of internet users. Zittrain explains that tinkerers can experiment on one layer without having to understand much about the others, and there need not be any coordination between those working on one layer and those on another. Thus, 'someone can write an application without knowing whether its users will be connected by modem or broadband'. New vistas can be opened up at the level of content without regard for the platforms from which it will be accessed. At the same time, each layer is open to further development. It seems inarguable that the collectively generated innovations of the internet—however compromised, contaminated and spied upon—have expanded the space for the free exchange of ideas and information, independent of today's ruling powers and interests; and that further collective innovations are likely to do so again. In that sense, however modest his reforms, Zittrain is signalling a real problem.