

Název: **The Future of Internet**
Autor: *Johnathan L. Zittrain*
Vydavatelství: USA: Caravan Books, 2008 (e-book downloadable from jz.com)
Kategorie: Web, inovace
Ev. číslo:

The Future of Internet

“As ubiquitous as Internet technologies are today, the pieces are in place for a wholesale shift away from the original chaotic design that has given rise to the modern information revolution. This counterrevolution would push mainstream users away from a generative Internet that fosters innovation and disruption, to an appliancized network that incorporates some of the most powerful features of today’s Internet while greatly limiting its innovative capacity—and, for better or worse, heightening its regulability.” P. 8

“But the crucial element of the PC’s success is not that it has a cheap processor inside, but that it is generative: it is open to reprogramming and thus repurposing by anyone.” P. 19
Comment: TV is also popular, but it cannot be modified.

“...at the bottom are the physical wires, with services above, and then applications, and finally content and social interaction. ... The physical layer had become generative, and this generativity meant that additional types of activity in higher layers were made possible.” P. 22

CompuServe example: a system (1983) with similar services like internet (mail, chat, games, bulletin board) but paid and closed to user innovation. P. 23

“In the early 1990s the future seemed to be converging on a handful of corporate-run networks that did not interconnect. ... Each service had the power to decide who could subscribe, under what terms, and what content would be allowed or disallowed, either generally (should there be a forum about gay rights?) or specifically (should this particular message about gay rights be deleted?).” P. 24

“... the proprietary services could tell, they had only one competitor other than each other: generative PCs that used their modems to call other PCs instead of the centralized services.” P. 25

BBS based on phone system was build for user cooperation in 80’s. FIDOnet (1984) software was based on BBS and it was a messaging service.

“The Internet’s founding is pegged to a message sent on October 29, 1969. It was transmitted from UCLA to Stanford by computers hooked up to prototype ‘Interface Message Processors’ (IMPs). ... The UCLA programmers typed ‘log’ to begin logging in to the Stanford computer. The Stanford computer crashed after the second letter, making ‘Lo’ the first Internet message.” P. 27

“It was up to the people connected to figure out why they wanted to be in touch in the first place; the network would simply carry data between the two points.” P. 27

“The design of the Internet reflected not only the financial constraints of its creators, but also their motives. They had little concern for controlling the network or its users’ behavior.³³ The network’s design was publicly available and freely shared from the earliest moments of its development.” P. 28

“A more generative device [than one managed by a single vendor] like a PC makes innovation easier and produces a broader range of applications because the audience of people who can adapt it to new uses is much greater.” P. 30

“These proprietary networks were not user-programmable but instead relied on centralized feature rollouts performed exclusively by their administrators. The networks had only the features their owners believed would be economically viable. Thus, the networks evolved slowly and with few surprises either good or bad. This made them both secure and sterile in comparison to generative machines hooked up to a generative network like the Internet.” P. 41

“On the Internet, the channels of communication are also channels of control.” P. 42

“... generative systems are powerful and valuable, not only because they foster the production of useful things like Web browsers, auction sites, and free encyclopedias, but also because they can allow an extraordinary number of people to express themselves in speech, art, or code and to work with other people in ways previously not possible.” P. 42

“With increasing pressure from these experiences [security threat], consumers will be pushed in one of two unfortunate directions: toward independent information appliances that optimize a particular application and that naturally reject user or third-party modifications, or toward a form of PC lockdown that resembles the centralized control that IBM exerted over its rented mainframes in the 1960s, or that CompuServe and AOL exerted over their information services in the 1980s.” P. 57

“That applanization might come from the same firms that produced some of the most popular generative platforms.” Microsoft’s PC OS and Xbox. P. 57

“In 2006, AMD introduced the ‘Telmex Internet Box,’ which looks just like a PC but cannot run any new software without AMD’s permission. It will run any software AMD chooses to install on it, even after the unit has been purchased.” P. 59

“Problems with generative PC platforms can thus propel people away from PCs and toward information appliances controlled by their makers.” P. 59

“If PCs cannot reliably perform these tasks, most consumers will not see their merit, and the safety valve will be lost. If the PC ceases to be at the center of the information technology ecosystem, the most restrictive aspects of information appliances will come to the fore.” P. 59

“Recall the fundamental difference between a PC and an information appliance: the PC can run code from anywhere, written by anyone, while the information appliance remains tethered to its maker’s desires, offering a more consistent and focused user experience at the expense of flexibility and innovation.” P. 59

“Generativity is a system’s capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences.” P. 70

“What makes something generative? There are five principal factors at work: (1) how extensively a system or technology leverages a set of possible tasks; (2) how well it can be adapted to a range of tasks; (3) how easily new contributors can master it; (4) how accessible it is to those ready and able to build on it; and (5) how transferable any changes are to others—including (and perhaps especially) nonexperts.” P. 71

The factors:

“Leverage makes a difficult job easier. Leverage is not exclusively a feature of generative systems; non-generative, specialized technologies can provide leverage for their designated tasks.⁶ But as a baseline, the more a system can do, the more capable it is of producing change.”

“Adaptability refers to how easily the system can be built on or modified to broaden its range of uses.” Both p. 71

“A technology’s ease of mastery reflects how easy it is for broad audiences to understand how to adopt and adapt it.” P. 72

“The easier it is to obtain access to a technology, along with the tools and information necessary to achieve mastery of it, the more generative it is.” P. 72

“Transferability indicates how easily changes in the technology can be conveyed to others.” P. 73

Generativity: “The first good is its innovative output: new things that improve people’s lives. The second good is its participatory input, based on a belief that a life well lived is one in which there is opportunity to connect to other people, to work with them, and to express one’s own individuality through creative endeavors.” P. 80

Zittrain talks about innovation theories of Christensen and Von Hippel

“Consumers can become enraptured by an expensive, sophisticated shooting game designed by a large firm in one moment and by a simple animation featuring a dancing hamster in the next.” P. 89
Comment: No sense of importance?

Zittrain talks about J.S. Mill and Yochai Benkler

“Through these twin characteristics—transparency and participation— the networked information economy also creates greater space for critical evaluation of cultural materials and tools. The practice of producing culture makes us all more sophisticated readers, viewers, and listeners, as well as more engaged makers.” P. 91 Y. Benkler in *The Wealth of Networks*.

“...the Internet’s very generativity— combined with that of the PCs attached—sows the seeds for a “digital Pearl Harbor.” If we do not address this problem, the most likely first-order solutions in reaction to the problem will be at least as bad as the problem itself, because they will increase security by reducing generativity.” P. 97

“...the most natural reactions to the generative problem of excess spontaneity and individuality will be overreactions, threatening the entire generative basis of the Net and laying the groundwork for the hostile and dreaded censorship...”P. 100

“The fundamental problem arises from too much functionality in the hands of users who may not exercise it wisely: even the safest Volvo can be driven into a wall.” P. 102

“Tethered appliances belong to a new class of technology. They are appliances in that they are easy to use, while not easy to tinker with. They are tethered because it is easy for their vendors to change them from afar, long after the devices have left warehouses and showrooms.” P. 106

“These tethered appliances receive remote updates from the manufacturer, but they generally are not configured to allow anyone else to tinker with them—to invent new features and distribute them to other owners who would not know how to program the boxes themselves.” P. 106

“Appliances become contingent: rented instead of owned, even if one pays up front for them, since they are subject to instantaneous revision.” P. 107

“For instance, the BBC has made a deal with the technology firm Azureus, makers of a peer-to-peer BitTorrent client that has been viewed as contraband on many university campuses and corporate networks.” P. 121

“Then, as with tethered appliances, when Web 2.0 services change their offerings, the user may have no ability to keep using an older version, as one might do with software that stops being actively made available. This is an unfortunate transformation. It is a mistake to think of the Web browser as the apex of the PC’s evolution, especially as new peer-to-peer applications show that PCs can be used to ease network traffic congestion and to allow people directly to interact in new ways.” P. 125

“The prospect of tethered appliances and software as service permits major regulatory intrusions to be implemented as minor technical adjustments to code or requests to service providers.” P. 125

“The keys to maintaining a generative system are to ensure its internal security without resorting to lockdown, and to find ways to enable enough enforcement against its undesirable uses without requiring a system of perfect enforcement.” P. 126

Interesting example on Dutch traffic experiment – removal of road signs caused improvement in traffic safety. P. 127

“The greater the number of prescriptions, the more people’s sense of personal responsibility dwindles.” From Der Spiegel. P. 128

“Together these tools and conventions facilitate a notion of “netizenship”: belonging to an Internet project that includes other people, rather than relating to the Internet as a deterministic information location and transmission tool or as a cash-and-carry service offered by a separate vendor responsible for its content.” P. 142

“This book has explained how the Internet’s generative characteristics primed it for extraordinary success—and now position it for failure. The response to the failure will most likely be sterile tethered appliances and Web services that are contingently generative, if generative at all.” P. 149

“This is the story of the PC against information appliances, and it is the story of the Internet against the proprietary networks.” P. 149

“...mainstream success brings in people with no particular talent or tolerance for the nuts and bolts of the technology, and no connection with the open ethos that facilitates the sharing of improvements. It also attracts those who gain by abusing or subverting the technology and the people who use it. Users find themselves confused and hurt by the abuse, and they look for alternatives. The most obvious solution to abuse of an open system is to tighten or altogether close it.” P. 150

“If generativity and its problems flow from one layer to another, so too can its solutions.” P. 151

Separation. “In an effort to satisfy the desire for safety without full lockdown, PCs could be designed to pretend to be more than one machine, capable of cycling from one split personality to the next. In its simplest implementation, we could divide a PC into two virtual machines: “Red” and “Green.” The Green PC would house reliable software and important data—a stable, mature OS platform and tax returns, term papers, and business documents. The Red PC would have everything else. In this setup,

nothing that happens on one PC could easily affect the other, and the Red PC could have a simple reset button that sends it back to a predetermined safe state.” P. 155

Measurability. “These toolkits would have the same building blocks as spyware, but with the opposite ethos: they would run unobtrusively on the PCs of participating users, reporting back—to a central source, or perhaps only to each other—information about the vital signs and running code of that PC that could help other PCs figure out the level of risk posed by new code. Unlike spyware, the code’s purpose would be to use other PCs’ anonymized experiences to empower the PC’s user. At the moment someone is deciding whether to run some new software, the toolkit’s connections to other machines could say how many other machines on the Internet were running the code, what proportion of machines of self-described experts were running it, whether those experts had vouched for it, and how long the code had been in the wild.” P. 159

Volunteer neighbor watch. “This is an emerging form of netizenship, where tools that embed particular norms grow more powerful with the public’s belief in the norms’ legitimacy. ...But with the right tools, users can also see themselves as participants in the shaping of generative space—as netizens.” P. 161

“If the OS remains open to new applications created by third parties, the maker’s responsibility should be duly lessened. ... Such a regime permits technology vendors to produce closed platforms but encourages them to produce generative platforms by scaling liabilities accordingly.” P. 163

“... the site owner figured that security against malware was the primary responsibility of his visitors—if they were better defended, they would not have to worry about the exploit that was on his site. ... With the Google/StopBadware project in full swing, Web site owners have experienced a major shift in incentives, such that the exploit is their problem if they want Google traffic back. That is perhaps more powerful than a law directly regulating them could manage— and it could in turn generate a market for firms that help validate, clean, and secure Web sites.” P. 171/2

“Because traditional software has clearly demarcated updates, users can stick with an older version if they do not like the tradeoffs of a newer one.” P. 176

“there is little reason to think that people have—or ought to have—any less of a reasonable expectation of privacy for e-mail stored on their behalf by Google and Microsoft than they would have if it were stored locally in PCs after being downloaded and deleted from their e-mail service providers.” p. 185

“When our diaries, e-mail, and documents are no longer stored at home but instead are business records held by a dot-com, nearly all formerly transient communication ends up permanently and accessibly stored in the hands of third parties, and subject to comparatively weak statutory and constitutional protections against surveillance.” p. 186

“As we move our most comprehensive and intimate details online—yet intend them to be there only for our own use—it is important to export the values of privacy against government intrusion along with them.” p. 187/8

“Perhaps it is best to say that neither the governor nor the governed should be able to monopolize technological tricks.” p. 196

“We can identify three successive shifts in technology from the early 1970s: cheap processors, cheap networks, and cheap sensors.” p. 205

“Who could be found near the entrance to the local Planned Parenthood clinic in the past six months? The answers need not come from government or corporate cameras, which are at least partially secured against abuse through well-considered privacy policies from Privacy 1.0. Instead, the answers come from a more powerful, generative source: an army of the world’s photographers, including tourists sharing their photos online without firm (or legitimate) expectations of how they might next be used and reused.” p. 215

“Cheap sensors generatively wired to cheap networks with cheap processors are transforming the nature of privacy.” p. 221

“The lasting lesson from robots.txt is that a simple, basic standard created by people of good faith can go a long way toward resolving or forestalling a problem containing strong ethical or legal dimensions. The founders of Creative Commons created an analogous set of standards to allow content creators to indicate how they would like their works to be used or reused.” p. 225

“For the purposes of privacy, we do not need such a radical reworking of the copy-and-paste culture of the Web [references only]. Rather, we need ways for people to signal whether they would like to remain associated with the data they place on the Web, and to be consulted about unusual uses. ... it could forestall many of the conflicts that will arise in the absence of any standard at all.¹²⁵ Most importantly, it would help signal authorial intention not only to end users but also to the intermediaries whose indices provide the engines for invasions of privacy in the first place. One could indicate that photos were okay to index by tag but not by facial recognition, for example.” p. 227

“The key is to realize that we can make design choices now that work to capture the nuances of human relations far better than our current systems, and that online intermediaries might well embrace such new designs even in the absence of a legal mandate to do so.” p. 229

“The Harvard Kennedy School’s Joseph Nye has suggested that a site like urban legend debunker snopes.com be instituted for reputation, a place that people would know to check to get the full story when they see something scandalous but decontextualized online.” p. 230

“The most common scheme to separate kids from adults online is to identify individual network endpoints as used primarily or frequently by kids and then limit what those endpoints can do: PCs in libraries and public schools are often locked down with filtering software, sometimes due to much-litigated legal requirements. A shift to tethered appliances could greatly lower the costs of discerning age online. Many appliances could be initialized at the time of acquisition with the birthdays of their users, or sold assuming use by children until unlocked by the vendor after receiving proof of age. ... This is a variant of Lessig’s idea for a ‘kid enabled browser,’ made much more robust because a tethered appliance is difficult to hack.” p. 232

“The most salient feature of privacy for MySpace users is not secrecy so much as autonomy: a sense of control over their home bases, even if what they post can later escape their confines.” p. 233

“Instead of being subject to technology that automates and reinforces the worst aspects of contemporary education—emphasizing regurgitation and summarization of content from an oracular source, followed by impersonal grading within a conceptual echo chamber—our children ought to be encouraged to accept the participatory invitation of the Net...” p. 244

“... we can use our generative technologies to teach our children to take responsibility for the way the world works rather than to be merely borne along by its currents. This will work best if our teachers are on board.” p. 244