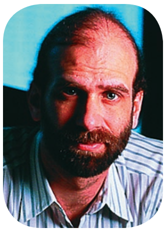
Architecture of Privacy

The Internet isn't really for us. We're here at the beginning, stumbling around, just figuring out what it's good for and how to use it. The Internet is for those born into it, those who have woven it into their lives from the beginning. The Internet is the greatest generation gap since rock and roll, and only our children can hope to understand it.



Bruce Schneier
BT

Larry Lessig famously said that, on the Internet, code is law. Facebook's architecture limits what we can do there, just as gravity limits what we can do on Earth. The 140-character limit on SMSs is as effective as a legal ban on grammar, spelling, and long-winded sentences: KTHXBYE.

As architects of the Internet, we have a special responsibility to our children to build an Internet that future generations will be proud of, one that encompasses basic human rights and values. We do this when we build systems that offer universal access support, open interfaces, and net neutrality, bypass censorship, limit surveillance, fight repression, give people control over their digital presence and digital personas, and foster individual liberty and privacy—especially privacy.

This would all be easier if the choices we made were temporary. But if history is any guide, they're not. Architecture, both physical and virtual, stays around far longer than we intend it to. College campuses built in the 1970s to limit student protests are still standing, as are buildings designed to defend against medieval siege engines. ASCII and TCP/IP aren't going anywhere anytime soon; neither are domain names, email addresses, or HTML. It's been many years, and we still haven't managed to get either DNSSEC or IPV6 deployed. A "just for now" decision can easily remain for decades.

Business and political realities make privacy harder. Some business models depend on walled gardens or invasive digital rights management controls. Other business models depend on collecting and selling personal data. Some countries depend on censorship to enforce morality or keep ideas out, while others depend on surveillance to control their citizens.

The natural tendencies of the Internet make privacy harder. Technology is the friend of intrusive tools. Digital sensors become smaller and more plentiful. More data is collected and stored every year. Privacy isn't something that occurs naturally online, it must be deliberately architected.

Companies that retain personal information put their customers at risk. Security breaches, court orders, and disgruntled employees are just a few of the ways to lose control of data. Good architectures that minimize data collection reduce these risks, just like guardrails on highways prevent more serious accidents when drivers lose control of their vehicles.

We need to be more deliberate. A lot of information-age architecture is about data: what is collected, who controls it, and how it is used. Data is the lifeblood of the information age, but much of it is very personal. We need to design systems that limit unnecessary data collection, give individuals control over their data, and limit the ability of those in power to use that data for mass surveillance.

Data is the pollution of the information age. It's a byproduct of every computer-mediated interaction; all processes produce it. It stays around forever, unless it's disposed of. It can be recycled, but it has to be done carefully. And, like physical pollution during the early decades of the industrial age, most people completely ignore the problem.

Just as we look back at the beginning of the previous century and shake our heads at how the titans of the industrial age could ignore the pollution they caused, future generations will look back at us—in the early decades of the information age—and judge our architecture, and what we did to foster freedom, liberty, and democracy. Did we build information technologies that protected people's freedoms even during times when society tried to subvert them? Or did we build technologies that could easily be modified to watch and control? History will record our choices. □

__Bruce Schneier__ is chief security technology officer of BT. Read his blog at www.schneier.com.