What is freedom? It's not simply the right to be able to do and say whatever we want. Freedom is also about respecting the fact that everybody has that right. Freedom is about taking other people into account, and doing so in such a way that every individual can thrive and develop safely.

The Internet can help every individual thrive and develop safely. Vint Cerf, generally recognized as one of the “fathers” of the Internet, says that “permissionless innovation” is the Internet's greatest asset.1 Indeed, the unbridled innovation of the Internet has been made possible by the high degree of freedom it enjoys. The innovation of the Internet can be subdivided into (roughly) four categories: infrastructure, equipment, services, and applications.
The essential features of the Internet—collaboration and accessibility—enable the most unexpected developments, with no restrictions or impediments. That's the creative freedom of permissionless innovation.

- Infrastructure forms the basis but, at the same time, is the least visible. Indeed, it is so invisible that my teenage kids don’t even realize there is an infrastructure and that it has to be paid for, managed, and maintained. Innovations in this field come from major and minor Internet providers and are mainly driven by ISPs, equipment suppliers, nonprofit coordinating bodies (such as ARIN) and research networks such as SURFnet and Internet2.

- Equipment is the “sexiest” category. Innovations in this field lead to queues of people waiting outside shops to snap up the latest gadget. Innovations in computers, laptops, tablets, and smartphones are the domain of big corporations like Samsung and Apple. These companies innovate constantly in order to keep their devices appealing. That is their business model. And then sometimes there’s an external stimulus, such as the Phonebloks created by Dave Hakkens.

- Services are no longer the exclusive domain of companies, ever since the development of the World Wide Web (WWW) in the early 1990s. On the Internet, anyone with an idea and dedication can start providing a service, such as an online shop, and make it a success. Innovation in this field is a wonderful mix of private individuals, start-ups, public authorities, and large corporations.

- Applications require the development and sale of software and as a result were, for a long time, the preserve of companies and public authorities. Thanks to app stores like those from Apple and Google, there has been a “democratization” of applications, which are now called apps, and the speed of innovations in this field has increased beyond recognition.

All in all, this results in an extremely positive dynamic in which the essential features of the Internet—collaboration and accessibility—enable the most unexpected developments, with no restrictions or impediments. That's the creative freedom of permissionless innovation.

The Internet as an Anarchy
How is the Internet organized and governed? Is it an anarchy, as many people claim? I would argue that the Internet does have anarchic tendencies: there is no central Internet authority and there is no Internet police telling you what you can and cannot do. But it's certainly not an anarchy: there is definitely a degree of organization (even though, yes, it's a loose kind of organization).

To understand the way the Internet is organized, we should define it. In 1992, when the web came into being, the Internet Engineering Task Force (IETF), the organization responsible for Internet standards, defined it as follows (RFC 1310): “The Internet, a loosely-organized international collaboration of autonomous, interconnected networks, supports host-to-host communication through voluntary adherence to open protocols and procedures defined by Internet Standards.”

The Internet is a network of autonomous networks that voluntarily interconnect with each other and talk to each other on the basis of Internet standards. You can use protocols other than the Internet Protocol, but other people wouldn't “understand” you. It would be as if you were speaking Chinese when the rest of the world is speaking English.
You can also use the Internet Protocol without connecting your own network to the Internet. Only when you connect your own network and use the Internet standards will your network become part of the Internet. But that doesn’t take away the fact that your network is and remains yours.

So, the Internet exists specifically because everyone adheres to the Internet standards. The agreements required to develop, maintain, and implement these standards are not achieved through anarchy; rather, they require a great deal of conciliation and consultation. These consultations are certainly well organized and take place in multi-stakeholder forums such as the IETF (for standardization) and ICANN (for names and addresses). Multi-stakeholder means that anyone who wants to get involved can do so and can have their say with as few obstacles as possible. Users and companies, not just governments, are stakeholders. In a multi-stakeholder environment, governments have no more power than other stakeholders.

A Free and Open Internet

The Declaration of Internet Freedom (http://www.internetdeclaration.org/) explains why freedom on the Internet is so important. It sums up precisely what the Internet is all about:

We believe that a free and open Internet can bring about a better world. To keep the Internet free and open, we call on communities, industries and countries to recognize these principles. We believe that they will help to bring about more creativity, more innovation and more open societies.

We are joining an international movement to defend our freedoms because we believe that they are worth fighting for.

Let’s discuss these principles—agree or disagree with them, translate them, make them your own and broaden the discussion with your community—as only the Internet can make possible.

Join us in keeping the Internet free and open.

I have signed this declaration because, in my view, it paints an idealistic picture that—however unachievable it may seem—we should always keep in our minds as a goal. Will countries like Russia, China, or North Korea ever give their citizens Internet freedom? As things stand at the moment, this would seem to be a very long way off.

The declaration does have a purpose, if only as a trigger for discussion. Fortunately, this discussion is now under way. At the NETmundial meeting in spring 2014 in Brazil, many countries, including Russia and China, agreed on a multi-stakeholder statement that marks a major step in the right direction in terms of Internet freedom and the associated multi-stakeholder governance of the Internet. But as is so often the case, the devil is in the detail. It will be a long time yet before there is agreement on how countries interpret freedom and governance. Still, as long as we’re discussing these issues in a multi-stakeholder environment (and not in a forum dominated by governments), we have a basis on which to build and to grow closer.

The Internet as a Leveler

What do we in the West see as the positive aspects of the Internet? In the first instance, the Internet is a great leveler. As the “Declaration of Internet Freedom” (cited above) states, access to the Internet makes for a more open society in which where you’ve come from no longer determines what you achieve in your life; rather, your own intelligence and dedication determine your future. So, for example, in 2012 a 15-year-old boy from Mongolia saw his life take an unexpected turn when his talents were spotted through an online course he was taking at MIT. He received an offer to study there and, at the age of 17, was taken on by members of an MIT/Harvard consortium called edX to help them identify other talented individuals like himself.3

The Internet has also made people more savvy about governments. Previously, we had to rely on a person sitting behind a counter for most government information. Now, not only can we find, by ourselves, a lot of information about and produced by the government; we also can share that information and discuss it with other people. This has forced governments to be increasingly transparent. If governments aren’t transparent, the Internet gives people the opportunity to find allies and rise up, as we saw with the Arab Spring.

Another benefit of the Internet is that the consumer is now in control. Whereas for years consumers were forced to base their purchasing decisions on limited information supplied by the manufacturer or retailer, the Internet gives them the freedom to share their experiences regarding a product or service with the rest of the world and to base their decisions on other people’s experiences. As a result, manufacturers have realized the importance of providing a good service; if they don’t, their ratings will plummet. The Internet has made conventional word-of-mouth advertising many times more powerful. The flip side is, of course, that commercial companies use the very same channels to try to manipulate consumers.

The Internet is the perfect place to find like-minded people, whether they are people who have purchased the same product or service you are considering, people who have the same hobby as you, people who like the same clothes as you, or people who have the same musical tastes or the same illness. These
like-minded people organize themselves and force suppliers to take their requirements and wishes into account.

However, if we are to enjoy all of the benefits of the Internet, we must do two things. First, the gap between people with access to the Internet and those without access is widening. To avoid the global imbalance this causes, we need to strive to give everyone in the world the option to access the Internet.

Second, we need to let the Internet play a larger part in our upbringing and education. For example, we must teach people (especially children) how to deal with the almost endless amount of information that is often not verified or explained. We must teach our children how the images, videos, and information they find on the Internet relate to our cultures—that is, teach them how to determine what is fiction and what is nonfiction. What we need to teach our children today is vastly different from what we needed to learn fifty years ago.

The Internet offers so much to educators, students, parents, and researchers. The Internet not only is a nearly unlimited source of knowledge but also allows us to easily discover other cultures, to exchange ideas, and to develop solutions to common problems.

**New Business Models**

One remarkable consequence of the Internet is that it gives rise to new business models in which customers and suppliers can find each other directly, without the need for a middleman. After Airbnb, SnapCar, and Uber, I wonder when we’ll see the first crowd-funded airplane flight? The tourist industry, the music industry, and the film industry have all suffered from the transforming power of the Internet. The banking world too has discovered how quickly things can change: the fact that, during the economic crisis, traditional bankers were loathe to lend money to start-ups created a wonderful opportunity for Kickstarter, the crowd-funding platform that is now the first port-of-call for many start-ups looking for funding. Would-be companies no longer need help from a bank to realize their dream.

Another sector that’s worried is retail, which is discovering that a lot of people who used to buy a new bike, a new toy, or a new wardrobe are now looking to see whether a good second-hand alternative is available on classified advertising sites such as Craigslist, eBay, and thredUP or whether an expensive purchase could perhaps be shared with somebody else (Snappcar). Take MUD Jeans, for example, which introduced the concept of Lease a Jeans. When you’re fed up with your jeans, someone else can wear them for a small monthly fee. And the manufacturing industry will also find things tough in the future now that 3D printing is starting to take off and change the playing field in an irreversible way.

These examples show that innovation is happening more quickly now than ever before, partly thanks to the freedom that the Internet offers. This freedom is due to technology and also, to a greater extent, to creativity and social factors. The latter are turning business models upside down. Anyone in the publishing industry should be worried: the spread of broadband Internet has rendered conventional distribution on CD or paper practically obsolete—consider the success of music industry initiatives like iTunes and Spotify. Different models are being developed, and those who blindly persist in defending their existing model will be the first to go under.

**Freedom under Pressure**

Freedom on the Internet is not all a bed of roses. It is never absolute and is generally under quite some pressure. Perhaps the most annoying example of this relates to the fact that we’re more overtly confronted with differing opinions. Whereas in our day-to-day lives we may be able to avoid opinionated views, on
the Internet there’s no getting away from them. Publish an opinion anywhere, and you’re sure to get reactions from people who clearly don’t hold the same views as you. That’s all part of online freedom, and frankly, I believe it’s good for our social fabric. Unfortunately, there are always people who go too far and react with threats, some of which are so serious that they restrict your freedom to express your opinion.

And there are other threats to Internet freedom, from both foes and “friends.” Crooks restrict our freedom by stealing our identities. They send phishing emails, for example, in which they claim to be your bank or the tax office. Once they’ve stolen your identity, they can post things on Twitter or Facebook in your name, often with fairly unpleasant consequences. Sometimes even people you know will put photos of you or other information about you on the Internet without asking your permission. This can be, and often is, completely innocent. Other instances amount to cyberbullying.

Freedom on the Internet is certainly not something we can take for granted. It is under constant pressure from all sides.

Invasion of Privacy
Another major threat to the Internet is the fact that commercial players encroach on our freedom. Our surfing habits, our viewing preferences, and our social media opinions are monitored by all kinds of companies that use the information for their own commercial gain. And I’m not talking just about Google and Facebook. Less-visible companies often know far more about our daily lives than we realize. They too know about us as a result of combining different (big) data sources such as our purchasing behavior as indicated by our loyalty cards, our online habits tracked using cookies (which we blindly accept), our Tweets and other social media messages (which are analyzed using text analytics), our parking habits if we pay using our mobile phone, and our travel habits as read from public-transport smartcards and sometimes even our mobile phones, which can be monitored using Wi-Fi tracking.

Individually, this data is of some significance, but few of us regard it as an invasion of our privacy. When taken together, these diverse data sources provide a fairly accurate picture of an individual’s lifestyle. The question is whether consumers want to exchange this information about themselves in return for the small percentage discount they can get as a loyal customer if they respond to offers.

In 2012, the Girls Around Me app caused an outcry. This app combined...
publicly available data from Foursquare, Facebook, Twitter, and other apps into a database of girls in an area. It let users see which girls were in a bar or nightclub, whether they were single, what their hobbies and interests were, and so on. That way, users would have a far greater chance of success in starting a conversation. The invasion of privacy and stalker connotations associated with this app should extend to any other app that combines databases, because even if the original aim is commendable, abuse can rarely be avoided, and use of these apps quickly degenerates into something far less elevated.

**Government Surveillance**

While companies are monitoring us as consumers, governments are keeping an eye on us as citizens. Some governments (such as Singapore and China) decide what we can and cannot see; they generally claim the right to track the movements of freedom-fighters, journalists, and even ordinary citizens via the Internet. They conduct tracking not simply if they suspect that citizens are acting fraudulently, are planning an attack, or are doing something else suspicious. As a general measure, these governments follow Twitter and Facebook accounts to prevent terrorism, and they monitor parking habits to track down fraudulent lease-car drivers.

But Western governments know a thing or two about this also, as was revealed by the whistle-blower Edward Snowden. Many democratic governments are endeavoring to undertake mass surveillance under the guise of security. Because who doesn't want to help fight terrorism and child pornography? So the surfing habits of all of us are being monitored to catch the handful of people who are doing something wrong.

The measures taken are often totally disproportionate to the number of offenders and the seriousness of the offenses. For example, should all three million Dutch passengers traveling through Amsterdam Airport Schiphol have to be registered in order to track down some 100 individuals who plan to join the Jihadists in Syria? Is it justifiable to collect the data of all UK Internet users to catch criminals? The question is, does the
end justify the means? In the latter case, the United Nations found that the justification was disproportionate. I wonder where all this overkill in monitoring is heading, especially since there is still no proof whatsoever that these measures help to prevent or solve crimes and terrorist attacks.

According to Snowden's revelations, the U.S. government is also embarking on a deliberate weakening of commercial technologies by trying, for example, to ban encryption and by building “backdoors” into systems. This will lead irrevocably to a less secure Internet. And clearly, these built-in weaknesses won't be exploited only by well-meaning governments. As security expert Bruce Schneier stated in his blog: “You can't build a backdoor that only the good guys can walk through.”

These examples demonstrate that a government view of privacy and freedom is sometimes totally different from the views of citizens. The fundamental question is, can democracy exist in a country where the government doesn't trust its own citizens—in a country where, as a citizen, you're guilty unless proved otherwise? Recent revelations indicate that many governments are currently linking databases in order to create a profile of each and every citizen. A degree of profiling that just a few years ago was reserved for those suspected of serious offences is now being applied to all citizens. Anyone who displays a slight divergence in behavior (say, using more water than average) is immediately under suspicion. Of course, politicians hasten to assure us all that we have nothing to fear if we have nothing to hide.

The problem is, of course, that freedom is exactly that: the right to have secrets. Dutch Loesje, an international poster organization that spreads ideas in order to stimulate creativity and initiative, quips: “I've nothing to hide, but nobody needs to know that.” Everybody has secrets! Obviously the government or Google can collect data about us for a delimited purpose. But when the linking of databases gives an insight into our lives and restricts our privacy and freedom, it is disproportionate to any benefits gained. And what if a totally different government comes into power? A government that's more dictatorial? In that case, we may well have far more to hide, and we certainly won't be happy about the orderly linking of our files. For example, the Nazi government in World War II was very grateful for the well-ordered records that many European governments had kept, especially for Jewish citizens.

What is needed, and what so far has been lacking, is an in-depth public and political debate around proportionality. Which freedoms and which privacies do we want to retain, and which are we willing to sacrifice for a little more security? Most governments don't want to accept that there's a price to pay for an open democratic society. Terrorism cannot be dispelled. The same politicians who claim they support freedom of expression can be found the next day proposing to ban encryption, reduce the usage of social media, and link databases. Limiting our acquired liberties would mean a victory for Al-Qaeda and ISIS.

The price to pay for an open democratic society is that sometimes, things happen that should never have happened—things that go beyond anything we could possibly have imagined—and lives are lost. Every year, thousands of people die in accidents on motorways. But we don't close all the motorways. The same factors we take into account when assessing the proportionality of measures to prevent these deaths should be applied to tracking and preventing crime and terrorism.

**Dependence**

Another disadvantage of the Internet is that we've become heavily dependent on it. We don't know what to do when we can't pay online with PayPal or when we can't use our smartcards or when our Internet service goes down. Services have gone digital very quickly, often to such an extent that there is no longer an analog alternative. But who can guarantee that the Internet will always be available? As we've already seen, the Internet is a network of autonomous networks—there is no owner who is responsible for the availability and reliability of the Internet as a whole. And the bad guys know this.
Experience tells us that it’s easier to attack than to defend. This is also the main conclusion of the World Economic Forum’s Global Risks 2014 report, which states: “The world may be only one disruptive technology away from attackers gaining a runaway advantage, meaning the Internet would cease to be a trusted medium for communication or commerce.” Attackers are indeed inventive and are constantly coming up with new methods. The defense can only react, and that means, effectively, that we’re always one step behind. One thing is certain, however: the days when a password was sufficient to protect a digital identity are long gone.

As the Internet moves into a future where more devices and sensors are connected (i.e., the Internet of Things), we will become even more dependent on the Internet. The monitoring of our health, our comfort, and our safety (e.g., flood control) is becoming highly dependent on all kinds of sensors, and these sensors are connected to diagnostic systems and sometimes even to controlling systems. People will increasingly use “wearable technologies” that disclose ever more data about them to the Internet (i.e., the “quantified self” movement). Collecting data is often done for a good reason, but clearly, doing so makes us even more dependent on the technology and more open to abuse.

The Future of the Internet
When considering Internet freedom, we need to keep governance in mind. As noted earlier, the Internet may not be a total anarchy, but it does have anarchic tendencies. And these tendencies mean that there are no, or at least very few, centralized rules that everyone must follow. In offline society, on the other hand, it is clear who makes the rules, and it is also clear when the rules are broken and how these infractions will be dealt with. Rules can increase citizens’ freedom because everybody is clear on what they can and cannot do. It is this clarity that is sometimes lacking on the Internet.

I don’t think we should, or indeed could, put the responsibility for “regulation” of the Internet entirely in the hands of governments. There must be a multi-stakeholder decision process based on discussions in which citizens, consumers, interest groups, and commercial players are all involved. And it must be an international discussion. The rules will be different in every country because nondemocratic countries will never fully agree with what democratic countries understand as freedom. But that doesn’t mean we shouldn’t all be involved in the discussion.

Major challenges lie ahead: cybercrime, cyberterrorism, online child pornography, and even digital warfare. These problems exist in offline society as well, but for most people, the challenges have come closer to home through the Internet. These problems can’t be solved in isolation. The only way to tackle them is by working together—on all fronts and with all stakeholders involved.

If we don’t succeed, we risk a “Balkanization” of the Internet, a division into different regions, each with its own access policy and other rules. Then, it would no longer be citizens who decide with whom or what they communicate; it would be the local government. Permissionless innovation would no longer exist. Unfortunately, this frightening scenario is not completely far-fetched. China has already partly achieved this, and Russia has threatened on several occasions to isolate the Russian Internet from the pernicious influences of the West.

Luckily, most democratic governments still believe that the Internet should be open, secure, and accessible to all. In recent Internet governance discussions, both the United States and the European Union have endorsed the multi-stakeholder model. At the same time, governments and politicians are often way off the mark when it comes to the impact of the Internet of Things, database linking, social media, and cybersecurity. At times this lack of understanding is amusing, but at others it can be dangerous.

This is why all countries in the world need to have an in-depth public and political debate on the development of the Internet, our dependence on technology, and privacy and freedom. Ideally, these debates could help shape a vision that future governments could use to develop suitable policies, legislation, and enforcement as part of a truly multi-stakeholder governance model for the Internet. After all, the Internet is no longer something that belongs only to the online world. It is a wholly integral part of our society.

Notes

© 2016 Erik Huizer. The text of this article is licensed under the Creative Commons Attribution 4.0 International License.