Permissionless Innovation, Cornerstone of a Successful Internet

An essay on the theme of "Freedom and the Internet" by Erik Huizer

MARCH 2015

Internet Society™

Freedom should not be taken for granted. Living in a Western country like the Netherlands it may be hard to see why, but watch the news and read the papers and it will soon be obvious just how hard people have to fight, firstly to achieve freedom and then to retain it. This fight takes place on the Internet too and, for most people, it's far closer than it is in the offline world.

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

The Internet can help people thrive and develop safely in this way. Vint Cerf, who is generally recognised as the 'father' of the Internet, says that 'Permissionless Innovation' is the Internet's greatest asset. Indeed, the unbridled innovation of – and as a result of – the Internet has been made possible by the high degree of freedom it enjoys. Roughly speaking, innovation of the Internet can be subdivided into four categories: infrastructure, equipment, services and applications.

Infrastructure forms the basis and, at the same time, is the least visible. So invisible that my kids don't even realise 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 and research networks such as SURFnet.

Equipment is the most 'sexy'. 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. They innovate constantly to keep their devices appealing. That is their business model. Sometimes there's an external stimulus, such as the phone blocks (www.phoneblocks.nl) of creative Dutchman Dave Hakkens.

Since the development of the world wide web (WWW) in the early nineties, *services* are no longer the exclusive domain of companies. 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 the appstore, there has been a democratisation 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 ultimate freedom of permissionless innovation.

Freedom under pressure

However, freedom on the Internet is not all a bed of roses. Because although most governments don't decide what we can and cannot see such as in countries like Russia and China, they do claim the right to track and trace us via the Internet. And that's not only if they suspect that we're acting fraudulently, planning an attack or doing something else that we shouldn't be. Even as a general measure to prevent terrorism or to track down fraudulent lease car drivers, the government can follow our Twitter and Facebook messages or monitor our parking habits.

In addition, commercial players encroach on our freedoms. Our surfing habits, our preferences and our opinions are monitored by all kinds of companies who use the information for their own commercial gain. And I'm not just talking about Google and Facebook either. Less visible companies often know far more about our daily lives than we realise. Take the smart card companies, for example.

Then there are the 'crooks' who restrict your freedom by stealing your identity, by sending you 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 put photos of you or other information about you on the Internet without asking your permission. Think of phenomena like cyberbullying.

In summary, freedom on the Internet is certainly not something we can take for granted and it's under constant pressure from all sides.

Is the Internet an anarchy?

But why should that be so? Is it because the Internet is an anarchy, as many people claim? The Internet does have anarchic tendencies, but it's certainly not an anarchy. There is definitely a degree of organisation, although it's a loose kind of organisation and there are no Internet police or Internet authorities telling you what you can and cannot do.

To clarify what exactly the Internet is, it's helpful to define it. In 1992, when the world wide web came into being, the IETF, the organisation responsible for Internet standards, defined it as follows (RFC 1603):

> *'The Internet is a loosely-organized international collaboration of autonomous, interconnected networks that 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 like you 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. It's not until you connect your own network and use the Internet standards that your network forms part of the Internet. But that doesn't take away the fact that it is and remains your network.

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 – they require a great deal of conciliation and consultation. These consultations are certainly well organised and take place in multi-stakeholder forums such as the IETF (standardisation) and ICANN (names and addresses). Multi-stakeholder means that anyone who wants to can get involved and have their say with as few obstacles as possible. Here, users and companies are also stakeholders, not just governments. So, in a multi-stakeholder environment, the government has no more power than other stakeholders.

Declaration of freedom

At www.internetdeclaration.org you can find a declaration that explains why freedom on the Internet is so important. You can find and sign the declaration on this website. But we're also printing it here, because it sums up precisely what the Internet currently 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, debate 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 – we should always keep in our minds as a goal. Will countries like Russia, China or North Korea ever give their citizens complete freedom? As things stand at the moment, this would seem to be a very long way off.

But the Internet Declaration does have a purpose, if only as a trigger for discussion. Fortunately, this discussion is now under way. At the Net Mundial 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 over how countries interpret freedom and governance. Our interpretation of it is in many respects different from theirs. But as long as we're discussing these issues in a multi-stakeholder environment (and not in a forum dominated by governments), at least we have a basis on which to build and grow closer together.

The Internet as leveller

What do we in the West see as the positive aspects of the Internet? In the first instance, the Internet is a great leveller. As the Internet Declaration says, access to the Internet makes for a more open society in which it's no longer where you've come from that determines what you achieve in your life but rather your own intelligence and dedication. So, for example, in 2012 the life of a 15 year-old boy from Mongolia took 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 an MIT/Harvard consortium called edX to help them identify other talented individuals like himself (source: www.internetsociety.org/blog/institutional/2014/06/introducing-global-internet- report).

Also, the Internet has made people more savvy about governments. Previously, we had to rely on a person sitting behind a counter for a lot of government information. Now, not only can we find a lot of information about and produced by the government ourselves but we can also share it and discuss it with other people. This has forced governments to be increasingly transparent. And, should it not be, the Internet gives people the opportunity to find like-minded individuals and rise up, as we saw with the Arab Spring.

Another real 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 of a product or service with the rest of the world and to base their decisions on other peoples' experiences. Finally, manufacturers have realised the importance of providing a good service, because, if they don't, their ratings will plummet. The Internet has made conventional word-of- mouth advertising many times more powerful.

The Internet is also the perfect place to find like-minded people, whether it be people who have the same hobby as you, who like the same clothes as you, or who have the same musical tastes or the same illness. These like-minded people organise themselves and force suppliers to take their requirements and wishes into account.

However, if we are to enjoy all the benefits of the Internet, we must let it play more of a part in our upbringing and education. So, for example, we must teach people (children) how to deal with the almost endless amount of information that is often not verified or explained. We also need to teach our children how the images, videos and information they find on the Internet relate to our cultures, what is fiction what is non-fiction etc. In other words, the knowledge we need to teach our children is vastly different from the knowledge that we had to learn 50 years ago.

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 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, they 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 would-be start-ups looking for funding. They no longer need a bank to realise their dream. Another sector that's worried is the retail sector, which is finding that a lot of people who used to buy a new wardrobe, bike or train set are now first looking to see whether a good second-hand alternative is available on the classified advertising sites like Craigslist and eBay or whether an expensive purchase could perhaps be shared with somebody else. 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 also show that innovation is happening more quickly now than ever before, partly thanks to the freedom the Internet offers. This is due in part to technology but to a far greater extent to creativity and social factors, because the latter

in particular are turning business models upside down. Anyone in the publishing industry should be worried now that the spread of broadband Internet has rendered conventional distribution on CD or paper practically obsolete – witness 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.

Invasion of privacy

But the Internet doesn't just offer advantages in relation to our freedom, it also has disadvantages. The most obvious of these perhaps is the fact that we're more overtly confronted with different opinions. Whereas in our day-to-day lives we may be able to avoid them, 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. Luckily, that's all part of online freedom too. 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.

Another major disadvantage of the Internet is that there are companies that know almost everything about you. Naturally, the first ones that come to mind are Facebook and Google, and they probably go the farthest.

But don't underestimate how much far smaller companies know about you from combining different data sources such as your purchasing behaviour as indicated by your loyalty cards, your online habits as tracked using cookies (that we blindly accept), your Tweets and other messages on social media, which are analysed using text analytics, your parking habits if you pay using your mobile, your travel habits as read from your public transport smart card and, sometimes, even your mobile phone itself, which can be monitored using WiFi tracking. Individually this data is of some significance, but few of us regard it as an invasion of our privacy. When taken together however, these diverse sources provide a pretty accurate picture of an individual's lifestyle. The question is whether consumers actually want this in return for the small per cent 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 you see which girls were in a bar or nightclub, whether they were single, what their hobbies and interests were and so on. That way, your chat-up lines would have a far greater chance of success (bits.blogs.nytimes.com/2012/03/30/girls-around-me-ios-app-takes-creepy-to-a-new- level/). The immediate aversion you feel to this app should also apply to any plan to combine databases, because even if the original aim of combining them is commendable, abuse can rarely be avoided and their use quickly degenerates into something far less elevated.

Spied on by government

And we're not only monitored as consumers by companies, governments are also keeping an eye on us – to say nothing of regimes in countries like Russia and China, as mentioned earlier, who happily use the Internet to track the movements of freedom-fighters and journalists. The US government knows a thing or two about this too, as was revealed so convincingly by whistleblower Edward Snowden.

In many democratic countries the government is endeavouring 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 a handful of people who are doing something wrong.

How proportionate these measures are, however, is often open to debate. Indeed, the measures taken are often totally disproportionate to the number of offenders and the seriousness of the offences. For example, should all three million Dutch passengers travelling through Schiphol airport have to be registered in order to track down some 100 individuals who plan to join the Jihadists in Syria? Is it justifiable to check the parking data of all lease cars just to catch a couple of fraudsters? The question is, does the end justify the means? The examining magistrate found that it did. But I do wonder where all this overkill in monitoring is heading: phone tapping, databases, tracking all online behaviour... (and note that there is still no proof whatsoever that these measures help to prevent or solve crimes and terrorist attacks).

Snowden aftershock

An NTT investigation into the impact of the NSA's online surveillance as leaked by whistle-blower Edward Snowden reveals that, of ICT decision-makers at organisations:

- **88 percent** have changed the way they use the cloud; 38 percent have even changed the terms of existing contracts;
- **5 percent** think it doesn't matter where their data are stored – which means that 95 percent do want to know where their data are located and also want to have control over it;
- **97 percent** of EU respondents and 92 percent of US respondents prefer a cloud service that uses data centres on their own continent;
- **31 percent** are moving their data out of locations they no longer trust to locations where they know that their data are safe;
- **62 percent** of those who currently don't use the cloud are now more hesitant about using it.

According to Snowden's revelations, the US government is also embarking on a deliberate weakening of the technologies used. They're trying, for example, to ban encryption and are building 'back doors' into systems. This will lead irrevocably to a less secure Internet. And clearly, these built-in weaknesses won't just be exploited by well-meaning governments. Bruce Schneier recently described this perfectly in an essay: www.schneier.com/blog/archives/2014/10/iphone_encrypti_1.html.

These examples demonstrate that governments often have a totally different view of privacy and freedom from their citizens. That applies to both democratic countries and regimes where citizens can't say what they want to anyway. The fundamental question is, can democracy exist in a country where the government doesn't trust its own citizens? Where, as a citizen, you're guilty unless proved otherwise. Recent revelations indicate that many governments are currently linking databases together 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, because it can be, being applied to all citizens. Anyone who displays a slight divergence in their behaviour (say, using more water than average) is immediately under suspicion. Of course politicians hasten to assure that you've nothing to fear if you've nothing to hide.

But freedom is actually the right to have secrets. As Dutch Loesje quips: 'I've nothing to hide but nobody needs to know that.' And 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 the benefits that linking files in this way achieves. And what if a totally different government comes into power? A government that's less parliamentary and 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 files that the present government has undertaken. Take, for example, the Second World War, when the Germans were only too grateful for the well-ordered records many European governments had kept, especially of 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?

What most governments don't want to accept is that there's a price to pay for an open democratic society. As the recent attacks in Paris and Copenhagen have once again confirmed, terrorism cannot be dispelled. The same politicians who claim they support freedom of expression can be found the next day they proposing to ban encryption, reduce the usage of social media and link databases – while the only fitting response would be to defend our acquired liberties. Indeed, limiting these would mean a victory for Al-Qaeda and ISIS.

So the price to pay for an open democratic society is that sometimes things will happen which should never have happened – things which go beyond anything we could possibly have imagined – and that lives will be lost. Every year, thousands of people in Europe die on motorways. But we don't close all the motorways. We should apply the same factors we take into account when assessing the proportionality of measures in that instance 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 if we can't pay online with PayPal or we can't use our smart cards, let alone when the whole of the Internet goes down. Services have gone digital very quickly, and often to such an extent that an analogue alternative is no longer available. 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 crooks know that too.

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. It reads as follows:

> *'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 defence can do no more than 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 ever more devices and sensors are connected (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 increasingly dependent on all kinds of sensors, and these sensors are connected to diagnostic systems and sometimes even controlling systems. People will increasingly use 'wearable technologies' that disclose ever more data about them to the Internet (Quantified Self). This is often done for a good reason but, clearly, it makes us even more dependent on the technology and more open to abuse.

Governance

One thing to bear in mind when considering Internet freedom is governance. Because whereas in offline society it is clear who makes the rules and it is also clear when the rules are broken and how this will be dealt with, on the Internet this is not the case. As we said earlier, the Internet may not be total anarchy but it does have anarchic tendencies. And these tendencies mean that there are no, or at least very few, centralised rules that everyone must follow.

At the same time, society as a whole tells us that rules are often useful, that they can increase the freedom citizens have because everybody is clear on what they can and cannot do. It is this clarity that is currently sometimes lacking on the Internet.

I don't think we should, or indeed could, put the responsibility for this 'regulation' of the Internet entirely in the hands of governments. There must be a multi-stakeholder discussion in which citizens, consumers, interest groups and commercial players are also involved. And it must be an international discussion. Ultimately, the rules will be different in every country because non-democratic countries will never fully agree with what democratic countries understand as freedom. But that doesn't mean we should simply not involve those countries in the discussion.

Major challenges lie ahead of us: cybercrime, cyberterrorism, online child pornography and even digital warfare. These problems also exist in offline society but, for most people, they have come closer through the Internet. In society as a whole these problems can't be solved in isolation, and the same applies in extremis to these problems in the online world. The only way to tackle them is by working together – on all fronts and with all stakeholders involved.

What we risk, if we don't succeed, is a 'Balkanisation' of the Internet, dividing the Internet into different regions, each with its own access policy and other rules. Then, it would no longer be citizens themselves who decide with whom or what they communicate, but 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 already threatened on several occasions to isolate the Russian Internet from the perfidious influences of the West.

Luckily, most democratic governments are still of the opinion that the Internet should be open, secure and accessible to all. The website of the US State Department says this:

> *'Internet freedom is a foreign policy priority for the United States, and has been for many years. Our goal is to ensure that any child, born anywhere in the world, has access to the global Internet as an open platform on which to innovate, learn, organize and express herself free from undue interference or censorship. Indeed, during his time in Congress, Secretary Kerry worked closely with then-Secretary Clinton to make certain that we could effectively promote long-standing values of openness and human rights in a networked world.'*

A fairly cynical statement in the context of the recent revelations by Snowden and Assange, which suggest that large US corporations such as Google, Apple and Facebook are at times just an extension of the Department of Homeland Security.

However, in recent Internet governance discussions, both the US and Europe have endorsed the multi-stakeholder model. At the same time, it is clear that when it comes to the impact of the Internet of Things, database linking, social media and cybersecurity, governments and politicians are often way off the mark. At times this lack of understanding is amusing, at others it can be dangerous, as the above examples make clear.

It's important that in all countries in the world we can have an in-depth public and political debate on the development of the Internet, our dependence on technology, its integration in education, the linking of databases, privacy and freedom. It would be great if we could use such debates to develop a vision that future governments can 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, by now it is a wholly integral part of our society.

Biography

Prof. dr. Erik Huizer is CTO at SURFnet, the Dutch national academic and research network. He is also part-time professor of Internet Applications at the University of Utrecht. His main research programs are:

- Internet Governance
- Open, accessible and trustworthy Internet
- Internet usage and social media
- Internet and research/education

For over 30 years he has been involved in Internet standardization and Internet governance. For his contributions to the Internet he was inducted into the Internet Hall of Fame in 2014.

Before SURFnet he served as Managing Director Information Society and scientific director for ICT and Media at the Netherlands Organisation for Applied Scientific Research (TNO).

Erik currently serves as chairman of the permanent stakeholders group of the Dutch National Cyber Security Center (NCSC). He is chair of the board of Enset (the non-profit registrar for NGO's), Scientific Captain of the Dutch Creative Industries Top sector, chair of the Dutch national IPv6 Task Force and the Advisory Board of the Internet Society. He is a co-founder of the Dutch chapter of the Internet Society.

He has been teaching at various developing countries workshops on Internet policy and technology.

Internet Society
Galerie Jean-Malbuisson, 15
CH-1204 Geneva
Switzerland
Tel: +41 22 807 1444
Fax: +41 22 807 1445
www.internetsociety.org

1775 Wiehle Ave.
Suite 201
Reston, VA 20190
USA
Tel: +1 703 439 2120
Fax: +1 703 326 9881
Email: info@isoc.org