The Internet We Want or the Internet We Deserve?

David Rogers, Copper Horse Solutions Ltd: david.rogers [@] copperhorse.co.uk

A Paper prepared for the W3C/IAB Workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT), 28th February – 1st March 2014, London

Introduction

Governments have undermined user trust and confidence in the whole Internet, as has been revealed by Edward Snowden's continued revelations about government pervasive monitoring via the Internet. Governments are not the only ones carrying out this kind of activity and it is important that there is an open debate about the entirety of pervasive monitoring on the Internet. This paper discusses monitoring by corporate entities, whilst showing that the Internet community should work more closely with law enforcement to ensure they have the ability to investigate crimes properly as expected by people living in a democratic society. It also makes recommendations for standards bodies to consider the ethics of certain functionality, ensuring user protection is properly built-in, whilst ensuring that the Internet is not hijacked by governments bent on the authoritarian control of their people.

Pervasive Monitoring by Corporations

Pervasive monitoring is not just the conserve of governments - almost all websites make use of basic web analytics. However, what consumers should be really worried about are large companies that continue to fail to respect the real privacy of users and who are employing ever-developing invasive technologies such as Deep Packet Inspection to do it. Lucrative business lines have been created by selling the information that is collected by companies on the users of their own services. Indeed, the very data that has been generated by users and shared with their friends is used at will by certain services [http://www.dailymail.co.uk/news/article-2212178/New-privacy-row-Facebook-begins-selling-access-users-boost-ailing-profits.html]. It is therefore not in the business interests of such companies to allow standards bodies to create features within standards that would enhance the privacy of users by default. Many privacy policies now exist, but users are still put into a situation whereby they have no choice but to accept this situation if they are to use the service, despite it not being in any of the users' best interests.

The perception of such corporate data collection and usage seems to be generally benign amongst users. Nothing bad has directly happened, so therefore it doesn't matter. In reality, data collection is entirely opaque to the user and they probably wouldn't agree to the uses of their data. It is often down to eagle-eyed researchers or users to discover potential abuses and for the media to report them, for example in the cases of Linkedin's Intro service [http://thehackernews.com/2013/10/linkedin-intro-ios-app-can-read-your.html] and Phorm [http://www.badphorm.co.uk]. There is little evidence to suggest that the service that you would purchase would in some way be cheaper or more enhanced by the fact that your network provider sold all your data to a marketing firm. It is clear that this is already out of control; in December 2013, the World Privacy Forum discovered that data companies were selling lists of rape victims and AIDS patients [http://money.cnn.com/2013/12/18/pf/data-broker-lists/].

The point here is that the companies that are providing the service themselves have already signed users up to consent to handing over their data for virtually any use. If such services were to be secured, users are still likely to be at risk of the abuse of their data, merely because a) users don't have time to read long privacy policies and b) users don't see where or how their data is used.

Ethical Choices in Building and Standardising Technology

The processing and analysing power of computers in the world today means that we have reached the point as a world society where our choices are about what we "should do", rather than what we "can do". The connected

world is reaching out towards self-application of medicine, for example with the GSMA mHealth programme [http://www.gsma.com/connectedliving/mhealth/], but it carries a large societal impact if it goes wrong (for example Barnaby Jack's demonstration of remotely delivering fatal overdoses via insulin pumps [http://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/]. We have to realise that "just because we can, doesn't meant we must".

Just as in medicine, ethical decisions have to be made. Perhaps it is time that the bodies that are involved in building the Internet start to put consideration into the ethical implications of certain technologies and whether it is acceptable to provide even the platforms for services which are damaging to users, unless measures are designed to protect users in the first place. This has started to a certain extent, for example the Wassenaar Arrangement [http://www.wassenaar.org/] has listed "intrusion software" as a controllable export [http://www.wassenaar.org/controllists/2013/WA-LIST%20%2813%29%201/WA-LIST%20%2813%29%201.pdf]. It may be that future standards bodies also have ethics boards which are part of the standards development process, such that they can assess whether the standard is ethically acceptable.

Dealing with Internet security in a Non-Privacy Invading Way

Of course, different societies have different values and different ways of looking at things. China's response to the problem of mobile malware in the country has been to propose collecting all the information transmitted by mobile phones into one authority database, analyse it for malware and then strip any potential maliciousness, thus protecting the privacy of users [http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=9430]. At best, most people would read this as using a sledgehammer to crack a very small nut. At worst, it could be seen as a thinly veiled attempt at state-led pervasive surveillance of users' mobile communications, using the ITU-T (International Telecoms Union, Telecommunications Standardization Sector) as a vehicle to give them the capability to have this put into regulation at a global level. The 'ethics' of this are that the solution is far more invasive than the problem it sets out to solve. Not only this, but the solution is being put into a UN global standards body under international treaty [http://www.itu.int/] which has the potential for becoming therefore a national regulation.

An alternative, more privacy-sensitive and acceptable approach to tackling mobile malware would be to combine strong regulation, action and licensing against authors and distributors of mobile malware and also counterfeit device makers and retailers. This model has been successful in the UK and some other western countries, without impacting the privacy of users. As a citizen, what solution would you rather have? – We don't necessarily have to use technology to solve every problem.

The Potential Abuse of Internet Encryption by Corporations

The conclusion of some in the Snowden debate has been to "just encrypt everything" [http://arstechnica.com/security/2013/11/encrypt-all-the-worlds-web-traffic-internet-architects-propose/], however this is slightly naive. Not only does it not guarantee security or prevent further snooping, but it may cause monopolistic power shifts. The (expired) httpbis 'Security Properties for HTTP' Internet Draft specifically states that: "TLS does not protect against a breach of the credential store at the server or against a keylogger or phishing interface at the client." [http://tools.ietf.org/html/draft-ietf-httpbis-security-properties-05]. We can also guarantee that without a concerted effort to educate, developers are going to implement security badly. Education of developers on security should be a key outcome of the work that takes place on protecting the future Internet.

Even if it were possible to agree upon an end-to-end encryption scheme, the beneficiaries of such tightly secured protocols are going to be the providers of such services. For example, it is in the interest of a company like Google for such encryption to exist, because a mobile network operator would not be able to look at the data transiting its network. This would eliminate all competing advertising and the information market in one fell swoop, with the net result, a monopoly on user data for a small number of very large companies. One could imagine a situation where network operators would have to negotiate contracts with Google that allow them to

perform network and performance management, based on exchanging timestamps or encrypted blobs. Whilst this may seem appealing to some it serves a commercial goal rather than one about user privacy.

The announcement of Google's acquisition of Nest on the 13th of January 2014 shows that the company is interested in data in the user's home and potential mechanisms to control that via a "conscious home", in the Internet of Things space [https://nest.com/blog/2014/01/13/welcome-home/]. The home is the one place that users should feel complete privacy, but we are in danger of slipping into a world where that is not the case. It is within the power of bodies like the W3C to ensure that they don't deliberately facilitate invasiveness by ensuring that recommendations and APIs (for example in SysApps [http://www.w3.org/2012/sysapps/] / DAP [http://www.w3.org/2009/dap/]) are designed in such a way that an end-user can intervene and cleanly express their wishes in a way that is user-friendly to a web application.

Law Enforcement Access and Criminal Investigations

As a citizen living in a democracy, I expect that the Police will investigate crimes and prosecute under the rule of law. I am prepared to give up some privacy in order to have safety and that is enshrined under Article 8 of the European Convention on Human Rights [http://www.echr.coe.int/Documents/Convention_ENG.pdf].

Aside from the obvious examples of investigating paedophiles or counter-terrorism, there are examples of cases where citizens actively require their own, loved-ones or a criminal suspect's privacy to be breached, which can actually be more common. These real-world requirements must be considered when we develop systems that require confidentiality:

> Example 1 – A hiker, lost and injured on a mountain. Emergency services need to locate and find this person, but the hiker is not in a position to communicate their location due to their injuries.
>
> Example 2 – A missing child or vulnerable person (e.g. older person or mentally ill). In this case, the person that needs to be found by the authorities is not mentally capable of protecting themselves from harm or communicating that they are in danger and the authorities may need to locate them quickly.
>
> Example 3 – A dangerous armed person on the loose – e.g. situations such as Raoul Moat [http://www.bbc.co.uk/news/10583120], the Hungerford massacre [http://news.bbc.co.uk/onthisday/hi/dates/stories/august/19/newsid_2534000/2534669.stm] or the Christopher Dorner killings in California in 2013 [http://edition.cnn.com/2013/02/07/us/lapd-attacks/]. The priority here is to stop someone randomly killing people and all technology options should be open to finding them.

These examples broadly come down to citizens requiring privacy and confidentiality to be breached in limited and time-sensitive circumstances in order to protect their safety or the safety of others. In most cases, life is at risk so the time imperative is crucial.

As has been seen with incidents such as the missing child Madeleine McCann who disappeared in Portugal in 2007 [http://en.wikipedia.org/wiki/Disappearance_of_Madeleine_McCann], reacting quickly to discover all the circumstances in such a fluid situation, would in most people's views be considered a proportionate breach of privacy, as long as the information is only used for finding the child and prosecuting a kidnapper and nothing else. We have to be pragmatic about how the real world works. This is an important example of the point that to discover the real situation, the communications of people completely unrelated to the incident will have to be looked at in order to eliminate them from the investigation. However, we must consider carefully how that can be made possible whilst preventing such technical functionality being attacked for reasons of pervasive monitoring.

As a global society, we have opted in to such measures already through the laws that exist in our countries and the aforementioned. We should be careful that we don't accidentally create a worse situation for law enforcement. The resulting civil and legal backlash may ultimately reverse privacy gains made by (bluntly) "encrypting absolutely everything". At that point we may truly get "the Internet we deserve".

In summary, it is clear that there is a balance in the privacy and security debate. Not just technical security, but the security that we demand as a global society to be able to speak freely and to live safely. Law enforcement and governments have a valid voice in a democratic, multi-stakeholder Internet and it is important that as a technical community that those requirements and needs are not dismissed.

A Dystopian Future for the Internet?

If we are not careful, the Internet of the future could be a much less open and free place than we have now. Some countries have been openly talking about "control" and "managing" the Internet for some time. One mechanism to achieve this, proposed by Russia is to give control to the ITU or some other institution led by governments.

Russian Foreign Minister Sergei Lavrov's comments published on the 18th of December are somewhat concerning. In an interview with Russia's RT, he said:

> "But for a few years running, there's been another issue in the spotlight, and that is managing the internet. The International Telecommunication Union is heavily discussing ways to prevent the web from becoming a tool to promote someone's unilateral interests. This is a complex issue." [http://rt.com/politics/official-word/lavrov-syria-geneva-ukraine-746/]

Further, in his speech to the Council of Federation of the Federal Assembly of the Russian Federation in Moscow on the 18th of December 2013, he stated:

> "A question about Internet control rises. It has been discussed at Russia's initiative in the International Telecommunication Union. Western colleagues elaborately resist to have transparent and clear procedures of formation of an international intergovernmental structure, which would ensure control for inadmissibility to misuse the Internet for any purposes." [http://www.rusembassy.ca/node/827]

This was reported by Voice of Russia as: "Russia to insist on establishment of int'l organization to control Internet – Lavrov" [http://voiceofrussia.com/news/2013_12_18/Russia-to-insist-on-establishment-of-intl-organization-to-control-Internet-Lavrov-4128/].

The question of 'misuse' of the Internet is of course subjective. As industry bodies, continuing to build, uphold and develop an open and free Internet, we should be careful not to slip into a situation where we facilitate authoritarian rule by ignoring legitimate concerns around cyber-crime and child protection. This will only cause more draconian rules and laws which then facilitate censorship. To avoid this, industry bodies need to concentrate more closely on the societal concerns around the criminal uses of technology that is developed. Working more closely with law enforcement bodies and understanding how to build services that are both privacy-protecting and also allow legitimate criminal investigation must surely be the most sensible way forward. This also applies financially, we don't have a global tax body, so for those companies profiting from internet services – if they don't pay taxes in the country in which the service is consumed, how can that country possibly fight the criminal usage of those services?

Attempts to Fragment the Internet

Eugene Kaspersky has been a big supporter of internet control and has talked about "creating islands of the internet" in the past, essentially nation-state controlled and enclosed versions of the web and Internet. He has also advocated a form of 'Schengen' on the Internet [http://www.computerworld.com.au/article/270988/eugene_kaspersky_malware_internet_future/ and http://www.computerworld.com.au/article/386790/auscert_2011_eugene_kaspersky_calls_internet_interpol_/]. In a presentation entitled "Taking responsibility for the Internet" [http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-

Presentations/2079if09pres_EugeneKaspersky.pdf] he proposes more policing, regulation of the Internet and an "Internet Government", with Internet passports for all users.

In an interview in 2009, he said that:

> "I'd like to change the design of the internet by introducing regulation - internet passports, internet police and international agreement - about following internet standards," he continued. "And if some countries don't agree with or don't pay attention to the agreement, just cut them off." [http://www.theregister.co.uk/2009/10/16/kaspersky_rebukes_net_anonymity/]

He appeared to reverse his position on December 17th of 2013 in an article for the Guardian by presenting this as a bad thing:

> "..I fear that we are at a turning point for the internet, and may even be going into reverse. The utopia of a borderless digital global village may be coming to an end."

And:

> "Internet fragmentation will bring about a paradoxical de-globalisation of the world, as communications within national borders among governmental bodies and large national companies become increasingly localised." [http://www.theguardian.com/media-network/media-network-blog/2013/dec/17/internet-fragmentation-eugene-kaspersky]

Some of this is already happening – the so-called 'Halal web' has been created by Iran [http://www.newscientist.com/article/mg21628865.700-first-evidence-for-irans-parallel-halal-internet.html] and the "Great Firewall of China" largely cuts off the people of China from the rest of the world's popular Internet services such as Facebook and Twitter. Domestic social media services are used, such as QQ, Renren and Weibo, within the bounds of Chinese censorship.

Recommendations Summary

Whilst much of the pervasive monitoring debate has rightly focused on the need for more openness in the way that governments are conducting their activities in order to prevent future abuses, the same can be said about the need for companies to clean up their acts. We need to be careful that we approach these problems such that we get the "Internet that we want" as citizens of an open and free online world. Many actions that could be taken are not listed here, but in order to better secure the privacy of users and keep an open and free, borderless Internet consideration should be brought to the following recommendations:

- Increase developer security education and awareness through mechanisms such as webplatform.org
- Encourage within standards bodies such as the W3C, the responsible development of user-level & controllable functions which will enable privacy and protect security. The user should be able to express their intent and wishes as much as the developer.
- Establish ethics boards within internet standards bodies.
- Resist the government led creation of "internet islands" and a fragmentation of the internet along national lines and avert inadvertently bringing about the circumstances which may cause this (such as blocking all law enforcement investigations).
- Improve engagement and dialogue between the internet community and government stakeholders within existing standards and industry bodies such as W3C and IETF.