How to Thwart Internet Spying

Many are beginning to wonder if the Internet was America’s great “Trojan horse” gift to the world, a clever way to get past barriers and into everyone’s private information. The recent PRISM spying disclosures have especially riled Europeans. But there are techniques for fighting back, says Dutch technology expert Arjen Kamphuis.

By Arjen Kamphuis

On July 11, 2001, the European Parliament published a report on the Echelon spy network and the implications for European citizens and businesses. Speculations about the existence of this network of Great Britain-and-her-former-colonies had been going on for years but it took until 1999 for a journalist to publish a report that moved the subject out of the tinfoil-hat-zone.

The report of the EU Parliament contains very practical and sensible proposals, but because of events two months later across the Atlantic, they have never been implemented. Or even discussed further.

Under the heading “Measures to encourage self-protection by citizens and enterprises,” the report listed several concrete proposals for improving data security and confidentiality of communications for EU citizens. The document called on Parliament to inform citizens about the existence of Echelon and the implications for their privacy, adding that this information must be “accompanied by practical assistance in designing and implementing comprehensive protection measures, including the security of information technology.”

The report also urged “appropriate measures to promote, develop and manufacture European encryption technology and software and, above all, to support projects aimed at developing user encryption technology, which are open-source” and “promote software projects whose source text is published, thereby guaranteeing that the software has no ‘back doors’ built in (the so-called ‘open source
software’)."

The document cited the unreliability of security and encryption technologies whose source code is not published. This topic is a strict taboo in Dutch and UK discussions on IT strategy for governments (probably because certain major NATO partners might be offended).

Also, governments must set a good example to each other and their citizens, the report said, by “systematic use of encryption of e-mails, so that in the longer term this will be normal practice.” This should, in practice, be realized by “ensuring the training and publication of their staff with new encryption technologies and techniques by means of the necessary practical training and courses.”

Even candidate countries of the EU should be helped “if they cannot provide the necessary protection by a lack of technological independence,” the report said.

That one paragraph from the summer of 2001 before rational security policies were completely destroyed by 9/11, described the basis for a solid IT policy to ensure security and privacy of citizens against threats from both foreign actors and the government itself (historically always the greatest threat to its citizens and the reason why we have constitutions).

Had these policies been implemented over the last decade then the recent PRISM revelations would have been met mostly with indifference. European citizens, governments and companies would be performing most of their computing and communications on systems controlled by European organizations, running software co-developed in Europe and physically located on European soil.

An American problem with an overreaching spy apparatus would have been just that, an American problem like teenagers with machine guns or lack of universal healthcare, just one more of those crazy things they do in the USA to have their “freedom.”

**From Frying Pan to Fire**

Around that time, I was talking to Kees Vendrik (Dutch MP) about the problematic European software market. Not only was it impossible to buy a brand laptop without having to buy a Microsoft Windows licence, it was also impossible to visit many websites (municipalities, railways and many others) without using Internet Explorer. Since then, the latter area has greatly improved and I can today lead my life using my OS and browsers of choice.

The Dutch dependence on products such as MS Windows/Office has not really diminished however, despite all the wishes expressed by Parliament and attempts
at government policies. Today it is not possible to finish secondary school as a student without owning and using several pieces of proprietary software, making the students vulnerable to being spied upon.

Imagine making a certain brand of pen mandatory for schools and picking a brand of pen that comes with a spying microphone (not under control of the user). That is the current situation in practical terms in the Netherlands and UK among others. Germany, France and Spain are doing slightly better by at least acknowledging the problem.

Meanwhile, the technological seismic shift that frightened Microsoft’s Bill Gates so much back in 1995 (the Web makes the operating system irrelevant) is fast becoming reality. Almost all new developments discussed by IT power players and specialists are Web-based or based on open specifications and the most commonly used applications are running quite well as service in a browser.

So while the 15-to-20-year old problem of software dependency has never really been resolved (governments, with tens of thousands of IT workers, are still unable to wean itself off the familiar Microsoft technology stack), its impact is slowly becoming less relevant. Meanwhile, new dependencies based on “cloud” providers are now proven to be even more detrimental.

Excessive use of proprietary software creates the risk of foreign manipulation and potential attacks on critical infrastructure (see Stuxnet). But at least if your systems are attacked in this way, there are some ways to track this. If you are working on the computer that does not belong to you, that is based in a foreign country and is managed by people you don’t know in ways you cannot check, it will be very difficult to have any control over what happens to your data.

The old assumption, that using local servers could be part of the solution, seems unfortunately to be an illusion under the post-9/11 Empire. All “cloud” services offered by companies based in the U.S. are subject to U.S. legislation, even if the servers are physically in another country. And U.S. law is now somewhat, shall we say, problematic.

Just with an allegation of involvement in “terrorism” even without evidence systems can be closed down or taken over – without any warning or the possibility of adversarial judicial review. The term “terrorism” has been stretched so far in that anyone who allegedly breaks U.S. law, even if they’re not a U.S. citizen and even if they’re not in the U.S. can still be deemed “terrorist.” just on the word of one of the many three-letter services (FBI, CIA, NSA, DIA, DHS, TSA, etc.).
The EU was not happy about this but until the PRISM leak did not want to go so far as recommending its citizens and other governments to no longer use such services. PRISM is making it possible to at least have a serious discussion about this for the first time.

The long arm of the U.S. Patriot Act goes even further than merely the servers of U.S. companies on European soil. Thus domains can be “seized” and labelled in a highly prejudicial way, such as “this site was involved in handling child pornography.” Try explaining that as a business or non-profit organization to your clients, contributors or business partners.

Just using one .com, .org or .net extension as your domain name now makes you liable under U.S. law. All Europeans can now be seized from their homes for breaking U.S. law. So a .com domain name makes your server effectively U.S. territory.

We were already aware that proprietary platforms like Windows and Google Docs were not suitable systems for important things such as running public or critical infrastructure. However, now it turns out, that every service delivered through a .com / .org / .net domain places you under de facto foreign control.

Solution? As much as possible, change to free/opensource software on local servers. Fortunately there are quite a few competent hosting companies and businesses in Europe. Use local country domains like .nl, .de, .fr or, if you really want to be bullet proof, take a .ch domain. These are managed by a Swiss foundation and these people take their independence seriously.

If you still want to use Google (including Google Docs), Facebook, Evernote, Mind Meister, Ning.com, Hotmail or Office 365 please do so with the awareness that you have no privacy and fewer civil rights than English noblemen had in the year 1215.

Fighting Evildoers

A few months ago, a government speaker was defending the ‘Clean IT’ project at a meeting of RIPE (the organization that distributes IP addresses for Europe and Asia). Clean-IT is a European project of Dutch origin which aims to combat the “use of the Internet for terrorist purposes.” The problem with this goal is that “Internet,” “use” and “terrorism” remain undefined, nor does it seem anyone is very interested in sorting this out.

This lack of clarity in itself can be useful if you are a government because you can then take a project in any direction you like. A bit like when data retention was rammed through the EU Parliament in 2005 with the promise that it would be used only against “terrorism” – a promise that was broken within a few
months.

In Germany, data retention has now been declared unconstitutional and been abolished, while the Netherlands has rampant phone tapping, despite a total lack of evidence of the effectiveness of these measures. That all the databases of retained telecommunications data themselves become a target is not something that seems seriously to be taken into account in the threat analyses. All rather worrying for a government that is still usually unable to secure its own systems properly or ensure that external contractors do so.

Also, during the lecture on Clean-IT much emphasis was placed on the public-private partnership to reassure the audience. It’s strange that a government first makes itself incompetent by outsourcing all expertise, then it comes back after ten years and claims it cannot control those same companies, nor indeed their sub-contractors.

The last step is then to outsource the oversight function to companies as well and reassure the citizens: “We let companies do it! Don’t you worry that we would do any of the difficult technical stuff for ourselves, it’s all been properly outsourced to the same parties that messed up the previous 25 projects.”

Terrorism is obviously the “access all areas pass” – despite the fact that many more Europeans die slipping in the shower or from ill-fitting moped helmets than from “terrorism.” Moreover, we as Europeans have experience of dealing with terrorism. ETA, IRA and RAF were rendered harmless in previous decades by police investigations, negotiations and encapsulation. This was done without jeopardizing the civic rights of half a billion European citizens. Even when IRA bombs were regularly exploding in London, nobody suggested dropping white phosphorous on Dublin or Belfast.

I hope that the pre-9/11 vision of the EU Parliament will be rediscovered at some point. It would be nice if some parts of the “Free West” could develop a policy that would justify our moral superiority towards Russia, when we demand that they stop political censorship under the guise of “security.”

Backup Plan

If all else fails (and this is not entirely unlikely) we need a backup plan for citizens. Because despite all petitions, motions, actions and other initiatives our civil liberties are still rapidly diminishing. Somehow a slow-motion corporate coup has occurred where the government wants to increase “efficiency” by relying on lots of MBA-speak and corporate management wisdoms that worked so well for the banking sector.
The fact that the government’s primary function thereby evaporates does not seem to bother most civil servants. And meanwhile the companies themselves are apparently too busy making profits and fighting each other to worry about civil rights and other archaic concepts from the second half of the 20th Century.

So rather than always trying to influence a political system that so very clearly ignores our interests, we can simply take care of ourselves and each other directly. This conclusion may not be pleasant, but it gives clarity to what we have to do.

One good example would be to have educational and civil liberties organizations providing weekly workshops to citizens on how to install and use encryption software to regain some privacy. These organizations should use their clout to get the slogan of “crypto is cool” on everyone’s lips.

Technologists and designers should focus their energies on promoting the hip and user-friendly aspects of these pieces of software. This may be a lot more fun than lobbying ossified political institutions and actually provide some concrete privacy results.

Since 2006 I have ensured my own email privacy by no longer relying on the law, but by using a server outside the EU, SSL connection to it through a VPN tunnel entering the open Internet also outside the EU. I encrypt as many emails as possible individually with strong crypto (using Free GPG software).

The fact that all those hordes of terrorists (who, our government asserts, are swamping the planet) have no doubt also adopted such measures – for less than 20 Euros a month makes most of the low-level spying a complete and pointless waste of resources. Assuming the point truly is fighting “terrorism” something that is becoming a bit doubtful in light of the above.

Despite what some of the “but I have nothing to hide” apologists say, we have privacy rights and other civil liberties for the same reason we have a constitution. Not for situations where everything is OK but for those rare situations where things are not OK.

Privacy is the last line of defense against governments who lose sight of their reason for existing (to serve their people). Privacy is therefore not the enemy of security but the most basic part of it because governments are much scarier than any would-be cyber-criminal or even terrorists. Criminals may steal some money and terrorists may kill a few people but when it comes to wars, mass repression or genocide you always need a government.

It is very obvious what European governments should be doing to promote the safety and security of their citizens and states. They already wrote it down in
the summer of 2001. The fact that these measures are never part of any current “cyber-security” policy proposals should make people very suspicious, at least of their governments’ competence.

Arjen Kamphuis is co-founder and Chief Technology Officer of Gendo. He studied Science and Policy at Utrecht University and worked for IBM and Twynstra Gudde as IT architect, trainer and IT strategy adviser. Since late 2001, Arjen has advised clients on the strategic impact of new technological developments.