Adrian Farrel : Why Responding to Terrorism with Curtailed Digital Freedom is Wrong [1]

Written by Adrian Farrel on 24 May, 2017 - 11:30

comments [2]

24. 05. 2017

It is hard for anyone to continue the political debate in the aftermath of the events of Monday 22nd may in Manchester. Our thoughts are all occupied with concern for all those affected, and with love for our own children.

But one of the objectives behind this sort of attack is to disrupt our political system, to damage democracy, and cause us to change our way of life. The intention is to instil fear into us all, to cause us to hide and become hostile, to make us different from the open and culturally diverse nation that we are. It is important, as a way to mitigate this attack, that we strengthen the political debate and act to preserve our freedoms, rights, and civil liberties. We cannot bring back those who were killed, and we can only hope that the wounds, both physical and psychological, heal with time, but we can show the terrorists that we will not allow them to take our society down.

Several questions that are close to the centre of Pirate Party politics need to be addressed immediately. They are fundamental to the debate about freedom and yet appear to offer direct methods to reduce the likelihood of future attacks.

1. Information on how to make bombs is available online

It is true that all manner of very horrible things can be found on line. Some can be put to bad uses by people who want to do us harm. Some things are of their nature unacceptable.

In general, where illegal material is hosted on servers in the UK, the police already have powers to have that content removed. No new laws or powers are needed.

Where content is hosted overseas, the problem is much greater. In many cases (for example, child sexual abuse) law enforcement around the world cooperates to see the illegal material removed. However, we also know that the Internet is very large and very hard to control, so it is impossible to find and remove all instances of such material.

A suggestion has been made that web site blocking may be used to restrict access to web pages that contain material that we do not want to be visible within the UK. In this approach, the domain name server (DNS) system that resolves web page names into the location of the servers that host those web sites would fail to return a result meaning that a web browser cannot reach the intended site. DNS blocking is, however, relatively easy to bypass since the web pages concerned remain accessible on the Internet via their IP addresses.

Another approach is IP address blocking: the Internet Service Providers that we all use to access the Web simply ensure that no communications between our home computers and the servers that host the undesirable web pages are possible. Superficially, this approach is very powerful, it is like the remote party having their phone cut off - you cannot call them. However, when the web site is outside the country the parallel with the phone system breaks down - they have not been cut off, it is your ability to call them that has been restricted, and if you call someone else on another number outside the country, they will be able to put you through. And this is exactly how it works for web sites on the Internet, so IP blocking is ultimately ineffective.

DNS blocking and IP address blocking have been used a few times in the UK, most famously to block access to the Pirate Bay web site. But in practice the only effect this has had is on the majority of technology-unaware people - the normal users. All people with an element of understanding about how the Internet works (and this includes most people who might illegally stream content) can easily find and access the Pirate Bay web site. These mechanisms have been proven to not work against someone who is determined to find the material we seek to ban.

Furthermore, management of blocking is complex. Web sites proliferate at an amazing rate, and each web page could carry the information we might seek to suppress. Proposals have been made to use algorithms and even artificial intelligence to sift through web pages and flag those that should be banned. But what we know about existing methods is that they produce a massive management overhead that costs a vast amount to run, and that they result in 'false positives'. Indeed, a recent attempt to cut down on online child pornography led to very many web sites being inadvertently blocked (including health service and news media sites). Manually handling and rectifying complaints of false blocking takes a lot of time and resource.

While we might consider some loss of freedom to be a price worth paying. What would it matter if one web site, perhaps for a demolition company, was temporarily blocked yet we managed to prevent another outrage? But this is the thin end of a wedge and we need to look at what it really means for our freedoms. How many web sites would we lose in this way? How much legitimate information would be hidden? Who would be the arbiter of what information can be legitimately suppressed? And would we not be sacrificing our way of live in exactly the way that the terrorists intend?

Perhaps the most famous use of restriction of the Internet is in China. There is very significant restriction of access to the wider Internet from within the borders, and we term this censorship.

Let us also recall that while the IRA never had the Internet they were still unfortunately able to kill a large number of people using home-made bombs. It is clear that, while the Internet can be used to share information, it is not the only source, and determined terrorists will not be stopped simply by us censoring ourselves.

By all means police and reduce hateful content, especially that hosted within the UK. But look more widely at this social problem - the presence of information about how to do bad things is not a concern if there are no people who want to commit those acts. Why are our own citizens so disturbed that they would go to these extreme lengths?

2. Social media is used to recruit, radicalise, and inspire terrorists

Blanket bans of social media are commonly used by oppressive regimes to curtail free speech and to prevent the populace from organising against the government. Most famously such a ban was used in Turkey, but that is by far not the only country to have clamped down on the use of social media.

Banning access to social media is also likely to drive those planning similar atrocities underground, into using

networks that are less easy for authorities to monitor, and making it more likely that these killers will go undetected until they carry out their attack. In fact, keeping social media as a free and open forum makes it possible to spot the places where radicalisation takes places and to engage in debates. Careful and constructive debate is one good way to bring people back into society, and to recognise and address their concerns.

3. Online monitoring is the best / a good way to intercept terrorist planning and prevent attacks

The UK authorities have always had the ability to conduct targeted surveillance of known suspects. This provides an excellent way to monitor known individuals who may be planning illegal activities. And this approach is properly regulated by the authorities through the use of warrants and subject to the "probable cause" condition.

Pirate Party UK does not believe that extra powers or legislation are needed to prevent further attacks. In fact, we think that recent legislation such as the Investigatory Powers Bill actively harms investigations by "adding more hay to the haystack". It has been shown repeatedly that the additional information gathered by mass surveillance can mask real and useful knowledge of suspects, and that valuable leads are dropped when there is too much material arising from data collected from the whole population.

Furthermore, pervasive monitoring of our online lives can open us up to false accusations. Just because you clicked on a link does not mean you are a terrorist. Just because you exchanged an email with someone else who exchanged an email with a terrorist suspect does not mean you, yourself, should be subject to investigation. Association is not defined so loosely, and freedom of association is one of our core rights - governments have to understand that in the new, online world, freedom of association must include the right to associate in new ways.

It is often said that "if you have nothing to hide, you have nothing to fear." But this argument is bogus. There are locks on toilet doors not because we use those spaces for nefarious purposes, but to protect our privacy. The fact that people then go on to use those locked places for acts of questionable legality does not result in a call to install CCTV in all toilet cubicles - we value our own privacy too much for that.

Those who call for increased surveillance, for the ability to store "metadata" about all aspects of our online lives, are perhaps unaware of the details of their own activities that will be revealed and how it might be used in the future. Not only will the security services have access to this information, but it will be shared across multiple government agencies and even with non-governmental companies such as utility providers and large administrative companies providing out-sourced services to government

It is also true that the general user of the Internet is not aware of these facts and the trails that they leave each time they go online. That part of modern life is significantly lacking from the education system and it is critical that we teach young people what governments, big businesses, and criminals can do with the information about our daily online lives. We need to teach our children, and the whole of society, how to keep safe on the Internet.

We should also note that the ability for organisations to keep data secure is highly questionable. We know, from recent painful experience in the NHS, that government systems are not secure. The ransomware attack that caused so much disruption could just have easily led to theft of data. We have repeatedly hear how large companies have "lost control of" large customer databases including login details and sometime credit card numbers and billing addresses. So how long would it be before organised crime gained access to our metadata? What harm might criminals do with this information? Would it lead to blackmail and extortion - they could threaten to tell your family about the gay porn sites you visit? Would it lead to identity theft - possibly through better targeting of phishing attacks?

Pirate Party UK also does not agree with the Government's argument that end-to-end encryption should be controlled or prohibited. The Government is worried that criminals may use standard applications, such as email, to encrypt messages so that they cannot be read by anyone else. Their proposed solution to this is to ban end-to-end encryption and only make it available through services that offer the security services a "back door" that allows them to unlock hard drives and read encrypted messages.

But the security of encryption is fundamental to how we operate on line. When we access our bank account on line, pay for our shopping, or exchange commercially sensitive data, we use encryption. It is how we ensure that our transactions are safe from interception and that we are not vulnerable to fraud. When you make a backdoor you can expect other people to try the handle. And organised crime has far more resources to throw at this than even national governments, so we can assume that it will only be a matter of time before criminals gain access to everything that you could encrypt.

And, worse, the Government's approach is to ask us all to hand over the keys to our encryption. That is like asking us to leave a key to our house under the doormat. "Don't worry," they say, "we will only use the key in an emergency." But what about other people who know where to look for the key? And, anyway, who is going to judge what constitutes an emergency? The black and white cases are easy to talk about, but there is a fuzzy line in between where objection to government actions or legitimate protest become excuses to use the key. After all, the police don't have a perfect record in their undercover investigations of legal protest groups.

4. Fake news and random social media posts only serve to cause additional chaos immediately after an event

Twitter and Facebook were awash with claims, counter-claims, and speculation in the hours after the Manchester Arena attack. Some posts were helpful, the very many were wild speculation or random comments, and a few were vile fake reports and even pictures and photos that been doctored or showed other places and events.

It is clear that social media is an environment that we, as humans, are still learning how to use, but that does not mean it should be regulated as proposed in the Conservative Party manifesto and as suggested by many others.

In fact, any such regulation would immediately become censorship - there would need to be someone (or more likely an office of very many people) responsible for determining which posts are acceptable, and which fake. Who would perform such tasks? Would it be a branch of government, or would we expect the social media companies to do this filtering on our behalf? Do we really want a form of government where what we say and how we say it is subject to filters and controls? Isn't this the objective of the terrorists: to change our society and to make a major impact on our freedoms?

Another suggestion is that social media should be temporarily turned off following a major incident. That would prevent wild speculation, false reports, and panic. But it should be clear that social media provided a really valuable safety net following the events of the 22nd May. Children were able to Tweet that they were safe so that friends and family could be reassured even when phone systems were overwhelmed. The local community used Facebook and Twitter to coordinate temporary accommodation and shelter for lost or unaccompanied minors, and to arrange travel and lifts to get people home. Obviously, social media, used responsibly, is a great asset.

Instead, we all need to be aware of how social media works as a viral gossip network. We need to grow up in our use of these new platforms. We should teach their use in schools, we should spread the word through the established media, and we should all take responsibility for our own actions. Security hoaxes tend to proliferate in the aftermath of high-profile terrorist attacks, especially via web-based social networks. Ensure you have access to reliable intelligence and refrain from acting on the basis of or of propagating unverified

information.

The reason that responsible news outlets like the BBC were slow to report the details of the Manchester attack was that they wanted to be sure to get the facts right. Of course, we all want up-to-date news, and increasingly we want that news instantly especially when our loved ones might be involved, but relying on social media for news stories and facts can add to the fears and stress when properly checked facts and reputable sources provide a more stable approach.

- - -

As we continue these discussions, our first thoughts must remain with the victims and their families. Our first efforts must be to provide support and comfort to them.

At the same time, we must not allow these events to serve as a trigger for ever more authoritarian legislation by our Government. New legislation must be subject to proper scrutiny to understand its effectiveness. Policy-making by knee-jerk is never a good thing, and a politician that acts only to address the demand that "something must be done and something must be seen to be done" is falling victim to populism and is giving the terrorists exactly what they want.

In forming new policy we must, of course, listen to the police and security services, but we must not let them dominate the debate. If we ask the security services what tools they need they will naturally request every possible tool - their job is not to preserve civil liberties or to maintain an open society; their job is to track down terrorists and prevent attacks. The job of politicians, and it is a very difficult job, is to strike a balance between authoritarian measures and our freedoms. And above all, politicians need to understand the effectiveness and appropriateness of the policies they intend to impose.

- - -

This article was written by Harley Faggetter and Adrian Farrel (members of the Board of Governors of Pirate Party UK) with contributions from Imre Oks, David A Elston, and other members of Pirate Party UK.

Tags:

Surveillance [3]
Snooping [4]
Freedom [5]
Social Media [6]
Harley Faggetter [7]
Adrian Farrel [8]

Links
[1] http://legacy.pirateparty.org.uk/party-magazine/why-responding-terrorism-curtailed-digital-freedom-wrong
[2] http://legacy.pirateparty.org.uk/party-magazine/why-responding-terrorism-curtailed-digital-freedom-wrong#comments
[3] http://legacy.pirateparty.org.uk/tags/surveillance
[4] http://legacy.pirateparty.org.uk/tags/snooping
[5] http://legacy.pirateparty.org.uk/tags/freedom
[6] http://legacy.pirateparty.org.uk/tags/social-media
[7] http://legacy.pirateparty.org.uk/tags/harley-faggetter
[8] http://legacy.pirateparty.org.uk/tags/adrian-farrel