Why People Need the Dark Web

https://www.e-ir.info/2018/10/07/why-people-need-the-dark-web/

ROSS BELLABY, OCT 7 2018

Never before has the real world been so interconnected with the cyber. In developed societies, almost every aspect of life is becoming digitised, facilitating social and commercial interactions in ways previously unseen. What is said and to whom; what information was looked at and when; what was traded and for how much; and where people are going is all being digitised and, importantly, constantly recorded and stored. This is something that has not escaped the attention of the intelligence community who argue that by collecting and examining this data they can detect, locate, and even predict threats. Unsurprisingly, people are concerned about this access and have begun to utilise anonymising technology to secure their identity and online activity behind encryptions and auto-deletes. One popular tool for this is TOR, an easily downloadable program that allows online anonymity through onion routing – a form of layered encryption where the traffic is processed through three nodes, encrypted at each stage so that the sender and destination are unknown as each intermediary knows only the location of the immediately preceding and following nodes (Abbott el at, 2007). Through this TOR circuits, many kinds of 'hidden services' are available such as website hosting denoted by the .onion URL, online messaging and VOIP communications, and data sharing (TOR Project). These protections have created what is commonly referred to as the 'dark web', the collected sum of these websites that allows anonymity to those who visit or conduct business through it.

This technology, however, represents a new ethical challenge. On the one hand, intelligence actors have an ethical obligation to prevent threats from harming the political community, and having access to online information when justified can play an important role in this. While on the other hand, this cyber-data represents something that is most intimate and private to the individual. Moreover, anonymising technologies that allow the individual to 'go dark' go further than any previous protections, creating what former-FBI Director James Comey termed as 'warrant proof' spaces – technological black boxes that no matter what some authority might deem as being legitimately searchable is protected to the extent that there are very limited or non-existent means of forcing oneself in (Judiciary Committee). This has the potential to sway the balance against the intelligence community irrevocably, preventing them from monitoring online activity or accessing digital information, even when they have a legitimate reason for doing so.

As a consequence, some states have reacted in a confused, knee-jerk or draconian way, including calls to ban the technology entirely; insisting on built-in backdoors or lower protection standards for authorities to exploit, or to assume all those who use such technology are inherently guilty. For example, China's 'Golden Shield Project' – also known as the Great Firewall of China – not only censors online content but also systematically probes for and shuts down any programs that might try to aid access to outside information or the dark web (TOR Project 2015). While after Adrian Ajao's terrorist attack on Westminster killing four people, London 2017, where his last message was communicated through WhatsApp, the then UK Home Secretary Amber Rudd stated that it was 'completely unacceptable' to allow terrorists to communicate 'in secret', calling for an outright ban of such encrypted technology (Rayner, 2017). Similarly, in the USA in early 2016 the FBI sought to compel technology company Apple to lower some of their security measures on their phones to enable them to force attack devices and gain access to stored data (Cook, 2016).

Privacy, Security, and Anonymising Technology

This debate is made more problematic by narratives that portray security and liberties as opposing qualities that must be traded or balanced. This framing, while widely pervasive, is highly dangerous. By framing them as a trade-off,

where one must be sacrificed in order to have the other (and often where national security is the trump card), it is not surprising that 'After 9/11 countries around the globe unhesitatingly adopted policies to enhance their government's capacity to prevent terrorism… at the expense of individual civil liberties' (Dragu, 2011: 64). However, security is not separate from people's vital interests, but an overarching formula by which they are ensured. That is, security is the means by which all of our vital interests – which include physical and mental integrity, autonomy, liberty and privacy – are provided for. Security is the overarching formula by which all vital interests are protected. Granted, physical safety is often seen as most important and the central concern of national security, but it does not override all other vital interests. Vital interests exist in a complex matrix, where an excess of one will not necessarily make up for the lacking of another interest: all the physical security in the world cannot be used as a justification for undermining people's privacy. This understanding, therefore, both limits and licenses the power of the state, something often expressed as the social contract where rational individuals agree to sacrifice some of their freedoms in return for the state's duty to protect their vital interests. The danger is when the state incorrectly makes this negotiation often fearing physical insecurity to the detriment of other vital interests.

In terms of cyberspace, the vital interests of privacy and autonomy are both significantly prominent. If we view information in terms of concentric circles where the closer one goes to the centre the more intimate the information and the greater the expectation of privacy there is, it can be argued that online information should be considered as being highly private (Marx, 2004: 234). This is because, first, there has developed a high expectation of privacy in one's everyday online activity, especially given the increased and pervasive use of cyberspace throughout people's lives; second, because real-world protections on analogous datasets – medical, financial, social, and political – already have high expectations of privacy; and third because it involves trespassing across a clearly defined barrier in terms of a person's personal computing devices or communication while in transit (McArthur, 2001: 123-128). Access to URL information (even restricted to before the first / slash), for example, can reflect intimate details about a person's life such as sexuality, political or social views, medical details, and financial activity, and even analysis of people's meta-data can be used to access sensitive personal data on where a person goes and with whom he communicates. The individual, therefore, has a clear interest in protecting their online information.
The implications of anonymising technology are, however, still striking given the 'privacy-plus' they provide. Anonymising technology such as TOR and auto-deletes undermine the ability of the state to ever collect intelligence, hampering its ability to detect, locate, and prevent a range of potential threats. Arguments could be made, therefore, that they indeed distort the negotiation too far against protecting the political community as the state, even when justified, cannot access necessary information. However, from the point of view of the individual, this does not diminish their right to establish whatever privacy protection they see fit. Judith Thomson discusses privacy in terms of a collection of property rights: that if an individual wishes to put something precious to them in a safe to prevent others from looking at it, then it is their right to do so, and indeed represents a clearer demonstration that they wish to stop others from looking at what they own. Breaking in would be a clear violation of their privacy (Thomson, 1975). Importantly, they are not locking their private items away with the knowledge or expectation that should the need arise the door can be blown off. It is not the responsibility of the individual – or safe manufacturers – to ensure this option. If we make Thomson's safe crack-proof this does not undermine the individual's right to use it, even to the detriment of possible future intelligence collection. Moreover, it is the state's duty to demonstrate why such protections for specific individuals should be necessarily pulled down. The individual is assumed innocent until proven guilty and the danger of demanding presumed access to an individual's property flips this; that there is an assumption that they will be guilty of something and so the state will need access; or that using such protections is an inherent indication of future guilt as a form of pre-crime (Zedner, 2005; Solove, 2007). What this means is that the state must be able to prove why particular individuals are warranted for surveillance – probable cause/balance of probabilities for example – to justify its coercive powers. Any demand that insists on weakening systems for all individuals assumes everyone is potentially guilty and therefore in need of being surveilled. Therefore, it can be argued that even though anonymising technology provides a nearly impenetrable barrier, the individual has the right to exert what protections they feel is required to ensure their privacy.

Not Only a Right But an Ethical Need

This argument can be pushed one step further, however, in that not only is there a right but it is ethically mandatory to establish such privacy protections at a fundamental level of cyberspace, to create defences that automatically and

systematically anonymise an individual's identity and activity whether or not they have expressed an explicit desire. While this might raise liberal concerns regarding overreach and interference in people's lives, paternalism can actually help highlight why there is a need for such interventions. Indeed, some argue that any interference in an individual's life is unjustified because it is infantilising to the individual (Anderson, 1999), or a 'violation of the person's autonomy' as people are not choosing their own destiny (Dworkin, 1988: 123). However, if the main concern about paternalism is the impact on people's autonomy then the context of the interference becomes important. Being fully autonomous requires people having the capacity to plan, choose, and reflect on options in terms of arguments, with the relevant information and without excessive outside influence (Frankfurt, 1971:7). If individuals do not have the full facts or could not reasonably be able to comprehend their meaning then they are unable to make an informed decision and are therefore unable to act autonomously. Moreover, lacking the capacity for full autonomy demands an obligation on others to help provide or facilitate their realisation of their good life, whether the support is physical or in aiding in the necessary rational, critical reflection. It can be argued, therefore, that anonymising technology protects people by providing them with their necessary privacy in a situation where their lack of knowledge or ability to understand means that they are non-autonomous agents, while also securing their autonomy through providing protected spaces for deliberation free from state surveillance influencing their decision-making processes.

An important part of this argument is the overall general ignorance of people in understanding how their information is being collected. This includes a general lack of awareness in regards to privacy settings and an understanding of the implications of the publically stated abilities of corporations and governments to collect data, as well as a specific lack of awareness on the secretive surveillance powers of intelligence actors such as the USA's National Security Agency (NSA) and UK's Government Communications Headquarters (GCHQ) that were revealed by Edward Snowden.

Indeed, there is wide-ranging evidence showing that while people do value their online privacy, they do not recognise the need to act to protect it. For example, in terms of social media, even though there should be a greater awareness on the ability of others to access one's information given its outward-looking nature, people view access like a 'walled-garden' – expecting their friends to be able to view the information but not the wider world (Dwyer et al, 2007; Livingstone, 2008; Tufekci, 2008). Moreover, even when people consent to access to their information – in terms of HTTP cookies (also known as browser cookies or just cookies) or by accepting website 'terms and conditions' for example – there are significant technical barriers to people fully understanding the implications of such agreements. This, therefore, fails to meet the standard of informed consent, especially when there is a culture of pervasive and habitual nature of agreeing to the terms coupled with the lack of technical understanding.

Concluding the Need

The conclusion, therefore, is that while anonymising technology and the dark web represent a clear challenge for the intelligence community, in order for people to have the level of privacy they need or think they are receiving then greater protections need to be erected for them. These protections are very difficult for intelligence actors to circumvent and so prevent large-scale surveillance. This technology therefore not only represents a useful means of people erecting protections over their cyber-privacy, but it is this very en masse surveillance – from both governments and corporations – coupled with people's limited awareness and ability to comprehend such data collections that makes such technology ethically mandatory. Therefore, anonymising technology should be built into the fabric of cyberspace to provide a minimal set of protections over people's information, and in doing so force the intelligence community to develop more targeted forms of data collection.

References

Abbott, T. el at (2007) 'Browser Based Attacks on TOR' Privacy Enhancing Technologies Vol.4776, 184-199

Anderson, E. (1999) 'What Is the Point of Equality?' Ethics 109, 287-337

Cook, T. (2016) 'A Message to Our Customers' Apple 16th February 2016 Available at http://www.apple.com/customer-letter/

Dragu, T. (2011) 'Is There a Trade-Off Between Security and Liberty? Executive Bias, Privacy Protections, and Terrorism Prevention' American Political Science Review 105/1, 64-78

Dworkin, G. (1988) The Theory and Practice of Autonomy (Cambridge: Cambridge University Press)

Dwyer, C., Hiltz, S. and Passerini, K. (2007) 'Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace' Proceedings of AMCIS, 339

Frankfurt, H. (1971) 'Freedom of the Will and the Concept of the Person', Journal of Philosophy 68/1, 5-20

Judiciary Committee (2016) 'Hearing on Apple iPhone Encryption', 1st March 2016. Available at http://www.c-span.org/video/?405442-1/hearing-encryption-federal-investigations

Livingstone, S. (2008) 'Taking Risky Opportunities in Youthful Content Creation: Teenagers' Use of Social Networking Sites for Intimacy, Privacy and Self-Expression' New Media & Society, 10/3 (2008) pp.393–411

Marx, G. (2004) 'Some Concepts that May be Useful in Understanding the Myriad Forms and Contexts of Surveillance', Intelligence and National Security, 19/2, 226-248

McArthur, R. (2001) 'Reasonable Expectations of Privacy' Ethics and Information Technology 3, 123–128

Rayner, G (2017) 'WhatsApp accused of giving terrorists 'a secret place to hide' as it refuses to hand over London attacker's messages' The Telegraph 27 March 2017. Available at: http://www.telegraph.co.uk/news/2017/03/26/home-secretary-amber-rudd-whatsapp-gives-terrorists-place-hide/ Accessed 27 March 2017.

Solove, D. 'I've Got Nothing to Hide and Other Misunderstandings of Privacy' San Diageo Law Review, 44, (2007), 745-772

Thomson, J. J. (1975) 'The Right to Privacy' Philosophy and Public Affairs 4/4, 298-303

TOR, What Protections Does TOR Provide. Available at https://www.torproject.org/docs/faq.html.en#WhatProtectionsDoesTorProvide

TOR (2015) 'Learning more about the GFW's active probing system' The TOR Project Available at https://blog.torproject.org/category/tags/china

Tufekci, Z. (2008) 'Can you see me now? Audience and Disclosure Regulation in Online Social Network Sites' Bulletin of Science, Technology & Society 28/1, 20–36.

Zedner, L. (2007) 'Pre-Crime and Post Criminology' Theoretical Criminology 11/2, 261-281

About the author:

Ross Bellaby is a lecturer in Security Studies at the University of Sheffield's Politics Department. His research focuses on designing ethical frameworks for the intelligence community and for cyber-activity. His ethical framework is set out his book, *The Ethics of Intelligence: A New Framework* (2014). This work is further developed in papers on counterterrorism and the CIA's extraordinary rendition program (2017), the justifiability of cyber-intelligence (2017), the ethical obligation of whistleblowing (2017), and the need for more dark web technology to protect against state surveillance (2018).