Article:
Bellaby, R. (2018) Going dark : anonymising technology in cyberspace. Ethics and Information Technology, 20 (3). pp. 189-204. ISSN: 1388-1957

https://doi.org/10.1007/s10676-018-9458-4

Ethics and Information Technology
https://doi.org/10.1007/s10676-018-9458-4

ORIGINAL PAPER

Going dark: anonymising technology in cyberspace

Ross W. Bellaby[1]

Abstract
Anonymising technologies are cyber-tools that protect people from online surveillance, hiding who they are, what information they have stored and what websites they are looking at. Whether it is anonymising online activity through 'TOR' and its onion routing, 256-bit encryption on communications sent or smart phone auto-deletes, the user's identity and activity is protected from the watchful eyes of the intelligence community. This represents a clear challenge to intelligence actors as it prevents them access to information that many would argue plays a vital part in locating and preventing threats from being realised. Moreover, such technology offers more than ordinary information protections as it erects '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. However, it will be argued here that not only is using such anonymising technology and its extra layer of protection people's right, but that it is ethically mandatory. That is, due to the *en masse* surveillance—from both governments and corporations—coupled with people's limited awareness and ability to comprehend such data collections, 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.

Keywords Dark web · Privacy · Cyberspace · Intelligence · Surveillance · Paternalism · Security

Introduction

In a world where the Internet and cyberspace have permeated almost every aspect of modern life, never before has the real world been so interconnected with the cyber. In developed societies, almost every aspect of life is becoming digitised and processed through a computer system of some form. This computer revolution, however, is a double-edged sword. That is, while people are now able to interact with a level of ease and expediency previously unseen, all the data on these interactions are constantly recorded and stored. This is something that has not escaped the attention of the intelligence community, who argue that by collecting all of this data and examining it for patterns not only can they tell what someone has done but predict what they might do next.[1] Unsurprisingly, people are concerned about access to their information and have, as a result, begun to utilise anonymising technology that secures their identity and online activity behind encryptions and auto-deletes. One of the most renowned tools for this is TOR, an easily downloadable program that allows a user online anonymity through onion routing—a form of layered encryption where the traffic is processed through three nodes and 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.[2] TOR circuits protect many kinds of 'hidden services' including website hosting denoted by the .onion URL, online messaging and VOIP

✉ Ross W. Bellaby
r.bellaby@sheffield.ac.uk

[1] Department of Politics, University of Sheffield, Elmfield Building, Northumberland Road, Sheffield S10 2TU, UK

[1] Oscar Gandy, 'Data Mining and Surveillance in the Post 9/11 Environment' in Bell K and Webster F (eds.) *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age* (London; Sterling, VA: Pluto Press, 2003) p. 28; Patrick Keefe, *Chatter: Dispatches From The Secret World Of Global Eavesdropping* (New York: Random House, 2005) p. 99; Christopher Yang et al. 'An Analysis of User Influence Ranking Algorithms on Dark Web Forums' *Proceedings of ACM SIGKDD Workshop on Intelligence and Security Informatics* (ISI-KDD), Washington, D.C., July 25, 2010.

[2] Timothy G. Abbott el at 'Browser Based Attacks on TOR' *Privacy Enhancing Technologies* Vol. 4776 (June 2007) p. 2. End-to-end encryption can play an important (though not necessary) part of this communication process as this can add an extra layer of protection by encrypting the information that is being sent to the server at the end of the chain and so can ensure that the message is encrypted to even

Published online: 22 June 2018

communications, and data sharing.[3] This has resulted in the creation of 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.

Information protection, however, is not limited to bespoke software being used by a few individuals. Technology companies have spent considerable time and effort to develop the most secure devices possible that prevents the individual's data from being accessed by others. Most notably this has included storage devices such as mobile phones possessing auto-delete functions whereby if too many incorrect password attempts are made the data on the device is erased. This prevents the use of force attacks, where another computer tries all possible combinations in quick succession in the hope of identifying the correct one as the multiple incorrect attempts prompts a complete wipe of the memory.[4] Or equally prominent is the use of end-to-end 256-bit encryption on instant-messaging applications such as WhatsApp, making the transmitted data for its some 900 millions users near impossible to access.[5]

The problem is that this technology has the potential to upset the relationship between the protections people have surrounding their privacy and the state's ability to access that information when it is justified in order to protect the political community. This tension is itself not necessarily new. On the one hand intelligence actors have an ethical obligation to prevent threats from harming the political community, and having access to this information when justified can play an important role in this. While on the other hand this online-data represents something that is most intimate and private to the individual. As people increasingly carry out their social and private lives online their virtual-self is ever more synonymous with their real-self and even just a cursory glance can give an insight into some of the most intimate aspects of someone's life.[6] Anonymising technologies that allow the individual to 'go dark'[7], however, 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.[8] This, therefore, adds a new problem to the debate as it potentially sways 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, prompting many government organisations to actively try to compromise TOR 'not only in regions with repressive regimes but also in the free world'.[9] In China, for example, its '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.[10] While WhatsApp's complex end-to-end encryption has raised questions in India where the new 256-bit encryption is far above the officially allowed and much

Footnote 2 (continued)

those at the end node and only accessible to the intended recipient. Michael G. Reed, P. Syverson, and David Goldschlag 'Anonymous Connections and Onion Routing' *IEEE Journal on Selected Areas in Communications*, 16/4 (1998) p. 482; David Goldschlag, Michael Reed and P. Syverson 'Onion Routing for Anonymous and Private Internet Connections' Communications of the ACM 42/2 (1999) 39–41.

[3] TOR, *What Protections Does TOR Provide*. Available at https://www.torproject.org/docs/faq.html.en#WhatProtectionsDoesTorProvide Other tools include Covercast, which is a 'censorship circumvention system that broadcasts the content of popular websites in real time, encrypted videos streams on common live-streaming services such as YouTube'. See Richard McPherson, Amir Houmansadr, and Vitaly Shmatikov, 'Covertcast: Using Live Streaming to Evade Internet Censorship' *Proceedings on Privacy Enhancing Technologies* 3 (2016) p. 212–225.

[4] Judiciary Committee, 'Hearing on Apple iPhone Encryption'.

[5] WhatsApp, 'End to End Encryption' *WhatsApp Blog* 5th April 2016 Available at https://blog.whatsapp.com/10000618/end-to-end-encryption accessed 5/4/16. Rao, Leena 'WhatsApp Hits 900 Million Users' *Fortune* 4th September 2015 Available at http://fortune.com/2015/09/04/whatsapp-900-million-users/.

[6] Ian Sample, 'Even basic phone logs can reveal deeply personal information' *The Guardian* May 16th 2016 Available at https://www.theguardian.com/science/2016/may/16/even-basic-phone-logs-can-reveal-deeply-personal-information-researchers-find; David Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004) p. 4.

[7] The phrases 'go dark' and 'anonymising technology' will be used very broadly to cover all those technologies that protect the individual's personal data from intelligence access to such an extent that they essentially cannot be forced open through conventional means. This covers the more traditional understanding of the 'dark-web' tools such as Tor and Onion Routing that have created a particular section of cyberspace where online activity is anonymous. But it will also include technology that offers other forms of protection, such as end-to-end encryption used by communication applications or security measures on data storage devices such as mobile phones that prevent outside access and delete the data if force is applied.

[8] Judiciary Committee, 'Hearing on Apple iPhone Encryption', 1st March 2016. Available at http://www.c-span.org/video/?405442-1/hearing-encryption-federal-investigations accessed 1/03/16.

[9] Mauro Conti, Stephen Crane, Tommaso Frassetto, Andrei Homescu, Georg Koppen, Per Larsen, Christopher Liebchen, Mike Perry, and Ahmad-Reza Sadeghi, 'Selfrando: Securing the Tor Browser against De-anonymization Exploits' *Proceedings on Privacy Enhancing Technologies* 4 (2016) p. 454.

[10] TOR, 'Learning more about the GFW's active probing system' The TOR Project 14 September 2015 Available at https://blog.torproject.org/category/tags/china accessed 8th April 2016.

quicker to crack 40-bit encryption.[11] Indeed, 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.[12] 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.[13]

As a result there are important unanswered questions in terms of if and when the individual has the right to erect such immovable barriers, and, as a result, how the state should respond. This paper will argue that privacy is a fundamental interest to individuals and when it falls below a certain level in key areas they are harmed. Also, that anonymising technology offers a way of protecting this privacy and so represents a good in people's lives. Moreover, not only do people have a right to use anonymising technology, but because online privacy is being routinely violated and given that there is a significant mismatch between what people perceive their privacy to be and the reality that surrounds it, it should be made a mandatory feature of cyber-systems. In turn this will raise the bar on people's privacy protections significantly and prevent routine intrusions. However, privacy is part of a matrix of vital interests that individuals have that can occur to different degrees, others include their physical and mental integrity, liberty, self-worth and autonomy, and that in combination they represent an individual's security. Anonymising technology provides more than just privacy, but 'privacy plus'—a set of barriers that make intrusions difficult or near impossible. For the intelligence community this presents a limit on their ability to collect data and prevent threats to people's other vital interest, often their physical integrity. This means that is raises important concerns for the state on how it should react, and given the potential to overreact and unduly harm people's interest in privacy this paper will examine what, if any, are the correct responses to be had by the state when dealing with anonymising technology.

Privacy, security and anonymising technology

The moral value of privacy in cyberspace cannot, and should not, be ignored. While privacy as a concept is extensively discussed, this does not necessarily mean it is particularly cohesive and has a 'bewildering variety of meanings' in both theory and practice.[14] But regardless of whether one considers privacy as being boundaries of protection,[15] or the ability to control information either related to or created by the individual,[16] it is clear that it has fundamental importance to both the individual and society as a whole.[17] At the heart of the moral importance of privacy is the argument that there are some interests that are fundamental to the human condition, pre-requisites to the furthering of an individual's interpretation of the good life. Joel Feinberg calls these requirements 'welfare interests' and John Rawls calls them 'primary goods', but essentially they both amount to the same thing, that is, regardless of what conception of the good life the individual holds, these preconditions must be satisfied first in order to achieve them.[18] If these vital interests fall below a threshold level, the ability to realise their

[11] Andrew Griffin, 'WhatsApp end-to-end encryption update might have made chat app illegal in India' *Independent* 8th April 2016 Available at http://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-end-to-end-encryption-update-might-have-made-chat-app-illegal-in-india-a6974921.html accessed 8th April 2016.

[12] Gordon Rayner, '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.

[13] Tim Cook, 'A Message to Our Customers' *Apple* 16th February 2016 Available at http://www.apple.com/customer-letter/.

[14] Niel Richards *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (New York: Oxford University Press, 2015) p. 8.

[15] Anita Allen, *Uneasy Access: Privacy for Women in a Free Society* (Totowa, N.J.: Rowman and Littlefield, 1988); L. Brandeis and S Warren, 'The Right to Privacy' *The Harvard Law Review* 4/5 (1980) pp. 193–220; P. Fairfield, *Public/Private* (2005) p. 15; Ruth Gavison. 'Privacy and the Limits of the Law' *Yale Law Journal* 89 (1980), pp. 421–471; Adam Moore 'Privacy: Its Meaning and Value' *American Philosophical Quarterly*, 40 (2003) pp. 215–227; Sissela Bok, '*Secrets: On the Ethics of Concealment and Revelation*' (New York: Pantheon, 1982).

[16] G. Stoney Alder, Marshall Schminke, and Terry W. Noel, 'The Impact of Individual Ethics on Reactions to Potentially Invasive HR Practices' *Journal of Business Ethics*, 75/2 (2007) pp. 201–214; James Boyle, *Shamans, Software and Spleens: Law and the Construction of the Information Society* (Cambridge, Mass.; London: Harvard University Press, 1997) p. 54; Jerry Kang, 'Information Privacy in Cyberspace Transactions' *Stanford Law Review* 50/4 (1998) p. 1207; Edward Shils, 'Privacy: Its Constitution and Vicissitudes' *Law and Contemporary Problems* 31/2 (1966) p. 290; Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967).

[17] David Bazelan, 'Probing Privacy' *Georgia Law Review* 2/1 (1997) p. 588; Diane P. Michelfelder, 'The moral value of informational privacy in cyberspace' *Ethics and Information Technology*, 3, (2001) pp. 129–135; William Parent, 'Privacy, Morality and the Law' *Philosophy and Public Affairs* 12/4 (1983) p. 276; David Solove, 'Conceptualising Privacy' *California Law Review* 90/4 (2002) p. 1143; Michael Weinstein 'The Uses of Privacy in the Good Life' in *Privacy: Nomos XIII* edited by Pennock, J. R. and Chapman, J. W. (New York: Atherton Press, 1971) p. 99; Alan Westin, *Privacy and Freedom* (1967) p. 34.

[18] Joel Feinberg, *Moral Limits of the Criminal Law: Vol. 1 Harm to Others* (Oxford: Oxford University Press, 1984) p. 37; John Rawls, *Theory of Justice* (Cambridge: Harvard University Press, 1971) p. 62.

more ultimate needs, goals or activities become dramatically hindered. In this way, these interests are the most important interests a person has, and thus demand protection. These vital interests include the need for physical and psychological integrity, liberty, autonomy, a sense of self-worth, and privacy. These vital interests are ends in themselves and are intrinsically valuable to the individual. The value of these interests is such that, as Feinberg argues, wronging them, even though someone might not directly experience it, means the individual is still harmed. For example, a camera inside an individual's home constitutes a violation of his interest in privacy even if he is not aware of it and so does not 'feel' it in a 'tangible or material way'.[19] In addition, many interests are interrelated and can play an important role in each other's realisation. For example, privacy is necessary in order for individuals to relax, find emotional release, self-reflection and self-analysis, all key in maintaining psychological and emotional health.[20] Equally, Beate Rossler argues that 'ensuring autonomous life and behaviour… can only be successfully developed if there are protected private realms and dimensions in one's life'.[21] In addition, privacy plays an important part in both promoting and maintaining the individual's social role, facilitating social cohesion as individuals need a society with properly functioning privacy norms and rules to aid their interactions and to carry out their interests. As Raab argues, privacy represents a '"constitutive public good": a societal good, understood as an integral and essential element of society itself'.[22] As social beings privacy represents an important means through which the individual interacts with society, helping them determine what, if and when they reveal about themselves as well as forming a key part of their political expression and interaction.[23]

Understanding the value of privacy—as well as other vital interests—is important as it shapes the value that security has both for the individual and society as a whole. While Zedner is correct in that security is another 'promiscuous concept'[24]—ranging in content, referent object and means of provision[25]—the value of security, and from there the right or expectation to have security, for this paper is directly linked to the value that an individual has in maintaining their vital interests.[26] That is, security is the condition by which one's vital interests are maintained and protected. This means contemplating security as the processes and protections designed to maintain people's vital interests. For example, at its core the vital interest in maintaining one's physical integrity gives rise to the understanding of security as personal safety, thus 'usually understood to refer to the protection against physical or other harm' and to provide security therefore includes 'the prevention of or resilience against deliberate attack'.[27] Or, in terms of privacy, security refers to the protections one has, both physically and symbolically, that prevent outsiders from intruding on private spaces or accessing personal information without authorisation.

What this means for national security is that it has value in terms of protecting the individual's vital interests as well as the health of the political community as an important means through which the individual enacts or realises both vital and further interests. As Adam Moore argues, 'we value national security, not because some specific political union is valuable in itself, but because it is a necessary part of protecting individual rights'.[28] The value of the state, and the need for national security, is therefore drawn from the value of those individuals it is charged with protecting: 'whatever

[19] Joel Feinberg, *Harm to Others* (1984) p. 35.

[20] See Alan Westin, *Privacy and Freedom* (London: Bodley Head, 1967) p. 34; Bazelan, D. 'Probing Privacy' *Georgia Law Review* Vol. 2 No. 1 (1997) p. 588; M. A. Weinstein, 'The Uses of Privacy in the Good Life' in *Privacy: Nomos XIII* edited by Pennock, J. R. and Chapman, J. W. (New York: Atherton Press, 1971) p. 99.

[21] Beate Rossler, *The Value of Privacy* (John Wiley & Sons, 2015) p. 72; Also see Boudewijn de Bruin, 'The liberal value of privacy' *Law and Philosophy*, 29/5 (2010) p. 513; Andrei Marmor, 'What is the right to privacy?' *Philosophy & Public Affairs*, 43/1 (2015) p. 10.

[22] Charles D. Raab 'Security, Privacy and Oversight' in Neal, A. W. (ed.) *Security in a Small Nation: Scotland, Democracy, Politics* (Open Book Publishers, 2017) p. 87.

[23] Charles D. Raab 'Security, Privacy and Oversight' (2017) p. 87; Anita Allen *Privacy Law and Society* (Minneapolis: West/Thomson Reuters, 2011) p. 7–9.

[24] Lucia Zedner, *Security (Key Ideas in Criminology)* (London: Routledge, 2009), p. 9.

[25] For work on 'security studies' and the changes in referent object, the construction of security threats and security actors see Barry Buzan, Ole Waever and Jaap De Wilde, *Security: A New Framework for Analysis* (Boulder: Lynne Rienner, 1998); Christopher Browning and Matt McDonald, 'The Future of Critical Security Studies: Ethics and the Politics of Security' *European Journal of International Relations* (2011): 1–21; Peter Katzenstein (ed.) *The Culture of National Security: Norms and Identity in World Politics* (New York: Columbia University Press).

[26] For more on there being a 'right' to security see: Liora Lazarus 'Mapping the Right to Security' in Benjamin J. Goold and Lazarus L. (eds.) *Security and Human Rights* (Hart Publishing, Oxford, 2007); Liora Lazarus 'The Right to Security—Securing Rights or Securitising Rights' in R Dickinson et al. (eds.), *Examining Critical Perspectives on Human Rights* (Cambridge: Cambridge University Press, 2012).

[27] Bruce Schneier, *Beyond fear. Thinking Sensibly About Security in an Uncertain World* (Berlin: Springer, 2006) p. 12. This is different from the instrumentalist arguments made by people such as Henry Shue whereby security is necessary for the enjoyment of other rights. See Liora Lazarus 'The Right to Security—Securing Rights or Securitising Rights' in Dickinson R. et al. (eds), *Examining Critical Perspectives on Human Rights* (Cambridge: Cambridge University Press, 2012).

[28] Adam Moore, 'Privacy, Security, and Government Surveillance: Wikileaks and the New Accountability', *Public Affairs Quarterly*, 25/2 (2011), p. 142.

rights and privileges states have, they have them only in so far as they thereby serve individuals' fundamental interests'.[29] Indeed, Ross Bellaby argues that the ethical value found within intelligence activity comes from their role in protecting the individual and the political community and this end shapes what activities they can justly carry out.[30] The state and its institutions therefore has value as the most current and appropriate means by which an individual's vital interests are protected and allowed to flourish, as well as the most suitable representation of the political community.

This means that narratives that portray security and liberties as opposing qualities that must be traded or balanced, while pervasive, are dangerous.[31] By framing it as a trade-off between privacy and security, where you can have either security or privacy but not both and, importantly, where security is seen as a trump card,[32] 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'.[33] While Jeremy Waldron warns that even these framings are problematic in terms of unequal distribution of the trade-off, unclear returns for any given exchange and the problem of trading liberties at will,[34] it is argued here that these framings fails to see how the matrix of vital interests should be taken as a whole, viewed holistically in order to provide an individual with enough of his vital interests that he can carry out his goals, and therefore be deemed secure. This means that 'the overlapping or even isomorphic relationship between privacy and security is far more subtle than it might be imagined, and cannot be glossed over by a rhetoric of 'opposed' rights or values of security and privacy'.[35]

Security is therefore not separate from people's interests, but an overarching formula by which they are ensured, and the role of the state is to negotiate the tensions between the various vital interests and seek to provide the necessary protections so that individuals can fulfil their own version of the good life. Indeed, a 'defining characteristic of liberal societies is that they provide their citizens with possibilities for living their life in accordance with their own particular ideas of the individual good'.[36] This involves both limiting and licensing the power of the state, something expressed through the social contract that outlines the agreement of rational individuals to sacrifice some of their freedoms in return for the state's duty to protect their vital interests. Through public deliberation and debate these various vital interests are negotiated between people within a political community, holding the state to account in both its own coercive power over the population as well as in terms of its obligation to provide the necessary security.[37] This relationship and the limit/licensing power of state is then manifested in terms of human rights legislation which enable individuals to hold the state to account and its duty to secure those conditions.

In calculating how the different vital interests interact it is important to understand that they are not binary, whole one min and utterly destroyed the next, but exist to varying degrees given the context. The negotiation therefore involves understanding which and to what extent both the state and a perpetrator are threatening vital interest(s). As a process this involves, first, all other things being equal, understanding what vital interests are under threat as some interests such as physical and mental integrity can take precedence over the other interests such as autonomy, liberty, self-worth or privacy.[38] Berlin declared that liberty and autonomy are

[29] Cecile Fabre, 'Cosmopolitanism, Just War Theory and Legitimate Authority' *International Affairs* 84/5 (2008): p. 964.

[30] Ross W. Bellaby, *The Ethics of Intelligence: A New Framework* (London: Routledge, 2014).

[31] Jeremy Waldron 'Security and Liberty: The Image of Balance' *The Journal of Political Philosophy* 11/2 (2003) pp. 191–210; David Pozen, 'Privacy-Privacy Tradeoffs' *The University of Chicago Law Review*, 83/1 (2016), pp. 221–247; Robert McArthur, 'Reasonable Expectations of Privacy' *Ethics and Information Technology*, 3 (2001) pp. 123–128.

[32] Paul B. Thompson 'Privacy, secrecy and security' *Ethics and Information Technology* 3 (2001) pp. 13–19; Tiberiu Dragu, 'Is There a Trade-off between Security and Liberty? Executive Bias, Privacy Protections, and Terrorism Prevention' *The American Political Science Review*, 105/1 (2011), pp. 64–78; Derek E. Bambauer, 'Privacy Versus Security', *The Journal of Criminal Law and Criminology*, 103/3 (2013) pp. 667–683. For arguments against security necessarily trumping privacy see Adam Moore, 'Privacy, Security, and Government Surveillance: Wikileaks and the New Accountability', *Public Affairs Quarterly*, 25/2 (2011) pp. 141–156. Arguments for security trumping privacy see Ken Himma, 'Privacy vs. Security: Why Privacy Is Not an Absolute Value or Right' *San Diego Law Review*, 44, (2007) p. 857.

[33] Tiberiu Dragu 'Is There a Trade-Off Between Security and Liberty? Executive Bias, Privacy Protections, and Terrorism Prevention' American *Political Science Review* 105/1 (2011) p. 64–78; Also see Bruce Ackerman *Before the Next Attack: Preserving Civil Liberties in the Age of Terrorism* (New Haven, CT: Yale University Press, 2006); Russell Hardin, 'Civil Liberties in the Era of Mass Terrorism' *Journal of Ethics* 8/1 (2004) p. 77–95.

[34] Jeremy Waldron, 'Security and Liberty: The Image of Balance' *Journal of Political Philosophy* 11/2 (2003) pp. 191–210.

[35] Charles D. Raab 'Security, Privacy and Oversight' in Neal, A. W. (ed.) *Security in a Small Nation: Scotland, Democracy, Politics* (Open Book Publishers, 2017).

[36] Beate Rossler, *The Value of Privacy* (John Wiley & Sons, 2015) p. 43.

[37] John Rawls *Lectures on the History of Political Philosophy*, Samuel Freeman (ed.), (Cambridge, MA: Harvard University Press, 2007) p. 226.

[38] Berlin declared that in much the same way that boots were more important than the words of Shakespeare, liberty and autonomy are not necessarily the total first needs of an individual. Isaiah Berlin, *Four Essays on Liberty* (Oxford: Oxford University Press, 1969), p. 124.

not necessarily the first need of an individual: 'the peasant needs clothing or medicine before, and more than, personal liberty'.[39] This is not to say that the other vital interests are not truly vital, for they are, but without physical and mental integrity the individual's interest in autonomy, liberty, self-worth or privacy can become redundant. Secondly, depending on the context the severity of the violation needs to be taken into account. Indeed, Nissenbaum argues for a context analysis of privacy where different social, structural or normative understandings of privacy can be enacted through people's daily lives, which can overlap and come into conflict.[40] For example, privacy can be perceived as consisting of different levels where the more personal or intimate the information the greater the expectation of privacy.[41] Therefore there must be a greater threat to someone's other vital interests to justify the privacy intervention. Importantly, the point of 'other things being equal' demonstrates that the degree of harm caused is dependent on all aspects brought together. For example, saying that the interest in physical integrity is more important than autonomy is done while the severity or context of the violation is equal. It would be folly to argue that a prick on the finger is more harmful than being locked away for 20 years simply because it was a physical attack. Significantly, vital interests make a chain whereby the whole is no stronger than its weakest link.[42] This means an excess of one will not necessarily make up for the lacking of another interest: all the self-worth in the world 'will not help you if you have a fatal disease and great physical strength will not compensate for destitution or imprisonment'.[43] So an excess of physical security cannot be used as a justification for undermining people's privacy; it cannot be argued that people are physically very safe in exchange for having no privacy. In making this negotiation it needs to be understood whether the target has acted in some way to waive or forfeit their immediate vital interest protects; if there is a threat to the vital interests of another to a greater degree or in a more fundamental way; and that people's vital interests being provided for to a minimum standard.

So in making this calculation it should be understood that the value of privacy in cyberspace is significantly high. By viewing 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. Access to URL information (even restricted to before the first/slash), for example, can reflect intimate details about a person's life such as an individual's 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.[44] Indeed, arguments have been made that unauthorised access to this data represents a serious violation of someone's privacy 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 data sets—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. [45]

Therefore people can expect a significant degree of protection around their online activity. The implications of anonymising technology, however, are striking as it provides 'privacy-plus'; warrant proof spaces where a higher level of protection is achieved. Anonymising technology such as TOR and auto-deletes undermines the ability of the state to collect intelligence and in doing so hampering its ability to detect, locate and prevent a range of potential threats. However, even though these protections will hinder the intelligence community's abilities, from the point of view of the individual this does not diminish their right to establish whatever privacy protection they see fit. Judith Thomson gives the example whereby if an individual wishes to put something precious to him in a safe to prevent others from looking at it, then it is his right to do so, and indeed represents a clearer demonstration that he wishes to stop others

[39] Isaiah Berlin, *Four Essays on Liberty* (1969) p. 124.

[40] Helen Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Standford Law Books, 2009) p. 127.

[41] Gary Marx, 'Some Concepts that May be Useful in Understanding the Myriad Forms and Contexts of Surveillance' *Intelligence and National Security* 19/2 (2004) p. 234; and Andrew von Hirsch, 'The Ethics of Public Television Surveillance' in *Ethical and Social Perspectives on Situational Crime Prevention* edited by Hirsch, A., Garland, D. and Wakefield, A. (Oxford: Hart Publishing, 2000) pp. 59–76.

[42] Feinberg, J. *Harm to Others* (1984) p. 37; Nicholas Rescher, *Welfare: The Social Issue in Philosophical Perspective* (Pittsburgh: University of Pittsburgh Press, 1972) p. 5.

[43] H. E. Baber, 'How Bad is Rape' *Hypatia* 2/2 (1987) p. 129.

[44] Gary Marx, 'Some Concepts that May be Useful in Understanding the Myriad Forms and Contexts of Surveillance', Intelligence and National Security, 19/2, 2004, p. 234; Andrew Hirsch 'The Ethics of Public Television Surveillance' in *Ethical and Social Perspectives on Situational Crime Prevention* edited by Hirsch, A., Garland, D. and Wakefield, A. (Oxford: Hart Publishing, 2000) pp. 59–76.

[45] Robert L. McArthur 'Reasonable Expectations of Privacy' *Ethics and Information Technology* 3 (2001) pp. 123–128; Charles Fried, 'Privacy: A Moral Analysis' *Yale Law Review* 77/1 (1969) p. 475; Hyman Gross, 'Privacy and Autonomy' in *Privacy: Nomos XIII* edited by Pennock, J. R. and Chapman, J. W. (New York: Atherton Press, 1971) p. 169; P. J. Steinberger, 'Public and Private' *Political Studies* 47/2 (1999) p. 292.

from looking at what he owns. Breaking in would be a clear violation of his privacy.[46] Moreover, when individuals lock away their private items it is not done in the knowledge 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.[47] What this means is that the state must be able to prove why particular individuals are warranted for surveillance—probably cause/balance of probabilities for example—to justify its coercive powers. Any method that relies or uses bulk rather than targeted surveillance would fail this requirement. 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

Therefore, there is clearly an argument that can be made that people have the right to use anonymising technology despite it creating near impenetrable protections. This argument, however, can be pushed one step further 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 include defences that automatically and systematically anonymise an individual's identity and activity whether or not they have expressed an explicit desire. While such an argument might raise liberal concerns regarding overreach and interference in people's lives, understanding such paternalist concerns can help highlight why there is a need for such interventions.

Broadly speaking the paternalism literature is extensive and wide-ranging, crossing philosophy,[48] political theory,[49] law,[50] and economics,[51] though as a general definition paternalism is the 'interference with a person's liberty of action justified by reasons referring exclusively to the welfare, good, happiness, needs, interests or values of the person being coerced';[52] or 'that it involves acting towards people in a way that promotes their own best interest whether or not they see this themselves'.[53] While some argue that this interference is unjustified because it is infantilising to the individual,[54] most state the problem as the 'violation of the person's autonomy'[55] or liberty as the ability for the person to chose their own destiny and carry it out is circumvented.[56]

However, these concerns surrounding autonomy can be used to highlight why there is a need for mandatory anonymous technology. First, if the main concern about paternalism is the impact on people's autonomy then the context of the interference becomes important. Autonomy is another vital interest and broadly speaking is the capacity

[46] Judith Jarvis Thomson, 'The Right to Privacy' *Philosophy and Public Affairs* 4/4 (1975) p. 298–303.

[47] Lucia Zedner 'Pre-Crime and Post Criminology' *Theoretical Criminology* 11/2 (2007) 265; David Solove 'I've Got Nothing to Hide and Other Misunderstandings of Privacy' *San Diageo Law Review*, 44, (2007) p. 748.

[48] Gerald Dworkin, 'Paternalism' in *Philosophy, Politics and Society: Fifth Series*, in Laslett P. and Fishkin J. (eds.) (Basil Blackwell, 1979); Joel Feinberg, 'Legal Paternalism' in *Paternalism*. R. Sartorius (ed.). (University of Minnesota Press, 1983).

[49] Albert Weale, 'Paternalism and Social Policy' *Journal of Social Policy* 7 (1978) pp. 157–172.

[50] Herbert L. A. Hart, *Law, Liberty, and Morality* (Oxford University Press, 1963); Seana Valentine Shriffrin 'Paternalism, Unconscionability Doctrine, and Accommodation' *Philosophy & Public Affairs* 29/33 (2000) p. 205–250; Paul Burrows, 'Analyzing Legal Paternalism,' *International Review of Law and Economics* 15 (1995) pp. 489–508; Duncan Kennedy, 'Distributive and Paternalist Motives in Contract and Tort Law, with Special Reference to Compulsory Terms and Unequal Bargaining Power' *Maryland Law Review* 41 (1982) pp. 563–658; William Glod 'Political Liberalism, Basic Liberties and Legal Paternalism' *The Southern Journal of Philosophy* 48/22 (2010) pp. 177–196.

[51] Paul Burrows, 'Analysing Legal Paternalism' International Review of Law and Economics 15 (1995) pp. 489–450.

[52] Gerald Dworkin, 'Paternalism' in *Mill's On Liberty: Critical Essays* edited by G. Dworkin (Roman and Littlefield Publishers: Plymouth, 1997) p. 62.

[53] Peter Hobson, 'Another Look at Paternalism' *Journal of Applied Philosophy*, 1/2 (1984) pp. 293–304.

[54] Peter de Marneffe, for example, suggests paternalism is insulting as it substitution of the target's judgement; while X characterises paternalism as treating another 'like a child or someone who cannot be trusted to look after their own good' Peter de Marneffe, 'Avoiding Paternalism *Philosophy & Public Affairs'* 34 (2006) p. 68. Or as Anderson more bluntly puts it, paternalism involves 'effectively telling citizens that they are too stupid to run their own lives'. Elizabeth Anderson, 'What Is the Point of Equality?' *Ethics* 109 (1999) p. 301.

[55] Gerald Dworkin *The Theory and Practice of Autonomy* (Cambridge: Cambridge University Press, 1988) p. 123.

[56] Shane Ryan 'Paternalism: An Analysis' *Utilitas* 28/2 (2016) pp. 123–135; Gerald Dworkin *The Theory and Practice of Autonomy* (Cambridge: Cambridge University Press, 1988) p. 123.

for self-rule, that one must be able to decide for oneself, without external manipulation or interference, what shape one's own life will take. As Nussbaum puts it, autonomy is being able to 'form a conception of the good and to engage in critical reflection about the planning of one's life—the protection of the liberty of conscience'.[57] This requires that the individual's ability to function rationally is protected; that the individual has the capacity to plan, choose, and reflect on options in terms of arguments, evidence and potential choices so as to make a decision; and can do it without excessive influence or control from another.[58] While anti-paternalism seeks to prevent interference with another's autonomy, even for their benefit, those who lack the capacity for critical self-reflection whether it is due to an absence or reduced knowledge or ability—such as children or those who are physically or mentally unable—they are incapable of understanding what is in their best interests and so need paternalistic help to ensure they are protected. For example, Mill, on the subject of how long should children have their decision-making ability limited by parents, sets the limit as once the children are 'capable of being improved by free and equal discussion'.[59] As Feinberg puts it, interventions in only non-voluntary self-regarding actions do not affect people's autonomy and should not be considered as paternalistic at all.[60] Pro-paternalists, therefore, shape the justification and need for intervention in terms of the lack of information had by the individual—their ignorance or ability to understand what information they are given—or their hypothetical consent. That is, if individuals do not have the full facts before them or could not reasonably be able to comprehend its meaning then they are unable to make an informed decision; their capacity to reflect on options available to them and determine for themselves what the most appropriate version of the good is prevented and they are therefore unable to act autonomously. Indeed, in Mill's example where we witness someone about to cross a dangerous bridge and we intervene to turn them back there is no 'real infringement of his liberty' as they are not aware of the structural weakness and it would not be their desire to fall.[61] In fact, it can be argued lacking in the capacity for full autonomy demands an obligation on others to help provide or facilitate their realisation of a good life, whether the support is physical or in aiding in the necessary rational, critical reflection.[62] Bill New expands this ignorance to include 'failures of reasoning' highlighting the technical inability to complete or understand the issues involved, a weakness of will, the distortive effect of emotions, and a lack of knowledge or experience.[63] Feinberg further argues that the intervention is required until the target is adequately informed, and if they continue to be mistaken the intervention must continue until they realize their error.[64] If an individual lacks autonomy then they are being harmed and so it is required that they be aided in order to restore their autonomy and stop the harm they are suffering under.

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. The first aspect of this argument is the general ignorance of people; that there is a significant disconnect between the sort of privacy people think they have and what is provided, as well as a

[57] Martha Nussbaum, *Women and Human Development* (2000) p. 79. Feinberg calls this the 'Condition of self-government', and Richard Lindley refers to it as 'authorship' and 'self-rule', but it is essentially referring to the same phenomenon. See Joel Feinberg, 'The Idea of a Free Man' in *Educational Judgments: Papers in the Philosophy of Education* edited by Doyle, J. F. (London: Routledge, 1973) pp. 143–165; R. Lindley, *Autonomy* (Basingstoke: Macmillan, 1986).

[58] H. Frankfurt, 'Freedom of the Will and the Concept of the Person', *Journal of Philosophy* 68/1 (1971) p. 7.

[59] See John Kleinig *Paternalism* (Manchester University Press, 1983) p. 146.

[60] Joel Feinberg, *Moral Limits of the Criminal Law: Vol. 3 Harm to self* (Oxford: Oxford University Press, 1986) p. 12; Heidi Malm, 'Feinberg's Anti-Paternalism and the Balancing Strategy' *Legal Theory* 11 (2005) p. 194; Bill New, 'Paternalism and Public Policy' *Economics and Philosophy* 15 (1999) pp. 68–69; Tom Beauchamp, 'Paternalism and Biobehavioral Control' *Monist* 60 (1977) p. 67.

[61] John Stuart Mill, "On Liberty", *Utilitarianism, Liberty and Representative Government* (New York: Dutton, 1910), ch. iv.

[62] This argument turns from the paternalist literature to the good Samaritan one where, arguably, there is a general obligation to help those in need if we can at little cost to ourselves. See John Kleinig, 'Good Samaritanism' *Philosophy and Public Affairs* 5/4 (1976) p. 385; Adam Smith, *The Theory of Moral Sentiments* (Oxford: Clarendon Press, 1976) p. 9; John Rawls, *Theory of Justice* (Cambridge: Cambridge University Press, 1977) p. 111, 152; E. Mack, 'Bad Samaritanism and Causation of Harm' *Philosophy and Public Affairs* 9/3 (1980) p. 235. There is an extensive literature regarding the expectations of the good or minimal Samaritan. Peter Singer, 'Famine, Affluence, and Morality' *Philosophy and Public Affairs* 7/2 (1972) 229–243; Alan Gewirth, *Reason and Morality* (Chicago: University of Chicago Press, 1978) p. 217–230; Patricia Smith, 'The Duty to Rescue and the Slippery Slope Problem' *Social Theory and Practice* 16/1 (1990) p. 19–41; John M. Whelan, 'Charity and the Duty to Rescue' *Social Theory and Practice* 17/3 (1991) p. 441–456; and David Copp, 'Responsibility for Collective Inaction' *Journal of Social Philosophy* 22/2 (1991) p. 71–80. However, while this is a general and arguably weak requirement, stronger obligations can be placed on the state to protect those who it has a duty to protect by virtue of the social contract.

[63] Bill New, 'Paternalism and Public Policy' *Economics and Philosophy* 15 (1999) p. 71–74.

[64] Joel Feinberg, *Moral Limits of the Criminal Law: Vol. 3 Harm to self* (Oxford: Oxford University Press, 1986) pp. 127–128, 130–131.

lack of awareness on the dangers of revealing too much information. This includes a general mismatch between assumed online protections and the realities of cyberspace as well as a specific lack of awareness on the surveillance powers of intelligence actors such as the USA's National Security Agency (NSA) and UK's Government Communications Headquarters (GCHQ).

This includes, first, a lack of awareness over what sort of protections people have when they surf the web, whether in terms of their daily online activity or in regards to their more public facing activities on social media websites such as Facebook.[65] Firstly, evidence shows that people value their online privacy: when the UK public were asked specifically about online privacy in May 2014 they saw this being either 'essential' or 'important' by a very large margin: for web browsing 85% saw privacy as being essential/important; for email content 91% saw privacy as essential/important; while for mobile phone location 79% saw privacy as essential/important. Moreover, the level of public concern about online privacy is reflected in the yearly TRUSTe Privacy Index conducted by Ipsos-MORI, which reported that in 2014 89% were frequently or always worried about their online privacy, which rose to 92% in 2015. [66]

However research also shows that people are unaware of what information is being stored and transmitted. Indeed, there is a significant body of research that reports that in terms of online 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, there was a discrepancy between the level of privacy people expected in terms of who had access to what information and the actual safeguards in place.[67] For example, Jones and Soltren reported that 89% percent of those users surveyed admitted that they had never read the online privacy policy and 91% were not familiar with any of their terms of service.[68] One important part of the problem is that people do not conceive that outside audiences can view their information. Again, even public social media pages—whether Facebook, forums, blogs or web-chats—people see access to their data as being closer to a wall-garden rather than an open field; that is, people believe that their information is only 'visible to the peer group more than to adult surveillance',[69] imaging an ideal audience 'which is often a mirror-image of the user'.[70] There is no expectation that the wider world (ranging from complete strangers, through to corporations and the government institutions) can access their online data, with research showing a particularly strong aversion to authority figures having access.[71] Indeed, the backlash following Edward Snowden's revelations highlight a real lack of knowledge as to the abilities, willingness and drive had by the intelligence community to collect data *en masse*. Even when people reported the recognised need for data to be collected,

[65] Catherine Dwyer, Starr Roxanne Hiltz, and Katia Passerini, 'Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace' *Proceedings of AMCIS* (2007); Sonia Livingstone, '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; Zeynep Tufekci, 'Can you see me now? Audience and Disclosure Regulation in Online Social Network Sites' *Bulletin of Science, Technology & Society* n28/1 (2008) pp. 20–36; Yabing Liu, Krishna Gummadi, Balachander Krishnamurthy, and Alan Mislove 'Analyzing Facebook Privacy Settings: User Expectations vs. Reality'. In *Proceedings of the 2011 ACM SIGCOMM Internet Measurement Conference* (2011) pp. 61–70; Michelle Madejski, Maritza Johnson, and Steven Bellovin, 'A Study of Privacy Settings Errors in an Online Social Network' in *Fourth International Worksop on Security and Social Networking* (pp. 340–345). Lugano, Switzerland.

[66] Vian Bakir, Jonathan Cable, Lina Dencik, Arne Hintz, Andrew Mcstay, 'Public Feelings on Privacy, Security and Surveillance' *A Report by DATA-PSST and DCSS* November 2015. Available at https://sites.cardiff.ac.uk/dcssproject/files/2015/11/Public-Feeling-on-Privacy-Security-Surveillance-DATAPSST-DCSS-Nov2015.pdf p. 6. Also see Jupiter Research, 'Security and privacy data' *Presentation to the Federal Trade Commission Consumer Information Security Workshop*. (2002) Available online at http://www.ftc.gov/bcp/workshops/security/0205201leathern.pdf; Harris, *National Survey on Consumer Privacy Attitudes*. Available at http://www.epic.org/privacy/survey/.

[67] Catherine Dwyer, Starr Roxanne Hiltz, and Katia Passerini, 'Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace' *Proceedings of AMCIS* (2007); Sonia Livingstone, '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; Zeynep Tufekci, 'Can you see me now? Audience and Disclosure Regulation in Online Social Network Sites' *Bulletin of Science, Technology & Society* n28/1 (2008) pp. 20–36.

[68] H. Jones and J. H. Soltren, *Facebook: Threats to Privacy* December 14, 2005. Available at from http://www-swiss.ai.mit.edu/6805/student-papers/fall05-papers/facebook.pdf. Also see Ralph Gross and Alessandro Acquisti, 'Information revelation and privacy in online social networks' P*roceedings of the 2005 ACM Workshop on Privacy in the Electronic Society* (2005) pp. 71–80.

[69] Sonia Livingstone, Taking Risky (2008) p. 396. Also see C. Lampe, N. B. Ellison, C Steinfield, 'Changes in Use and Perception of Facebook' *Proceedings of the ACM 2008 Conference on Computer Supported Cooperative Work* p. 729.

[70] Alixc E. Marwick & danah boyd, 'I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience' *New Media & Society* 13 (2010) p. 7.

[71] See Zeynep Tufekci, 'Can you see me now? Audience and Disclosure Regulation in Online Social Network Sites' *Bulletin of Science, Technology & Society* n28/1 (2008) p p. 34; Scott Lederer, Jason Hong, Anind Dey, and James Landay. 'Personal Privacy Through Understanding and Action: Five Pitfalls for Designers' *Personal and Ubiquitous Computing* 8 (2003) pp. 440–454; Kate Raynes-Goldie. 'Aliases, Creeping, and Wall Cleaning: Understanding Privacy in the Age of Facebook' *First Monday* 15/1(2010) available at http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2775/2432; Bernhard Debatin, Jennette P. Lovejoy, Ann-Kathrin Horn, and Brittany N. Hughes, 'Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences' *Journal of Computer-Mediated Communication* 15/1 (2009) pp. 83–108.

often it was assumed that it would be other people's data and not their own being amassed, and responses have thus been that the NSA had gone too far in both the breadth of surveillance carried out and depth of information collected.[72] It is therefore not surprising that Snowden's revelations received significant shock in terms of the level and pervasiveness of the NSA surveillance apparatus and sparked demands to review surveillance powers.[73]

Another problem is that in addition to the harm caused by violating people's intrinsically valuable privacy, people are unaware of the instrumental danger that access to private online information can represent, including 'damaged reputation… unwanted contact and harassment or stalking, surveillance like structures due to backtracking functions, use of personal data by third parties, and hacking and identity theft';[74] while there are additional concerns over the dangers of state surveillance in the form of a panoptic 'chilling effect' that deters internet users from engaging in their online activities because of the fear caused by the belief they are being watched and the negative impact this can have on freedom of expression and the realisation of people's autonomy.[75] Therefore, anonymising technology would promote a realm of greater autonomy exploration as people's actions would be unmonitored and so they would not have to worry about a panoptic gaze. This works well for one of the concerns of many liberal and anti-paternalist theorists on the stifling effect outside intervention can have as particular standards of 'correct', 'right' or 'true' are imposed. What anonymising technology creates is a more open space for individuals to explore these issues themselves. Therefore, the technology not only restores people's lost privacy but also their lost autonomy.

Moreover, even when there are instances where individuals have consented to access to their information—in terms of HTTP cookies (also known as browser cookies or just cookies) or accepting website 'terms and conditions' for example—there are significant technical barriers to understanding that limit the user's ability to fully comprehend what it is they are agreeing to. For example, cookies are packets of information shared between user and websites on their activities, and even though the EU determined that websites should requests consent on their use, there is not sufficient information provided and understanding required by the user for it to meet the standard of informed consent.[76] Equally, when terms and conditions are presented to users before they can access various online content, their 'web-wrap' or 'shrink-wrap' nature raises concerns about how informed the user truly is.[77] In both instances, the pervasive and habitual nature of agreeing to the terms coupled with the lack of technical understanding and opportunity to reflect would fail an informed consent standard.[78]

Finally, people are already having their autonomy impacted when it comes to determining what privacy protections they should erect given the existing pressures and

[72] Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, R. B. J. Walker 'After Snowden: Rethinking the Impact of Surveillance' *International Political Sociology* (2014) 8 pp. 121–144; George Lucas, 'NSA Management Directive #424' *Ethics and International Affairs*, 28/1, (2014) p. 31; Michael Kelly, 'NSA: Snowden Stole 1.7 MILLION Classified Documents And Still Has Access To Most Of Them,' *Business Insider*, 13 December 2013, http://www.businessinsider.com/how-many-docs-did-snowden-take-2013-12 accessed 14 May 2014.; *The Washington Post*, 'NSA Slides Explain the PRISM Data-Collection Program', 10 July 2013 available at http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ accessed 14/05/14.

[73] Sari Horowitz and William Branigin, 'Lawmakers of Both Parties Voice Doubts about NSA Surveillance Programs' *The Washington Post* July 17th 2013; Nick Hopkins and Matthew Taylor 'David Blunkett Calls for Urgent Review of Laws Governing Security Services' *The Guardian* 4th Nov 2013.

[74] danah boyd, and Nicole Ellison, 'Social Network Sites: Definition, History, and Scholarship' *Journal of Computer-Mediated Communication* 13 (2008) pp. 210–230. For work on third party access and the creation of digital profiles without the users awareness see Ralph Gross and Alessandro Acquisti, 'Information Revelation and Privacy in Online Social Networks' P*roceedings of the 2005 ACM Workshop on Privacy in the Electronic Society* (2005) pp. 71–80. For work on people's lack of awareness of the dangers Bernhard Debatin, Jennette P. Lovejoy, Ann-Kathrin Horn, Brittany N. Hughes 'Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences' *Journal of Computer-Mediated Communication* 15 (2009) p. 83–108.

[75] By August 2013 Germany and Brazil led the need for UN General Assembly resolution based on both the right to respect privacy and the right to freedom of expression as outlined in the Universal Declaration and International Covenant on Civil and Political Rights 1966 (ICCPR), arguing that if people are subjected to en masse surveillance the affect on their autonomy would be such that they would not be able to express themselves freely. Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, R. B. J. Walker 'After Snowden: Rethinking the Impact of Surveillance' *International Political Sociology* (2014) 8 p. 133. Also see Titus Stahl, 'Indiscriminate Mass Surveillance and the Public Sphere', (2016) *Ethics and Information Technology* 18/1 pp. 33–39.

[76] Vicki Ha, Kori Inkpen, Farah Al Shaar, Lina Hdeib, 'An Examination of User Perception and Misconception of Internet Cookies' in *Proceedings from CHI 2006 Extended Abstracts on Human Factors in Computing Systems*, (2006); Stephan Haller, Stamatis Karnouskos, Christoph Schroth 'The Internet of Things in an Enterprise Context' in Domingue J., Fensel D., Traverso P. (eds) *Future Internet—FIS 2008* Vol. 5468 (Berlin and Heidelberg: Springer; 2009); Edewede Oriwoh, Paul Sant, Gregory Epiphaniou, 'Guidelines for Internet of Things Deployment Approaches—The Thing Commandments' *Procedia Computer Science* 21 (2013) pp. 22–31; Luigi Atzori, Antonio Iera, Giacomo Morabito, 'The Internet of Things: A Survey' *Comput Netw* 54 (2010) pp. 2787–805.

[77] Jennifer Femminella 'Online Terms and Conditions Agreements: Bound by the Web' *Journal of Civil Rights and Economic Development* 17/1 (2003) pp. 87–126.

[78] See Ruth Faden and Tom Beauchamp *A History and Theory of Informed Consent* (New York: Oxford University Press, 1986).

biases that distort their decision-making processes. That is, if people existed in a neutral position, able to critically reflect on their own desires and needs with all the relevant information then they would be able to make an autonomous decision, but because cyber-systems—web browsers, settings, data agreements—exist in a complex set of arrangements people are already being interfered with. Indeed, behavioural economics and cognitive psychology have extensively outlined the distortive effect that defaults and framings can have on people without them consciously realising it.[79] It is not surprising, therefore, that there has been a turn in the literature towards 'libertarian paternalism' to counter such biases, argued for by Cass Sunstein and Richard Thaler who outlined a 'relatively weak and non-intrusive type of paternalism'.[80] Taking the 'presumption that individual choices should be respected is often based on the claim that people do an excellent job of making choices that promote their welfare, or at least better than third parties could do' is flawed given that there is 'little empirical evidence to support this claim'.[81] External influencers are already in existence that distorts the decision-making process. Given this it is not inconsistent to have a libertarian paternalist position that moves people in the direction that will make their lives better—resetting a default position or encouraging a particular decision—while not shutting down or blocking alternatives. As Anita Allen argues, 'governments should not mandate, block… injurious choices… but should nudge' and that 'in the absence of such intervention by government or the private sector it is predictable that people will fall prey to the perils of procrastination, self-control, information deficits, overreliance on rules of thumb, and cognitive biases'.[82] People are not always consciously aware that they would have to alter their privacy settings from the defaults, which is especially problematic given that these settings are predominantly set to being more open than closed and that the procedures for changing these settings have been reported as being too difficult, time-consuming, or obscure for people to enact on a regular basis.[83] Indeed, in surveys the default setting have reportedly only matched 39% of people's expectations, with a minority of people thinking or knowing how to change their privacy settings. [84]

An argument can therefore be made that people would consent to the intervention. Indeed, generally we 'call a policy paternalist only if it makes you behave differently than you would have otherwise'.[85] That is, 'As a general matter, A isn't acting paternalistically toward B if B consents to A's action'.[86] If the clearest cases of paternalism involve an interference (forcibly or non-forcibly) with the individual's autonomy, then it would be inconsistent to claim that if the target's autonomous decision is to agree then it is not paternalistic.[87] Interferences that are inline with an individual's will do not violate their autonomy. The debate, therefore, rests more on whether there is a hypothetical, assumed, implicit or forthcoming consent.[88] For example, 'hypothetical consent' is that whereby if the situation is 'such that it could be said that any rational person would consent to the interference if he knew the relevant facts' can be used to justify interventions on the assumption that it would not

[79] Richard H. Thaler and Cass Sunstein, *Nudge: Improving Decisions About Health, Wealth and Happiness* (New Haven: Yale University, Press 2008) p. 7. Also see Cass Sunstein and Richard H. Thaler, 'Preferences, Paternalism and Liberty' in Olsaretti, S. (ed) *Preferences and Well-Being* (Cambridge: Cambridge University Press, 2006) pp. 233–264; Daniel Kahneman, Jack L. Knetsch, and Richard H. Thaler 'Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias' *Journal of Economic Perspectives* 5/1 (1991) p. 197.

[80] Richard H. Thaler and Cass Sunstein, *Nudge: Improving Decisions About Health, Wealth and Happiness* (New Haven: Yale University, Press 2008) p. 5.

[81] Cass Sunstein and Richard H. Thaler, 'Preferences, Paternalism and Liberty' in Olsaretti, S. (ed) *Preferences and Well-Being* (Cambridge: Cambridge University Press, 2006) p. 237.

[82] Anita Allen, *Unpopular Privacies: What Must We Hide?* (Oxford: Oxford University Press, 2011) p. 13.

[83] See Krisna Gummadi, Balachander Krishnamurthy and Alan Mislove, 'Addressing the Privacy Management Crisis in Online Social Networks' in *Proceedings of the IAB workshop on Internet privacy*, (2010) p. 1; K. Lewis, J. Kaufman, and N. Christakis, 'The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network' *Computer-Mediated Communication*, 14/1 (2008) pp. 79–100.

[84] Yabing Liu, Krishna Gummadi, Balachander Krishnamurthy, and Alan Mislove 'Analyzing Facebook Privacy Settings: User Expectations vs. Reality'. In *Proceedings of the 2011 ACM SIGCOMM Internet Measurement Conference* (2011) p. 62; and Bernhard Debatin, Jennette P. Lovejoy, Ann-Kathrin Horn, and Brittany N. Hughes, 'Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences' *Journal of Computer-Mediated Communication* 15/1 (2009) pp. 83–108.

[85] Sarah Conly 'Paternalism, Coercion and the Unimportance of (Some) Liberties' *Behavioural Public Policy* 1/2 (2017) pp. 207–218.

[86] Douglas Husak 'Paternalism and Consent' in Miller, F. and Wertheimer, A. (eds) *The Ethics of Consent: Theory and Practice* (Oxford: Oxford University Press, 2009) pp. 107–130.

[87] See Peter Hobson, 'Another Look at Paternalism' *Journal of Applied Philosophy*, 1/2 (1984) p. 294; Gerald Dworkin 'Defining Paternalism' in Coons, C. and Weber, M. (eds) *Paternalism: Theory and Practice* (Cambridge: Cambridge University Press, 2013) p. 29; Richard J. Arneson 'Joel Feinberg and the Justification of Hard Paternalism' *Legal Theory* (2005) 11 (2005) p. 262; Rosemary Carter, 'Justifying Paternalism' *Canadian Journal of Philosophy* 7/1 (1977) p. 134; Douglas Husak 'Paternalism and Autonomy' *Philosophy & Public Affairs* 101 (1981) p. 30.

[88] Various versions of consent as a justification for paternalism are discussed by the following writers: Gerald Dworkin, 'Paternalism' in: Wasserstrom, A. (ed) *Morality and the Law* (Belmont, California, Wadsworth, 1971); Joel Feinberg 'Legal Paternalism' *Canadian Journal of Philosophy* 1/1 (1971) pp. 105–124; Rosemary Carter, 'Justifying Paternalism' (1977) pp. 133–145.

interfere with the rational individual's autonomy.[89] If this is the case then it should be clear by now that given the threat represented to people's privacy both as a result of routine intelligence surveillance and individual systematic ignorance, that there can be an assumed hypothetical consent or even a hypothetical request for intervention.[90] This does not mean that people must have their data eternally protected. In line with the libertarian paternalist argument, the protections should offer a more beneficial status quo for people; they are protected from the outset. But if people wish to move towards a more open system then they could opt to revealing their identity and activity publically, choosing to communicate unencrypted or without going through multiple anonymous nodes. But by shifting systems so that people are anonymous unless they wish otherwise would protect their privacy to a much greater extent. Importantly, this would significantly raise the bar on data collection and prevent *en masse* surveillance techniques. As one of the main concerns raised post-Snowden was the ease with which people's data was accessed as well as the encompassing nature of the data-trawls and by making the access to people's data significantly more difficult the intelligence community would be forced to restrict its efforts to only those cases that really mattered to them, giving them the opportunity to make a clearer case as to why the data is needed.

The state's justified response

The technology needed to protect people's privacy can be quite varied given the range of different ways people have their personal information collected. This should include, for example, preventing access to someone's everyday browsing activity, stored data, and their meta-data including where they have been and with whom they have communication, as well as a shift in the privacy protocols on social media and web-browsers so that the default is set to a closed position, each with the option to move to a more open position if the user wished. Determining who and how this is achieved, however, is difficult. In terms of who should set the standard, a normative argument can be made that the state through human right legislation represents the most appropriate and direct means of initiating change. The state through the social contract has the obligation to protect all vital interests and so has an ethical mandate to establish these systems. Therefore in terms of who should act, the state appears at the top of the list. However, states are unlikely to instigate a change that would significantly limit their own intelligence collection activity.[91] Equally, corporations that rely on selling or utilising people's data are unlikely to limit their own profitability. Therefore, it will fall to those in the middle; those who are not likely to lose profit from such a change and could see the financial or even ethical benefit of offering a more protected system. For example, Apple has already noted the benefit that providing a more secure device to their users in terms of the competitive advantage it would give their product as well as their claimed desire to act ethically and protect people's data. For web browsing, given technical limitations in order to create protections for online surfing two main options present themselves: first, Internet Service Providers should make changes to their infrastructure at the point where an individual accesses the internet, mainly the home router, which would also require the router manufacturer to change the software on their devices. Or secondly, the operating system vendor (Microsoft, Apple, etc.) can initiate protections at the operating systems level. In both of these options there would be significant benefits for these agents to put forward the case for their product offering the user greater privacy.

The individual's right to anonymising technology does not, however, undermine that the state can, when justified, try to circumvent such barriers. It is not being argued that cyber-intelligence is always unjustified. Indeed, when it is charged with protecting the political community from threats the intelligence community can be justified in carrying out their own operations. The state has an ethical obligation to locate and prevent threats to people within the political community, and so some data collection can be justified. However, what is unclear is that given the extra-layers of protection afforded by anonymising technology what new forms of state intervention are justified. Indeed, the state has a limited number of options available, ranging from banning such technology altogether and making its possession or use illegal; forcing companies to leave backdoors for

[89] Danny Scoccia 'In Defense of Hard Paternalism' *Law and Philosophy* 27/4 (2008) pp. 351–381; Jack Lively 'Paternalism' *Royal Institute of Philosophical Supplements* 15 (1983) pp. 147–165. Though some paternalists now argue for a subjective understanding whereby the intervention is consented inline with the individual's particular and personal conception of good rather than that of the paternalist, this arguably increases the chance that the intervention will be inline with the individual's autonomy. See Richard Thaler and Cass Sustein *Nudge: Improving Decisions About Health, Wealth and Happiness* (New Haven: Yale University Press, 2008); Julian Le Grand and Bill New, *Government Paternalism: Nanny State or Helpful Friend* (Princeton, NJ: Princeton University Press, 2015).

[90] Consent and requests for intervention are essentially opposite sides of the same coin. Paternalism assumes a drive for intervention for people's own good—in this case the need for more online privacy protections—and so a hypothetical consent can be seen as a hypothetical request for intervention.

[91] Bellaby argues that the intelligence community is still dominated by a Cold War, realist focus traditional understandings of national security that distort the perception of security to promote physical security often to the expense of other vital interests.

exploitation; develop new technology that breaks the anonymity; or use web-crawlers to collect that data that is available to detect patterns that would predict threats. This means understanding the different threats that various intelligence activities can represent to people's autonomy and privacy, which is to be negotiated against the threat that anonymising technology poses both broadly and specifically.

Possessing and banning

The first state-response could be to ban the possession or development of any technology that would allow people to go off-grid. This position has already found purchase in regimes such as China where it is illegal to try and circumvent their Golden Shield, but it is also gaining momentum in traditionally liberal societies such as the UK which after the terrorist attack in 2017 has stated a need to review encrypted communication as Home Secretary Amber Rudd has called for a ban on end-to-end encrypted communications.[92] There are arguments that could be made that the individual, by simply owning or using dark web technology, for example, is entering a realm that is known to be used to carry out actions that can bring harm to others and threaten the political community and so intelligence actors could be justified in targeting those who download the software given the high propensity for illegal activity being carried out through it. Indeed, one of the problems levied at the intelligence community for collecting data on the open web was that there was no real reason for suspecting everyone and they were unable to discriminate between those who were a threat and everyone else who was innocent; those who lacks any form of probably cause. Therefore, by focusing on the dark web it does mean that intelligence is narrowing down to a subset of the community. Large swathes of the population are left out. Also, those within the dark web community have a high propensity to use it for criminal or terrorist activity and so pose a direct threat to a lot of other members of society. From the online trade of drugs and guns fuelling the wider drugs industry, through the millions in financial costs that hackers represent to individuals and companies, to the sites that offer 'violence on order' including rape and assassination,[93] the costs are significant and should be prevented.

However, rather than focusing down on a threatening actor in regards to what they have done, in reality it targets the individual according to the group to which he belongs; that is, labelling those who use the dark web as guilty by cyber-proximity to other dangerous elements and nothing else. At this stage, there is nothing that a dark web user has done wrong other than being in an arena where other individuals are known to carry out illegal activities. It is therefore closer to guilt by proximity. This is problematic as it represents a new form of profiling where one is profiled according to who one is in the cyber-vicinity of. This is indicative of a larger move in security towards pre-emptive risk assessment as security or justice techniques are 'not based on individual suspicion but on the probability that an individual might be an offender'.[94] This raises the prospect of individuals being targeted as a form of pre-crime, where they do not have to actually have done anything wrong but show a propensity that they might do wrong in the near future. Moreover, this type of examination is problematic as it relies, promotes and reinforces the use of profiling as a means of locating threats. This profiling takes the characteristics of an offender and overlays it over the group in order to identify and classify suspect populations.[95] By focusing on singular attributes this type of profiling is problematic as it uses this as the base for locating pre-threats even though these other individuals do not have any of the other 'threatening' attributes seen in the original offender. That is, it 'identifies a certain number of people who do not share all the attributes of the group's profile. […] one person may be identified as a member of this group without having the same attributes and without sharing all the attributes. This kind of profiling has a higher probability of mistakenly identify people as members'.[96] For example, online drug dealers can use the dark web as a means of selling their goods and so are profiled as being dark web users. Yet, not all dark web users are drug dealers. Targeting those individuals who use dark web technology therefore distributes a singular criminal aspect onto the rest of the online population even though there is no other attribute that marks them as a threat. Simply having the technology and using it to protect data or using it to explore the dark web itself is not sufficient to count as a legitimate reason for targeting someone and is more about guilt by proximity rather than actually representing some form of threat. Therefore, possession of such technology

[92] Andrew Griffin, 'WhatsApp is Used by Paedophiles and Gangsters and Needs to be Stopped, Home Secretary Amber Rudd Says' *The Independent* 3 October 2017. Available at http://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-amber-rudd-government-home-secretary-encryption-paedophiles-shut-down-a7981616.html.

[93] United Nations Office on Drugs and Crime, *Economic and Social Consequences of Drug Abuse and Illicit Trafficking* (1998) Available at https://www.unodc.org/pdf/technical_series_1998-01-01_1.pdf.

[94] Clive Norris and Michael McCahill 'CCTV: Beyond Penal Modernism' *British Journal of Criminology* 46/1 (2006) p. 98.

[95] Lucia Zedner 'Pre-Crime and Post Criminology' *Theoretical Criminology* 11/2 (2007) 265.

[96] V. Ferraris, F. Bosco, G Cafiero, E. D'Angelo, Y. Suloyeva. *Defining Profiling, Working Paper, Protecting Citizens' Rights Fighting Illicit Profiling*, 29 July 2013. Available at http://profiling-project.eu/defining-profiling-first-paper-of-profiling-project-online/ p. 5.

alone is not sufficient to warrant being investigated by the intelligence services. The bar must be higher than this.

Back doors

A second option highlighted by the debate between the USA's FBI and technology manufacturer Apple and the state's desire to force companies to create backdoors into equipment to ensure access by the intelligence community at a later date. Phones record information in both quantity and variety unlike anything previously seen and researchers have shown that they can be used to collect key presses,[97] location,[98] recorded speech,[99] and a person's general daily activities both online and in real life. Equally, communication platforms such as WhatsApp have come to dominate how people communicate and organize their affairs. This has, in turn, prompted intelligence actors—most notably the FBI in its debate with Apple—to ask or even force companies to build in backdoors into to their programs in order to allow access when they wish.

Therefore arguments can be made that commissioning such backdoors offers an opportunity for the intelligence community to act when they have a device they know has been used in the commission of a crime. Such an activity in theory would only target a particular phone for those individuals who have been involved in a crime or represent an immediate threat. However, demanding such backdoors can become problematic on a few fronts. Firstly, it again presumes that people are going to be a threat; that people are all potentially guilty and the backdoor is needed for when they commit a crime. Most individuals at the time of buying a phone have done nothing wrong and so should not be forced to have a substandard product because of their potential to cause a future crime. Creating such backdoors is unable to discriminate between individuals as they would have to ubiquitous to work, and while the backdoor would not be used against everyone, all devices' security are being degraded; everyone is being treated as a potential threat rather than an actual threat. If, as it was argued, that all individuals have a right to protect themselves from intelligence protections in the absence of a threat, then these backdoors would directly impinge on this regardless of who they were or what they have done.

Second, once established there is nothing to prevent widespread and unmonitored use of the backdoor and so lowers the bar to allow *en masse* surveillance. This contradicts the drive to make surveilling people difficult so as to limit its use. Third, the development of any backdoor system would place the individual under threat of being exploited by criminals, meaning that the cost is transferred to the individual and not the state. Finally, the framing of the threat is often in terms of impending terrorist attack, however in reality security services have expressed that there are several criminal (mainly drug) cases they would use the backdoor to aid in prosecution.[100] Not only does this immediate indicate a creep of usage but does not have the same threat and urgency and so there is not the same perceived instant positive that can be used to outweigh the costs that would be faced by the individual.

Dark-web crawling and analytics

A final avenue available is to scan all dark web activity automatically looking for patterns and trying to detect if there are any threat signifiers. By carrying out such large data-mining and dataveillance scans it is possible to extract 'useful information from large datasets or databases'.[101] Given the protection offered by anonymising technology analytical scanning collects that information available by using crawlers: 'software programs that transverse the World Wide Web information space by following hypertext links and retrieving web documents'.[102] These crawlers have become a rapidly growing area where 'web-mining techniques can be used to detect and avoid terror threats'.[103] For example, these crawlers collect visible data across forums, blogs, messaging

[97] Zhi Xu, Kun Bai, and Sencun Zhu, 'Taplogger: Inferring User Inputs on Smartphone Touchscreens Using On-Board Motion Sensors' in *WiSec'12* (2012); Liang Cai, Hao Chen, 'Touchlogger: Inferring Keystrokes on Touch Screen from Smartphone Motion' In *HotSec* (2011) p. 9.

[98] Jurgen Krumm and Eric Horvitz, 'LOCADIO: Inferring Motion and Location from Wi-Fi Signal Strengths' in *MobiQuitous* (2004); Jurgen Krumm and Eric Horvitz, 'LOCADIO: Inferring Motion and Location from Wi-Fi Signal Strengths' in *MobiQuitous* (2004); Jun Han, Emmanuel Owusu, Le T. Nguyen, Adrian Perrig, and Joy Zhang, 'Accomplice: Location Inference Using Accelerometers on Smartphones' in Communication Systems and Networks (2012); Yan Michalevsky, Gabi Nakibly, Aaron Schulman, and Dan Boneh, 'PowerSpy: Location Tracking Using Mobile Device Power Analysis,' in SEC'15 *Proceedings of the 24th USENIX Conference on Security Symposium* (2015).

[99] Yan Michalevsky, Dan Boneh, and Gabi Nakibly, 'Gyrophone: Recognizing Speech from Gyroscope Signals' in Proceedings of the 23rd USENIX Security Symposium (2014).

[100] Spencer Ackerman, Sam Thielman, and Danny Yadron, 'Apple Case: Judge Rejects FBI Request for Access to Drug Dealer's iPhone' *The Guardian* 29 February 2016 Available at https://www.theguardian.com/technology/2016/feb/29/apple-fbi-case-drug-dealer-iphone-jun-feng-san-bernardino.

[101] Frans A. J. Birrer 'Data Mining to Combat Terrorism and the Roots of Privacy Concerns' *Ethics and Information Technology* 7 (2005) pp. 211–220.

[102] Fah-Chun Cheong, *Internet agents: Spiders, Wanderers, Brokers, and Bots* (Indianapolis, IN: New Riders, 1996).

[103] Ablistek Sachan, 'Countering Terrorism Through Dark Web Analysis' *Computing Communication & Networking Technologies* (Third International Conference), 2012 p. 1.

boards, and websites looking for key terms that might indicate a threat. While 'stylometry is a form of authorship attribution that relies on the linguistic information to attribute documents of unknown authorship based on the writing styles of a suspect set of authors'.[104] Or in another example, in order to determine who has been visiting or downloading material from a dangerous website 'website fingerprinting' can be used where a 'local passive-eavesdropper (an ISP) observes packets to and from a web-browsing client, and attempts to guess which pages the client has visited'; that is, by monitoring volume changes and matching times of those changes programs can link up which individual has visited a particular website.[105]

Such models argue that 'Security analyst can use this model as a tool for assistance and may help to locate and analyse information quickly and effectively. The use of this model may be in the identification and analysis of the feelings/thinking of different posters belongs to a particular region or community' and that 'This model may help to predict and prevent violence by offering insight into the nature of the communications, communities, and participants'.[106] Indeed, with its promise of anonymity the dark web forums offers an powerful means of terrorist propaganda dissemination;[107] a quick, easily accessed and cheap form of communication between extremists to organise of attacks;[108] the dissemination of their 'message' to different audiences; and as a space for grooming and radicalising individuals.[109] By monitoring these interactions—what is being said, on what type of forum they are saying it, and the amount of traffic created—it is possible to predict potential threats. For example, The Dark Web Forum Portal maintains a collection of 29 online jihadist forums, which currently contains 14,297,961 messages and 1,553,122 threads from 362,495 authors—making it a prime target for monitoring what is said and drawing conclusions from what is implied.[110] As such these crawlers are being positioned as important counter-terrorism tools as the dark web becomes an arena for terrorists not only in terms of organising and facilitating their attacks but also in terms of recruitment and message dissemination.

In terms of its justifiability, one of the key problems with the *en masse* collections methods revealed by Edward Snowden in the open web is that they were unable by their very nature to discriminate between targets and that people's actions and identity were too easily accessed and connections made. All information was collected without concern for it whose it was. In comparison, these crawlers and website-finger printers offer a slightly different result when used on the dark web. The relatively high technical difficulties associated with matching up users with websites through fingerprinting means that while it is possible it is not likely to be systematic or all encompassing and while the crawlers can often highlight threats, determining identities requires a secondary set of analytics and matchmaking. Therefore, the crawlers can be used to first locate threats, but not identities, but once the threat has been located then only on those websites or forums can the other 'identifying' scan be used. The benefit of this system is that people's identity is protected unless they have shown indications of being a threat, while the technical limitations prevent *en masse* surveillance.

Conclusion

Anonymising technology and the dark web represent a clear challenge for the intelligence community. The protections that they offer are highly difficult for them to overcome and prevent large-scale surveillance. This means, some would argue, that the development and use of such technology represents a clear threat to society as it limits the ability of the intelligence community from locating and preventing threats from causing people destructive harm. However, the opposite has been argued here in that such technology 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

[104] Rebekah Overdorf and Rachel Greenstadt 'Blogs, Twitterfeeds and Reddit Comments: Cross-domain Authorship Attribution' *Proceedings on Privacy Enhancing Technologies* 3 (2016) pp. 155–171.

[105] Tao Wang and Ian Goldberg 'On Realistically Attacking TOR with Website Fingerprinting' *Proceedings on Privacy Enhancing Technologies* 4 (2016) p. 21–36. Also see Andriy Panchenko, Lukas Niessen, Andreas Zinnen, and Thomas Engel. 'Website Fingerprinting in Onion Routing Based Anonymization Networks' In *Proceedings of the 10th ACM Workshop on Privacy in the Electronic Society* (2011).

[106] Ablistek Sachan, 'Countering Terrorism' p. 4.

[107] A. T. Gustavson and D. E. Sherkat, D.E. 'Elucidating the Web of Hate: The ideological Structuring of Network Ties Among White Supremacist Groups on the Internet' Paper presented at *Annual Meeting of American Sociological Association* (2004) San Francisco, CA.

[108] K. Crilley, 'Information Warfare: New Battlefields, Terrorists, Propaganda, and the Internet' in *Proceedings of the Association for Information Management*, 53/7 (2001) pp. 250–264.

[109] Scott Gerwehr and Sara Daly, 'Al-Qaida: Terrorist Selection and Recruitment' in David Kamien (ed.) *The McGraw-Hill Homeland Security Handbook* (New York, McGraw-Hill, 2006) p. 83; Denning, Dorothy 'Terror's Web: How the Internet is Transforming Terrorism' in Jewkes Y and Yar M (eds.) *Handbook of Internet Crime* (Cullompton, Willan Publishing, 2010) pp. 194–213.

[110] Y. Zhang. et al., 'Developing a Dark Web collection and infrastructure for computational and social sciences' *Intelligence and Security Informatics* (ISI), 2010 IEEE International Conference on Vancouver, BC, Canada (2010) pp. 59–64.

such data collections that makes such technology ethically mandatory. That 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.