OPINION

HACKERS, HACKTIVISTS, AND THE FIGHT FOR HUMAN RIGHTS IN CYBERSECURITY

STEFANIA MILAN
Stefania Milan (stefaniamilan.net) is an assistant professor at the University of Amsterdam and the Principal Investigator of the DATACTIVE project, exploring the politics of massive data collection (European Research Council Starting Grant 639379). She is also a research associate at the Tilburg Institute for Law, Technology and Society (Tilburg University) and at the Internet Policy Observatory of Annenberg School of Communication (University of Pennsylvania). Her research explores cyberspace and cybersecurity governance, grassroots engagement with technology and data epistemologies. Stefania is the author of Social Movements and Their Technologies: Wiring Social Change (Palgrave Macmillan, 2013) and co-author of Media/Society (Sage, 2011).

1. Introduction

Edward Snowden, the US security contractor turned whistleblower, has exposed blanket data surveillance programs targeting citizens indiscriminately, regardless of their criminal record or passport. The current surveillance complex combines the state apparatus and the industry in unprecedented tight alliances, largely hidden to users and generally impermeable to democratic safeguards[1]. In the same year, the United Nations (UN) Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, has denounced threats this surveillance frenzy represent for human rights. He argued that 'Communications surveillance should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy, and threatens the foundations of a democracy society. He exposed, among others, the unregulated access to communications data, the lack of judicial oversight over massive data collection, the mandatory data retention requirements imposed on manufacturers and providers of electronic communication, the extra territorial application of surveillance laws and the extra-legal surveillance[2]. But if a variety of non-governmental organisations has made their voice heard, and the use of encryption is on the rise, the bulk of the citizenry ignores that their civic rights are progressively being eroded in the name of underspecified cybersecurity needs, spanning anything from the fight against global terrorism to the curbing of copyright infringement. Cybersecurity policymaking remains, to a large extent, a grey area which is exclusive to security agencies, top-level technocrats and the military. The state-industry alliance is rarely broken, and only when the manufacturers of the 'tethered' devices[3] that constitute the final link in the chain of surveillance publicly stand up against law enforcement requests, as the recent Federal Bureau of Investigations vs. Apple case shows[4]. But while from the perspective of the state the imperatives of national security are perfectly legitimate and dutiful, there remain some open questions for what concerns the human rights implications of (some of the) current cybersecurity arrangements, especially in light of the government's obligation to uphold and protect human rights following from the Universal Declaration of Human Rights (1948).

This article connects the current debate on surveillance of communications with human rights. It departs from the assumption that mass surveillance 'amounts to a systemic interference with the right to respect for the privacy of communications' . It provocatively posits hackers and hacktivists as the guardians of human rights in cyberspace and of individual freedoms of expression, and the right to privacy in particular. It explores a side of the hackerdom which is unknown to (or deliberately ignored by) most cybersecurity policymakers – the politically motivated use of tech expertise to enhance transparency, raise awareness and shield users from industry snooping and state monitoring.

2. A question of vocabulary

A rich mythology has flourished around the figure of the hacker, often pictured as exceptionally talented individuals, perhaps socially awkward and ready to provoke or exploit chaos in the digital realm. Hackers have been called many names, from heroes to criminals, from cyber bandits to digital Robin Hoods, regardless of the enormous differences that exist within the worldwide hackerdom. In order to position the core argument of this article, we ought to start from what is in a world, as it can help us understand the connection between hacking, ethics, and human rights – and position the variety of tactics hackers and hacktivists use in the attempt to create a better cyberspace or safeguard online freedoms.

'Hackers are VERY serious about forbidden knowledge. They are possessed not merely by curiosity, but by a positive LUST TO KNOW,' wrote cyberpunk novelist Bruce Sterling back in 1993. He linked 'these young technophilic denizens of the Information Age' to 'some basic shift in social values' that emerge as 'society lays more and more value on the possession, assimilation and retailing of INFORMATION as a basic commodity of daily life'[5].

But the politicisation of hackers is somewhat of a recent phenomenon. The first 'computer hackers', who appeared in the 1970s around the Massachusetts Institute of Technology in Cambridge, MA, were intrinsically apolitical. Highly skilled software writers, they enjoyed experimenting with the components of a system with the aim of modifying and ameliorating it, and operated under a set of tacit values which soon became known as the 'hacker ethics.' Such ethical code included freedom of speech, access to information, world improvement and the non-interference with the functionality of a system ('leave no damage' and 'leave things as you found them(or better)'). Around the same time, software developers and user communities started advocating and practising freedom in managing and using computer technology, for instance targeting software to individual needs. They were the pioneers of what became known as the open source movement. Similarly to hackers, they promoted a hands-on attitude to computing and information more in general; but while hackers emphasised a 'do not harm' approach, open source advocates championed collective improvement and selfless collaboration.

Since the 1970s, hacking, as well as the open source movement, went a long way. Commonly, we distinguish between 'black hat' hackers who violate computer security with malicious intents like fraud or data theft, and 'white hat' hackers, who on the contrary perform hacking duties in view of repairing bugs or 'making things better.' Between the two, a plethora of nuances and variations can be found amongst the many people who self-identify as 'hackers,' including civic hackers who use data and software to ameliorate the state output but often have no particular programming skills and 'ethical hackers' who, for example, support security agencies in their fight against terrorism or report vulnerabilities with the scope of helping an organisation fixing them.

[1] Deibert, R. (2013). Black Code: Inside the Battle for Cyberspace. Toronto: Signal

[2] United Nations General Assembly, A/HRC/23/40, 17 April 2013; http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

[3] Zittrain, J. L. (2008). The future of the internett–And how to stop it. New Haven and London: Yale University Press.

[4] Kravets, D. (2016). 'FBI vs. Apple is a security and privacy issue. What about civil rights?, ArsTechnica, 15 March; http://arstechnica.com/tech-policy/2016/03/fbi-v-apple-is-a-security-and-privacy-issue-what-about-civil-rights.

[5] Sterling, B. (1993). The Hacker Crackdown. Law and Disorder on the Electronic Frontier. New York: Batham, http://cyber.eserver.org/sterling/crackdwn.txt. Original capitals.

Hacktivism, in turn, represents a sort of activist evolution of early-day hacking. It involves the politically motivated use of technical expertise like coding: activists seek to fix society through software and online action. In other words, it is 'activism gone electronic'[6]. The first recorded instance of hacktivism dates back to 1995, when a group of activists organised a netstrike, 'a networked version of a peaceful sit-in' targeting the French government in opposition to its nuclear experiments in a Polynesian atoll. In the mid-1990s, the US tactical media collective Critical Art Ensemble theorised electronic disturbance and electronic civil disobedience as new forms of political resistance exploiting one of the main features of contemporary societies, namely decentralisation[7]. Hit-and-run online direct action such as virtual sit-ins, 'digital storms' and denial of service attacks were presented as the virtual equivalent of blocking a company's headquarters to send a message.

Fast-forward to the second half of the 2000s and hacktivism was popularised by online communities like Anonymous whose self-identified members engage in spectacular disruptive actions and nuisance campaigns using electronic civil disobedience in support of freedom of speech on the web (and more). The group and the moniker originated in online chat rooms dedicated to politically incorrect pranks, and although Anonymous later mutated into a politically engaged community, it maintained an orientation to the 'lulz,' a neologism that indicates the fun associated with pranks[8].

3. A matter of (hacker) ethicsn

To be sure, the 'hacker' rubric is highly contested today, as it is indiscriminately used to indicate a variety of phenomena. It subsumes different values, tactics and goals under its umbrella, from denial of service attacks to morally-motivated security breaches testing – not all of which are compatible. The hacktivists' repertoire, for example, crashes with the freedom of information and no-damage philosophy of earlier generations of hackers, for whom closing down a website equals to censorship, no matter the content of owner of such website. Certainly, the most disruptive forms of hacktivism such as sabotage cross the boundaries of acceptable practice in liberal democracies. However, with the distinctions outlined in the previous session in mind, this article suggests to look at hackers and hacktivists as specific forms of democratic participation that are heavily mediated by and address digital technology and the Internet. In other words, they express and reclaim democratic agency. In a society doomed by increasing disaffection towards representative democracy and declining citizen participation, hacking and hacktivism represent a quest for participation and an exercise of direct democracy. As such, they have the potential of fostering personal and collective empowerment, participation and self-determination – while promoting literacy and transparency. Such forms should be tolerated, as they are manifestations of an emerging grassroots social force pushing the boundaries of liberal democracy and questioning the relationship between citizens and the state, and the role of the latter as the sole guardian of individual freedoms. Rather than enemies of democracy, hackers and hacktivists are the carriers of grassroots demands concerning the present and the future of our society.

Hackers and hacktivists engage in disruptive and pre-figurative action, trying to create here and now the cyberspace as they would like it to be. As such, they harbour a message for society, one that has human rights at its core, also when human rights are not explicitly evoked. Such message addresses issues of transparency, positive freedoms but also negative freedoms (e.g. a freedom from state monitoring and surveillance) and an idea of democratic participation in the first person. It is grounded on ethics of technology which are also ethics of society, by virtue of which the two are seen as intrinsically related and dependable. Disruptive actions like 'watching the watchers' enacted by Anonymous have the ability of raising awareness of the dangers of massive data collection and poor data storage, or dodgy data sharing practices; whistleblowing increases transparency; shielding users by means of, for example, encryption defends their right to privacy. As such, hackers and hacktivists embody and voice the 'shift in social values' Sterling detected back in the 1990s and can be rightly seen as 'the new guardians of our civil liberties,' as Coleman put it[9]. ■

[6] | Jordan, T. And P.A. Taylor(2004). Hacktivism and cyberwars: Rebels with a cause?. London: Routledge, p. 1.

[7] | Critical Art Ensemble (1996). Electronic Civil Disobedience. New York: Autonomedia.

[8] | Milan, S. (2015). Hacktivism as a radical media practice, in Routledge Companion to Alternative and Community Media, edited by C. Atton, pp. 550-560.

[9] | Coleman, G. (2013). 'Geeks are the new guardians of our civil liberties,' Technology Review, 4 February; https://www.technologyreview.com/s/510641/geeks-are-the-new-guardians-of-our-civil-liberties/.