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

STEFANIA MILAN

1. Introduction

Edward Snowden, the US security contractor turned whistleblower, has exposed blanket surveillance programs targeting citizens indiscriminately, regardless of their criminal record or passport. The current surveillance complex combines the state apparatus and largely hidden to users and generally impermeable to democratic safeguards1. 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 these ‘Amount to a systemic interference with the right to respect for the privacy 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 policy-makers – the politically motivated use of tech expertise to enhance transparency, raise awareness and shield users from industry snooping and state monitoring. 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.

This article connects the current debate on surveillance 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 policy-makers – the politically motivated use of tech expertise to enhance transparency, raise awareness and shield users from industry snooping and state monitoring.


5. This article connects the current debate on surveillance 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 policy-makers – the politically motivated use of tech expertise to enhance transparency, raise awareness and shield users from industry snooping and state monitoring.

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’. 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. 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.

3. A matter of (hacker) ethics

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, clashes 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.

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.

---