ECONSTOR
Make Your Publications Visible.

A Service of
ZBW
Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Bodó, Balázs

Article

Hacktivism 1-2-3: how privacy enhancing technologies change the face of anonymous hacktivism

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Bodó, Balázs (2014) : Hacktivism 1-2-3: how privacy enhancing technologies change the face of anonymous hacktivism, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 3, Iss. 4, pp. 1-13, https://doi.org/10.14763/2014.4.340

This Version is available at:
https://hdl.handle.net/10419/213994

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

https://creativecommons.org/licenses/by/3.0/de/legalcode

WWW.ECONSTOR.EU

Mitglied der Leibniz-Gemeinschaft

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 3 | Issue 4

Hacktivism 1-2-3: how privacy enhancing technologies change the face of anonymous hacktivism

Balázs Bodó
Institute for Information Law, University of Amsterdam, Netherlands, bodo@uva.nl

Published on 28 Nov 2014 | DOI: 10.14763/2014.4.340

Abstract: This short essay explores how the notion of hacktivism changes due to easily accessible, military grade Privacy Enhancing Technologies (PETs). Privacy Enhancing Technologies, technological tools which provide anonymous communications and protect users from online surveillance enable new forms of online political activism. Through the short summary of the ad-hoc vigilante group Anonymous, this article describes hacktivism 1.0 as electronic civil disobedience conducted by outsiders. Through the analysis of Wikileaks, the anonymous whistleblowing website, it describes how strong PETs enable the development of hacktivism 2.0, where the source of threat is shifted from outsiders to insiders. Insiders have access to documents with which power can be exposed, and who, by using PETs, can anonymously engage in political action. We also describe the emergence of a third generation of hacktivists who use PETs to disengage and create their own autonomous spaces rather than to engage with power through anonymous whistleblowing.

Keywords: Hacktivism, Privacy enhancing technologies, Anonymous, Wikileaks

Article information

Received: 22 Aug 2014 **Reviewed:** 27 Oct 2014 **Published:** 28 Nov 2014
Licence: Creative Commons Attribution 3.0 Germany
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/hacktivism-1-2-3-how-privacy-enhancing-technologies-change-face-anonymous

Citation: Bodó, B. (2014). Hacktivism 1-2-3: how privacy enhancing technologies change the face of anonymous hacktivism. *Internet Policy Review*, *3*(4). DOI: 10.14763/2014.4.340

The 2007 official launch[1] of Wikileaks, a platform for potential whistleblowers designed to make sensitive documents anonymously public was a turning point in the history of computer based social activism (or hacktivism (Gunkel, 2005, p. 595), in short). The website has many distinct features which enable it to fulfill its role, such as its close relationship with mainstream media organisations, which both disseminated and fact-checked source documents. However, Wikileaks is particularly relevant for our analysis because of its use of Privacy Enhancing Technologies (PETs). PETs is a general name for a family of software and hardware solutions

which aim to shield their users from surveillance of their electronic communications and promise to preserve their anonymity. While many different PETs were developed and in use before it, Wikileaks was the first to provide easy to use PETs for the masses. It was also the first PET application that hit the headlines all over the world.

The easy availability of user-friendly PETs providing military grade online security to anyone enables a plethora of social practices. These practices affect, among other, international diplomacy, state security and counter-terrorism efforts. They have strong influence on the debate around online privacy and the legal and philosophical underpinnings of basic human rights. For the purposes of this article however, we will single out one out of the many possible transformations that PETs, their users and communities are a potential source of: how online political activism and electronic civil disobedience is being transformed.

This transformation is most easily understood through the rise and fall of Anonymous - the ad-hoc online swarm of vigilante activists that represented the "face" of hacktivism 1.0, and the way the launch of Wikileaks redefined what anonymous, and its potential really is.

ANONYMOUS 1.0

Anonymous was a name that frequently appeared in articles discussing the events around Wikileaks. It referred to a group of hacktivists who organised mass cyber-attacks in the late 2000s against various online adversaries: individuals that they deemed offensive, companies they disliked or despised. According to their self-description: "*Anonymous is not a person, nor is it a group, movement or cause: Anonymous is a collective of people with too much time on their hands, a commune of human thought and useless imagery. A gathering of sheep and fools, assholes and trolls, and normal everyday netizens. An anonymous collective, left to its own devices, quickly builds its own society out of rage and hate. [...] They have no leader, no pretentious douchebag president or group thereof to set in stone what Anonymous is and is not about. This makes them impossible to control or organize. Not really a collective at all - more like a stampede of coked-up lemmings. [...] Anonymous is not a single person, but rather, represents the collective whole of the internet. As individuals, they can be intelligent, rational, emotional and empathetic. As a mass, a group, they are devoid of humanity and mercy.*" (Encyclopedia Dramatica, 2011) [2] Anonymous, which started out as an ad-hoc online group committing mischiefs 'just for the lulz' (i.e., just for fun) soon transformed into a rather chaotic power of vigilante justice. They rallied against laws they thought of as unjust, they turned against what they have seen as corrupt businesses and individuals by using methods that usually bordered on (if not crossed) the threshold of legality (Coleman, 2012).

In the tumultuous last weeks of 2010 Anonymous hit the headlines again, that time because they launched a series of attacks against those companies that severed their business ties with Wikileaks. Soon after Wikileaks started to publish the Afghan war logs and the US diplomatic cables, the US government pressured several companies to stop doing business with Wikileaks. When Amazon.com kicked Wikileaks out from its servers, and when MasterCard, Visa and Paypal stopped processing donations for the organisation, Anonymous stepped in and started to organise large scale Distributed Denial of Service (DDoS) attacks against these companies in what they called 'Operation Payback'.

HACKTIVISM 1.0

Anonymous was the latest manifestation of hacktivism 1.0, the electronic civil disobedience that developed in the decades before. Ad-hoc groups of individuals using technology to advance their cause started to organise political actions in the digital space as early as the 1990s. Anonymous' predecessors, such as the Critical Art Ensemble, the Electronic Disturbance Theatre, or the Cult of the Dead Cow were small groups, experimenting with digital resistance and electronic civil disobedience, using the technology as a means for political action. (Critical Art Ensemble, 1996; Wray, 1999) Besides tailor-made interventions, these groups have experimented with what they called virtual sit-ins, or distributed denial of service (DDoS) attacks, in which they tried to take down the online web-services of target organisations by flooding them with simultaneous requests. Anonymous, which coalesced not long before the year 2008 in and around the online image board 4chan, followed that tradition, albeit with a twist: rather than being a highly selective group rooted in various artistic and/or political traditions, they were more open, less high-brow and certainly less formal. Their message was that any one and every one is a member of Anonymous who puts on stylised plastic Guy Fawkes mask borrowed from James McTeigue's Hollywood blockbuster V for Vendetta (Kaulingfreks and Kaulingfreks, 2013), and who joins the online swarm rallying for the latest cause. Anonymous updated and democratised the methods they inherited from earlier hacktivist groups: they organised massive DDoS attacks using custom written software tools that enabled participation for even the technically unskilled (Sauter, 2013, p. 984), while more skilled members of the group performed impressive hacks (cracking and defacing websites) and doxxes, i.e., revealing highly private information on a target individual, including bank account transactions, social security data, private emails, etc.

Anonymous as a group was at its heyday in 2010-2011. They were a group that rallied against something. They were resisting something they are left out of, trying to make their voice heard, trying to get in. This is the message of Anonymous: we are united in our position of being excluded. We are united in our position of being outsiders.

The power of Anonymous is that it is a swarm which "*attacks from all directions, and intermittently but consistently — it has no 'front,' no battle line, no central point of vulnerability. It is dispersed, distributed, and yet in constant communication. In short, it is a faceless foe, or a foe stripped of "faciality" as such.*" (Galloway & Thacker, 2007) The plastic Guy Fawkes mask, which became the ultimate symbol of Anonymous was not really about actually hiding the real identity of its members. Though the participation in DDoS attacks is an offence under US law as well as under the Council of Europe's Convention on Cybercrime, the DDoS tools the group distributed to the public made no efforts to hide the identity of its users. As a result, many who participated in Anonymous were arrested in subsequent years (Olson, 2012; Shankland, 2011). Rather, the mask symbolised the universally shared feeling of exclusion, which applied to everyone with no regard to individual differences. The mask was also a reference to the methods of hacktivists of the 1.0 kind: We re-appropriate the entertainment that was offered to us by the military-industrial-entertainment-complex as a substitute for resistance (Adorno & Horkheimer, 1979) and turn it against the status quo (Debord, 1994). Rather than just enjoying the Warner Bros. produced movie and buying the merchandise associated with it, Anonymous appropriated the props and the message, and used them as an inspiration to rally against those very structures that produced the film, which was certainly intended to be entertainment rather than educational material on how to revolt against governments and corporations.

Anonymous embodied the essence of hacktivism 1.0. The latter "*breaks down into two broad streams of actions: 1. Mass virtual direct actions, which use cyberspatial technologies of limited potential in order to re-embody virtual actions, [and 2.] digitally correct actions, which defend and extend the peculiar powers cyberspace creates.*" (Jordan & Taylor, 2004, pp. 114-116) On the one hand, hacktivism 1.0 gives technically less skilled individuals the chance to participate in electronic civil disobedience actions. These actions, like virtual sit-ins or DDoS attacks, fit into the tradition of sit-ins and other physical and electronic civil disobedience (Sauter, 2013). Some would argue that various social network-based actions, such as Facebook and Twitter campaigns also belong to this category, where individuals self-organise using Facebook pages and Twitter hashtags to express dissent, build resistance and achieve social change (Lindgren & Lundström, 2011). Such hacktivism requires no technical skills, it is easy to join the swarm and participate in the action. Hacktivism 1.0 could also mean complex technological stunts, committed by a few, highly skilled computer programmers. The cracking of websites and databases, the disruption of the 'infostructure' of the target organisations, or the development of highly specialised software tools (to aid, for example technically less skilled activists) may yield high rewards, but they are also high-risk, complex, costly and time consuming actions, and as a result they are relatively rare (Coleman, 2013). Hacktivism 1.0 is thus torn between highly effective but rare instances of hacking, and relatively frequent cyber-protests where the place of impact is separated from the place of resistance, and thus yield little more than symbolical results.

The Wikileaks related actions of Anonymous marked the apex of hacktivism 1.0. While such hacktivists gained enormous amounts of press attention, it soon turned out that this attention was the most they could hope for. The power of Anonymous was based on the belief that the sole number of participants would be enough to win any battle. But their effectiveness in terms of disrupting the everyday operations of these companies, or inducing a shift in their policies was nil. Their symbolic victories were short lived. Gladwell (2010) argues that this form of electronic civil disobedience is even counterproductive, since the technological tools of electronic civil disobedience "*make it easier for activists to express themselves, and harder for that expression to have any impact. The instruments of social media are well suited to making the existing social order more efficient. They are not a natural enemy of the status quo.*" The swarm-logic in itself turned out to be ineffective, and the swarm of what proved to be the important question. The lesson of Anonymous was that even if there are millions of them, the disruption technically unskilled outsiders can cause to the well-fortified corporate and governmental infostructures is very limited indeed.

ANONYMOUS 2.0

Ironically, while everyone was busy with Anonymous (the group, with a capital A), Wikileaks quietly introduced another type of anonymous (the individual, without any capitals), that turned out to be much more important than the "*stampede of coked-up lemmings*" that Anonymous was.

This new type of anonymous was protected by strong and reliable crypto technology rather than a cheap plastic mask. It was individual rather than a swarm, and most importantly it was on the inside, rather than being on the outside. The anonymous of Wikileaks are those powerful individuals in privileged positions within the existing power structures, who by leaking secrets can safely subvert the very power structures that they define (and that define them), because they can rely on PETs to safeguard their identity.

Leaking classified information to the press and whistleblowing has a long tradition (Alford, 2002; Glazer & Glazer, 1989), and many countries have laws that grant protection to journalistic sources in order to encourage the watchdog role of the press (Blasi, 1971; Privacy International, 2009; Committee of Ministers of the Council of Europe, 2014; McGonagle, 2014). Wikileaks offers a technological solution to the age old problem of how to protect the identity of a source whose willingness to cooperate ultimately depends on his/her ability to remain safe by staying anonymous. Relying on the traditional methods of conspired meetings and often contested legal safeguards is costly and risky. Wikileaks hoped to lower the threat of de-anonymisation through the creation of a safe technological space in which the identity of the source is protected by strong cryptographic algorithms, obfuscation and other software and hardware tricks. The sheer number of secrets exposed through Wikileaks, and their subsequent impact proves that access to low cost, easy-to-use PETs can significantly lower the costs of exposing and confronting power from within (Lipman, 2011, p. 119-123) and thus enable a new type of hacktivism with immensely greater transformative potential than what its predecessor ever hoped to have. Anonymity in the context of Wikileaks offers, through the technological identity protection of whistleblowers, a chance for the individual to expose and confront the very structure of power from within.

HACKTIVISM 2.0

Keeping power under control through coerced transparency was the original idea of Julian Assange, the creator of Wikileaks. In his essay, dating back to 2006, he described the role of Wikileaks in keeping power under control: "*The more secretive or unjust an organization is, the more leaks induce fear and paranoia in its leadership and planning coterie. This must result in minimization of efficient internal communications mechanisms (an increase in cognitive "secrecy tax") and consequent system-wide cognitive decline resulting in decreased ability to hold onto power as the environment demands adaption. Hence in a world where leaking is easy, secretive or unjust systems are nonlinearly hit relative to open, just systems. Since unjust systems, by their nature induce opponents, and in many places barely have the upper hand, mass leaking leaves them exquisitely vulnerable to those who seek to replace them with more open forms of governance.*" (Assange 2006)

The task of keeping power transparent requires a new type of hacktivist, who has the necessary tools to coerce that transparency on power. Anonymous 2.0 is the source of a new type of hacktivism, hacktivism 2.0. While hacktivism 1.0 was the activism of *outsiders*, and its organising principle was to temporarily get outsiders into the territory of the other, hacktivism 2.0 is done by *insiders*. While it is certain that technology in itself cannot and will not be the (sole) solution to anything (Morozov, 2013), in other words one cannot solve problems through technology only, having access to the right tools at the right time when the demand is there certainly helps. Hacktivism 2.0 cannot exist without PETs, whose one important purpose is to help people *get information out* from an organisation. PETs, like in the way Wikileaks put them into use, shift the source of potential threat from a few dangerous hackers and a larger group of mostly harmless activists - both outsiders to an organisation - to those who are on the inside. For mass protesters and cyber activists anonymity is a nice feature, but it isn't necessary or even desirable under every circumstance. Putting a name and a face next to a political action is sometimes the most powerful form of protest. On the other hand, for insiders trying to smuggle information out, anonymity is a necessary condition for participation.

Easy anonymity lowers the risks and costs associated with dissent, and thus radically transforms

who the activist may be. It turns a monolithic, crystal clear communal identity defined solely through opposition into something more complex, multilayered, individual and hybrid by allowing the cultivation of multiple identities, multiple loyalties. Being anonymous is an identity play, and as an identity play, it is a loyalty play. As an identifiable member of the society, the individual is bound by formal and informal attachments and hierarchies, the breaches of which are severely and instantly punished. Being anonymous means that one's identity and loyalty is up for grabs, it is fluid, it is independent, it is freed from its social base. PETs support the development of new loyalties that are detached from what is seen as corrupted and failing national identities, a debilitating chorus of corporate anthems, historical determination and the normalising judgment of Facebook peers. When this happens, one's 'proper' identity, one's real name turns into a mere pseudonym that serves to hide one's 'real' identity, one's true loyalties. "*People are asked to identify personally with organisations who can either no longer carry historical projects worthy of major sacrifices or expressly regard their employees as nothing but expendable, short–term resources. This [...] creates the cognitive dissonance that justifies, perhaps even demands, the leaker to violate procedure and actively damage the organisation of which he, or she, has been at some point a well–acculturated member (this is the difference to the spy). This dissonance creates the motivational energy to move from the potential to the actual.*" (Stalder, 2010)

Being anonymous allows those who do not want to define themselves – at least not publicly – as activist, radical or dissenter to enter the activist scene. The promise – or rather, the condition – of anonymity in the context of Wikileaks is that one can be on the inside and on the outside at the same time. Through anonymity the mutually exclusive categories of inside/outside, cooption/resistance, activism/passivity, power/subjection can be overridden and collapsed.

Assange's quest for a well mannered and well-behaving, ethical, productive and accountable power created by the Wikileaks transparency is very similar to the benefits Bentham assigned to his Panopticon design[3], as cited by Foucault: "*Morals reformed – health preserved – industry invigorated – instruction diffused – public burthens lightened – Economy seated, as it were, upon a rock – the gordian knot of the Poor-Laws not cut, but untied – all by a simple idea in architecture!*" (Foucault, 1979) Wikileaks' coerced transparency extends the Foucauldian disciplinary power to the very body of state and government by placing power under the surveillance of anonymous subjects. But while it may be true that the Panopticon produces more efficient, more productive, more obedient, and more controlled subjects, it remains to be seen whether the outcome of applying the panoptic schema to power yields anything more than more panopticism.

The way the US state apparatus has reacted to Wikileaks clearly illustrates this dilemma. In a memorandum issued on 3 January 2011, the National Counterintelligence Executive and the Director of the Information Security Oversight Office detailed the procedures by which they hoped to prevent any further leaks. The document is a 14-page long checklist covering all aspects of keeping secrets: "the measures in place to determine appropriate access for employees to classified information"; the existence of counterintelligence programmes; the use of back-up media; "a trend analysis of indicators and activities of the employee population which may indicate risky habits or cultural and societal differences other than those expected for current employees for security clearances" and the "*use [of] psychiatrist and sociologist to measure the relative happiness as a means to gauge trustworthiness, and the despondence and grumpiness as a means to gauge waning trustworthiness*" (Lew, 2011, p. 6).

This document, as well as the recommendations formulated in reaction to the Snowden

revelations (Office of Management and Budget, 2014) is the blueprint for an internal total transparency (i.e., total surveillance) programme that is designed to maximise the control over the state apparatus by detecting potential leakers and preventing information breaches. The state reacted to the threat posed by hacktivism 2.0 by creating a transparency of its own. This is the classic example of internalisation (Scott, 1971): the state, under surveillance, has internalised the expectations and now is busy learning how to make sure that what is not to be shown stays truly hidden. Secrets to outsiders can only be protected through total transparency on the inside. This is the problem with total control: it does not annihilate undesired behaviour, it does not mute and reform inappropriate and prohibited desires, it only suppresses them, and fosters secrecy and deceit. Transparency will not break the logic of power based on panopticism: "*The panoptic schema, without disappearing as such or losing any of its properties, was destined to spread throughout the social body; its vocation was to become a generalized function. […] On the whole, therefore, one can speak of the formation of a disciplinary society in this movement that stretches from the enclosed disciplines, a sort of social 'quarantine', to an indefinitely generalizable mechanism of 'panopticism'*" (Foucault, 1979, p. 207). The transparency of Wikileaks does not counter this process, it reinforces it. By putting the locus of power under surveillance it simply draws the state under this form of control, putting the last missing piece of the puzzle in place. In the same sense, Wikileaks only propagates the control it wishes to subvert. It only helps the logic of panopticism to fold and close upon itself.

ANONYMOUS 3.0

There are two types of anonymity: that of the observer, and that of the subject, both immensely empowering. The transparency which Wikileaks coerces on power through the leaks of anonymous whistleblowers extends the Foucauldian disciplinary power to the very body of state and government. But while the anonymity of the subject removes the individual from existing power relations, the act of surveillance, the idea on which Wikileaks is based, puts her right back to the middle.

Anonymity, in the context of PETs offers more than just the ability for the individual to put power under surveillance. Anonymity enables the individual to – at least partially – remove herself from the pre-existing discursive determinations and power relations and consider alternatives. Anonymity is more than just a technology to control power. It is also a technology of individual and collective freedom. "*If governmental rationalities operate through the nomination and specification of a positive identity through a series of constitutive exclusions, rarefactions and restrictions, then the practices of freedom are enabled by withholding the knowledge of oneself, resisting the injunction to a 'confessional' self-expression, declining the incitement to active participation in the governmentally sanctioned discourse. Anonymity may then serve 'to encourage freedom by increasing the scope of actions not susceptible to official observation, records and interpretation'*" (Prozorov, 2007, p. 62, citations omitted).

The Snowden revelations ("The NSA files," 2013) perfectly illustrate the difference between the potential of anonymous 2.0, engaged in the surveillance of power, and anonymous 3.0, which uses PETs to disengage and disappear altogether from the radar screen. Without Snowden, the whistleblower (who, in this case chose not to remain anonymous and thus now lives in exile), we would not have hard evidence on how power operates in the digital age, on how the ubiquitous surveillance of electronic communications trumps fundamental human rights and on how the lack of privacy is a direct assault on a number of individual and collective freedoms (La Rue, 2013, p. 15). The subject's position of being "*a multiplicity that can be numbered and*

supervised", its state of living in a "*sequestered and observed solitude*" (Foucault, 1979, p. 201) can only be subverted if there is a place, hidden from surveillance where we are free to make our choices (Bauman & Lyon, 2013; Bogard, 2006). PETs are important because they allow the individual to counter surveillance, and thus liberate individuals, when other safeguards of freedoms and liberties are lacking or lagging behind.

The PETs provisioned anonymity allows individuals to enjoy certain freedoms. If everyday citizens have an autonomous zone (Bey, 1991), a safe haven, hiding in the discontinuities of cyberspace, from where they not only can oversee and control the state apparatus; but which is safe from surveillance and outside interference, which is peer-produced and thus reflects the ethical and ideological consensus of its users (Bodó, 2014), then we have a virtual space which is not locked down in the oppositional struggles of the status quo, but has the potential to develop something completely independent from it. Free, autonomous individuals, having the potential to create their own world in the autonomous space without surveillance and interference: this is the promise of post-Wikileaks PETs, and the task ahead of hacktivists of the third generation.

POLICY IMPACT

As it stands now, PETs are the only at least relatively effective safeguard against total surveillance. On the other hand, the same PETs that protect the basic human rights on the digital networks are being used in a number of other situations by a number of other groups to, for example, trade drugs and arms, or exchange child pornography (Bodó, forthcoming). PETs are thus increasingly threatened by law enforcement (Masnick, 2014), and the often legitimate goals to catch PETs-using pedophiles and assassins is in clear conflict with the interest of many others who use the same technologies, the same networks to protect their privacy.

There are deeply vested economic and governmental interests to keep the network open for surveillance. If PETs are able to prevent surveillance, then we should expect a long term conflict between the technology-based and the normative and legal based agents for control. We have already seen similar conflicts in regard to file-sharing technologies, where rights holders have long been trying to delegitimise and outlaw the use of P2P software (Giblin, 2011). As a response, P2P software developers came up with ever more autonomous systems, which were always able to be one step ahead of any copyright enforcement effort. We should expect and be prepared to deal with policy interventions that aim to delegitimise and outlaw the use of PETs, in a similar manner. Unless we all have well defined and well protected digital rights, the second best option of PETs is all what we have. Academics and activists should be prepared to defend these technologies, as they seem to be one of the few technologies of freedom (De Sola Pool, 1983) we are left with.

CONCLUSION

With the fall of Anonymous, the era of hacktivism 1.0, done by swarms of harmless outsiders is nearing an end. It is superseded by a much more potent form of hacktivism, which relies on insiders to expose the ways power operates and create a more transparent society. This type of hacktivism, which may be an effective way to control power, relies on easily available military grade PETs to provide anonymity for insiders, making everyone a potential whistleblower. The same PETs and the same anonymity, however, allow for another type of hacktivism, which,

rather than being locked in a diametric relationship with power aims to create its own autonomy through avoiding surveillance.

Which type of hacktivism is more relevant for the future? It depends on our answer to the question of how to be truly free in the age of ubiquitous surveillance. If we think that it is enough to put the observers under surveillance, then the Wikileaks introduced hacktivism 2.0, which relies on anonymous insiders coercing transparency on power may be the answer. However, Galloway and Thacker (2007, p. 41) argue that control in a networked society functions through the data produced by individuated subjects. If we agree, then negating this control is not to gather data on the observers - which is nothing more than being engaged in the oppositional (symmetrical) power relationships, but to be what anonymous really means: invisible. Invisible in its strictest sense: being beyond the determinations that define the identity and the discourse. The function of hiding behind a mask, in this context only makes sense if rather than all of us hiding behind the same Warner Bros. licensed Guy Fawkes mask, we all have our own mask to wear.

Whatever we think of the right course of action, both types of civic activism depend on the easy availability of strong Privacy Enhancing Technologies. Software technologies, such as PETs or P2P file sharing software are created in the niches between the actual, the potential and the desired. They are the products of particular social, political, economic conditions and reflect the opportunities, the threats, and most importantly the perceived failures and deficiencies in and around the contexts in which they are born. Technologies enable the emergence of new and unexpected social practices, which in turn become subject of interpretation in multiple discursive contexts. The major impetus for Tor's development was the US military's need to communicate without the threat of foreign surveillance. Its easy availability for everyone is based on the understanding that secret communication is best hidden in the noise created by others communicating in secret. Allowing individuals to negate control may not have been the primary aim of providing governmental funding to, or the primary goal of the development of PETs. But now, lacking any other effective legal or political protection of human rights and other constitutionally protected freedoms, we rely on PETs to have at least a modicum of privacy. This situation is far from being ideal, but currently this is the best we can hope for. For this reason it is essential that PETs be protected from efforts of delegitimisation and illegalisation. PETs may come with the cost of giving up considerable amounts of security. But this has always been the price for freedom.

FOOTNOTES

1. In a previous version of this article the launch of Wikileaks was accidentally dated to 2010. This was a mistake.

2. Encyclopedia Dramatica (ED) is an open wiki collecting internet memes and providing satirical commentary on current events. Its tone and subject matter is closely related to the online subcultures with which the Anonymous movement is often associated. It hosts one of the several manifestos attributed to and descriptions of the Anonymous group. Since it is rhizomatic and anonymous, it is impossible to identify a single authoritative source of Anonymous' self-definition. The ED article on the topic should be considered collaboratively written and edited by anonymous individuals who feel related to the group, and as such, it is probably as good of a self-definition as one can get.

3. In the 18th century the English philosopher Jeremy Bentham proposed the 'Panopticon', a new, unique prison design, in which all the prison cells are observable from a single, centrally

located watchtower. It is designed to force inmates to adjust their own behaviour to what they believe is expected from them by the invisible observers in the watchtower.

REFERENCES

Adorno, T. W., & Horkheimer, M. (1979). The Culture Industry: Enlightenment as Mass Deception. In *Dialectic of Enlightenment*. London: Verso.

Alford, C. F. (2002). *Whistleblowers: Broken lives and organizational power*. Ithaca : Cornell University Press.

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance: a conversation*. Cambridge, UK ; Malden, MA : Polity.

Bey, H. (1991). *T.A.Z.□: the temporary autonomous zone, ontological anarchy, poetic terrorism*. Brooklyn, NY: Autonomedia.

Blasi, V. (1971). The Newsman's Privilege: An Empirical Study. *Michigan Law Review, 70*(2), 229–284.

Bodó, B. (2014). Set the fox to watch the geese: voluntary IP regimes in piratical file-sharing communities. In M. Fredriksson & J. Arvanitakis (Eds.), *Piracy: Leakages from Modernity*. Sacramento, CA: Litwin Books.

Bodó, B. (forthcoming). Piracy vs privacy – the analysis of Piratebrowser. *International Journal of Communications*.

Bogard, W. (2006). Surveillance assemblages and lines of flight. In D. Lyon (Ed.), *Theorizing surveillance* (pp. 97–122). Portland, OR: Willan.

Coleman, G. (2012). *Our Weirdness Is Free, The logic of Anonymous—online army, agent of chaos, and seeker of justice*. Triple Canopy (15).

Coleman, G. (2013). *Anonymous in Context: The Politics and Power Behind the Mask*. Waterloo, Ontario : Center for International Governance Innovation.

Committee of Ministers of the Council of Europe (2014, □April 30). Recommendation CM/Rec(2014)7

of the Committee of Ministers to member States on the protection of whistleblowers. Strasbourg: Council of Europe

Critical Art Ensemble. (1996). Electronic civil disobedience and other unpopular ideas. New York: Autonomedia.

Debord, G. (1994). The Society of the Spectacle, trans. Donald Nicholson-Smith. New York: Zone Books.

De Sola Pool, I. (1983). Technologies of freedom. Cambridge, Mass.: Belknap Press.

Encyclopedia Dramatica. (2011). Anonymous/Original. *Encyclopedia Dramatica*. Retrieved November 10, 2014 from https://encyclopediadramatica.se/Anonymous/Original

Foucault, M. (1979). *Discipline and punish: the birth of the prison*. New York : Vintage Books.

Galloway, A. R., & Thacker, E. (2007). *The exploit□: a theory of networks. Electronic mediations*. Minneapolis: University of Minnesota Press.

Giblin, R. (2011). *Code Wars: 10 Years of P2P Software Litigation*. Cheltenham, UK□; Northampton, MA: Edward Elgar Publishing.

Gladwell, M. (2010, October 4). Small Change. *The New Yorker*. Retrieved November 10, 2014 from http://www.newyorker.com/magazine/2010/10/04/small-change-3

Glazer, M., & Glazer, P. M. (1989). *The whistleblowers: Exposing corruption in government and industry*. New York : Basic Books.

Gunkel, D. J. (2005). Editorial: introduction to hacking and hacktivism. *New Media & Society, 7*(5), 595-597.

Jordan, T., & Taylor, P. (2004). *Hactivism and Cyberwars - Rebels with a Cause?* London: Routledge.

Kaulingfreks, R., & Kaulingfreks, F. (2013). In praise of anti-capitalist consumption: How the V for Vendetta mask blows up Hollywood marketing. ephemera, 13(2), 453-457.

La Rue, F. (2013, April 17). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/23/40. Geneva: United Nations Human Rights Council.

Lew, J. J. (2011). Initial Assessments of Safeguarding and Counterintelligence Postures for Classified National Security Information in Automated Systems . (EXECUTIVE OFFICE OF THE PRESIDENT OFFICE OF MANAGEMENT AND BUDGET, Ed.). Washington, D.C.

Lindgren, S., & Lundström, R. (2011). Pirate culture and hacktivist mobilization: The cultural and social protocols of WikiLeaks on Twitter. *New Media & Society, 13*(6), 999–1018.

Lipman, F. D. (2011). *Whistleblowers: Incentives, Disincentives, and Protection Strategies* (Vol. 575). Hoboken, New Jersey: John Wiley & Sons.

Masnick, M. (2014, July 2). Austrian Tor Exit Node Operator Found Guilty As An Accomplice Because Someone Used His Node To Commit A Crime [Web log post]. Retrieved November 10, 2014 from: https://www.techdirt.com/articles/20140701/18013327753/tor-nodes-declared-illegal-austria.shtml.

McGonagle, T. (2014). Committee of Ministers:: Protection of whistleblowers. *IRIS: Legal Observations of the European Audiovisual Observatory*, (7), 2-3.

Morozov, E. (2013). *To save everything, click here: The folly of technological solutionism*. PublicAffairs.

Office of Management and Budget. (2014). Suitability and Security Process Review. Washington D.C.: White House.

Olson, P. (2012). *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. New York : Little, Brown and Co.

Privacy International. (2009). Model brief on the protection of journalists' sources. London: Privacy International.

Prozorov, S. (2007). *Foucault, freedom and sovereignty*. Hampshire: Ashgate.

Sauter, M. (2013). “LOIC Will Tear Us Apart”: The Impact of Tool Design and Media Portrayals in the Success of Activist DDOS Attacks. *American Behavioral Scientist, 57*(7), 983-1007.

Scott, J. F. (1971). Internalization of norms: A sociological theory of moral commitment.Oxford, England: Prentice-Hall.

Shankland, S. (2011, June 13). Turkey arrests 32 after Anonymous' Web attacks [Web log post]. Retrieved November 10, 2014, from http://www.cnet.com/news/turkey-arrests-32-after-anonymous-web-attacks/

Stalder, F. (2010, November 6). Leaks, Whistle-Blowers and the Networked News Ecology [Web log post]. Retrieved November 10, 2014, from http://felix.openflows.com/node/149

The NSA files. (2013). *The Guardian*. Retrieved December 30, 2013, from http://www.theguardian.com/world/the-nsa-files

Wray, S. (1999). On electronic civil disobedience. *Peace Review, 11*(1), 107-111.