IS HACKTIVISM THE NEW CIVIL DISOBEDIENCE?

Candice Delmas

Presses de Sciences Po (P.F.N.S.P.) | « Raisons politiques »

2018/1 N° 69 | pages 63 à 81

ISSN 1291-1941
ISBN 9782724635485

Is Hacktivism the New Civil Disobedience?

Candice Delmas

What do Edward Snowden's leaks of classified documents to journalists, the Pirate Bay's peer-to-peer file-sharing program BitTorrent, and Anonymous' distributed denial-of-service (DDoS) attacks in "Operation: Avenge Assange" have in common? What does Aaron Swartz's downloading of millions of academic publications on JStor share with Telecomix's provision of anti-censorship software to international pro-democracy groups under surveillance? Not much at first glance, beyond their involving the principled, unauthorized use of computers: they were undertaken through different methods, against different targets, and in opposition to different kinds of perceived injustices including governmental secrecy, intellectual property law, and human rights abuses; some were led by small, tight-knit and organized groups, others by lone individuals, yet others by many unrelated people.

One interesting and perhaps surprising commonality is that sympathizers of these actions submitted that they were instances of *civil disobedience*. Molly Sauter defends DDoS actions as a form of "civil disobedience on the Internet".[1] Peter Ludlow extolled Swartz as a courageous civil disobedient.[2] William Scheuerman praised Snowden's whistleblowing as justified civil disobedience.[3] Telecomix's provision of anti-surveillance and anti-censorship software (aka Digital Care Packages) has been considered a form of civil disobedience.[4] Hacktivism in general – the principled, unauthorized use of computers or computer networks – has been dubbed the new civil disobedience, electronic civil disobedience (ECD), or "civil disobedience 2.0".

[1] - Molly Sauter, *The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet*, London: Bloomsbury Academic, 2014.

[2] - Peter Ludlow, "Aaron Swartz Was Right", *The Chronicle of Higher Education*, February 25, 2013 (retrieved May 24, 2016 at: http://www.chronicle.com/article/Aaron-Swartz-Was-Right/137425).

[3] - William E. Scheuerman, "Whistleblowing as Civil Disobedience: The Case of Edward Snowden", *Philosophy and Social Criticism*, 40: 7, 2014, pp. 609-628.

[4] - Taylor Owen, *Disruptive Power: The Crisis of the State in the Digital Age*, Oxford: Oxford University Press, 2015, p. 54.

Painting hacktivists as civil disobedients highlights their principled motivations and communicative intentions: their actions are speech-acts, grounded in sincere political commitments. This gloss makes hacktivism legible to the broader public as a protest, and situates it within a well-known and respectable tradition of civil disobedience, along the likes of Rosa Parks and Martin Luther King, Jr. In particular, it seeks to make a place for hacktivism in liberal democracy – a crucial endeavor in the face of states' crackdown on hacktivists.

States have indeed developed very stringent laws to protect the security of cyber systems. The United States government, for instance, uses not only the Computer Fraud and Abuse Act (CFAA), but also the Racketeer Influenced and Corrupt Organizations (RICO) Act, which initially targeted Mafia groups, as well as anti-terrorism and anti-treason statutes, to suppress hacktivism. Before becoming president, Donald Trump repeatedly called for Snowden's execution. Swartz risked a 35-year sentence at the time of his suicide. U.S. Attorney General Jeff Sessions recently said that arresting WikiLeaks founder Julian Assange was a priority for the Justice Department. Though once hailed as the "heroes of the Computer Revolution", hackers and hacktivists have become the "villains of the Information Age". [5]

My goal is to articulate an approach to hacktivism that is phenomenologically accurate (that reflects to some extent agents' experiences, attitudes, and self-understanding), politically useful (by helping to frame public discourse), and open to its justification (contra states' lack of good faith engagement with hacktivists). This paper begins this project by laying the groundwork for a multi-lens approach to hacktivism and briefly sketching some dimensions for its normative assessment.

But why look further than the understanding of hacktivism as the new civil disobedience? This understanding seems, at first glance, to satisfy the desiderata just laid out: it reflects at least some practitioners' self-understanding – for instance, Telecomix conceives of its hacktivism as civil disobedience; and Swartz called for a movement of civil disobedience against the privatization of knowledge, which he described as "this theft of public culture" [6] – and it helps to counter state officials' and media's vilification of hacktivists by situating them within a venerable political tradition. Yet as I argue in this paper, most recent hacktivism isn't, and shouldn't be shoehorned into the category of, civil disobedience. Instead, I will sketch a broad matrix of electronic resistance, attentive to the many shapes and goals of hacktivism.

The paper proceeds as follows. Sections 1 and 2 focus on the two approaches that theorists tend to adopt to classify hacktivism as civil disobedience: Either they apply the defining criteria standardly associated with traditional, offline

[5] - Steven Levy, *Hackers: Heroes of the Computer Revolution*, O'Reilly Media, 1984; Helen Nissenbaum, "Hackers and the Contested Ontology of Cyberspace", in R. J. Cavallier (ed.), *The Impact of the Internet on Our Moral Lives*, Albany: SUNY Press, 2005, pp. 139-160.

[6] - Aaron Swartz, *Guerilla Open Access Manifesto*, 2008 (Stable URL, retrieved April 20, 2017: https://archive.org/stream/GuerillaOpenAccessManifesto/Goamjuly2008_djvu.txt).

civil disobedience (I call it the standard ECD approach); or they broaden the concept of civil disobedience so that it encompasses hacktivism (the inclusive ECD approach). Section 1 argues that the standard account of hacktivism as ECD is too narrow, prejudiced against hacktivists, and based on problematic assumptions. Section 2 argues that the inclusive account of civil disobedience strains to fit many hacktivist operations and is neither productive nor helpful since it stretches beyond recognition the ordinary understanding of civil disobedience. Section 3 articulates a matrix of electronic resistance and locates five clusters on it, briefly sketching possible dimensions of normative assessment for each: vigilantism, whistleblowing, guerrilla communication, electronic humanitarianism, and electronic civil disobedience.

The standard ECD approach

The theoretical framework applied to hacktivism is often the one used to identify and assess traditional (offline) civil disobedience. Proponents of the standard ECD approach hold that hacktivist acts that meet the criteria of traditional civil disobedience belong to the category of "electronic civil disobedience" and may then be justified, while hacktivist acts that fail to meet the criteria cannot be justified. John Rawls's theory of civil disobedience, articulated in the 1960s and 1970s, during the civil rights and antiwar protests in the United States, looms large here. In Rawls's view, which is considered (or was, until recently) the standard account, civil disobedience is a public, nonviolent, politically motivated, and conscientious breach of law undertaken with the aim of bringing about a change in laws or government policies. [7] In addition, agents of civil disobedience are to appeal to the community's shared conception of justice in their pleas and to demonstrate their general "fidelity to law" and endorsement of the state's legitimacy by accepting, or even seeking out, the legal consequences of their actions.

Scheuerman explicitly uses Rawls's conception of civil disobedience in a recent article on Edward Snowden's leaks, stressing the whistleblower's "fidelity to law". [8] Other theorists of ECD have chosen a framework very similar to Rawls's, if not Rawls's own. For instance, Brian Huschle lays out seven criteria to identify civil disobedience – including conscientiousness, publicity, nonviolence, respect for law, and exhaustion of legal means – most of which feature in Rawls's theory as either definitional or justificatory requirements. [9] Mark Manion and Abby Goodrum take themselves to be offering a "noncontroversial" – again, essentially Rawlsian – account of civil disobedience, which involves: nonviolence, understood to prohibit damage done to persons or property; ethical motivation; and willingness to accept responsibility for

[7] - John Rawls, *A Theory of Justice*, Cambridge: Harvard University Press, 1999 [1971], § 55-58.

[8] - William E. Scheuerman, "Whistleblowing as Civil Disobedience".

[9] - Brian J. Huschle, "Cyber Disobedience: When is Hacktivism Civil Disobedience?", *International Journal of Applied Philosophy*, 16:1, 2002, pp. 72-73.

outcome.[10] Kenneth Himma's proposed definition similarly echoes Rawls's as he conceives of civil disobedience as "(1) the open, (2) knowing, (3) commission of some non-violent act, (4) that violates the law, (5) for the expressive purpose of protesting the law (or the legal system) or calling attention to its injustice".[11] A hacktivist act is thus an act of ECD, and can be justified, if it meets a series of defining features typically associated with traditional civil disobedience. Hacktivist acts that fail to meet the criteria of civil disobedience are mere cyber crimes and cannot be justified.

In fact, few hacktivist acts are found to satisfy the identifying criteria of ECD, let alone its justificatory conditions. Himma's ECD framework, for instance, requires hacktivists do not cause damage to innocent third parties; be prepared to accept responsibility; and pursue a plausible and well-supported political agenda. Himma evaluates the latter requirement in light of popular political morality and finds that it justifies protests against human rights violations but excludes hacktivist operations intended to promote "digitally correct" values such as electronic freedom and privacy.[12] Because of this rigid application of the traditional, Rawlsian framework, Himma cannot account for the quite reasonable possibility that hacktivists' novel forms of resistance speak to novel issues. His a priori restriction of ECD to a certain agenda at the exclusion of another is unwarranted and arbitrary, as was Rawls's own restriction of justified civil disobedience to blatant and long-standing violations of the first principle of justice, according to many critics.[13] The standard ECD approach, in short, seems unfairly stacked against hacktivists.

The problem is that theorists unreflectively and wrongly assume that the online world is strictly analogous to the offline world. Consider what is missing online: there are no streets; no public forum where one can be heard; no democratic authority; and although there are many opportunities for voicing one's opinion online, speech is always mediated, and potentially regulated and censored, by Internet providers. Protesting against a company on one's personal blog is akin to shouting from one's living room; there is no lawful online equivalent of protesting outside a company's storefront or headquarters. To do the latter, hacktivists have to digitally trespass on private property (e.g., through website defacement or DDoS actions), which already raises the stakes for disobedients, compared with their offline analogues.

[10] - Mark Manion and Abby Goodrum, "Terrorism or Civil Disobedience: Toward a Hacktivist Ethic", *Computers and Society*, 30:2, 2000, p. 15.

[11] - Kenneth Eimar Himma, "Hacking as Politically Motivated Digital Civil Disobedience: Is Hacktivism Morally Justified?", in K. E. Himma (ed.), *Readings on Internet Security: Hacking, Counterhacking, and Other Moral Issues*, Boston: Jones & Bartlett, 2006, p. 74.

[12] - "Digital Correctness" is Paul Taylor and Tim Jordan's term for hackers' informational politics. See Tim Jordan and Paul Taylor, *Hacktivism and Cyberwars: Rebels with a Cause?*, New York: Routledge, 2004.

[13] - See for instance Peter Singer, *Democracy and Disobedience*, Oxford: Clarendon Press, 1973, p. 88; William Smith, *Civil Disobedience and Deliberative Democracy*, New York: Routledge, 2013, p. 43; Robin Celikates, "Democratizing Civil Disobedience", *Philosophy and Social Criticism*, 42:10, 2016, p. 5.

Gabriella Coleman quotes an Anon's response to the charge of "promoting lawlessness" in Operation: Payback (a series of DDoS actions that included Operation: Avenge Assange): "We are not concerned with legality but with legitimacy".[14] This comment points to a larger issue. Rawls's theory of civil disobedience – and, by extension, the standard ECD approach – is supposed to apply to the special case of the near-just, legitimate society. This explains why civil disobedients ought to accept the moral duty to obey the law and respect the state's authority, and show it by their willingness to accept punishment, for instance. But this background condition of near-justice and basic legitimacy is conspicuously absent online – which is often precisely what hacktivists are protesting.

Lawrence Lessig has shown how the U.S. has shaped the digital world into a surveillance- and commerce-friendly space, by exporting an "architecture that facilitates control" through technology product sales.[15] Bernard Harcourt has recently argued that the Internet is governed by a "tentacular oligarchy" that ties private and public institutions in "state-like knots of power" and engages in increasingly sophisticated surveillance of people's on- and offline behavior.[16] Freedom of speech is not protected online since it can be constrained by the corporate decision-making of Internet intermediaries, including Internet service providers, web hosting providers, and social network operators (Facebook, Amazon, PayPal, Apple, etc.).[17] Ethan Zuckerman dubs this phenomenon the "threat of intermediary censorship".[18] This is the basic architectural issue which Lessig talks about: people's ability to speak online and reach an audience is always mediated by commercial entities, whose terms of service generally give a great deal of discretion to the content host and few protections for the end user. Rebecca MacKinnon has also made a persuasive case for the democratic deficit of the laws that govern cyber space, all the while expressing faith in the Internet's potential for invigorating democracy and being itself democratically controlled.[19]

[14] - Gabriela Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*, London: Verso, 2014, p. 112.

[15] - Lawrence Lessig, *Code and Other Laws of Cyberspace*, New York: Basic Books, 1999.

[16] - Bernard Harcourt, *Exposed: Desire and Disobedience in the Digital Age*, Cambridge: Harvard University Press, 2015.

[17] - A point of clarification: I support Internet companies' hateful conduct policy, their ability to ban users for violating terms of use, and their monitoring and reporting terrorist networks, among other regulations. But it is important to keep in mind that a majority of the world's Internet users live in countries that restrict Internet access and online speech, and often target activists, dissidents, and journalists; and that U.S. based platforms such as Twitter and Facebook by and large heed local governments' demands for censorship. There are insufficient legal protections today for Internet users and innovators, making it all too easy for governments and companies to undermine basic rights. See Electronic Frontier Foundation, "Free Speech", 2017 (retrieved May 24, 2017 at: https://www.eff.org/issues/free-speech).

[18] - Ethan Zuckerman, "Intermediary Censorship", in Ronald. J. Deibert, John G. Palfrey, Rafal. Rohozinski & Jonathan Zittrain (eds.), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, Cambridge: MIT Press, 2009, pp. 71-85.

[19] - Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom*, New York: Basic Books, 2010.

Not only do hacktivists have little option but to trespass on digital boundaries, but they shouldn't be required to display the kind of respect for authority that their civil disobedient counterparts are required to display, given the serious problems of online governance. Hence the standard ECD approach unreflectively applies a theory designed for a very different context. In contrast, champions of the inclusive account of civil disobedience have put forth a nuanced understanding of digital politics, but their concept of ECD has other flaws, as we shall see next.

The inclusive ECD approach

Some theorists, finding the Rawlsian conception excessively narrow, have replaced it with much more capacious concepts of civil disobedience that extend to all sorts of principled lawbreaking – and can easily incorporate hacktivism. Thus Kimberley Brownlee defines civil disobedience as "a deliberate breach of law taken on the basis of steadfast personal commitment in order to communicate our condemnation of a law or policy to a relevantly placed audience", and stresses that it need be neither public nor nonviolent. [20] Brownlee recently argued that Snowden's actions were civilly disobedient on her account but not on Rawls's. [21] Sauter also defends an inclusive account of civil disobedience that encompasses DDoS actions and is distinct from the narrow standard account. [22] For his part, Celikates, who spearheads the radical democratic approach, understands civil disobedience as:

> ... an intentionally unlawful and principled collective act of protest (in contrast to both legal protest and "ordinary" criminal offenses or "unmotivated" rioting), with which citizens – in the broad sense that goes beyond those recognized as citizens by a particular state – pursue the political aim of changing specific laws, policies, or institutions (in contrast to conscientious objection, which is protected in some states as a fundamental right and does not seek such change) in ways that can be seen as civil (as opposed to military). [23]

This broad and inclusive conception imposes no requirement on the agent's attitude toward the system, her target, or the principles she appeals to. Neither must the civilly disobedient act be necessarily public or nonviolent. It is, however, an act of protest that aims at political change. Both Brownlee's and Celikates's inclusive conceptions keep Rawls's core insight that civil disobedience is essentially a communicative act, leaving much else up for grabs.

[20] - Kimberley Brownlee, *Conscience and Conviction: The Case for Civil Disobedience*, Oxford: Oxford University Press, 2012, chap. 1.

[21] - Kimberley Brownlee, "The Civil Disobedience of Edward Snowden: A Reply to William Schueuerman", *Philosophy and Social Criticism*, 42:10, 2016, pp. 965-970.

[22] - Molly Sauter, *The Coming Swarm*, *op. cit.*

[23] - Robin Celikates, "Democratizing Civil Disobedience", *Philosophy and Social Criticism*, 42:10, 2016, p. 985.

Celikates has further offered a perceptive account of the specificities of the digital world. Following Critical Art Ensemble's seminal analysis [24], he conceives of the Internet as the new site of power, but also stresses that digitalization has structurally transformed and expanded the public spheres, in the process shifting and expanding the logic of power as well as the modalities of civil disobedience. [25] According to Celikates, Anonymous' hacktivist operations, including DDoS actions, embody new practices of civil disobedience that turn the technical infrastructure of power into the site of intervention. In particular, Celikates and Daniel de Zeeuw argue that Anonymous' use of botnets in Operation: Avenge Assange exemplifies "swarm-like forms of agency" that reveals the "algorithmification of politics", and constitutes a "symbolic-political intervention [that] allows it to be framed in terms of civil disobedience". [26] At the same time, the authors note, Anonymous' actions incorporates aspects of what has usually been seen as the "other" of civil disobedience – in this case, "pranksterism" (aka the "lulz").

Celikates pursues a worthwhile direction, as he aims to change and broaden our ordinary understanding of civil disobedience. And yet I don't think that we should try so hard to shoehorn DDoS actions in the category of civil disobedience, insofar as it stretches the concept of civil disobedience too far. Celikates himself recognizes the tension, when he and De Zeeuw note that Anonymous "explodes the traditional oppositions that delineate and define what civil disobedience can be". [27] They find that new practices of civil disobedience involve the "ambivalent introjection of civil disobedience's opposites", but assert that "it is only in its push forward, almost beyond itself, to the point of becoming something else altogether, that civil disobedience maintains its full importance". [28]

In short, much footwork is needed to frame hacktivism as the new civil disobedience. And to the extent that these supposedly new practices of civil disobedience involve features henceforth seen as incompatible with civility (like anonymity and pranksterism), as Celikates acknowledges, we may be skeptical of both the effort to categorize them as civil disobedience and of the likelihood that doing so could soon change public opinion. I thus agree with Scheuerman's argument that attempts to legitimize digital disobedience by including it in broadened categories of civil disobedience come at too high a price:

[24] - Critical Art Ensemble, *Electronic Civil Disobedience and Other Unpopular Ideas*, New York: Autonomedia, 1998.

[25] - Robin Celikates, "Digital Publics, Digital Contestation: A New Structural Transformation of The Public Sphere?", in Robin Celikates, Regino. Kreide, and Tilo Wesche (eds.), *Transformations of Democracy*, London, Rowman & Littlefield, 2015, p. 172.

[26] - Robin Celikates and Daniel De Zeeuw, "Botnet Politics, Algorithmic Resistance and Hacking Society", *Hacking Habitat*, Rotterdam: nai010, 2016, p. 213.

[27] - *Ibid.*

[28] - *Ibid.*, p. 211.

> Conflating digital with more conventional forms of civil disobedience risks distorting what may be distinctive about both. Doing so also risks forcing genuinely creative types of digital illegality into a conceptual and normative straightjacket that they should not be forced to wear. [29]

Not only inclusive accounts stretch civil disobedience beyond its common meaning, but, I shall submit, they may also miss the point of many hacktivist actions, which is to refuse to follow the standard script of civil disobedience.

Many hacktivist operations clearly violate the standard, publicly accepted defining criteria of civil disobedience, and are not styled as civil disobedience, even if they may fall within capacious conceptions of the latter. Mark Dery, early champion and theorist of culture-jamming, conceives of "hackers, slashers, and snipers" (i.e., government whistleblowers, billboard bandits, and media hoaxers), as "artistic terrorists" and "communication guerrilla" fighters, suggesting *incivility* rather than civility. [30] In order to launch an automated DDoS attack, Anonymous assembles zombie botnets by infecting computer networks with destructive malware. Client-sided DDoS actions, which involve all voluntary botnets, may evoke "virtual sit-ins", as Critical Art Ensemble argued, but zombie botnets summon other, more sinister visions... Note that one *might* have expected Anonymous, for instance, to explain why automatic DDoS actions using involuntary botnets must be conceived as the latest avatar of ECD, given websites' improved cyber security capabilities. But they have not tried to do that. Instead, many Anons brandish pranksterism as an identity and badge of pride and embrace their status as rebels or villains of the Information Age. They are not committed to the standards of civility.

All in all practitioners' understanding of hacktivism as ECD is not as common today as it once was. There are exceptions: Swartz and Snowden situate the open-access movement and government whistleblowing, respectively, within the tradition of civil disobedience. I discuss both types of hacktivism in the next section, agreeing with Swartz but taking issues with Snowden. As I tried to show in this section, we shouldn't think of hacktivism as the new civil disobedience, because doing so distorts the phenomena. To accommodate novel forms of digital resistance, we should enrich our conceptual and normative framework.

A matrix of electronic resistance

In the remainder of this paper, I propose to sketch a broad matrix of electronic resistance and begin to populate it with five categories or clusters. ECD is one, but I will suggest that it occupies a minor place on the matrix.

[29] - William E. Scheuerman, "Digital Disobedience and the Law", *New Political Science*, 38:3, 2016, p. 310.

[30] - Mark Dery, "Culture Jamming: Hacking, Slashing and Sniping in the Empire of Signs", *Open Magazine Pamphlet Series*, Unknown, 1993.

Others are vigilantism, whistleblowing, guerrilla communication, and electronic humanitarianism. The matrix I offer does not put forth necessary and sufficient conditions. It highlights instead central features of the concepts in question, like constellations on the matrix rather than sharply outlined categories. It also gestures at the kind of normative considerations that would justify each type of electronic resistance.

I use *resistance* to designate a broad range of dissident activities, which express principled – that is, morally or politically motivated – opposition, and perhaps refusal to conform, to a dominant system of values, norms, rules, and practices. It is *electronic*, quite simply, when it is undertaken online. The five-fold typology I offer is not exhaustive – it does not say anything about *cyber terrorism*, for instance, at one corner of the matrix, or hashtivism (short for hashtag activism) at another, which includes signing petitions, online fundraising, emailing one's representatives, boycotting web services, raising awareness about an issue, and expressing solidarity on social media. [31] I dub *hacktivism* or principled digital disobedience acts of electronic resistance that are unlawful or whose legality is contested, thereby making lawbreaking rather than hacking central to the definition. [32] All five types of electronic resistance – vigilantism, whistleblowing, guerrilla communication, electronic humanitarianism, and ECD – have offline analogues; yet their being digital begs particular questions for assessing them. Except for ECD, which by definition involves lawbreaking, the other types of electronic resistance below are not necessarily illegal. I focus on hacktivism, that is, digital disobedience, on the assumption that illegality is presumptively wrong. [33]

Vigilantism

After the shooting of unarmed black teenager Michael Brown by a police officer in Ferguson, MO, Anonymous collected all the available information under the hashtag #OpFerguson. The group also threatened to hack the Ferguson police department if they did not immediately release the identity of the shooter. The police did not comply and Anonymous doxxed the alleged police officer's identity, including his social security number, his home address, the name of his children and the school they attended. This, I submit, is a form of vigilantism, not civil disobedience, even though it was motivated by a

[31] - Note that according to cyber security and cyber terrorism law in the U.S., any use of computer or online network that facilitates a terrorist enterprise is unauthorized. This means that what I describe as hashtivism, including social media activism and online fundraising, is in fact cyber terrorism if it purports to help carrying out terrorist operations. The only prosecutions of cyber terrorists in the U.S. were for individuals who were engaged in online fundraising for terrorist operations.

[32] - One reason for doing so is that, if hacking were central, we would have to say that only the organizers, and not the participants of a hacktivist operation such as a client-sided DDoS action, which requires some level of technological mastery, are hacktivists. This strikes me as arbitrary.

[33] - I examine and challenge this assumption in Candice Delmas, *A Duty to Resist: When Disobedience Should Be Uncivil*, New York: Oxford University Press, 2018.

concern for social justice. It involves hacktivists taking the law into their own hands to retaliate against or punish wrongdoers.

I propose to conceive of *digital vigilantism* as the illicit use (or credible threat of use) of computers and computer networks, motivated by a concern for justice or the good of the (online or offline) community, undertaken by agents who are not willingly accountable to the state, for the purpose of controlling (preventing, punishing, and/or retaliating against alleged wrongdoer (individuals, corporations, institutions, states). The perceived wrongs may be committed online and/or offline and include anything from human rights violations to insensitive jokes. Digital vigilantes are not accountable to the state, though they may sometimes collaborate with it. For instance, Anonymous relayed evidence of cyber bullying to the authorities in #OpAntiBully. Digital vigilante methods include DDoS attacks, as in Operation: Payback; leaks, doxxing, trolling, and shaming, as in Hunt Hunter (in which Anonymous shut down a big "revenge pornography" website and exposed its creator, Hunter Moore); and hacking simpliciter (for instance, Intangir shut down links to child pornography in the Hidden Wiki).

In general, vigilantism constitutes an impermissible arrogation of state powers like enforcing the law, protecting rights, preventing crime, and punishing wrongdoers. Can particular digital vigilante acts be nonetheless justified? Mostly not, though some may be, depending on hacktivists' method, target, and goal.

Digital vigilantism that involves doxxing or trolling, as it so often does, cannot be justified, even if the target engaged in serious wrongdoing, given the serious risks of physical and emotional harm that these methods impose. As a matter of fact, Anonymous doxxed the wrong officer in OpFerguson, so it was clearly impermissible. But I don't think that it would have been justified, if it had exposed the actual shooter of Michael Brown, given the risks of subjecting him and his family to mob violence (as the alleged shooter was). Trolls not only annoy and provoke, but also harass and persecute. They often direct their vitriol at illegitimate, vulnerable targets, such as female gamers and comedians. Indeed, trolling seems to constitute the online enforcement arm of misogyny. [34] Even when vigilantes direct their ire toward legitimate targets, such as Hunter Moore, they are not justified in taking the law in their own hands but must leave its enforcement to the state.

Only when online vigilantes choose a course of action that does not endanger or unjustifiably intimidate particular individuals, and direct it at a legitimate target (an entity engaged in wrongdoing), in a context where one can reasonably expect authorities to do nothing (say, because the law is silent on the issue or the state unwilling or unable to prosecute), can they be (perhaps) justified. In Hunt Hunter, Anonymous incited online mob violence against Hunter Moore, and there was no reason to doubt that authorities would go after him – as they did (many of the photos and videos on his site having

[34] - Danielle K. Citron, *Hate Crimes in Cyberspace*, Cambridge: Harvard University Press, 2014.

been stolen from women's computers). For another example of unjustified vigilantism, the hacktivist collective known as the Impact Team exposed all registered patrons of the cheating website AshleyMadison.com, supposedly in order to denounce the site's weak privacy protections. Exposing cyber security flaws may well be a worthy goal from the standpoint of consumer protection, but doxxing users' information does not serve that purpose at all. Operation: Payback, on the other hand, could be justified insofar as it did not risk harming anyone (nor did it destroy any data) and was clearly framed as a protest against companies that heeded the government's request that they block donations to WikiLeaks. But more needs to be said to complete the justification, as these brief remarks merely purport to gesture toward it.

Whistleblowing

Whistleblowing in general consists in the intentional disclosure of information about an agent or entity's suspected illegal or unethical conduct. The act may be entirely lawful, and in accordance with appropriate legal channels or protocols, or it may be unlawful (or again, its legality may be a matter of controversy). The unauthorized use of computers or computer networks in the process makes it illegal – and, for our purposes, a type of hacktivism. The target may be a private corporation, a public entity, or a non-governmental organization; and the agent may be an insider to the conduct he seeks to denunciate, such as Snowden, who alerted the public to the NSA's massive, unconstitutional surveillance programs; or an outsider, such as hacktivist Jeremy Hammond, who exposed that the private geopolitical intelligence firm Strategic Forecasting, Inc. (Stratfor for short) spied on human rights activists.

Digitalization did not fundamentally alter the nature of whistleblowing, but it did facilitate it. Nowadays, most whistleblowing involves seizure and leaks of electronic data, because most information is stored online. One difference may be in the ease and magnitude of leaks: it took months for Daniel Ellsberg to photocopy the 700 pages of the Pentagon Papers report; and just a few days for Snowden to seize hundreds of thousands of classified documents (1.7 million according to the Department of Defense).

This partly explains states' fear of and crackdown on hacktivist whistleblowers and their willingness to impose very harsh punishments for the sake of deterring future whistleblowers. Hammond is currently serving 10 years in U.S. federal prison for hacking Stratfor and releasing the stolen documents to WikiLeaks. States are especially hostile to government whistleblowing, that is, the unauthorized acquisition (typically through theft of protected documents) and disclosure (typically through leaks to a news outlet) of classified information about misconduct in the state or government.

Government whistleblowing is presumptively impermissible because it involves transgressing the state's determination of, and exclusive control over, the proper scope of secrecy. As a result, classified information may fall into the wrong hands, undercover agents or informants may be exposed, and ongoing military operations may be revealed to the detriment of service members and national-security strategy. The Senate Select Committee on Intelligence considers leaks of classified information the second-greatest global security threat to the U.S., ahead of international terrorism.

For these reasons, government whistleblowing is different from, and harder to justify than, civil disobedience. Yet it can be justified as long as: (1) it exposes serious government wrongdoing or programs and policies that ought to be known and deliberated about; (2) the whistleblower exercises due care in the disclosure so as to minimize potential harms; and (3) the whistleblower attempts first to publicize the information lawfully.[35] When government whistleblowing is justified, it serves to enhance the democratic rule of law.[36] Snowden's leaks, in my view, satisfied these conditions and served that function.

One might point to WikiLeaks' release of the Democratic National Convention emails and then of Hillary Clinton's and John Podesta's emails, probably obtained thanks to Russian spies, as evidence of the need to take into account whistleblowers' motives. Whistleblowing, the objection goes, should only be justifiable when it is undertaken out of worthy motives such as patriotism and concern for justice and democracy. Suppose it is the case, on the one hand, that Russians sought to undermine U.S. democratic elections, as is widely believed, and, on the other hand, that Julian Assange decided to publish the emails to help Trump's chances and avoid prosecution under Clinton (he suggests thinking in terms of "better the devil you don't know than the devil you do" in *Risk*, Laura Poitras's 2017 documentary about him[37]). Surely, none of it can be justified.

In response, first, leaks that ultimately seek to interfere with democratic processes – as these did – are likely to fail the conditions mentioned above anyway. WikiLeaks published en masse the troves of emails from the DNC and Clinton's campaign staff without editing any of it, thereby violating the second condition, which requires exercising caution in the release and minimizing the potentially harmful effects of the disclosure. Nor was there any attempt to address the DNC's abuses of power through lawful channels first. But perhaps the objection's point is that the agent ought not only to act in the manner prescribed by the second and third conditions, but also *for the purpose* embedded in the first condition (that is, to address a significant informational deficit), and with a demonstrated commitment to all three. This would easily rule out ill-intentioned denunciations.

I find this specification tempting, but hesitate to incorporate it to the account for the following reason: some information may be of great public interest even if the agent who brought it to light did it for "disreputable"

[35] - I develop an account of the presumptive wrongfulness of government whistleblowing, and of its justificatory conditions in: Candice Delmas, "The Ethics of Government Whistleblowing", *Social Theory and Practice*, 41:1, 2015, pp. 77-105.

[36] - William Scheuerman makes this point about civil disobedience in general, using Snowden as an archetype in his: "Recent theories of civil disobedience: An anti-legal turn?", *The Journal of Political Philosophy*, 23:4, 2015, pp. 427-449.

[37] - Laura Poitras, *Risk*, Praxis Films: Berlin, Germany, 2017.

motives, such as self-interest. Thus the government invites criminal informants to testify against other criminals in exchange for reduced sentences; and the Dodd-Frank Wall Street Reform and Consumer Protection Act provides financial incentives to corporate whistleblowers by rewarding them with a share of the money they help the government save. More to the point, some philosophers have argued that the DNC leaks, regardless of the leakers' ulterior motives, indicate "a worrisome pattern of political corruption within the DNC with important implications on the overall dynamics of accountability of the electoral campaign" [38]; and that "the public interest of the DNC leaks shall not depend on the wicked intention of the Russian government, but on the content of those revelations". [39] This suggests that we should be wary of putting too much weight on whistleblowers' motives, and should carefully distinguish appraisal of persons from evaluation of actions.

Guerrilla communication

Though listed third in the present typology, *guerrilla communication* appears as *the* original hacktivist tactic, touted by Critical Art Ensemble, Cult of the Dead Cow, and other early hacktivists. Guerilla communication or "cultural jamming" is a form of media activism that consists of subverting or disrupting dominant systems of signification, including verbal and non-verbal, visual and other modes of communication such as mainstream cultural media. Dery conceives of culture-jamming as a kind of "guerrilla semiotics", following Umberto Eco's concept of "semiological guerrilla warfare". [40] With the latter, Eco urges "the audience to control the message and its multiple possibilities of interpretation" and to "restore a critical dimension to passive reception". [41]

Guerilla communication is the favored method of anti-consumerist activists, whose tactics include billboard banditry (altering billboards to create anti-corporate messages) and website defacement (aka e-graffiti). For instance, the No Border network created a fake Lufthansa website touting its "Deportation Class service... the most economic way to travel the world" ("special restrictions apply... no round trips available"). [42] For another example of hacktivist guerrilla communication – one that epitomizes a digitalized and artistic expression of anti-consumerism – consider the Random Darknet Shopper (RDS). The project is part digital disobedience, part performance art installation. It is an automated online shopping bot, which randomly chooses and

[38] - Emanuela Ceva, "The Surreptitiousness of Political Corruption", Guest post at *Daily Nous*, July 29, 2016 (retrieved May 22, 2017 at: http://dailynous.com/2016/07/29/philosophers-dnc-leaks/#Ceva).

[39] - Daniele Santoro, "The Value of Transparency" Guest post at *Daily Nous*, July 29, 2016 (retrieved May 22, 2017 at: http://dailynous.com/2016/07/29/philosophers-dnc-leaks/#Santoro).

[40] - Mark Dery, "Culture Jamming".

[41] - Umberto Eco, "Toward a Semiological Guerrilla Warfare", in *Travels in Hyper Reality: Essays*, William. Weaver (trans.), San Diego: A Harvest Book, 1986, p. 144.

[42] - No Border, *Deportation Class*, 2013 (retrieved May 22, 2017 at: http://www.noborder.org/archive/www.deportation-class.com/).

purchases one item per week from deepweb market places, and has it mailed directly to the exhibition space, where it is displayed. Items displayed include generic Viagra pills (date purchased: 10.02.16) and a tutorial on how to hack a Coca Cola machine (13.01.16). In the creators' words:

> The Random Darknet Shopper is a live Mail Art piece, an exploration of the deep web via the goods traded there. It directly connects the Darknet with the gallery. By randomizing its consumerism, the bot is guaranteed a wide selection of goods from the thousands listed on deepweb markets. [43]

Celikates and de Zeeuw use RDS to illustrate the transformations and algorithmification of civil disobedience. They conceive of guerrilla tactics as an integral part of civil disobedience, electronic or otherwise. Yet, to call it civil disobedience is to tame its aesthetic and radical disruptiveness. The risk is to misconstrue RDS as disobedience aiming to change specific laws or policies (per Celikates's concept of civil disobedience), when, instead, RDS invites reflection on the shadowy parts of the Internet without calling for any specific legal change, or articulating any specific political claim. Celikates wants to re-inject the concept of civil disobedience with the disruptiveness that made it powerful and attractive in the first place, but which the ordinary, sanitized and stale understanding of civil disobedience has much diluted. I am sympathetic with this ultimate goal but for now the fittest and most illuminating description of RDS, in my view, is as a form of guerrilla hacktivism.

For a last, striking example of guerilla communication (albeit legal), Jennifer Lyn Morone has responded to the Big Data economy with her own brand of hyper-capitalism as she turned herself into a corporation, Jennifer Lyn Morone Inc. JLM Inc. sells (1) "biological, physical and mental services, such as genes, labour, creativity, blood, sweat and tears", (2) "future potential in the form of shares", and (3) "accumulation, categorization and evaluation of data that is generated as a result of Jennifer Lyn Morone's life". [44] Her goal in doing so is to denounce our state of "data slavery", as Netizens willingly submit their every move to social media, lining the pockets of big business in the process. [45] JLM Inc. does not involve any digital disobedience – if anything it may be described as a form of what Jessica Bulman-Pozen and David Pozen call "uncivil obedience", that is, hyperbolic, literalistic, or otherwise unanticipated adherence to a legal system's formal rules or law. [46] Morone's piece indeed involves a hyperbolic observance of the norms governing the Age of Big Data,

[43] - Random Darknet Shopper, 2014-ongoing (official URL: https://wwwwwwwwwwwwwwwwwwwwww.bitnik.org/r/).

[44] - JLM Inc 2014. Jennifer Lyn Morone, Inc. *Vimeo*: http://vimeo.com/98300179 (retrieved February 21, 2017).

[45] - Bernard Harcourt, *Exposed*, *op. cit.*, Ch. 11.

[46] - Jessica Bulman-Pozen and David Pozen, "Uncivil Obedience", *Columbia Law Review*, 115:4, 2015, pp. 809-872. Examples include motorcyclists strictly adhering to the speed limit in order to protest it and the creation of a political action committee (Super PAC) by the TV host Stephen Colbert in order to ridicule Federal Election Commission rules.

for the purpose of subverting and denouncing them. In short, guerrilla tactics are provocative, versatile, and irreducible to civil disobedience.

While a project like JLM Inc. does not need any special justification, since it is neither illegal nor presumptively wrongful, guerrilla communication that involves digital disobedience does need to be justified. In my view, illegal yet harmless guerrilla campaigns such as Deportation Class and RDS simply need to exhibit some value to be justified. If their political and aesthetic value can weigh against potential costs such as brand infringement or the risk of tempting people to buy goods from the deepweb market, then they can be justified. More needs to be said, of course, but it's important to note both the highly disruptive potential of guerrilla communication and its low threshold of justification, where it does not risk inflicting any harms.

Electronic humanitarianism

The fourth cluster on the matrix of electronic resistance is *electronic humanitarianism*. Offline, humanitarianism broadly designates the organized effort to assist those in dire need everywhere. Authoritarian states routinely watch and censor dissidents and shut down the Internet to impede information access and the planning of popular protests. Hacktivists have created Digital Care Packages consisting of anti-censorship and anti-surveillance tools such as Tor, and Internet-back-up connectivity, and provided training to activists around the world on how to use these. Electronic Frontier Foundation offers free surveillance self-defense workshops. Anonymous helped Tunisian activists during the Arab Spring. And when Egypt cut off all Internet access in January 2011, Telecomix used European servers to set up dial-up connections and faxed the numbers to "every Egyptian office, university and coffee shop they could find".[47] Telecomix also "mapped" Syria (i.e., scanned the state's networks and servers for surveillance equipment) and established encrypted connections to help local activists make their online activity harder to monitor.

I propose to call the provision of Digital Care Packages electronic humanitarianism to frame these hacktivist operations as interventions against human rights violations. Some hacktivist participants view it as an anarchist rather than broadly liberal, human rights-centered enterprise. Telecomix, for instance, advocates "crypto-anarchism" and claims to seek "political disorganization".[48] Still, I don't think it misconstrues their activities to call them protective of human rights, insofar as they effectively empower dissidents and pro-democracy activists.

For a domestic example of electronic humanitarianism, hacktivists have manufactured and provided free social media tools to uphold civil liberties and monitor against officials' violations. For instance, the Mobile Justice App,

[47] - See https://www.washingtonpost.com/lifestyle/style/the-hacktivists-of-telecomix-lend-a-hand-to-the-arab-spring/2011/12/05/gIQAAosraO_story.html.

[48] - Telecomix.org (accessed February 28, 2017).

Hands Up 4 Justice, Stop and Frisk Watch, the Swat App, and Police Tape, allow citizens to (1) record: capture exchanges between police officers and themselves or other community members in audio or video files that are automatically backed up (e.g., uploaded to the Cloud); (2) witness: alert nearby app users when they are stopped by police (so as to watch for wrongful arrest); (3) report: provide a detailed account of citizens' interactions with police in an incident report, which, in Mobile Justice for instance, is transmitted directly to the American Civil Liberties Union (who can quickly provide legal assistance); and (4) know one's rights: provide legal information about the rights one has when one is dealing with law enforcement officers. These apps designed to monitor for police misconduct naturally fit in the cluster of electronic humanitarianism because of the broad concern with human – especially civil – rights. We could also identify sub-clusters of electronic humanitarianism, such as "electronic civil libertarian watchdog", to describe more precisely these apps against police brutality.

Finally, the Freedom of the Press Foundation, a non-profit organization dedicated to public-interest journalism manages an open-source whistleblower submission system that media organizations (including the New York Times) use to securely accept documents from and communicate with anonymous sources. SecureDrop, as the program is called, facilitates and empowers whistleblowers, in a sub-cluster of electronic humanitarianism we might label "whistleblower protection". Such protection is of course crucial not only to the prospective whistleblowers but to the public; it is a touchstone of journalism and a key to informed public deliberation.

Electronic humanitarianism is easily justified in many cases since it is of great public and democratic value. But here are some issues. First, opponents point to terrorists' own use of encryption tools to argue against their development. To be sure, the Darknet, which Tor enables, provides cover to terrorists as well as activists. Yet I do not see how this makes either hacktivists' provision or dissidents' use of these tools impermissible – rather, it simply points to a "dual use" problem inherent in the technology. Second, even in the developed world, the manufacture and distribution of data-encryption and censorship-circumvention tools is not legally protected. Worse, coders' tinkering with existing software programs often involves a breach of license that governments prosecute criminally. These adverse laws seriously hinder digital innovation in general and electronic humanitarianism in particular, in ways that I cannot begin to address here. [49] Third, the use of encryption tools, albeit lawful in the developed world, is often restricted or banned in the developing world, especially in authoritarian countries such as Egypt and China, whose governments monitor and crack down on activists. Yet the illegality of electronic humanitarianism under authoritarian regimes (as, say, breach of Internet regulations) does not make it even presumptively wrong. And

[49] - But see, for instance, Christophe Geiger, "Copyright as an Access Right: Securing Cultural Participation through the Protection of Creators' Interests", in Rebecca Giblin and Kimberlee Weatherall (eds.), *What If We Could Reimagine Copyright?*, Canberra, ANU Press, 2017, Ch. 3.

even if one thought it did, the benefits of electronic humanitarianism should clearly outweigh its putative costs.

Electronic civil disobedience

I answered the title of this paper negatively: much hacktivism is not, and should not be considered, the new civil disobedience. I also suggested that we need a better concept of electronic civil disobedience. Since the standard ECD approach is unduly restrictive and the inclusive approach is too broad, perhaps we should find a concept of ECD just right, according to some Goldilocks rule. But I will not propose such concept here because I have not yet found it. What I will say is this:

First, client-sided DDoS actions already seem to be relics of the past. Security systems are now so powerful that they can easily soak up huge amounts of traffic without experiencing any disruption. This suggests either that future mass online demonstrations would need to involve coerced botnets, or that there might not be anymore mass client-sided DDoS campaigns. It is also worth noting that states are responsible for the overwhelming majority of DDoS attacks against non-state actors, and have a superior capacity to destroy small sites, such as dissident blogs and pro-democracy NGOs' websites. [50]

Second, at the beginning of this paper I cited two hacktivist operations that I have not yet located on the matrix of electronic resistance: Swartz's JStor downloading and The Pirate Bay's peer-to-peer file sharing. Swartz was, and The Pirate Bay remains, champions of the Open Access Movement, which advocates for open-source software and an open-source repository of academic and scientific research. There is a way in which Swartz engaged in vigilantism when he downloaded millions of academic publications from JStor, since he considered the privatization of research, hidden behind paywalls, "theft of public culture": like Robin Hood, he wanted to take back what ought to belong to the people.

But my hunch is that if anything is the new civil disobedience, the Open Access Movement is. Swartz situates the movement within the "grand tradition of civil disobedience" in his *Guerilla Open Access Manifesto*. It epitomizes what ECD should be about: a public, geeks-and-grassroots mass movement advocating for the free flow of science and culture, with a coherent political platform (and even some seats in the European Union Parliament), and that constitutes the "avant-garde of the digital publics", in Celikates's phrase. [51] Some users of BitTorrent and other file sharing platforms may not think of themselves as engaged in principled, electronic resistance, but the fact that so many Netizens participate in a practice that prefigures and embodies the more just and legitimate online architecture the movement aspires to, spells, in my view, ECD.

[50] - Ethan Zuckerman *et al.*, *Report on Distributed Denial of Service (DDoS) Attacks*, Berkman Center for Internet and Security, December 20, 2010 (available at http://cyber.law.harvard.edu/publications/2010/DDoS_Independent_Media_Human_Rights).

[51] - Robin Celikates, "Digital Publics, Digital Contestation".

And it can be justified precisely as a popular practice pointing toward, and informing the public about, democratic online governance.

To conclude, what is called for to accommodate novel forms of digital resistance is neither an unreflective application of an ill-fitting and too narrow concept of civil disobedience, nor an extension of the latter concept beyond recognition. Instead, we need to enrich our conceptual framework and devise additional lenses besides ECD to approach these phenomena. I proposed above a matrix of electronic resistance populated by five clusters, outlining dimensions for the normative assessment of each: vigilantism, whistleblowing, guerrilla communication, electronic humanitarianism, and ECD. This typology paves the way for an ethics of hacktivism.

Acknowledgments

Versions of this paper were presented at the "Disobey!" Conference at the Institute of Sciences-Po, Paris; the ASPP conference at the London School of Economics; the PPL conference at Binghamton University; the workshop on Transformations of Civil Disobedience at Barnard College; and the United States Military Academy at West Point. I am very grateful to the organizers, participants, and audiences at these events for engaging discussions and useful suggestions. Special thanks to Guy Aitchison, Bernardo Caycedo, Robin Celikates, William Scheuerman, and anonymous reviewers for their valuable feedback on drafts of this paper. I completed this article while visiting the New York University School of Law's Center for Law and Philosophy as a Dworkin-Balzan Fellow in 2016-2017.

Author

Candice Delmas is Assistant Professor of Philosophy and Political Science at Northeastern University, and the Associate Director of the Politics, Philosophy, and Economics Program. She specializes in moral, legal, and political philosophy. Her work has appeared in *Ethics*, *Law and Philosophy*, *Res Publica*, *Analysis*, *Social Theory and Practice*, and *Oxford Journal of Legal Studies*, among other journals. Her book, *A Duty to Resist: When Disobedience Should Be Uncivil*, is forthcoming at Oxford University Press.

Abstract

Hacktivism is often dubbed the "new civil disobedience". Those who approve of particular leaks, DDoS attacks, illegal downloading, and anti-censorship software provision, among other hacktivist operations, often describe them as instances of electronic civil disobedience. They do so by either applying the defining criteria standardly associated with traditional, offline civil disobedience, or by broadening the concept of civil disobedience so that it encompasses hacktivism. Section 1 of this paper argues that the former approach to hacktivism as ECD is too narrow, prejudiced against hacktivists, and based on problematic assumptions. Section 2 submits that the latter, inclusive approach strains to fit many hacktivist operations and stretches beyond recognition the ordinary understanding of civil

disobedience. I thus suggest that much hacktivism is not, and should not be considered, the new civil disobedience, and articulate in section 3 a matrix of electronic resistance. I begin to populate this matrix with five clusters and briefly sketch possible dimensions of normative assessment for each: vigilantism, whistleblowing, guerrilla communication, electronic humanitarianism, and electronic civil disobedience.