Understanding Online Anonymity

Thais Sardá, Simone Natale, Nikos Sotirakopoulos, Mark Monaghan

Keywords

Online anonymity, privacy, technology, digital culture

In 1993, a famous cartoon published in the New Yorker proclaimed that 'On the Internet, nobody knows you're a dog'. At the time, the Web was a new technology that seemed destined to open novel ways for experiencing identity in interactions with other users. Early adopters were promised the opportunity to employ pseudonym and anonymity to play freely with their identities (Turkle, 1995). As the Web developed in the following years, new models of interaction and technical solutions appeared, showing the limits of this vision. Since personal identification was becoming a condition to use a number of services, and the continuities between offline and online identities appeared more contingent, scholars argued for the need to go "beyond anonymity" (Kennedy, 2006). Yet today, as the Web passed its twenty-fifth anniversary, the concept of online anonymity seems again extremely relevant to understand the social, political, economic, and cultural implications of the Internet. The importance of anonymous communications is evident from multiple perspectives. For instance, online anonymity is now regarded as a fundamental factor in the protection of private information and in reducing the dangers of the Web, such as hacking and malware (Hoang and Pishva, 2014), as a facilitator for participation in discussions about sensitive topics, health issues for instance, in computer-mediated communication (McLeod, 2011), and as an option for citizens to avoid government surveillance in highly repressive as much as highly liberal contexts (Jardine, 2016).

Since the emergence of the Web, then, much has changed that makes it necessary to revise basic assumptions around anonymity and the Internet. Arguably, the main dynamic igniting such change was the development and the increasing availability of new technical means that enable different degrees of online anonymity. This can be achieved in different degrees and through the use of a wide range of tools, including functions of the most widespread Internet browsers - such as the Incognito tab on Google Chrome -, proxies, virtual private networks (VPN), and the Tor Network, a browser employing multiple layers of encryption (Hoang and Pishva, 2014). The emergence of such technical tools forces us to reconceive online spaces as contexts in which different levels of anonymity and pseudonymity are performed through technical means, and to reflect more structurally on how both the technical and social dimensions inform the constructions of identity and the performance of privacy online.

A lively debate among policy-makers, security professionals, hacker communities, and human rights associations has recently ensued regarding the question if online anonymity is acceptable and in which form. This special Crosscurrents section aims to contribute to this discussion by highlighting some key aspects and applications of online anonymity, with particular emphasis on its uses and consequences. We invited three leading scholars in different fields to write short commentary pieces on the diversity of the topic. To each of them, we posed a question related to online anonymity, focusing on the relationship of

anonymity with activism, personal responsibility, and crime. The three responses, we hope, will help initiate further conversations and reflection around the issue. Despite their differences in topic and approach, these short contributions share the belief that understanding online anonymity in contemporary societies requires a new sensitivity by which the technical and the social dimensions are integrated and mutually reinforcing. In this introductory piece, we first provide some background to the topic of online anonymity before giving some consideration to the technical and social aspects that contribute to shape anonymity online, such as the technology employed, its social uses, and the different understandings and representations of online anonymity. Finally, we suggest that to fully understand the nature of online anonymity it is necessary to adopt a position that views anonymity not in absolute terms but as an inherently fluid and transitional condition that characterizes to a certain extent any kind of social interaction online.

The technical and social nature of online anonymity

If online anonymity is related to both social and technical issues, how should the role of these two different dimensions be investigated? Our answer to this question emerges from the tradition of social studies of media and communication that refuse to give primacy to either technological or social factors, but instead insists on the necessity to acknowledge and study how change emerges from the interactions between technology, society and culture (Williams, 1974). It is necessary, in this sense, to avoid a perspective that privileges one or the other dimension, developing an approach that looks instead at their mutual interrelations.

From a technical perspective, anonymous communications on the Internet can be achieved at different degrees using technologies such as modes of Internet browsers, proxy, VPN and Tor (Hoang and Pishva, 2014). For users who place a premium on privacy, one of the most established anonymity-granting technologies is The Onion Router (Tor). Tor is a browser that ensures a level of confidentiality through linking a network of computers which provide layers of encryption between user and the information source, making very unlikely for someone to trace back both sides (Minárik and Osula, 2016).

Although Tor is functionally neutral, since anonymity can be applied in multiple ways and shaped according to distinct purposes, there are two common appropriations of this technology: first, as a resource to circumvent political repression especially in highly repressive contexts to exercise freedom of speech; and second, as a new way to engage in illegal activity, taking advantage of online anonymity to escape law when committing crimes (Jardine, 2016). In fact, Tor is widely known for its illegal uses, and websites on this network are generically referred to as the Dark Net. Despite the variety of contents available through Tor, emphasis is often given only to crypto markets such as Silk Road, the most notorious online drug marketplace which connected thousands of sellers and buyers using Tor to preserve their identities from 2011 to 2013 (see Aldridge in this special section).

An anonymity-granting resource that is commonly available and widely used are VPN services, which are able to change the user's original IP address with another one in another location, typically offering multiple geographical locations around the world to the user to choose. As a result, tracking the user will lead to the IP address not of their computer, but of a server provided by the VPN. Data protection through VPN services has one primary advantage from a privacy point of view in that all the information shared by the user regardless of the applications is immediately encrypted and dispatched through a secure tunnel established by the VPN server. Due to the centralization of information by VPN

companies, however, this service alone is not considered completely secure. For instance, users' data may be used by this company for marketing purposes, or data about users may be released to authorities upon an official request (Hoang and Pishva, 2014).

Another key tool for privacy is end-to-end encryption, a form of electronic cryptography that works through a secret key shared by sender and receiver. This is a "core technology for data security and data protection and therefore constitutes a central component of the technical infrastructure of information society" (Winkel, 2003: 185). The instant messaging and calls service WhatsApp, for instance, employs such technology meaning calls and messages posted by users are secured with end-to-end encryption. This implies, according to WhatsApp (2018), that all the communications are protected from third parties, so that nobody apart from the sender and the receiver can access the content — not even WhatsApp (or Facebook, which owns this company). The same applies to the content of other messaging and email services, such as Gmail, which also offers a system of protection including in-transit encryption to preserve messages from interception.

Online anonymity, however, is defined as much by technical means as by their social uses and understandings. If technology provides multiple ways for users to protect, at least in part, their identity online, the ways through which users appropriate these technical tools are multiple, too. Given that privacy is related to the control over personal information about oneself and the right to decide how this information is available to others (Westin, 1967), anonymity is usually employed as a form of privacy enabler in the context of the Internet. In this regard, depriving the Web of one's personal data is a way to counterbalance the impact of online technologies, imposing a limit to the surveillance logic (Floridi, 2014). More broadly, in terms of social uses, online anonymity can be arguably compared to a weapon: on the one hand, it can be used to harm; but on the other hand, it is an instrument for self-defense. In fact, as a double-edged sword, online anonymity may help whistle-blowers to remain safe in totalitarian states, but also bullies to evade punishment. This has made the discussion about the social applications of anonymity in a context of interconnected surveillance particularly polarized (Jardine, 2016).

While anonymity plays a relevant role in the development of communication and collaboration tools, privacy-enhancing technologies are also regularly appropriated as a support to criminal activity. Illicit appropriations of online anonymity challenge the authority of law enforcements and restructure power relations and legal norms on the Internet, because the ability to hide the identity that protects users from prosecution can be used in multiple levels, such as creating new and more efficient forms of cybercrime (van Hardeveld et al., 2017), allowing the existence of drug crypto markets that capitalize on the anonymity tools (Martin, 2014; Morselli et al., 2017), adding sophistication to the hacking attack technology (Hoang and Pishva, 2014), and facilitating illegal file sharing, a practice that has been constantly growing on the Web (Larsson et al., 2012).

It is not only users' appropriation of technologies, but also their understandings and knowledge of these systems that informs online anonymity. As noted by Park (2011: 232), "knowledge plays a critical role in privacy behavior, the levels of understanding of surveillance practices common in websites remain miniscule among the majority of users." For this reason, promoting digital inclusion and reducing online inequality also passes through providing information about issues such as privacy and surveillance (Gangadharan, 2015). Additionally, as Tim Jordan demonstrates in this special section, people define anonymity in different ways, and as they navigate the Internet, use social media, or download the pirate copy of a film, they might have different degrees of consciousness about the extent

to which their identity is exposed or not. Users, for instance, might have the misguided belief that they are browsing completely anonymously when using the Incognito window on Google Chrome, while not even a sophisticated system such as Tor might seem safe enough to a skilled user for escaping surveillance. Not only rational choices but also emotions and affect play a role in these dynamics (Kennedy, 2006). On the same token, anonymity constantly intertwines with issues of race, gender and class. Despite the fact that visual and aural clues that mark people's identities in the offline world may be invisible online, even anonymity and pseudonymity do not allow to completely escape 'real world' identity (Kolko et al., 2013).

Finally, the social dimension of online anonymity also concerns representations that are given in the public sphere of issues related to online anonymity. In recent years, spaces of anonymity online have been often described through the label of Dark Web, usually described in negative terms as an obscure part of the Web exploited for illegal activities and endeavors. As documented by initial findings of a content analysis being conducted by Sardá on more than 800 articles published between 2001 and 2017 on the British newspapers Daily Mail, Daily Mirror, Daily Telegraph, The Guardian, The Sun, and The Times representations of the Dark Web are underpinned by a sharply negative characterization positing a strict link between online anonymity and criminal or antisocial activities. Counteracting the positive and optimistic representations of the Web as the harbinger of personal freedom, participation, and democracy, online anonymity is thus presented as related to the "dark side" of the Web (Flichy, 2007; Brunton, 2013). This may ultimately have an impact on uses and understandings of online anonymity, not only because media representations inform people's understandings and behavior, but also because discourses about the Internet inform public policies and may have therefore practical consequences (Crawford, 2007).

While it is important to highlight different dimensions of online anonymity, the study of this phenomenon cannot be conducted by considering any of these elements alone. Technical issues, uses, understandings, representations and policies are strictly interrelated, and it is within the space of their interrelation that anonymity is experienced and operationalised online. We propose, as a consequence, that the study of this phenomenon should rely on a deep understanding of the fluid nature of online anonymity. This implies that technical and social aspects are never to be taken as a given, because their meanings and implications only emerge from the mutual interactions between these dimensions.

The fluidity of online anonymity

Debates about online anonymity are often characterized by a high degree of polarization: on the one side, critics call for more restricted regulations of anonymity-enabling tools and send alarmed calls for the questionable uses of online anonymity, such as the lack of accountability on the publication of sensitive information by WikiLeaks (Zajácz, 2013); on the other side, supporters of the right to anonymity give emphasis to the positive role of anonymity in enabling privacy and political freedom (Jardine, 2016). A way to resolve whether claims to online anonymity are legitimate is to see this within the context of individual rights. Such rights are, or should be, absolute; yet at the same time they are contextual. As legal theorist Tara Smith mentions, while examining whether the right to freedom of speech is an absolute, 'rights that allowed a person to infringe on others' rights would kill the protection — the recognition of moral title — that the idea of rights affirms' (Smith, 2017). Thus, someone's right to freedom of speech is indeed absolute; yet, it does not allow someone to send death threats. In the same way, the right to property does not allow someone to loot their neighbor's garden and then deny entry to the police. Consequently,

one's claim to privacy or anonymity could be seen a derivative of basic rights, such as the right to property: individuals own their computers, and therefore any data in them should be excluded from the view of other parties (except when the owners have consented to it). Yet, such a right does not anymore apply when someone infringes someone else's property rights, such as in the cases of downloading copyrighted material. However, the issue becomes more complicated by the fact that there is no consensus on a) what constitutes one's fundamental rights, and b) what the role of the government in a rule of law society should be. Thus, one can see drug traders in crypto markets claiming they are only engaging in peaceful voluntary interactions, which have positive externalities, such as a reduction in street drug-related-crime, whereas prosecutors could at the same time claim that the individual right to peaceful trade is inferior to society's claim in maintaining some moral codes that exclude the free trade of substances (Sotirakopoulos, 2018).

Overall, while we believe that the use of different anonymity-enabling tools will be more and more essential to avoid omnipresent surveillance and to enable political activism in the Internet — as Gabriella Coleman convincingly shows in her contribution to this special section — the polarization between critics and supporters of the right to online anonymity fails to consider that online anonymity is not one thing but many; or, more precisely, that online anonymity is an inherently fluid concept whose meaning can only be established through the examination of specific contexts and situations. In fact, different technical tools are given different meanings and bring to different results based on the distinctive uses, understandings, skills and knowledge of each user, on the tools employed with the different degree of anonymity they enable, and on the particular situation and context in which these tools are used. Acknowledging the fluidity of online anonymity means defining it not as an absolute condition but rather as a wide space of movement within which users make different choices to protect their identity and privacy. Indeed, looking at the social and cultural dimensions of anonymity, scholars such as Turkle (2005) and Papacharissi (2002) attribute to anonymity the online reinvention of the individual, and therefore the combination of user and machine creates a new self that is shaped by sociality as well as by the technical affordances of online spaces.

One of the consequences of this approach is that, contrary to ongoing discussions of online anonymity that characterize this issue as relevant to the actions and motivations of specific groups of users such as hackers, criminals, activists, or journalists, one should acknowledge that online anonymity is a phenomenon that characterize to a certain extent any kind of social interaction online. Whenever users connect to the Internet, degrees of anonymity and non-anonymity are established that contribute to shape their experience online, its implications and effects. Understanding the fluid nature and the everyday character of online anonymity, in this sense, provides an antidote to approaches that attribute rigid values to online anonymity, denouncing it as a security threat or heralding it as a panacea against surveillance in the Web.

Acknowledgments

The project for this special section originated in a symposium on online anonymity organized with the support of the Centre for Research in Communication and Culture (CRCC) at Loughborough University.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

References

Brunton F (2013) *Spam: A Shadow History of the Internet*. Cambridge: The MIT Press.

Crawford S (2007) Internet Think. *Journal on Telecommunications and High Technology Law* 5: 467-486.

Flichy P (2007) *The Internet Imaginaire*. Cambridge: MIT Press.

Floridi L (2014) *The Fourth Revolution*. Oxford: Oxford University Press.

Gangadharan S (2017) The downside of digital Inclusion: Expectations and experiences of privacy and surveillance among marginal Internet users. *New Media & Society* 19(4): 597-615.

Hoang N and Pishva D (2014) Anonymous Communication and its Importance in Social Networking. Paper presented at the 2014 16th International Conference on Advanced Communication Technology (ICACT).

Jardine E (2016) Tor, what is it good for? Political repression and the use of online anonymity-granting technologies. *New Media & Society* 20(2): 435-452.

Kennedy H (2006) Beyond anonymity, or future directions for Internet identity research. *New Media & Society* 8(6): 859-876.

Kolko B, Nakamura L and Rodman G, eds. (2013) *Race in Cyberspace*. London: Routledge.

Larsson S, Svensson M and de Kaminski M (2012) Online Piracy, Anonymity and Social Change: Innovation through Deviance. Convergence: The International Journal of Research into New Media Technologies 19(1): 95-114.

Martin, J. (2014). Drugs on the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs. Springer.

McLeod P (2011) Effects of anonymity and social comparison of rewards on computer-mediated group brainstorming. *Small Group Research* 42(4): 475-503.

Minárik T and Osula AM (2016) Tor does not stink: Use and abuse of the Tor Anonymity Network from the perspective of law. *Computer Law & Security Review* 32: 111-127.

Morselli C, Décary-Hétu D, Paquet-Clouston M and Aldridge J (2017) Conflict Management in Illicit Drug Cryptomarkets. *International Criminal Justice Review* 27(4): 237-254.

Papacharissi Z (2002) The Presentation of Self in Virtual Life: Characteristics of Personal Home Pages. *Journalism & Mass Communication Quarterly*, 79(3): 643-660.

Park Y (2011) Digital Literacy and Privacy Behavior Online. *Communication Research* 40(2): 215-236

Smith T (2017) The Free Speech Vernacular: Conceptual Confusions in The Way We Speak About Speech. *Texas Review of Law & Politics* 22(1): 57-92

Sotirakopoulos N (2018) Cryptomarkets as a libertarian counter-conduct of resistance, *European Journal of Social Theory* 21(2): 189-206

Turkle S (1995) *Life on the Screen: Identity on the Age of the Internet*. London: Weidenfeld & Nicolson.

Turkle S (2005) *The Second Self: Computers and the Human Spirit*. Cambridge: MIT Press.

van Hardeveld G, Webber C and O'Hara K (2017) Deviating from the Cybercriminal Script: Exploring Tools of Anonymity (Mis)Used by Carders on Cryptomarkets. *American Behavioral Scientist* 61(11): 1244-1266.

Westin AF (1967) *Privacy and Freedom*. New York: Atheneum.

WhatsApp (2018) End-to-end Encryption. Available at https://faq.whatsapp.com/en/android/28030015/ (accessed 21 May 2018).

Winkel O (2003) Electronic cryptography: Chance or threat for modern democracy? *Bulletin of Science, Technology & Society* 23(3): 185-191.

Williams R (1974) *Television: Technology and Cultural Form*. London: Fontana.

Zajácz R (2013) WikiLeaks and the Problem of Anonymity: A Network Control Perspective. *Media, Culture & Society* 35(4): 489-505.