Paola Tubaro, University of Greenwich

WHY ONLINE PRIVACY IS NOT DEAD: NEGOTIATION AND CONFLICT IN SOCIAL MEDIA

The "end of privacy" is a recurring theme in current political and scientific debates about the internet. Popular books such as Jeff Jarvis's Public Parts announce the advent of a new ethos of "publicness" as the standard for today's connected existence. And younger generations, especially, are often described as prone to live open digital lives. Unprecedented intrusion by governments and corporations, as revealed by the recent NSA scandals, is only part of the story: the blame is frequently put on individuals themselves, who massively share contents on Facebook, Twitter, YouTube and other social media.

A closer look, however, brings out a more complex picture. Far from being animated by a mindless appetite for openness and self-disclosure, social media users continuously negotiate their privacy among themselves and with service providers. Their approach to online sharing is more strategic and controlled than commonly thought, and the recent public outcry around global surveillance is the latest episode in a long list of reactions to attempted erosions of privacy.

In a recently published book, my co-authors and I use agent-based computer simulation to analyse the social networks of users of popular web platforms. Our conclusion is that the hypothesized end of privacy is only one of the possible outcomes of online interactions –and not necessarily the most likely to occur.

Privacy vis-a-vis whom? The state, businesses, and individuals

The traditional notion of privacy opposes the individual and the state, with the aim of protecting an individual's own private sphere from public scrutiny. This conception still clearly holds, as is evident from the strong international reactions to NSA mass surveillance in the wake of the Snowden/Wikileaks revelations. But on social media, privacy also involves tensions in the relationships of each individual to other users, and to the companies that provide the service. This is where users are most ambivalent, so much so that they have often been seen as tolerant of, or willing to partake in, a "participatory surveillance system" (Albrechtslund 2008).

The reason why users share personal information with others is to form and maintain online ties; users do so as part of the complex relational strategies they put in place for their personal development, professional advancement, and political empowerment. They endeavour to build "social capital", using services such as Facebook to multiply the opportunities and the means to create and sustain relationships that provide access to information, support, and other resources. Self-disclosure is instrumental to this process: by unveiling aspects of themselves, users can attract ties with others who sympathize with their characteristics, practices or opinions; or they can reinforce existing links by creating a sense of commonality and mutual understanding.

This does not mean users are ready to divulge everything to everyone else: quite the opposite, they selectively choose what to tell to whom, positioning themselves along a continuum of which "open" and "closed" are the extremes. In each interaction with others, the disclosure choices of users reflect the intrinsic sensitivity of the information to be shared, as well as the structure and composition of their online personal networks.

If users adopt selective rather than full disclosure, it is in the interest of the companies providing online networking services to access as much user-generated content as possible. Their business model is based on the monetization of such content, extracting information from it so as to more efficiently match users/consumers and the corporate world of online sellers and advertisers. In this way, they can better segment the market, target ads and personalise commercial offers; thus, they undoubtedly benefit from disclosure of users' data. But users' responses are mixed, ranging from welcoming to contentious: for many, receiving better-targeted ads is hardly a worthwhile goal.

Privacy as penetration vs. privacy as negotiation

To understand the complex behaviours of users, we can no longer rely exclusively on the classical interpretation of privacy as "the individual's right to be left alone" (Warren and Brandeis 1890), seeing privacy protection as defence against any unwanted penetration of one's most intimate sphere by a third party. This approach (which we can label "privacy as penetration") typifies citizens' reactions to recent revelations of corporate and state intrusions, but does not account for differential disclosure in the social web.

To do so, a new model that can be called "privacy as negotiation", construes disclosure as dependent on the gradual process of individual adaptation to signals from the social environment. Online interactions are akin to negotiations in which an individual starts by disclosing some information, receives feedback from others, and adjusts contents accordingly, in a repeated process. User-generated data are not intrinsically private or public: it is the dynamic process of signalling, listening and adapting that ultimately makes the distinction apparent. In this perspective, the loss of privacy on certain items does not necessarily constitute an uncontrolled collapse, but can be a strategic retreat in cases in which agreement over data is difficult, to gain negotiating edge over some other points.

Cycles and conflicts

Inspired by Helen Nissenbaum's approach (2010), the negotiation perspective re-interprets privacy as context-dependent and network-based. It highlights how self-disclosure accompanies the complex process through which individuals build their social capital online. Web service providers themselves negotiate with users, and often try to take the lead by actively promoting disclosure as a behaviour and even as a value, acting as what Howard Becker (1963) calls, "moral entrepreneurs". Most prominently, Facebook's founder and CEO, Mark Zuckerberg, famously described one of the major changes in the Terms of Service of his platform as a simple adjustment to emerging "social norms" regarding privacy. To categorize those changes as "spontaneous" is to forget that Facebook has steadily and proactively increased the amount of information shared by default in a typical user profile.

A war over privacy settings has been fought for some years. Between 2006 and 2013, Facebook has proposed 10 revisions to its Terms of Service affecting personal data management. These led to protest campaigns supported by grassroots organizations and involving the US Senate, the Federal Trade Commission, as well as the data protection authorities of Ireland, France and Germany. In 8 out of 10 cases, Facebook had to back off and officially apologise (Casilli, 2013).

In such cases, what is normally micro-level negotiation escalates into macro-level conflict: large numbers of users simultaneously perceive that their negotiation power is under threat and react strongly, albeit temporarily. With computer simulation, my co-authors and I have detected a cyclical trend: when social networking services generate privacy incidents by forcefully publishing new information on their users, the latter revert to maximum protection, and so on in potentially endless fluctuations.

The cyclical patterns we detect are broadly in line with observed reactions to Facebook's privacy policies over time. Actually, this progression reveals a gradual institutionalization of the conflict, involving not only masses of individual users in loosely-coordinated associations, but more and more formal and durable organisations engaging activists, journalists and public authorities. Web companies' interventions are not only short-lived: they eventually backfire.

A major role for policy-makers

If a networked society can develop antidotes to attempts to impose full disclosure, difficulties remain, partly due to social inequalities. Especially less educated users may fail to detect threats to their privacy if they lack either the legal knowledge to understand the small print in the Terms of Service of online platforms, or the computing skills to suitably tune their privacy settings.

A more endemic problem is the opaqueness of network structures which often obfuscate the real extent of disclosure (for example, personal information may be revealed through other people's profiles, where one appears as a contact of someone else).

Data protection authorities, privacy watchdogs and user associations should remain vigilant: it is their task to monitor the technical and contractual conditions of social media services, to ensure that they remain widely accessible and that users can make as much informed a choice as possible. It is also their task to continue raising awareness and educating the public, also including (but not limiting to) younger generations of users.

References:

Albrechtslund, A. (2008). Online social networking as participatory surveillance. First Monday, 13 (3).

Becker, H.S. (1963). Outsiders: Studies in the Sociology of Deviance. New York: Free Press.

Casilli A.A. (2013). Contre l'hypothèse de la 'fin de la vie privée'. La négociation de la privacy dans les médias sociaux. Revue française des sciences de l'information et de la communication, 3 (1).

Jarvis, J. (2011). Public Parts: How Sharing in the Digital Age Improves the Way We Work and Live. New York: Simon & Schuster.

Nissenbaum, H. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford: Stanford Law Books.

Warren S. and L. Brandeis (1890). The right to privacy. Harvard Law Review, 4, 193-220.

Paola Tubaro is senior lecturer in economic sociology, and director of the doctoral programme, at the Faculty of Business of the University of Greenwich in London. Her research uses social network analysis to study socialization on the internet, online social movements, internet markets and organizational relationships.