The right to privacy in the digital age

Definition of Privacy and its importance

Privacy is the "right to be free from unwarranted intrusion and to keep certain matters from public view" (Law 2015). As such, "privacy is an important element in the autonomy of the individual. Much of what makes us human comes from our interactions with others within a private sphere where we assume no one is observing. Privacy thus relates to what we say, what we do, and perhaps even what we feel" (MacMenemy 2016).

A private space enhances autonomy. If we feel we may not be completely autonomous in our thoughts and actions, we may hold back crucial elements of ourselves. Privacy, therefore, "protects our subjectivity from the pervasive efforts of commercial and government actors to render individual and communities fixed, transparent and predictable. Privacy is an indispensable feature of a democracy where an individual maintains his identity while contributing to their civic duty" (Cohen 2016).

As set out in IFLA's own Statement on Privacy in the Library Environment, 'excessive data collection and use threatens individual users' privacy and has other social and legal consequences. When Internet users are aware of large-scale data collection and surveillance, they may self-censor their behaviour due to the fear of unexpected consequences. Excessive data collection can then have a chilling effect on society, narrowing an individual's right to freedom of speech and freedom of expression because of this perceived threat. Limiting freedom of speech and expression has the potential to compromise democracy and greatly limit civil engagement by making us "predictable" in our actions and thoughts (Cohen, 2016).

Surveillance and communications interception

The right to privacy in the digital age is threatened aggressively by data automation. In 1985 Spiros Simitis, Germany's leading privacy scholar recognized the risks data automation would cause to privacy, individuals and the democratic process. 'Privacy is not an end in itself, Simitis suggested, but an important tool to achieve a self-critical democracy where citizens are not unwitting suppliers of information to an all-seeing, and all-optimizing technocrats" (Morozov 2013). If privacy is at risk or threatened, we might miss the chance for personal assessment of the political process, one based on critical evaluation and self-reflection of our choices and preferences.

Data collection, through hacking or simple data harvesting, allows governments and commercial entities to amass huge banks of information about common citizens and their online behaviour. Privacy incursions occur frequently, affecting our search and digital behaviour patterns. These incursions are not only about a person or in this case a user – they can also affect a group, a family, a community.

Automated data gathering is carried out by government and private actors. Government surveillance includes communications interception, bulk data collection and processing, targeted intrusions in ICT systems and issues relating to cross-border surveillance and access to personal data.

As one of the many examples of governmental privacy infringement, the Pegasus software allowed the Mexican Government to spy on human rights defenders, journalists and anti-corruption activists. In this specific case of government sponsored cyberattacks, the WhatsApp feed of the son of a prominent lawyer and civil right journalist was the target of intrusion and privacy infringement (New York Times 2017).

Businesses can also contribute to surveillance activities based on data automation and collection and so encroach on our privacy. The latest scandal involves Facebook users and Cambridge Analytica researchers mishandling the data of over 40 million users. The dubious data gathering tactic included the use of Facebook Graphs API (application program interface) "that makes possible all the interconnectivity and the data delivery Facebook boasts when claiming that the platform was building a web where the default option is sharing" (Albright 2018). What is worrisome is that FB claims that its interface is based on the pretence that users are in control of what it is shared. In actuality, Facebook users have next to no control what is covertly shared about them – meaning the information and metadata others can extract.

Whether the threat comes from governments or private entities, these occurrences pose a significant question as to the right to live without arbitrary attacks on privacy (Article 12 of the Universal Declaration on Human Rights) and how our right to safeguard privacy can be defended.

Laws Are Not Enough

While data protection legislation has the potential to cut back on speculative data collection by companies, data privacy laws are not well placed to protect individuals' rights vis-a-vis automated technologies and privacy can all too often be undermined by laws elsewhere.

Currently, as a response to terrorist attacks in Europe, increased surveillance powers have been implemented at the national level, with much data shared across borders. Security has too often been cited as a reason for limiting use of encryption technologies, or for creating 'back-doors', which are likely both to facilitate incursions on privacy by both government and other actors.

There are already voices against blanket surveillance. The Council of Europe has called on Member States to refrain from indiscriminate mass digital surveillance. In 2016 the European Court of Human Rights (ECtHR) "delivered a judgement on secret surveillance in the case *Szabo and Vissy vs, Hungary*. The court found that Hungary's 2011 legislation on secret surveillance violated article 8 of the ECHR because it failed to safeguard against abuse" (Fundamental Right Report 2017).

Referring to the "Court of Justice of the European Union's (CJEU) judgment in Digital Rights Ireland v. Minister of Communications & Others, the ECtHR stated that, where national rules enable large-scale or strategic interception and where this interference may result in particularly invasive interferences with private life", the "guarantees required by the extant Convention case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices" (Fundamental Right Report 2017).

Regarding current legislation, even under the General Data Protection Regulation, governments still have ample scope to claim that national security – for right or for wrong – justifies attacks on privacy. This is not to say that steps to ensure that firms and others will have to be clearer about what information they are gathering, and how it will be used, are not welcome, alongside the possibility for citizens to ask to see what data is held, and for it to be deleted.

Nonetheless, faced with an uneven – and sometimes contradictory legal landscape, the most effective response is to empower the individual, giving them the knowledge and tools necessary to look after themselves.

Best practices for the promotion and protection of the Right to Privacy: the role of libraries

The benefits of digital technology in our daily lives are many. However, while enjoying these benefits, the amount of data we disseminate in living our lives online has serious implications for our privacy. While we may deem technology in and of itself as neutral, its impacts are not, and we need to address these. But how?

Libraries can play a powerful role in the promotion and protection of privacy given their long experience in working with information and helping users. Librarians agree that data privacy is a vital part of broader digital literacy – the ability to get the best out of the opportunities that digital technologies offer. Libraries can make the difference in the field of empowering individuals: teaching the meaning of digital privacy undoubtedly enhances security practices.

The International Federation of Library Association and Institutions (IFLA) statement on Privacy in the Library Environment (2015), emphasized the role of library crypto parties. They have taken place in the UK, France, the Netherlands, Australia, Sweden, the US, Canada, and Germany, to name just a few. These explore everything from specific tools, such as ToR browsers or anti-tracking software, to simpler behavioural changes which can reduce or manage risks. While much of the discourse around crypto parties focuses on government surveillance, good data hygiene is just as applicable in dealing with unwanted attention from businesses, hackers, or even members of personal networks.

Libraries also promote best practices by determining what user data they collect to limit information held about their users. Libraries can push partners (commercial or otherwise) to limit personal data collection and develop procedures to protect user privacy. In addition, to minimize the amount of data libraries' computers collect, many libraries instituted a set of practices where "Web browsers have temporary Internet files set to 2 MB, history retention set to 0 days, form-filling memory turned off, password memory turned off, and downloads turned off. In some libraries, all computers have special products installed to restore them to a standard template when rebooted. Computers will be set up to reboot after a set time of inactivity. This will clear any individual who forgot to log off and delete his activities from the computer" (Coombs 2005).

When there is a deep, systemic problem such as the current attacks to our privacy, the solution does not come from ad hoc deletion of problematic software or applications, but it comes from education, digital literacy, global cooperation and tirelessly advocating on best practices.

Conclusions

The growing prominence of the Right to Privacy in the Digital Age over the past years would not have occurred without the presence of a robust and expert civil society constituency.

This engaged constituency strived to achieve consensus on key issues ranging from the disproportionality of mass surveillance to the dangers associated with the bulk retention and acquisition of metadata. Also, the requirement to obtain legal authorization prior to the collection of personal data also remains central to consensus building. Civil society organizations have been highly effective in influencing the evolving discourse on the right to privacy in the digital age. They should continue to have a strong voice in the discussions.

Libraries and libraries associations, as important members of the civil society, can advance the Right to Privacy in the Digital age by cooperating with partner organizations in this area, both in order to advance relevant legislation, and to give their users the knowledge and skills required to protect themselves. They should, in this, receive the support necessary to keep abreast of continually advancing technologies and their implications for Privacy and human rights, and to help users.

In turn, governments need to take a consistent line on privacy. Action to prevent unwarranted and speculative data collection by private companies is welcome but is undone when security becomes an excuse for disproportionate harvesting of information by government agencies.

References

Ahmed, A.& Perlroth, N. (2017, 19 June). ‘Somos los nuevos enemigos del Estado’: el espionaje a activistas y periodistas en Mexico. *The New York Times.* Accessed online on 04/04/2018 https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group-espionaje/

Albright, J. (2018). *The Graph API: Key Points in the Facebook and Cambridge Analytica Debacle* Accessed on line at: https://medium.com/tow-center/the-graph-api-key-points-in-the-facebook-and-cambridge-analytica-debacle-b69fe692d747

Cohen, J.E. (2013) What is Privacy for? *Harvard Law Review* 126.

Coombs, K.A. (2005). Protecting USER PRIVACY in the Age of DIGITAL LIBRARIES. *Computers in Libraries 25*(6), 16-20.

Fundamental Rights Report (2017): Accessed online on 07/04/2018 http://fra.europa.eu/en/publications-and-resources/publications/annual-reports/fundamental-rights-2017#data-protection

Law. J. (2015) *Oxford Dictionary of Law*. Oxford: Oxford University Press

MacMenemy, D. (2016). (title) Accessed online on 05/04/2018 https://pure.strath.ac.uk/portal/files/54531639/McMenemy_IFLA_2016_rights_to_privacy_and_freedom_of_expression_in_public_libraries.pdf

Morozov, E. (2013). The Real Privacy Problem. *MIT Technology Review*. Accessed online at: https://www.technologyreview.com/s/520426/the-real-privacy-problem/