Stand Up For Digital Rights

Key Issues: Addressing Privacy Concerns Online

The right to privacy is internationally recognised as a human right, protected in Article 12 of the *Universal Declaration of Human Rights*:[1]

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

The right to privacy is also guaranteed by the ICCPR, the *American Convention on Human Rights*[2] and the *European Convention on Human Rights,*[3] as well as in most national constitutions.

In addition to its importance in its own right, privacy is linked to the fulfilment of the right to freedom of expression. Studies have shown that perceptions of control over one's communications, including over who has access to them, lead to franker and more extensive communications, while a loss of control leaves people feeling less free to engage earnestly.[4] The nexus between privacy and freedom of expression has been noted by the UN Special Rapporteur on Freedom of Opinion and Expression:

> States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy… Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny.[5]

---

[1] UN General Assembly Resolution 217A(III), 10 December 1948.
[2] Adopted 22 November 1969, O.A.S. Treaty Series No. 36, entered into force 18 July 1978.
[3] Adopted 4 November 1950, E.T.S. No. 5, entered into force 3 September 1953.
[4] Tamara Dinev, Heng Xu, Jeff H. Smith and Paul Hart, "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts" 22 European Journal of Information Systems (2013), p. 300. Available at: www.palgrave-journals.com/ejis/journal/v22/n3/pdf/ejis201223a.pdf.
[5] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HRC/23/40, 17 April 2013, para. 79.

Privacy has been particularly affected by digital developments to the point where the Internet has had a dramatic impact on our understandings of the very concept of privacy. On the one hand, the Internet provides for an unprecedented level of freedom and anonymity, where tastes can be explored or opinions expressed without regard to what one's family, friends or social circle might think. For a gay Ugandan or Russian, or a Saudi atheist, the Internet may provide the only avenue for self-expression or to network with likeminded communities.

On the other hand, the Internet is also the most heavily monitored and tracked medium of expression in history, where every move that users make is noted, followed and recorded. Reading a newspaper article, going out on a date or attending an event in the real world are transient events. For the most part, evidence of one's activity disappears after the fact. Online, however, a person's activities, even mundane ones, leave footprints which can be traced by commercial and government actors who are interested in studying, processing and collating this information for various reasons. The permanence of digital records compounds this, since actions taken years ago remain traceable. A poorly thought out blog comment or an erroneous news story can end up as the top result of a web search for a person's name even years after the event.

Commercial Models and Privacy

While the privacy issues noted above are troubling, the fact is that the sale of personal information, and the use of targeted advertising which is facilitated by the collection of personal information, are major economic forces behind the spread of Internet services, since they are the core business model which allows many tech companies to offer their products and services free of direct charges on users. Despite the success of this model, it has been referred to as the Internet's "original sin" and some people have urged private sector intermediaries to explore alternative business models which allow for sustainable growth without compromising user privacy.[6] In response to such demands, Google already offers a subscription version of its email service for businesses which is ad-free.[7]

Ultimately, of course, it remains the prerogative of companies as to whether they wish to pursue alternative business models subject, of course, to compliance with the law. However, even if one embraces the idea that exchanging privacy for free services online is a fair trade, ground rules are needed. The United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression noted in a 2011 report that States have a responsibility to protect consumers:

---

[6] Ethan Zuckerman, "The Internet's Original Sin", The Atlantic, 14 August 2014. Available at: www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041/.

[7] Available at: www.google.com/work/apps/business/.

> States parties are required by article 17(2) [of the ICCPR] to regulate, through clearly articulated laws, the recording, processing, use and conveyance of automated personal data and to protect those affected against misuse by State organs as well as private parties.[8]

A similar sentiment was expressed in the UN Human Rights Committee's General Comment on the right to privacy:

> 10. The gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant.[9]

It is arguable that the intrusiveness of State regulation over companies in this area should depend, at least in part, on the extent to which industry acts to offer effective protections of its own.

A key issue here is being clear and transparent with users about policies around collecting, sharing and processing information, so that they understand them and adapt their expectations and business patronage accordingly. For example, while users may implicitly understand that their private information is being processed by companies whose business model is based on advertising, such as Google and Facebook, revelations of data collection schemes by Apple, whose primary business is selling hardware, surprised consumers.[10] Intrusive behaviour from companies which explicitly market the privacy features of their services, such as the app Whisper, are particularly egregious.[11]

Similarly, users may implicitly understand that information will be used to track their actions in an automated or aggregated way, and for advertising purposes, but not expect it to be examined by human beings. In 2014, a tech blogger received leaked internal information via a Microsoft Hotmail account relating to the upcoming release of Windows 8.[12] When the blogger attempted to confirm the

---

[8] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/17/27, 16 May 2011, para. 58. Available at: www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

[9] Human Rights Committee, General Comment 16, U.N. Doc. HRI/GEN/1/Rev.1, p. 21 (1994). Available at: www1.umn.edu/humanrts/gencomm/hrcom16.htm.

[10] Andy Greenberg, "How to Stop Apple From Snooping on Your OS X Yosemite Searches", Wired, 20 October 2014. Available at: www.wired.com/2014/10/how-to-fix-os-x-yosemite-search/.

[11] Paul Lewis and Dominic Rushe, "Revealed: how Whisper app tracks 'anonymous' users", The Guardian, 16 October 2014. Available at: www.theguardian.com/world/2014/oct/16/-sp-revealed-whisper-app-tracking-users.

[12] Andrew Crocker, "Microsoft Says: Come Back with a Warrant, Unless You're Microsoft", Electronic Frontier Foundation, 21 March 2014. Available at: www.eff.org/deeplinks/2014/03/microsoft-says-come-back-warrant-unless-youre-microsoft.

veracity of the material with Microsoft, the company went through the blogger's Hotmail account to identify the source of the leak. Microsoft defended its behaviour by citing its terms of service, which included a line allowing access to users' accounts to protect the company's rights or property. However, commentators noted that the language of the policy was broad enough to allow access to virtually any account, for virtually any reason, and that the actions meant that Microsoft's broad claims about privacy protection were misleading. As a consequence of the backlash, Microsoft eventually refined its terms of service so that they would, in future, leave such cases to the law enforcement authorities rather than undertaking their own investigations.[13]

More generally, the increasing involvement of third party data brokers in collecting and processing users' information raises concerns due to the opacity of the process and the lack of any direct relationship between the users and the data brokers. The fact that most users have no idea what companies or even types of companies their data will be shared with, or even any idea what kind of uses it will be put towards, mean that it is hard to accept that their agreement meets the standard of "informed consent". Research carried out in May 2014 showed that 88 percent of the 950,489 most popular websites on the Internet sent user information to third-parties.[14] Of the sites which shared information with third parties, an average of 9.47 different web domains were contacted per user visit. The vast majority of this tracking was carried out surreptitiously, with only two percent of the third parties including a visible prompt alerting users to their presence.

Third-party advertising is a legitimate and even vital part of the Internet's economic ecosystem. However, the lack of clarity surrounding the practice and the impossibility for users to know who is doing what with their personal information raises serious privacy concerns. This is particularly true given that privacy invasions can become far more intrusive when personal information is collated from multiple sources. As an example, a mobile app called Girls Around Me draws information from social media, including photos, interests and the like, and combines it with data from Foursquare, a geo-location mobile app, to allow users to browse realtime information about women in their vicinity. The combination created a programme which was highly intrusive and which observers dubbed a "let's stalk women" app.[15] Girls Around Me raises additional concerns about physical and sexual violence, but

[13] Andrew Crocker, "Reforming Terms of Service: Microsoft Changes Its Policy on Access to User Data", Electronic Frontier Foundation, 28 March 2014. Available at: www.eff.org/deeplinks/2014/03/reforming-terms-service-microsoft-changes-its-policy-access-user-data.

[14] Timothy Libert, "Exposing the Hidden Web: Third-Party HTTP Requests on One Million Websites, International Journal of Communication, October 2015. Available at: ijoc.org/index.php/ijoc/article/download/3646/1503.

[15] Nick Bilton, "Girls Around Me: An App Takes Creepy to a New Level", The New York Times, 30 March 2012. Available at: bits.blogs.nytimes.com/2012/03/30/girls-around-me-ios-app-takes-creepy-to-a-new-level/?_r=0.

it is easy to see how combining datasets from various sources, as some apps do, can create a far more privacy invading picture of an individual.

A concrete manifestation of users' frustration with intrusive online tracking and advertising is the rise in popularity of ad blocking software. The most popular tool for this, AdBlock, has seen a steep rise in its user base since 2013.[16] The service was projected to exceed 236 million users by the end of 2015, with a particular concentration in Europe. This represents a serious challenge for private sector intermediaries whose business model is based on advertising. From their perspective, it does not seem fair for users to enjoy their services while opting out of the system which pays for it. Even if alternative revenue models are encouraged, there is a strong collective interest in maintaining the viability of ad-supported services, to ensure that useful websites remain accessible to everyone.

Some have drawn a connection between the rise in ad blocking and a decision by major private sector intermediaries not to respect "do not track" (DNT) messages from users.[17] DNT is a mechanism which allows users to indicate to websites they visit that they do not wish to be tracked. However, DNT is only effective if private sector intermediaries choose to respect the request. Several major players, including Google, Facebook and Yahoo!, have indicated publicly that they will not respect DNT requests.[18] Given the ability of AdBlock users to "whitelist" particular websites, and indications that their user base would be happy for them to do this for sites which respect user privacy and are not overly intrusive in their advertising methods, the spread of blocking software creates a growing incentive for the industry to develop better standards regarding advertising and user tracking.

Anonymity

Anonymisation tools can be very important to protecting online privacy, particularly in sensitive contexts. A 2011 report of the UN Special Rapporteur on freedom of expression noted that State limitations on the ability of users to communicate anonymously represented a restriction on freedom of expression which needed to be assessed using the three-part test for such restrictions:

> [The Special Rapporteur] also calls upon States to ensure that individuals can express themselves anonymously online and to refrain from adopting real-name registration systems. Under certain exceptional situations where States may limit the right to privacy for the purposes of administration of criminal justice or

[16] Ricardo Bilton, "The global rise of ad blocking in 4 charts", Digiday, 1 June 2015. Available at: digiday.com/publishers/global-rise-ad-blocking-4-charts/.

[17] See Doc. Searls Weblog, "Beyond ad blocking - the biggest boycott in human history", 20 September 2015. Available at: blogs.law.harvard.edu/doc/2015/09/28/beyond-ad-blocking-the-biggest-boycott-in-human-history/.

[18] Jim Edwards, "In A Further Humiliation To Microsoft, Facebook Will Not Honor 'Do Not Track' Signals On Internet Explorer ", *Business Insider*, 12 June 2014. Available at: www.businessinsider.com/facebook-will-not-honor-do-not-track-2014-6.

> prevention of crime, the Special Rapporteur underscores that such measures must be in compliance with the international human rights framework, with adequate safeguards against abuse. This includes ensuring that any measure to limit the right to privacy is taken on the basis of a specific decision by a State authority expressly empowered by law to do so, and must respect the principles of necessity and proportionality.[19]

The Council of Europe's *Declaration on Freedom of Communication* also calls on States to respect Internet users' wish not to be identified:

> In order to ensure protection against online surveillance and to enhance the free expression of information and ideas (…) States should respect the will of users of the Internet not to disclose their identity.[20]

Arabic Network for Human Rights Information

The majority of the Internet experts surveyed during the course of our research did not trust the ability of private sector intermediaries to protect their personal data, due to the absence of clear rules for the protection of personal data. The pervasive regime of surveillance in Egypt and the lack of laws and policies protecting Internet privacy led many users and online activists to rely on Tor, and other applications providing encryption or anonymity.

Unfortunately, despite the presence of a large number of companies that provide telecommunications and Internet services in the Arab region, we did not observe substantial differences between those companies in relation to the protection of the personal data of users.

As discussed earlier, the facelessness of online discussions facilitates the ability of users to express themselves without fear of social repercussions. As Oscar Wilde once said, "Man is least himself when he talks in his own person. Give him a mask, and he will tell you the truth."[21] Among many online communities, there is a strong taboo against "doxxing", publishing personally identifiable information about a person, particularly when they are using an online alias.[22]

The Internet has become an important means for communicating information about sensitive subjects, such as sexual or mental health issues and child abuse. The

[19] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, note **Error! Bookmark not defined.**, paragraph 84.
[20] Council of Europe, Declaration on Freedom of Communication on the Internet, 2003, Principle 7. Available at: coe.int/t/informationsociety/documents/Freedom%20of%20communication%20on%20the%20Internet_en.pdf.
[21] See: www.goodreads.com/quotes/3736-man-is-least-himself-when-he-talks-in-his-own.
[22] See: "What doxxing is, and why it matters", The Economist, 10 March 2014. Available at: www.economist.com/blogs/economist-explains/2014/03/economist-explains-9.

Internet has also become the key means for whistleblowers seeking to expose corruption or other wrongdoing. Although, for security reasons, Edward Snowden's main disclosures were delivered physically via USB sticks, he made contact with the journalists and set up the handoff through the Internet. Websites like Wikileaks could not exist without the promises of anonymity which they provide. Although some of their reporting has been controversial, they provide an important public interest service. For example, the negotiations over the Trans-Pacific Partnership, a sweeping trade deal involving twelve countries, were conducted in almost total secrecy, with civil society groups being excluded. Unauthorised releases of the draft text on Wikileaks provided these groups with the information they need to monitor the process.[23]

The centrality of the Internet to sensitive communications, and the level of trust that its users have in its capacity to protect their identities, when they are asking for that, means that failures on this front can have particularly stark consequences. In 2014, a researcher discovered a security glitch in "Grindr", a popular smartphone app targeting gay men, through which the location of any of its users could be identified to within a 30-metre margin of error. By exploiting this glitch, users were able to locate 189 users of the app in Iran, where homosexuality is illegal.[24]

Christopher Parsons

Companies can influence potential State surveillance capabilities based on how the companies collect and analyse telecommunications traffic data for their own business purposes. In the United States, AT&T engineers built a system in the late 1990s to data mine the company's telephone and Internet access records. It was "originally created to develop marketing leads and as an anti-fraud tool to target new customers who called the same numbers as previously identified fraudsters" but in 2007 "it was revealed that the FBI had been seeking 'community of interest' or 'calling circle' records from several telecommunications providers."[25] AT&T was able to comply with these requests because of the data mining system it had built for legitimate business purposes. One of its competitors, Verizon, was unable to perform equivalent surveillance for the FBI because it did not have a comparable data mining system.[26]

---

[23] Centre for Law and Democracy, Analysis of the Draft Intellectual Property Chapter of the TransPacific Partnership, December 2013. Available at: www.law-democracy.org/live/wp-content/uploads/2013/12/TPP.IP-final.Dec13.pdf.

[24] John Aravosis, "Grindr smartphone app outs exact location of gays across Iran", America Blog, 27 August 2014. Available at: americablog.com/2014/08/grindr-smartphone-app-outs-exact-location-gays-across-iran.html.

[25] Christopher Soghoian, "The Spies We Trust: Third Party Service Providers and Law Enforcement Surveillance," Doctoral Dissertation, July 2012, pp. 29. Available at: files.dubfire.net/csoghoian-dissertation-final-8-1-2012.pdf. Accessed 17 November 2015.

[26] *Ibid.* It must be noted, however, that the absence of the system did not prevent the US government from accessing or analysing communications records. Instead, Verizon and other telephone

In a related vein, the period of time for which private sector intermediaries retain data can affect the availability of information to government agents. In the Canadian context, one of the country's largest home Internet providers, Rogers, must retain records of the Uniform Resource Locators (URLs) that subscribers visit for at least 31 days; these records are needed in order to notify customers when they approach their allocated monthly bandwidth limits.[27] One of Rogers' competitors, Teksavvy, maintains a 0-day retention protocol. One consequence of these different business models is that government authorities could request Rogers to divulge a particular subscriber's web history and expect it to be provided retroactively. To get URL records from Teksavvy, however, the same authorities would need to compel Teksavvy to start keeping logs about a particular subscriber's communications activities, and these could only be available on a proactive basis. On the other hand, Rogers can retroactively provide details of its subscribers' call records going back as far as ten years whereas TekSavvy retains similar records indefinitely.

There are legitimate reasons why some private sector intermediaries may want to require real-name registration. For example, Airbnb, a website which allows users to rent lodging from one another, has been moving towards verifying their users as a security measure. This is fair enough, as a step to enhance trust between renters and hosts, who both have understandable safety concerns. It is worth noting that Airbnb also insures renters against property damage caused by guests, giving the website a direct reason for seeking information about its users. LinkedIn, a professional networking site, also requires real names. This too, seems fairly core to their business model, which relies on users believing that the CV they are browsing is reasonably accurate. Other services claim that requiring real-name registration improves the civility of the online discourse. Whether or not this is true in practice is open to debate, but it is a legitimate model to pursue. In an effort to improve the quality and tone of comments on YouTube, Google, which owns the video-sharing site, imposed a real-name requirement in 2013, but this was unpopular and Google reversed the move after less than a year.[28]

However, while online intermediaries have a legitimate interest in exercising discretion as to whether or not to require real-name registration, these decisions should also take into account the broader human rights implications, and the degree of impact that the requirement has on their users. For a site like Airbnb, the freedom

---

companies provided the National Security Agency (NSA) with access to call records and the NSA itself performed the community of interest analysis.

[27] Christopher Parsons, "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," *Telecom Transparency Project*, 2015, pp. 51. Available at: www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

[28] Samuel Gibbs, "The return of the YouTube troll: Google ends its 'real name' commenter policy", The Guardian, 16 July 2014. Available at: www.theguardian.com/technology/2014/jul/16/youtube-trolls-google-real-name-commenter-policy.

of expression impact of requiring real names is minimal. For a site like Facebook, on the other hand, their dominant market position, and the fact that so many people use it as a primary communications platform, including in many repressive States, alters the calculus. Facebook's real-name requirement has been criticised by some. To the company's credit, in 2015 they announced changes to their policy allowing for the use of pseudonyms under some circumstances, such as where a user is transgender, a victim of stalking or faces abuse or discrimination.[29]

All intermediaries have a responsibility to be fully transparent with their users as to the extent to which any anonymity they offer or appear to be offering will be respected. The reason why a data breach at Grindr is so serious is because the service is predicated on discretion, which significantly elevates the sensitivity of the information that users will entrust to it. Perceptions, and building realistic expectations, are of cardinal importance here.

As part of this, intermediaries should also make sure that, where they claim to have "anonymised" information before it is shared with third parties, they do so properly. In 2006, AOL Inc. published the Internet search histories of 650,000 of its users as a resource for academic researchers, after undertaking measures to anonymise the data. However, New York Times reporters and others were able to reconnect the data to identifiable individuals because anonymisation had not been done properly.[30] As a consequence, the researcher responsible for releasing the data and AOL's Chief Technology Officer both resigned. While making this sort of information available for research purposes is invaluable, at the same time it is important to anonymise it properly before releasing it.

Security and Encryption

Another means of protecting user privacy is through strong data security measures and the use of encryption. In 2015, the UN Special Rapporteur on freedom of expression specifically noted the importance of encryption to freedom of expression:

> Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity.

---

[29] Todd Gage and Justin Osofsky, "Community Support FYI: Improving the Names Process on Facebook", Facebook Newsroom, 15 December 2015. Available at: newsroom.fb.com/news/2015/12/community-support-fyi-improving-the-names-process-on-facebook.

[30] Castan Centre for Human Rights Law, International Business Leaders Forum, and Office of the United Nations High Commissioner for Human Rights, Human Rights Translated – A Business Reference Guide (2008). Available at: www2.ohchr.org/english/issues/globalization/business/docs/Human_Rights_Translated_web.pdf.

> ...
> The use of encryption and anonymity tools and better digital literacy should be encouraged. The Special Rapporteur, recognizing that the value of encryption and anonymity tools depends on their widespread adoption, encourages States, civil society organizations and corporations to engage in a campaign to bring encryption by design and default to users around the world and, where necessary, to ensure that users at risk be provided the tools to exercise their right to freedom of opinion and expression securely.[31]

While the report mainly targeted States, who have made significant efforts to undermine or prevent the use of encryption in recent years, it also included recommendations for corporate actors:

> Corporate actors should likewise consider their own policies that restrict encryption and anonymity (including through the use of pseudonyms).
> ...
> States, international organizations, corporations and civil society groups should promote online security. Given the relevance of new communication technologies in the promotion of human rights and development, all those involved should systematically promote access to encryption and anonymity without discrimination.
> ...
> While the present report does not draw conclusions about corporate responsibilities for communication security, it is nonetheless clear that, given the threats to freedom of expression online, corporate actors should review the adequacy of their practices with regard to human right norms... Companies, like States, should refrain from blocking or limiting the transmission of encrypted communications and permit anonymous communication.

Edward Snowden, who is famous for exposing major mass surveillance programmes by Western governments, also pointed to the role that encryption could play in restoring user privacy on the Internet, noting that consumers and corporations held the keys to the effective use of encryption:

> We have the means and we have the technology to end mass surveillance without any legislative action at all, without any policy changes. By basically adopting changes like making encryption a universal standard—where all communications are encrypted by default—we can end mass surveillance not just in the United States but around the world.[32]

In the aftermath of the Snowden revelations, several major players announced moves to encrypt more user information by default.[33] In addition to facilitating and promoting the use of encryption, online intermediaries should consider other means to encourage strong data security among their users, potentially through offering inducements.

---

[31] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, 22 May 2015, para. 56-63.
[32] James Bedford, "The Most Wanted Man in the World", Wired, August 2014. Available at: www.wired.com/2014/08/edward-snowden.
[33] Lorenzo Franceschi-Bicchierai, "Reddit Switches to Encryption By Default", Motherboard, 17 June 2015. Available at: motherboard.vice.com/read/reddit-switches-to-https-encryption-by-default.

Private sector intermediaries should also minimise the amount of data that they hold, including by considering whether maintaining particular information is necessary to accomplish their goals. The more information an organisation maintains, the greater the risk of a security breach.[34] This was a particular lesson from the Ashley Madison hack, since the website maintained information on users who had ceased using their services years ago.[35]

Once security has been breached, it is important for private sector intermediaries to inform those who have or might have been impacted promptly and fully. Where personal information has been compromised, speed can be of the essence in minimising damage. Again, Ashley Madison provides a good example of what not to do. Although the Ashley Madison hackers first announced their intrusion on 15 July 2015, by publishing a small amount of stolen user information, the website initially denied the attack, claiming their system was completely secure and that the hackers had not been successful.[36] Ashley Madison's denials continued until the website's full user information was published the following month.

Right to be Forgotten

Given the Internet's transformative impact on a range of social functions, from work to shopping to socialising, a person's online footprint can be an important aspect of their identity. Employers, colleagues, romantic connections and even casual acquaintances are increasingly likely to look a person up online to find out more about them. While users are able to control the information that they post to websites and social media pages, they have little control over what others post, whether is officials posting information about legal infractions or friends posting pictures. Furthermore, a search for a person's name on a search engine provides information based on the engine's own algorithms. These may promote trivial or negative aspects of a person's background, such as an arrest for underage drinking or a poorly thought out comment. A person's past mistakes can follow them virtually forever on the Internet, becoming an indelible part of their online identity.

There are benefits to making peoples' pasts more accessible. A holocaust museum, for example, has a legitimate interest in knowing if a person they are considering for

[34] Federal Trade Commission, Internet of things: Privacy and Security in a Connected World, January 2015. Available at: www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
[35] Indeed, this was part of the website's extortionate business model. They charged former users to have their information removed, although the hack demonstrated that even some users who had paid them had not had their information fully deleted. Ashley Madison offered to waive their deletion fee in the aftermath of the hack, in an attempt to close the stable door after the horse had left.
[36] Alex Hern, "Ashley Madison customer service in meltdown as site battles hack fallout", The Guardian, 21 July 2015. Available at: www.theguardian.com/technology/2015/jul/21/ashley-madison-customer-service-meltdown-hack-fallout.

a job has a history of racist statements, while a women's shelter has a legitimate interest in knowing whether a job applicant has a history of sexism. However, everyone makes mistakes and does things that they do not want to remain fully public, forever. From this perspective, the indelibility of digital records raises concerns.

The particular way information is presented can exacerbate the problem. A decision by a prosecutor to drop charges or a trial which fails to result in a conviction may not generate as much media coverage as the initial arrest and may not feature as prominently on a later web search. Similarly, an erroneous and sensational media report may attract more attention than a later retraction. In these cases, a web search may paint a false and unfair picture of the individual.

Steps have been taken in other areas of life to accommodate these concerns. For example, reflecting the idea of giving people second chances, some countries have laws which state that, after a particular period of time, a prior criminal conviction may no longer be taken into account for applicants seeking insurance or employment. Another manifestation of this is the emergent "right to be forgotten", which gives individuals a right to have certain information about themselves removed or blocked from search results.

The right to be forgotten gained particular prominence in 2014, when the European Court of Justice (ECJ) found that Europe's data protection legislation granted EU citizens a right to request that Internet search engines, in that case Google, not display results relating to them which were "inadequate, irrelevant, or no longer relevant, or excessive in relation to the purposes for which they were processed".[37] In processing removal requests, Google is mandated by the ECJ decision to consider whether the overall public interest weighs in favour of continuing to point to the information or not. Assessing this public interest involves a difficult balancing between freedom of expression, the right to information, the right to data protection and the right to privacy. Within three months of the ruling, Google had blocked over 170,000 URLs from being displayed through its searches.[38]

Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE)

The right to freedom of expression, and a person's right to publish content, was completely ignored in the ECJ's analysis of the balance of rights in the Costeja case. Instead, the case was treated as a conflict between the "fundamental rights" of the

[37] Case C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:2014:317. Available at: eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.

[38] David Kravets, "Google has removed 170,000-plus URLs under 'right to be forgotten' edict", Ars Technica, 10 October 2014. Available at: arstechnica.com/tech-policy/2014/10/google-has-removed-170000-plus-urls-under-right-to-be-forgotten-edict/.

holder of the data and the "mere economic interest" of the intermediary.

The ECJ held that it was legitimate in certain contexts to request that an Internet intermediary remove or block user-generated content. This raises a question for courts and regulators in Latin America as to whether there may be similar results under the Inter-American Court of Human Rights.

There are many legitimate criticisms of the ECJ's right to be forgotten ruling. For a start, the ruling failed to account properly for freedom of expression and included troubling statements that the interest of the general public in finding information is, as a "general rule", overridden by privacy and data protection rights. This is absolutely not the case under international human rights law. Competing rights must always be balanced against each other. In recognition of this, for example, access to information or right to information laws around the world provide for a balanced weighing of the right to access information and privacy.

A second problem is that search engines, to which the key decision-making responsibilities under this right are delegated, are not well-placed to undertake the delicate balancing between core rights which is required. Determinations about where the larger public interest lies should be made by courts or at the very least publicly constituted decision-makers rather than being foisted onto the private sector. Previous experience with copyright takedowns demonstrates the potential problems with this, as private sector intermediaries have been criticised for failing to consider exceptions to copyright such as fair use or fair dealing properly, given that the easiest and safest choice is to delete anything that might breach the rules. Indeed, in such situations companies can face a conflict of interest or at least tension between their business interests and their broader social and human rights responsibilities.

This problem is compounded by the fact that the ECJ proposed very vague standards for assessing whether material should be removed. Indeed, the ruling is almost irresponsibly vague and general in this respect, given the magnitude of its impact. At the same time, the EU has been working to provide a bit more clarity on the applicable standards through the Article 29 Working Party.[39]

An additional problem with delegating this responsibility to search engines is that it significantly raises the costs and legal complexity of running a search engine. While Google, and some well-funded competitors like Bing, can afford this, the ruling may

[39] "Guidelines on the implementation of the Court of Justice of the European Union judgment on 'Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González' C-131/12", Article 29 Data Protection Working Party, 26 November 2014. Available at: ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

have served to entrench the competitive advantage that established players enjoy by significantly raising the bar for entry into this market.

Criticisms aside, as binding law in Europe, search engines have a duty to implement the right to be forgotten and they should take the human rights impact into account when doing so. Despite the ECJ's failure to afford freedom of expression its proper place in their ruling, this interest should play a strong role in search engines' decision-making about whether to acquiesce to a right to be forgotten request. Given the important impact that the right to be forgotten could have on the character of the Internet, search engines should develop clear and sophisticated policies and decision-making standards regarding requests to block results from searches pursuant to the right to be forgotten ruling. This should, among other things, include an assessment of the various public interest considerations that are likely to weigh on each side of the equation (i.e. in favour of privacy and of maintaining access to information). To this end, search engines should carry out robust consultations with key stakeholders to inform their policies on this issue.

Transparency is also important when implementing the right to be forgotten and search engines should be clear about how their decision making works, including by publishing the policies and policy guidance noted above, along with periodic aggregated information about removal requests and how they were processed.

A third important value is due process. Search engines should promptly inform any party whose content is the subject of a removal request and give them an opportunity to counter the claim, including by arguing that the public interest lies in keeping the information available. For more difficult or cutting edge requests, consideration should be given to putting in place an appeals mechanism or opportunity for more in-depth consideration of the matter. In addition, search engines should avoid taking the easy route, which is just to remove information from search results, given that incentives almost inherently line up this way, and instead undertake a proper and fair consideration of the matter. Should the matter go back to the courts, search engines should argue that their responsibility is limited to reaching a reasonable decision rather than getting the matter right, in the sense of coming to the same decision as a court might after a full hearing on the matter (which search engines obviously cannot do for each case). In legal terms, this means that their decisions should simply be subject to a judicial review standard.

Finally, given the troubling elements of the right to be forgotten as set out in the ECJ ruling, content providers should explore avenues to push back as far as possible. The websites of several media outlets, such as the BBC and The Telegraph, have sought to limit the negative impact of the right to be forgotten by maintaining special lists on their websites of any material which has been removed from searches, including links to the original articles and descriptions of the content.[40]

[40] Neil McIntosh, "List of BBC web pages which have been removed from Google's search results", BBC, 25 June 2015, available at: www.bbc.co.uk/blogs/internet/entries/1d765aa8-600b-4f32-b110-

Google's decision to appeal against an order by a French court that it apply blocks carried out under the right to be forgotten globally to all of its websites, as opposed to just to European websites, is another welcome move.[41]

d02fbf7fd379; and Rhiannon Williams, "Telegraph stories affected by EU 'right to be forgotten'", The Telegraph, 3 September 2015, available at: www.telegraph.co.uk/technology/google/11036257/Telegraph-stories-affected-by-EU-right-to-be-forgotten.html.

[41] Julia Fioretti and Mathieu Rosemain, "Google appeals French order for global 'right to be forgotten'", Reuters, 19 May 2016. Available at: www.reuters.com/article/us-google-france-privacy-idUSKCN0YA1D8.

Stand Up For Digital Rights

Recommendations for Addressing Privacy Concerns Online:

Communicating With Users

- **Intermediaries should publish clear and transparent information about their policies and practices regarding the collection, processing and sharing of user information and the level of privacy protection they afford their users. This should include a list of the specific types of third parties who may be given access and information about how the information may be used by these third parties. Where policies need to be complex due to the fact that they form the basis of a legal contract with users, they should be accompanied by clear, concise and easy to understand summaries or explanatory guides.**
- **Intermediaries should make sure that any representations they make to users regarding privacy or anonymity are clear and reasonable, and they should then respect those commitments.**
- **Intermediaries should allow their users to view personal information they have gathered or shared which relates to them.**
- **Intermediaries should take reasonable steps to educate their users about security online and should consider introducing incentives to encourage users to adopt good security practices.**
- **Where a security breach occurs, intermediaries should inform their users promptly and fully, particularly anyone whose information has or may have been compromised.**

Data Minimisation

- **Intermediaries should limit the amount of personal user data they collect and store to what is reasonably necessary for operational or commercial reasons.**
- **Intermediaries should make reasonable efforts to limit the ways in which they process personal user data to what is reasonably required to sustain their business models, including by limiting personal data processing to fully automated systems whenever possible.**

- **Intermediaries who rely on a business model whereby users trade their personal information for services should consider offering customers the possibility of opting out of the model in exchange for paying for the service.**
- **Intermediaries should allow users to request that their accounts be permanently deleted, including all information that the intermediary has gathered about them (except where this information has been aggregated or processed with other information and extraction is not practical or it is needed for ongoing operational purposes).**

Securing Data

- **User information should, whenever this is legally, operationally and technically possible, be encrypted and anonymised during storage.**
- **Intermediaries should, whenever possible, support end-to-end encryption.**
- **When releasing data for research purposes, which is a recognised public interest action, intermediaries should make sure that adequate measures have been taken to protect private content in the data, for example through proper anonymisation of the data or by requiring researchers to limit further dissemination of the data.**

Anonymity

- **Intermediaries should take into account the human rights impact of real-name registration policies and should work to mitigate any negative impacts, including by allowing use of pseudonyms or by allowing parts of the service to be used anonymously. Intermediaries should not require real-name registration where this would significantly harm the rights of their users.**

The Right to Be Forgotten

- **Search engines which are subject to the right to be forgotten should publish detailed information about their policies, standards and decision-making processes in assessing removal requests, as well as aggregated information about the number of requests received and how they were processed.**
- **Search engines should develop robust and detailed policies and standards regarding how they apply the right to be forgotten which ensure a proper balancing between freedom of expression and the right to information, on the one hand, and privacy, on the other. They should carry out robust consultations with key stakeholders, including civil society actors, when developing these policies and standards.**

- **Search engines should respect due process when applying the right to be forgotten, including by informing those whose content is subject to a removal request, as far as this is legally permitted, and by giving them an opportunity to argue that the material should not be blocked, including because the public interest lies in continuing to display the content. Consideration should be given to putting in place some sort of appeals or reconsideration mechanism for more difficult or cutting edge cases.**