Internet freedom for all: Public libraries have to get serious about tackling the digital privacy divide.

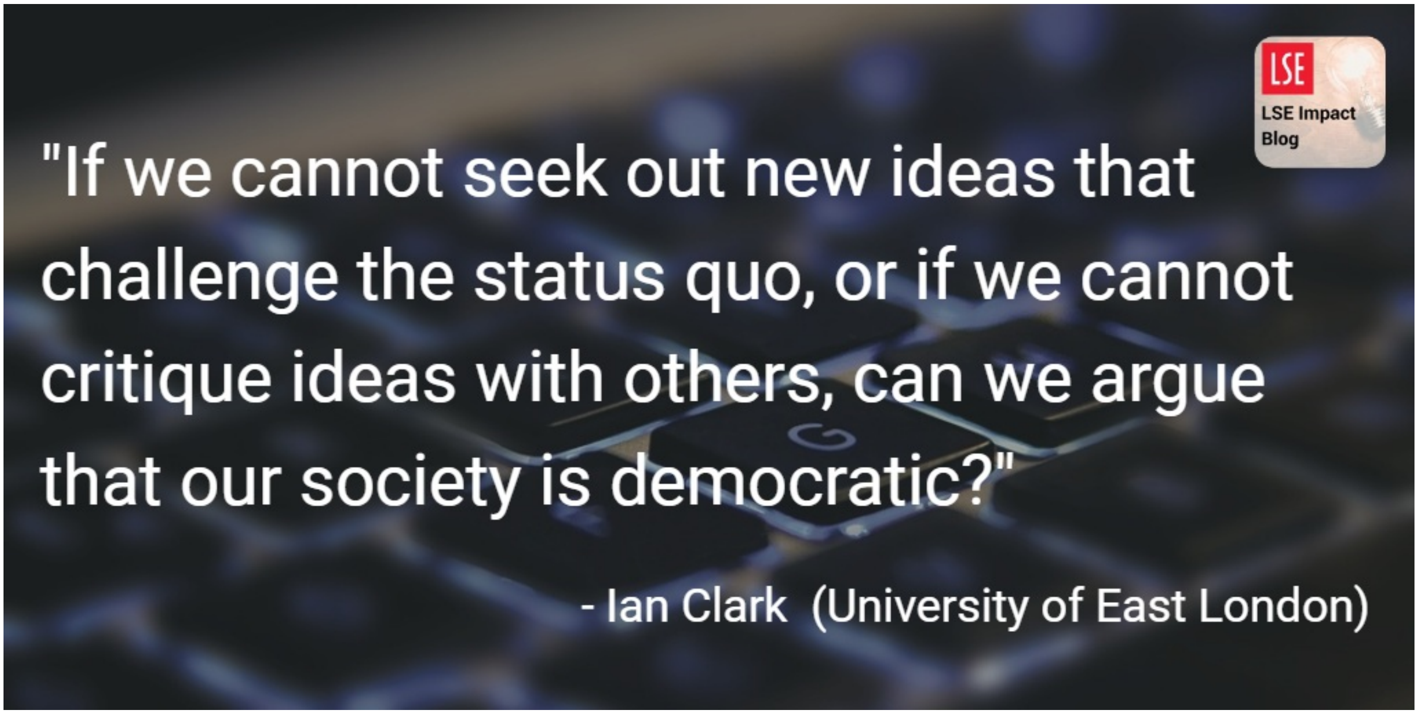
blogs.lse.ac.uk/impactofsocialsciences/2016/06/21/internet-freedom-for-all-public-libraries-have-to-get-serious-about-tackling-the-d

Democratic engagement depends on critique and dialogue. **Ian Clark** *looks at emerging issues related to digital literacy, online privacy and surveillance. Not only is a security divide emerging between those with digital knowledge and skills to protect themselves and those without, but also an intellectual privacy divide. There is scope for public libraries in the UK to teach the skills people need to ensure they can use the internet securely and privately, enabling wider engagement in the democratic process.*

The revelations that Britain's intelligence agencies have been secretly collecting personal data since the 1990's, coupled with Edward Snowden's revelations about mass online surveillance online, have underlined the extent to which our data is vulnerable. As a consequence, it further undermines the potential of the internet to deepen democratic engagement. Rather than a tool we can use to seek more information on and engage with those governing us, it is increasingly a tool for the governing to extract more information about the governed.

The internet has offered governments around the world new opportunities to observe what people are reading, who they are communicating with and what they are communicating. The disclosures of mass surveillance result in a "chilling effect", inhibiting our ability to communicate and seek out information freely. This effect was noted by the Presidential Commission on Law Enforcement and Administration of Justice in 1967 who observed that the fear of being monitored can have "a seriously inhibiting effect upon the willingness to voice critical and constructive ideas". More recently, a study by Oxford's Jon Penney demonstrated that such an effect is evident in our online activities. Penney found that following Snowden's revelations, there was a significant decline in page views on Wikipedia articles on topics related to terrorism such as "Al Qaeda" and "car bomb". As Penney notes, if individuals are deterred from seeking out information on these topics, "democratic deliberation will be weakened".

The ability to voice critical and constructive ideas is crucial to a functioning democracy. Suppression of criticism ensures the status quo and therefore inhibits the democratic process. Democracy requires a "relentless critique and dialogue about official power, its institutions and its never ending attempts to silence dissent". If we cannot seek out new ideas that challenge the status quo, or if we cannot critique ideas with others, can we argue that our society is democratic? For those already excluded or marginalised from the democratic process, surveillance therefore presents an additional barrier to democratic engagement. As Virginia Eubanks argues, marginalised groups are particularly likely to be the focus of surveillance, and are often subjected to "some of the most technologically sophisticated and comprehensive forms of scrutiny and observation in law enforcement".


LSE
LSE Impact Blog

"If we cannot seek out new ideas that challenge the status quo, or if we cannot critique ideas with others, can we argue that our society is democratic?"

- Ian Clark (University of East London)

The Investigatory Powers Bill, introduced in the House of Commons last month and currently undergoing scrutiny, further underlines this threat to intellectual freedom. The Bill aims to ensure that, to an extent, there is no means of communication the state cannot read. But only to an extent. For those that have the knowledge and skills, it is still possible to protect ones communications from prying eyes. Whilst the Bill intends to tackle end-to-end encryption that the service provider controls (and therefore can "break" on request), individuals are increasingly moving towards encryption that the provider *cannot* control. For those aware of such technologies and those who have the skills and knowledge to use them effectively, the impact of such a Bill can be limited. For those without, the reality is that their communications will be subject to collection and storage. In effect a security divide, but also an intellectual privacy divide.

Despite growing access to the internet, there are still many that lack the skills to use such access effectively. According to a report prepared by Ipsos MORI for GO ON UK found that although only 13% of ABC1s lacked basic digital skills, the figure was as high as 35% for C2DE social groups. Furthermore, many do not observe basic online security principles. According to an Ofcom report, 64% of internet users use the same password for most or all websites, 26% do not read privacy statements at all (43% say they "skim-read") and 68% say that they are happy to provide personal information online "as long as they get what they want".

When it comes to online privacy, how many of us can be confident that the tools that we use are providing us with the security we require? Increasing numbers of people use mobile devices to connect online and communicate with others. Yet when it comes to our Whatsapps, Vibers, Telegrams and Signals, can we be sure which messaging app provides us a relatively secure environment to communicate freely with others? (It is Signal by the way.) Relatively because mobile apps are always vulnerable, particularly as mobile devices have a tendency to expose data such as location, numbers dialled and various other identifiers. The best option to communicate securely electronically is by using encrypted email. But email encryption systems such as PGP (Pretty Good Privacy) aren't exactly easy to use and require a greater degree of effort than freely available alternatives. Equally, Tor Browser provides the opportunity to seek out information securely, but it suffers from something of a negative perception.

Cost is another factor inhibiting the ability for individuals to communicate securely. Despite the controversy surrounding the San Bernadino case, Apple's iPhones still offer the best security for users, not least because the latest versions of iOS (from iOS8 onwards) enables encryption by default. Whereas the majority of iPhone users (around 90%) tend to migrate to the latest iOS the picture is more mixed for Android phones. Although the latest versions of the Android operating system offers full disk encryption by default, older versions do not and, unlike Apple, devices using the older Android operating system are still very much in circulation. Needless to say, such devices also tend to be cheaper, making privacy the domain of those not only with knowledge, but also with money (as if it has ever been any other way).

In the United States, librarians have long been seen as being in the vanguard of intellectual privacy. It was librarians in Connecticut in 2005 that stood up to the demands of the Patriot Act to provide patron library records on request. And it is librarians that are at the forefront of fighting the intellectual privacy divide. The Library Freedom Project, for example, has sought to ensure that the skills and knowledge required to ensure internet freedoms are available to all. Not only has the Project delivered workshops on internet privacy for the public, it also successfully stood up to the Department of Homeland Security in their attempts to clamp down on the use of encryption technologies in libraries. Imagine, in an environment where public libraries are facing threats of mass closures, a library service here even attempting something comparable.

In the UK there have been no comparable efforts to make Tor the default browser in public libraries, however there are increasing efforts taking place to support individuals in developing privacy skills. In May 2016, for example, a "crypto party" organised by the north east branch of the Open Rights Group was hosted in Newcastle's City Library. During the event individuals learned how to use Tor, PGP and full disc encryption (amongst others). Although it is unlikely that public libraries in the UK will start installing Tor browsers on their PCs any time soon, there is scope for public libraries to teach the skills people need to ensure they can use the internet securely and privately. If we want to be serious about tackling the digital divide, then we have to be serious about tackling the online privacy divide. Teaching digital privacy skills not only protects individuals from harm, but can enable their full engagement and participation in the democratic process.

This blog post is based on the journal article, "The digital divide in the post-Snowden era" originally published in the Journal of Radical Librarianship.

Featured image: Surveillance Camera By EFF-Graphics (Own work) [CC BY 3.0], via Wikimedia Commons

Note: This article gives the views of the author, and not the position of the LSE Impact blog, nor of the London School of Economics. Please review our Comments Policy if you have any concerns on posting a comment below.

About the Author

Ian Clark is a subject librarian at the University of East London, co-founder of Voices for the Library and is involved in the Radical Librarians Collective.