



**Gus Hosein**

## They know where you are

"It is almost as though freedom and flexibility is being designed out of the Internet, where previously they were essential." Gus Hosein of Privacy International on how the Internet is turning into a data goldmine for governments that want to keep track of their citizens.

Privacy and free expression are bedfellows. Strange as it may sound, the history of both rights are often bound, and not always in antagonistic ways. In the context of Internet and global communications networks, the relationship is actually quite complementary: free expression may be both enabled and protected through privacy rights such as anonymity. (We have long known that the converse is true. Privacy rights have been protected through free expression — every time a new secret spying programme is uncovered by journalists around the world, privacy advocates breathe a sigh of relief that Article 19 or the First Amendment exists, then prepare for a gritty battle.)

Early privacy laws and standards hinged on free expression. For instance, in the US, where there is no explicit constitutional right to privacy, the US Supreme Court built the right to privacy in the 1950s and 1960s from the foundations of the First Amendment. The court ruled that individuals could be members of groups such as the National Association for the Advancement of Colored People without having to disclose their names to the Governor of Alabama (*NAACP v Alabama*, 1958), and that states could not order pamphleteers to include authors' names on pamphlets calling for policy change (*Talley v California*, 1960). In its decisions, the Supreme Court repeatedly referred back to the more oppressive times in England of yore, where the exposure of names of dissenters who made use of the printing press would lead to harsh punishment.

This link between privacy and free expression led to one of the first online censorship regimes being found unconstitutional. The US Communications Decency Act from 1996 required that indecent content on the Internet should be made accessible only to those over 18. The courts contended that on the Internet there is no way of identifying individuals, let alone their ages. The Internet at the time was in a state of affairs where it was difficult to differentiate between individual users, as this often relies on the state and companies being able to identify them. Put simply, "it ain't built that way". As a result, they ruled, the law would create barriers preventing individuals with constitutional rights from gaining access to this very information.

Now the situation is far more dynamic and much more perilous. Ten years on from that court decision in the US, the Internet is quite a different environment. We have services that were previously unimaginable such as

video uploading and downloading. Copyright and defamation fears are widespread. Terrorism laws have imposed further legal obligations upon Internet service providers. Personal information (including identity information) can now be harnessed, and even combined with location data. This is not your parents' Internet. Social networking sites have multiplied where personal information is flowing willingly from the company-owned hosted page. Journalist bloggers are uncovering major stories with the help of confidential sources. We can not only identify those sources, but we can also identify the readers.

In this modern communications environment we still have the privacy and free expression collision, for sure. Concerns arose recently regarding Google's Streetview application. It takes snapshots of streets across America, including photographs of individuals who felt their privacy was invaded. After complaints, Google promised it would take down any offending photograph and, when possible, blur the identifying features of these snapshots. Interestingly, free speech advocates did not stand up to defend Google's right to collect this information in the first place, which possibly shows we've turned a corner in this conflict.

With this hyper-interactivity on the Internet as it is today, every user is now a communicator. Every reader of a news story can in turn become a commentator, appending his or her comments at the bottom of articles. For years now bloggers have been gaining traction and recent studies have shown that many Internet users rely heavily on blogs for their news.

It is hardly a surprise that governments are clamoring to go after these bloggers. Fortunately the very same media that enables their arrest also garners attention. Abdelkareem Nabil Soliman, an Egyptian blogger charged by the Egyptian government for "spreading information disruptive of public order", "incitement to hate Muslims" and "insulting the president", gained worldwide coverage for his case (not that this led to his release). Syrian student Mesud Hamid was arrested for posting photos of Kurdish rights campaigners. These investigations were all made possible through the identification of Internet users. This is why China has worked so hard to establish a registry of all the country's bloggers, of which there are apparently 20 million. Anonymous websites and blogging have been banned since 2005.

Even when the identity is not immediately clear through some government registry, the data can be garnered from service providers. International companies like Yahoo! were subjected to international condemnation for co-operating with undemocratic governments that seek the names of the users of their services, including journalists. For anyone who has ever set up a webmail account this sounds like an easily avoidable situation where you can register your name as the ever stolen identity of Mickey Mouse.

But this will not stop governments from getting what they want. They can follow two paths to get their suspects: follow the data footprints or change the law. Many governments, including even Germany and Italy, have rules requiring identification of Internet customers. Parliaments are passing laws that require cybercafes to check ID cards and passports before granting access, while other countries now require webmail providers to record the real names of their customers.

Governments also know that so long as you have to pay for Internet access, someone somewhere knows your name. They also know that with all this

inter- activity there are footprints being left everywhere on the Internet. This "traffic data" exists in logs that identify who has been talking with whom, who has been emailing and messaging whom, when, possibly where, and sometimes even why. Under the banner of counter-terrorism policy, governments across Europe banded together to force the EU to pass laws requiring all telephone, Internet and mobile phone providers across Europe to start harvesting this information so that it can be made available to police for any investigation, regardless of whether it is for terrorism.

A simple comments post on a blog can be traced back to the blog service provider who will have a log of the Internet protocol address, a unique identifier, which can then be used to track down the comment-maker's Internet service provider who will then be compelled to identify the account holder who was assigned that unique address. So essentially, every phone call or email made by every Internet user across Europe, whether consumer, journalist or dissident is now logged, and this data can be used by governments with impunity to identify habits, friends, colleagues, sources, networks and sympathisers. And this data will be shared internationally.

Now this isn't to say that there aren't sometimes useful and amusing applications of this level of surveillance. Recently, this very same technique was used to see who had been making changes to entries on Wikipedia, the online interactive encyclopedia. When the log data was analysed, it was revealed that CIA computers made changes to entries about Iran, while an FBI computer deleted images of Guantanamo Bay. The Australian government was caught recently removing hundreds of negative comments from Wikipedia (and adding a now famous arbitrary statement, "poo bum dicky wee wee").

Meanwhile, companies are not always reluctant to take on this responsibility. There are increasing commercial incentives and pressures to profile and identify users. This can be due to advertising imperatives, where user profiles are generated by most large service providers to decide who may be interested in seeing more advertisements from adult pornography companies for instance. Companies are increasingly profiling based on geographic location by region-coding the Internet, often for intellectual property rights protection. Users from specific countries are blocked from gaining access to resources to protect financial interests. While 1990s' censorship laws tried and often failed to compel service providers to differentiate between users and block access to specific resources, companies have since then created the very same techniques for their own benefit. So when governments return with a new censorship initiative, it won't be so easy for us all to argue that the Internet just isn't built that way.

Technologies such as the anonymous routing network Tor permit the circumvention of these measures, allowing individuals to express themselves freely and anonymously. Even simple open wireless networks also permit communication without identification, where we connect to the Internet without having to identify ourselves through payment or other mechanisms. But these techniques are being crowded out by increasing numbers of legal requirements to close these networks down and to log our online interactions with impunity. It is almost as though freedom and flexibility is being designed out of the Internet, where previously they were essential (though possibly accidentally so). It is being built in a way that enhances opportunities to identify and profile, which are the key ingredients to censorship.

We must recognise that this is not just about the Internet. Ten years ago it was fun to think about free speech online merely as the protection of cyberdissidents and pornographers (both probably operating from dark and dank basements). Now, not only do we have more Internet users with more varied interests, but the Internet is being freed from the desktop computer and integrated into our lives. This could previously be said to be categorically a "good thing". But because we have all become so good at leaving our traces behind for companies to keep and governments to follow, this will lead to a very different reality. Real world protesters will be tracked using these same techniques, as protests will be monitored by tracking the location of mobile phones in the protest area.

Recently, Iran announced that university lecturers must disclose all foreign trips — but governments need not worry about requiring citizens to fill out papers and forms when instead the email and mobile phone logs will disclose every location by default (and over a period of years). Under despotic regimes, journalists and dissidents would have to report on every individual he or she spoke to on any given day; wireless logs will now also disclose locations and times of arrival and departure of everyone everywhere. This is not your parents' version of censorship.

Interactivity and global data flows are certainly on the rise and play important roles in our lives. In the age of interactivity, freedom of speech, freedom of expression, freedom of association and freedom of assembly are essential ingredients of an open society. Ironically, however, in this same interactivity lie the seeds of repression enabled through mass and indiscriminate surveillance. The relationship between privacy and free expression is set to become even more perplexing.

---

Published 2008-02-05  
Original in English  
Contribution by Index on Censorship  
First published in *Index on Censorship* 4/2007  
© Gus Hosein  
© Eurozine