Anonymity online: a brief introduction.

Open Rights Group note, June 2013.

Contact: Jim Killock, Executive Director – jim@openrightsgroup.org

This briefing introduces anonymity online. It sets out how people can seem anonymous, why this is often not the case, and explains why some people might seek anonymity for good reasons.

Whilst it might seem that being anonymous online is the norm, in fact most people leave digital traces from which they can be easily identified.

1. *What kinds of 'anonymity' exist?*

There are a number of ways that people can seem anonymous online. But people leave a digital trace that could be used to identify them. There are also ways to try to hide that digital trace.

a. Using a pseudonym

When people go online, it can seem that they are anonymous if they don't make their everyday name obvious. For example, if I post a comment on YouTube I may do so from a username such as “Awesome0221” rather than “Peter Bradwell”. Somebody reading my comments may not know my name from this interaction.

These are pseudonyms. 'Pseudonymous' is not the same as 'anomymous'. It might be simple for a member of the public to link these pseudonyms to other details about them - a simple search may reveal more information about who is associated with that username. The owner of a website like YouTube is likely to have more information about “Awesome0221”, depending on what is required in registering to use that service. That may include their 'address' (email or physical) or everyday name.

b. Avoiding leaving a digital trace

When somebody is online, they leave traces of various types of information behind them. That can include their “IP address” (the unique identifier of their current connection to the internet)[1], the web browser they are using, the other websites they are looking at, or where they are.

This sort of information can be visible to a number of people. That includes for example the operators of websites visited (for example, the BBC). It also includes those who place adverts or other content on those websites, such as 'like', 'tweet' or 'share' buttons. These usually track users' behaviour. Some information will also be collected by the person's internet service provider (or “ISP” – meaning companies such as BT or Talk Talk).

There are ways to try to mask or hide this information. For example, you can turn off 'cookies' – which are small files that are installed on your computer by a website which help that website track your behaviour across the Internet.

Other measures that can be used to restrict the amount of information available include the use of Virtual Private Networks (VPN). VPNs pass internet communications via another separate network. These are mainly used by companies to help them access secure networks remotely. But they are also popular with internet users who wish to use a service or visit a website without disclosing their real IP address (and thus approximate geographic location).

A variation on the VPN is Tor, which is a network of virtual tunnels distributed widely across the network. It not only obscures the user's IP address, but also reduces the risk of traffic analysis being used to link both

1 For more information on what an IP address is, see https://en.wikipedia.org/wiki/IP_address

ends of a connection.[2]

Masking all of this data is extremely difficult, partly because it is difficult to know what is being tracked, by who, and when. For example, even the many settings on people's Internet browsers can be unique. In their research into 'browser fingerprinting', EFF found that 84% of browsers had unique configurations.[3]

2. How anonymity can be removed or undermined

Requiring registration with popular services for the purposes of reducing anonymity can lead to the collection of more sensitive information. Proving who you are to an Internet company will more firmly link your 'real' identity to your browsing history, the things you read online, who you contact and so on. It is then possible that this information will be accessed by people or organisations who have nothing to do with the original service or site.

a. Legal powers to get information

It is sometimes possible to use the information mentioned above to identify somebody with varying levels of confidence – even if the person posts messages as an 'anonymous' or 'pseudonymous' user. For example an ISP may try to 'match' an IP address with one of their subscribers. There are various legal powers that in some circumstance, require Internet companies to disclose this data, and which permit the use of it in various contexts for the purposes of trying to identify a user.

Currently these powers are almost exclusively for access to information that companies already collect for business purposes. There are currently some proposals, for example in the Communications Data Bill, to force Communications Service Providers to collect information that may be useful in the future for other reasons, for example law enforcement.

As the “Prism” story has recently revealed, there are various powers for security services to access personal information held by the Internet companies whose services we use. The nature of those powers, for example whether they are proportionate or are subject to sufficient oversight and accountability, is currently a matter of significant public concern.

b. Leaks or inappropriate access to information

As mentioned above, lots of the information people leave behind is very revealing and often sensitive – including the things we read or people we know and speak to. This is stored in a number of places. It is possible that through malicious access, breaches of the rules or law, or just mistakes, this sort of information can end up in the hands of people who should not have access to it. That could be used to punish, exploit or just embarrass somebody.

3. Who needs anonymity and what is lost if it is forcibly undermined

When somebody is not confident about who knows what about their communications, it can have a chilling effect and discourage them from saying particular things or from meeting or speaking with some others. Information about us now also determines how we are treated in a number of ways. Further, if somebody believes they are being observed, they are likely to conform to what they believe the observers expect.[4]

So anonymity is important to everyone. There are many specific reasons why people seek anonymity 'offline'. The same reasons apply online, especially as most now use a number of digital, networked devices and services. Indeed, it is now possible to gather more information about us and our communications than ever before.

---

2 https://www.torproject.org/about/overview.html.en

3 See https://panopticlick.eff.org/ and https://www.eff.org/deeplinks/2010/05/every-browser-unique-results-fom-panopticlick

4 For research on this issue, see http://www.bis.gov.uk/assets/foresight/docs/identity/13-507-surveillance-and-privacy-technologies-impact-on-identity.pdf

1. **Whistleblowers,** and other sources of information, who often reveal information of public interest but face likely punishment as a result[5].

2. **Those seeking or receiving confidential legal or medical advice**.

3. **People seeking refuge from abusive relatives or acquaintances.** This includes somebody visiting websites to find out information – somebody's browsing history may reveal their activities to an abusive partner.

4. **People trying to contact organisations such as the Samaritans,** who will want to feel that they do so in confidence.

5. **People lobbying or campaigning against laws, governments or businesses.** For example, there are many cases of sometimes very oppressive regimes trying – often with success – to find out through information from online activity who is organising or taking part in political activity they disapprove of, or to punish protestors or political activists for doing so.

6. **Journalists.** For example, the organisation Reporters Without Borders use Tor to protect the journalists, sources and dissidents they work with.[6]

7. **Consumers**. Some online retailers use information about consumers – such as where they are, or what they have previously browsed - to change the price of their offers. This may counteract any efforts by consumers to use price comparison sites, for example.

4. Examples of policies trying to remove anonymity forcibly

1. **South Korea** instituted a 'real names' policy in 2007. It was ruled unconstitutional in August 2012.[7] One contributing factor was the hacking of details of 35 million users of popular Internet sites including IDs, passwords, resident registration numbers, names, mobile phone numbers and email addresses.[8]

2. **China** has policies enforcing 'real name' policies, which extend to blogs, services like Twitter and accounts with Internet Service Providers.[9] It does not seem in practice to be well enforced[10].

5 For some examples, see the briefing from Public Concern at Work, https://www.openrightsgroup.org/assets/files/files/pdfs/ORGAnnexBLeakingCaseStudies.pdf
6 https://www.torproject.org/about/torusers.html.en
7 http://www.bbc.co.uk/news/technology-19357160
8 http://www.chinadaily.com.cn/world/2011-08/11/content_13095102.htm
9 http://www.wired.co.uk/news/archive/2012-06/07/china-microblog-restrictions
10 http://asia.cnet.com/blogs/real-name-registration-in-china-a-bad-joke-that-turned-into-a-farce-62213948.htm