Privacy and Security

Jeremy Wagstaff

When the internet was invented, privacy was not the main issue. Everyone was too nice, and behaved themselves. Those days, sadly, have gone.

The internet that emerged in the 1960s and early 70s was primarily a place for academics, and those technical and curious enough to scale the barriers to entry. It was mostly American, and resolutely uncommercial; when someone sent an email to lots of people, he was scolded so much that no one thought of doing it again for nearly 20 years. No one was supposed to make any money out of it. For years, the internet was a small town, where everyone felt they knew everyone else, where having an email address was enough to grant you residency, just so long as you were polite and helpful. But it was still quite a rarefied atmosphere, because only those with access to university or military computers could get in.

In 1991, I fought my way in, when the barriers were considerably lower. All I needed was a modem, serial cable, telephone line and an account with an internet service provider. Then, there were only a handful of such services, even in supposedly advanced cities like Hong Kong. Sure, there were bulletin boards and arguments, but for the most part it was a generous, sociable community. I would pay for the equipment (computer, modem, telephone line) and my internet service provider account, but not for anything else. Everything on the internet was freely provided and freely shared.

An email would be from a real person, and you would usually reply, a little as if it was a real letter. I was a journalist then, but still convinced I was a pop star in disguise, and I remember getting helpful advice from other internet users on how to connect all my synthesisers together. There was rarely a rude or impatient word spoken.

When I moved to Indonesia a couple of years later, I used the internet to connect with academics, exiles and East Timorese rebels outside the country who could help me analyse what was going on. Most were not allowed into Indonesia so it was helpful for them to know what I was seeing and hearing, and I was more than grateful for their encyclopaedic knowledge about the country.

The internet began to change around 1994 and 1995, with the arrival of HTML, or hypertext mark-up language, which was simply a way to convert a page of boring text into something more exciting: images, colours and sound — all of which could link to another page elsewhere on the internet. It was intuitive too: blue and underlined text stood out invitingly, luring the reader to click on it and be transported to another page. It did not matter where, or require complicated addresses. Yahoo, and later Google, organised it all and made everything just a click away.

Suddenly everyone began to think of the internet differently; from a place of learning, it became a place for selling. Amazon sold books first, only because they were the easiest things to store, and ship. Companies thought up ways they might make money out of what was now called the world wide web, and spam and computer viruses followed quickly (both in 1994). Today, we are in a different world, where much of the internet is on mobile phones, really just portable computers. Behind the touch screen and graphics, the plumbing is pretty much the same, using the same protocols and pipes that the internet was built on. Supporting it is a network of infrastructure companies that build cables under the sea, fling satellites into the sky, build cell phone towers and base stations, all to carry internet traffic around the world at the speed of light.

Oddly, we still do not pay for things, for the most part. We have to buy a phone, and the bandwidth we use, but we do not pay for Facebook, Google, Twitter, Instagram, or WhatsApp, not because they are providing their expertise free of charge, but because they have found a way to monetise us. We are the product. They sell us to advertisers. Our private lives are the product.

Traditionally, every society perceives "privacy" differently. For some, it means covering our face with a veil. For others, it means not staring at other people, even if they are wearing very little; or giving our first name but not our second. I'm a Brit; we do not like being asked overly personal questions, but after decades in Asia I've become used to it, even enjoy it. Our social caution is probably down to the fact that we Brits give away much more information than we would like — our clothes, shoes, how we walk and speak, etc., reveal our class and regional data. It might be an inaccurate picture, but it is very hard to dispel.

So what does privacy mean online, and why is it so valuable to advertisers? How Brits interact is actually a good way of thinking about it. Offline, in the old days, advertising used to be hit-and-miss — if you wanted people to know about your product you would pay an advertising company to splash the name over billboards, in newspapers, on TV, and in mailshots. But you could not tell what worked and what didn't; the old joke was "you know that half of your advertising budget is wasted; you just don't know which half".

The internet has changed that. Now advertisers have a very good idea what works and what doesn't, through whether or not we click on their links in an email, on a website or in an app. They will know if you are interested in their product; they may not know exactly who you are, but they will know you are the same person who searched for inflatable bouncy castles or teeth whiteners. Putting together these bits and pieces of information, they try to figure out what kind of person you are: man, woman, child, married, pregnant, well or sick, interested in skiing holidays, etc. etc.. The so-called data exhaust from our time online builds a revealing picture about who we are. Then advertisers will assign you to buckets of types of consumers, which can be sold to the highest bidder.

So how did we get from an internet of like-minded souls to one of advertisers snooping on our every click? The story of the internet since 1995 has been the story of companies desperately trying to find a way to turn this amazing medium into something they can make money from. Jeff Bezos of Amazon figured out that the best way, at least in the early days of the Web, was to use it as a sort of glorified shop window. Instead of going to a bookshop you went to amazon.com, found the book you wanted, paid for it with your credit card and Jeff would ship it to you. Even then a lot of people baulked — firstly, not everyone wants to buy just books, and secondly, how could you pay for something securely on the internet?

It became obvious that the solution to these problems was a combined single one: the best products to sell using the internet were the users themselves, because then they did not have to pay anything. The internet, after all, is all about scale; it is subject to the network effect, i.e, it is more valuable the more people are on it. Most of us choose to live near other people, partly because we are sociable creatures, but we also know that with more people around us, there will be more shops, more services, more willing hands at harvest time, or when you need a babysitter. Like the first telephone, the internet became more useful when more people came aboard. In the early days, when I found someone else with an email address on their business card, we would crack open some champagne and celebrate.

As the internet grew, so did the idea that the best service one could make money from was one which had the most users. This meant they were likely to stick around, because all their friends were there, but it also meant more and more data to collect about those users. The internet was less like a shop window, and more like a bait-and-switch university psychology experiment. You lure people in off the street by asking them to test coffee. While they are chatting and sipping, you are watching through a one-way mirror how they hold their coffee cups depending on who they are talking to. The coffee was just to get you inside and loosen your tongue.

This is, more or less, the business model of most of what goes for internet activity nowadays. From your emails and chats, photos you post, stories you read and ads you click on, to how long you spend watching a video of cats — all this determine which of those buckets I mentioned you end up in. This only works if as many of us use the same service, and spend as much time on it as possible.

Google replaced Altavista and Yahoo because it made a better search engine, and so collected a lot more data about what we are interested in. Facebook replaced Myspace and Friendster and other social networking services because it threw all its efforts into getting as many people to sign up as possible. That meant Facebook could learn a lot more about us because if all our friends and family are on Facebook, why should we spend time anywhere else? That meant making it free for us, because, with that network effect all maxed out, we were a hostage audience to advertisers who could choose which bucket to throw their ads at.

So what does privacy mean anymore when someone is watching almost everything we do online? They may not know it's exactly us, as in our name, but that's scant compensation. They know a lot , down to where we live (or at least the block, or floor) and — because we tend to view things on our phone or laptop when we are alone — they know more about us than some of our nearest and dearest. We are the product, which we are updating every time we switch on our phone.

In a way, this does not matter; the worst that can happen for now is that we will be pitched products and services that seem a little too personal. Friends who recently lost a child in pregnancy have had their grief rekindled by ads for baby products, and another friend had his searches for oncologists on Google come back to haunt him with disconcertingly specific ads relating to cancer drugs. But the bigger problem is that we do not know exactly what is being collected, how it is being used, and into whose hands this information will fall.

Think, for example, about what Facebook knows about you, should you use it. They have your name, probably your age, phone number, email address, and lots of other fields you may have completed for them — your schools, employer, and interests. Then there is what they call your social graph — the network of friends, relatives, and colleagues you have added on Facebook, or you have tagged in photos and posts, or those who have tagged you. All this assembles a picture of you that is once again thrown into buckets, some very specific, say, men aged 25-30 who like heavy metal music and wildlife photography and who live in a particular part of Singapore. Advertisers do not need to know your name to be able to advertise very specifically to you. This information is so valuable that every time you load your Facebook page, or search for something on Google, a very fast auction is taking place behind the scenes, where the highest bidder gets to put their ad in front of you.

This might seem relatively harmless: all it means is the ads you see are going to be more relevant and specific for you, right? Some might even be useful. But the surveillance economy has gone a lot further. Many organisations now depend on it to make money, and when they are granted access to this data, we start to enter the realm of the unknown.

Any company in this space is working hard to have an edge, which means that all that data you thought was anonymous might not be so anymore. If it can be linked to you, then whoever has access to it will know a lot of what interests you, ails you, motivates you, upsets you, or what you do or think about when no one is looking (assuming you do it on a computer or phone, including Google searches you thought were private). This is why some countries like the US demand to know some applicants' social media details before they issue a visa, as do some employers. That trail you leave is permanent. Facebook has been around for 15 years, and many of us have been users for at least 10. That's a lot of likes.

So can that data be linked to you without your knowledge or say so? Yes, say researchers from France and the UK, who in a paper published last year that used only 15 demographic attributes — think of them as data points, like birthdates and birthplaces — of an anonymised profile, wrote that they could correctly identify 99.98 percent of Americans. With four characteristics, they could identify someone — meaning connect the anonymised profile with its owner's real name — with 79.4 percent accuracy. Their results, they said, "suggest that even heavily sampled anonymised datasets are unlikely to satisfy the modern standard for anonymisation" set under privacy regulations in the European Union, regarded as the strongest currently in force. Whether companies are already doing this isn't clear, but it's obviously possible. And once one chunk of your online records is tied to you, the rest will follow.

This is happening in a world where we are constantly being asked to give up data. It's more or less impossible not to do so. In Singapore, I use my phone to book a taxi or a car-hailing service like Grab. So they now have details of my movements. If I buy something with a credit card, then my bank, the credit card company, and the place where I made the payment have details about me.

Apps on my phone may be tracking my movements even if I'm not using them. They may know that I regularly visit the hospital, gym or the police station. Some data might be used in what sounds like a positive way: a company called Tala lends money to individuals based in part on how, where and how often they use the device and app. These services do help to reach those who may previously not have had access to formal credit, but researcher Alain Shema of Syracuse University in the US argues that such apps "collect massive amounts of data from the users' phones". The user is often not informed about all of them, Alain says, but he points out that versions of Tala's application request permission to access sensors and sensitive data on the user's phone, which includes "running applications, web bookmarks, SMS content, contacts list, and call logs".

If you end up with the loan that you have been looking for, you might regard all this as a necessary evil. After all, banks ask a lot of personal questions too. But because this is data drawn not from questions asked but by using your own phone to spy on you, then you might find you are giving away data you did not intend to. Is everywhere you go with your phone something you are OK sharing with others? Are you OK sharing your address book and SMS history? You may baulk at answering these questions from a bank, but when the only question is "do you accept our terms?", or when you are presented with a list of permissions the app needs to function, you will probably give the matter less thought.

As with the lending apps, much of this new internet-driven world would not function unless you allow this data harvesting to take place. Google would not let you use most of its services — meaning most Android phones — without an account. That means a profile is already being constructed of you. Ditto with Twitter, Facebook, Amazon, and nearly every service you have ever used.

It is impossible for individuals to police this but there are things you can do. If you are searching online for something sensitive — say, a medical issue — then use a privacy-focused search engine like Duck Duck Go. Do not share more than you need to on Facebook, including in your profile. Facebook will keep bugging you to complete your life story, but resist it. It is not helpful to anyone but advertisers. Do not share pictures of your children, unless they are adults (and even then only with their permission). These are baby steps. Gradually you will begin to think differently about the data you put online and realise that what was for you just an "Instagrammable moment" is a also permanent record that others will make money from, and which a future employer or consular official might view in a way you did not intend.

It's the internet. Just not the one that was intended.