The biggest myth about phone privacy

Smartphones have transformed our lives in so many ways. They connect us to the outside world through email and social networks, direct us if we are lost, and recommend all manner of shops and services near us. But this level of convenience comes at a cost, and one that the general public is only beginning to recognise.

In a world where online privacy is a growing concern, security experts say one of our biggest assumptions is that if our identities are hidden we should be safe and anonymous. But evidence shows how little it takes for our identities to be outed. Last week a study of credit card data showed only four pieces of information are needed to match any individual to their “anonymised” credit card records – one of those being the GPS coordinates that can be extracted from your smartphone.

So what seemingly harmless pieces of information pose the greatest threat to your privacy, what exactly can be gleaned from this, and how can you better protect your personal data in the future?

What types of data put you most at risk?
Date, time, geographical location, and smartphone serial number, are the items most likely to reveal your movements. Altogether known as metadata, or smartphone EXIP files, these fragments of information can be linked together to formulate your identity.

People see geotagging as being the most common threat, a feature many applications use to pinpoint and publicise your exact location. On Facebook, geotagging is offered as a service you automatically opt into whenever you post a status or chat on Instant Messenger – unless you disable it. Geotags also feature on other applications like Instagram and Twitter, and have been known to reveal people’s locations when they didn’t think anyone was watching.

How can this reveal what I do?

Earlier last year a burglar named Ashley Keast was arrested after posting a celebratory selfie on a smartphone he had stolen. Despite the fact that he changed the Sim card of the stolen device before uploading the photo to WhatsApp, friends of the robbed victim recognised the location and called the police.

More recently, the mobile dating app Grindr has been under investigation for revealing too much about its users' locations. Colby Moore and Patrick Wardle at the cybersecurity firm Synack found that if an individual created three separate profile accounts on Grindr and searched for a specific user, each profile could provide the means to triangulate the user's position. Synack also said other dating apps are prone to the same issue as they use the same technology.

Fortunately, computer security expert Graham Cluley says that geographical location on social media is something you can control, through adjusting your data location services settings on your phone and applications. However, metadata can still be collected from your smartphone even while you're performing its most basic task – making a phone call.

"It's not as though someone is listening to your phone calls," says Cluley about the information cell phone companies glean from their customers. "But what they do collect is information about who you rang, how long you spoke to them, and where you were when you did it."

So even though the conversation is hidden, people can still fill in the gaps, and this can have serious implications. "If you rang a phone sex service at two o'clock in the morning and spoke for 18 minutes, no one knows what was spoken about," says Cluley. "But I think people can put two and two together."

But I didn't sign up for this, is this legal?

Actually, you did, and it is. Each time you log on to a social networking site or use a free online service like Facebook, you're opting in to having your every move documented just by using the service.

Unfortunately, having access to these conveniences can leave a very detailed data trail behind you, which can easily be pieced together to form a narrative about you and your identity. Just as mobile phone companies have the right to record the metadata of your calls, so do social media companies when you choose to use their services to communicate with friends or followers. Instagram's privacy policy illustrates what they do with user data by stating under the subheading How We Use Your Information, "….to provide, improve, test, and monitor the effectiveness of our service."

Not all of these documents are as short, sweet, and to the point, meaning that most people are unlikely to read them. According to the consumer group Which?, Paypal's total word count for its terms and conditions document is 36,275 words, which is longer than Shakespeare's *Hamlet*. Last year, the UK's House of Commons Science and TechnologyCommittee criticised social media firms like Facebook and LinkedIn for their obscurity and length – the head of the committee describing some of the worst offenders as being "meaningless drivel to anyone except an American trained lawyer".

What else can my phone reveal?
Celebrities and other high-profile individuals find metadata especially troublesome. Last year, a dataset was released by the NYC Taxi and Limousine Commission containing every cab ride taken by the organisation in 2013, according to Neustar Research, "including the pickup and drop off times, locations, fare and tip amounts, as well as anonymised (hashed) versions of the taxi's license and medallion numbers."

As this information was made public, Anthony Tockar, a Northwestern graduate student interning for Neustar, was able to work out where stars like Bradley Cooper and Jessica Alba had taken their taxis in NYC, speculate why, and see how generous (or not) they were at tipping. He did this by realising that paparazzi photographers often capture celebrities entering or exiting New York City's yellow taxis, and that many of their pictures showed the cab's unique medallion number.

Thankfully, I'm not a celebrity, who cares about me?
Taxicab documents can be used to determine your whereabouts – whether you've been dropped off at a strip club or your apartment, for instance. Elsewhere, metadata can also be used to illustrate more opaque information about us. The status of peoples' mental health could be determined from phone call frequency and overall smartphone usage, according to a report by MIT Technology Review. A new app developed at Dartmouth College can match patterns in user data with stress, depression and loneliness. Authenticated by survey research on student moods, user activity also correlated with student grades.

How worried should I be that someone will target me?
The more online platforms you use to communicate, the more you increase your chances of being hacked. On a more intimate level, a hacker could also be someone you know, like a jealous partner.

According to Cluley spyware is sold openly online and can be applied to jailbroken devices in order to monitor another's smartphone activity, such as the GPS location, calls, and texts. Jailbroken devices are iOS Apple products that have been released from their operating system, which can be beneficial for hackers who want to download applications that Apple does not approve. Although this spyware is often advertised for parents to monitor their children, that doesn't always mean that's what the spyware is used for.

Then there is facial recognition software. The most popular of these services is DeepFace, which Facebook uses to recognise your friends' photographs. John Bohannon in Science magazine says the US government is also seeking to develop this technology further and has "poured funding into university-based facial recognition research". Fears as to what this means for privacy and surveillance are escalating.

What should companies do about this?

It is important to realise that when you're using social media you're not only the consumer but also the product. Therefore, it would be quite a disadvantage to the social media companies now to change their business model to convenience users. However, this does open opportunities for other companies to create software that can disguise or disrupt your metadata.

An app called CacheCloak is being developed to mask your GPS coordinates, by sending Google or Yelp multiple possible routes to your destination instead of just the actual one you took. Voice-authentication passwords are also another form of privacy protection technology in high demand. Capable of being used to unlock your smartphone, voiceprintsmay be how we unlock our technologies of the future.

What should I do if I'm worried?

Luckily there here are many things you can do to minimise the amount of metadata you're disseminating. The simplest solution is to go to the privacy settings of your smartphone, and choose which apps you either would or would not like to use data location services. By default, "Allow Location Access" will be turned on for each of your listed apps. You have the option to choose: Always, While Using, or Never. If necessary, you can also turn your data location services completely off, but this prevents you from enjoying the basic luxury your smartphone can offer you – maps.

As for social media you can privatise your accounts on apps like Facebook, Instagram, and Twitter so that only your friends can see your posts. On Facebook you can enable the, "Review posts friends tag you in before they appear on your timeline?" toggle so that nothing goes on your profile without your consent. Also, don’t forget to turn off geotagging, which is a small location pin that can be found on your status bar and within Instant Messenger that you can enable or disable at your will.

As a fundamental rule remember this: if you don’t want information like your photos to end up in unwanted hands, then don’t send it.

http://www.bbc.com/future/story/20150206-biggest-myth-about-phone-privacy