THEY KNOW WHERE YOU ARE

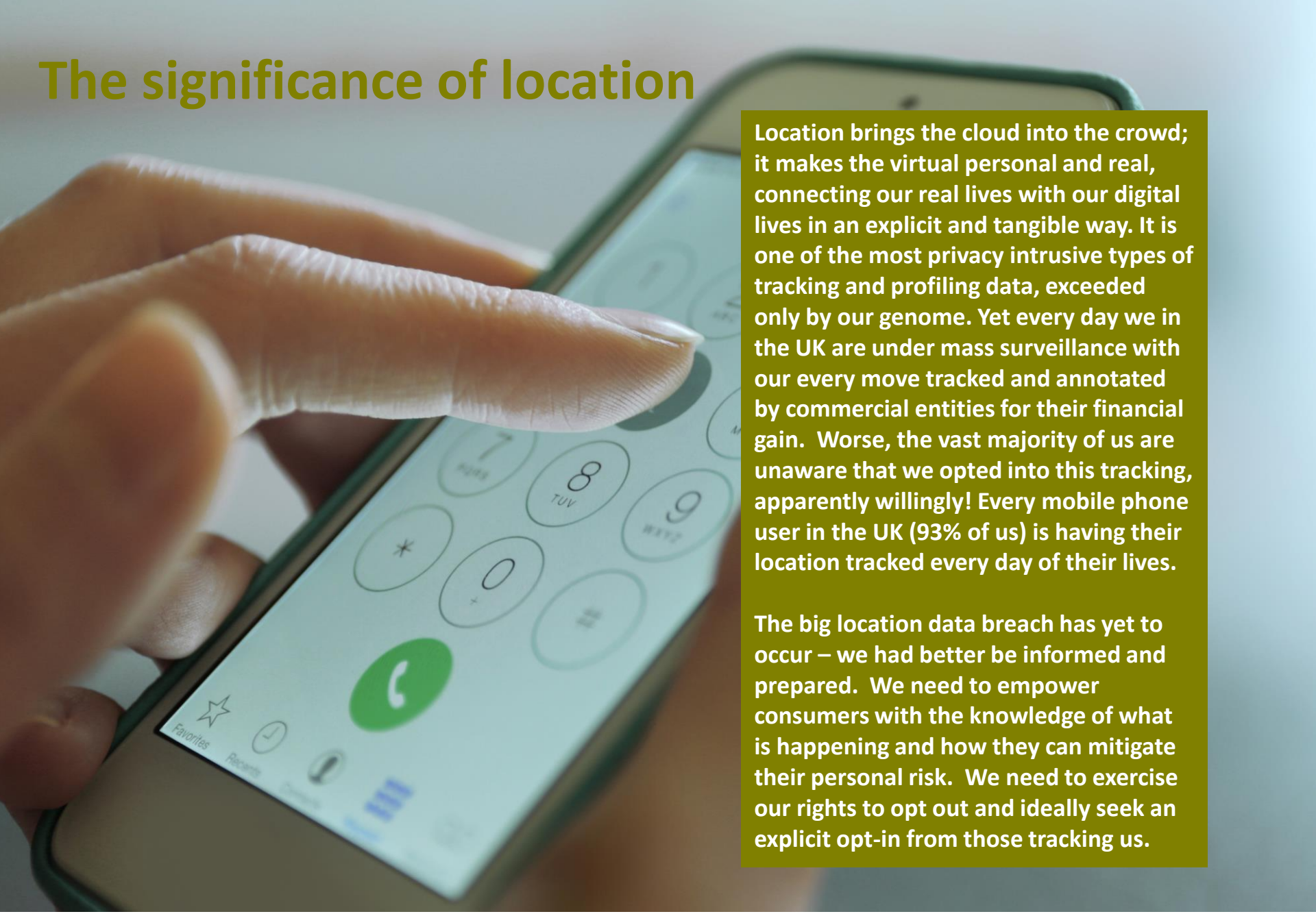
An investigation into the contracts, policies and practices of mobile and Wi-Fi service providers in relation to location tracking

"The fact of the matter is your mobile and Wi-Fi service providers know – without you knowing - where you are, how you got there and can figure out where you are going."

Geoff Revill, Founder, Krowdthink

Krowdthink

The significance of location



Location brings the cloud into the crowd; it makes the virtual personal and real, connecting our real lives with our digital lives in an explicit and tangible way. It is one of the most privacy intrusive types of tracking and profiling data, exceeded only by our genome. Yet every day we in the UK are under mass surveillance with our every move tracked and annotated by commercial entities for their financial gain. Worse, the vast majority of us are unaware that we opted into this tracking, apparently willingly! Every mobile phone user in the UK (93% of us) is having their location tracked every day of their lives.

The big location data breach has yet to occur – we had better be informed and prepared. We need to empower consumers with the knowledge of what is happening and how they can mitigate their personal risk. We need to exercise our rights to opt out and ideally seek an explicit opt-in from those tracking us.

Executive summary

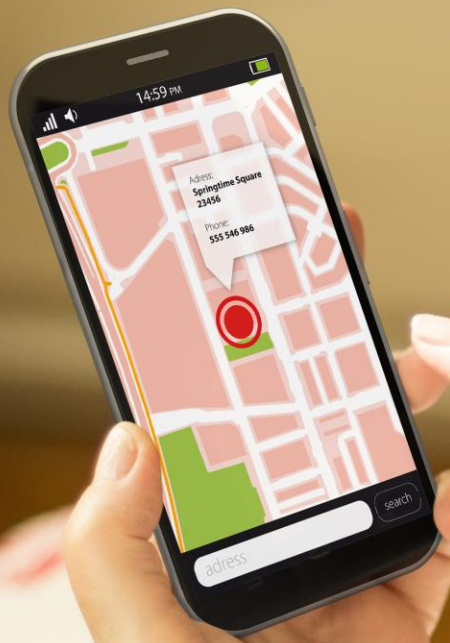
This report reveals that mobile and Wi-Fi service providers are:

- **not telling customers upfront either in store at point of contract signature or online via their websites that all their movements will be tracked and historic location data will be used for marketing purposes and often sold to third parties;**
- **hiding in the detail of their contracts that customers can indeed opt out of location tracking as well as the marketing and sharing of related data; and not making clear the means to opt out;**
- **putting the customer communications focus on the need for location information to route calls and meet the requirements of government security legislation.**

The investigations also highlight that:

- **some public Wi-Fi service providers claim that they have to collect location data for security purposes, which is not the case as with mobile service providers;**
- **anonymisation of data is opaque and questionable as a personal data protection tool;**
- **unless customers know what to ask for when interrogating their mobile or Wi-Fi service providers about the location data they hold on them, they will never be any the wiser; and even when they do know, they don't always get the information they have requested.**

Research methodology



This report has been collated through a combination of:

- **desk research into contracts and policies of mobile and Wi-Fi service providers**
- **software development to confirm technical location tracking capabilities,**
- **interviews with a wide range of research report writers and acknowledged experts in their fields of study and work**
- **multiple SAR (Subject Access Requests) for both Wi-Fi and mobile cell tower tracking information;**
- **direct interrogation of senior staff at the various service providers**
- **'mystery shopping' activities**

The findings have been discussed with acknowledged legal experts in consumer privacy in order to add perspective to this report. The report thus spans technical, legal and business perspectives of location tracking in the mobile sector.

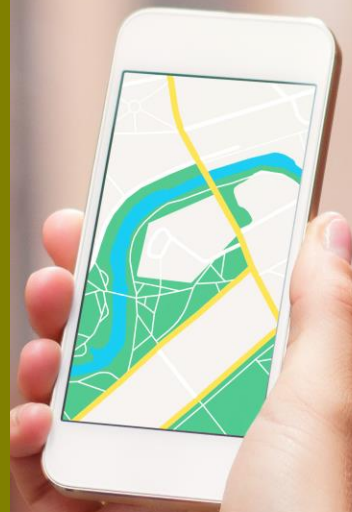
"Location tracking data would be gold dust for the criminal fraternity and would be very saleable on the black market.
Pete Woodward, founder of information security experts Securious

Location data is dangerous

Our location data should be treated as carefully as the health data of our genome, such is the potential for insight into whom we are.

Location and genome are both what data technologists refer to as high-dimension datasets; which basically means that analysis can provide a wide variety of detailed insights with no additional correlated data – when you add correlating data the opportunities for personal insight are extremely significant and highly privacy intrusive.

A simple data set of unique ID combined with location and time provides tremendous insight



Examples of location tracking and data risks

- **High net worth individuals could be targeted, based on where they live, work, eat, shop and combining the location data with a resource like Zoopla shows the locations worth targeting!**
- **Perfect for burglars who will know when occupants of a house are not in**
- **Places your children at risk by identifying if parents pick them up or drop them off at school opening and closing time.**
- **Presents blackmail opportunities, for example by identifying any cases of infidelity – including when, where and how long for**
- **Identifies your sex, probable sexual orientation, your religion and many other personal preferences**

Location data is dangerous

It can be readily understood why companies like O2 and Vodaphone have built entire multi-million pound businesses (O2 Data Insights and Vodaphone Analytics) to feed mobile phone user location information to for revenue purposes.

Some may argue that all this insight is useful, and indeed it potentially is, if in trusted hands and if we knew it was being obtained and for what purpose. But in short we don't know. So when (not if), it gets hacked, we won't even know it existed, we certainly won't know the insights it could give to the nefarious and we'll be totally unprepared for the criminal minds use of the information.

We all need to be far better informed, and if at all concerned about the risks then we should opt out – arguably we should not have been opted in by default in the first place!

Just as we all have a unique fingerprint, we all have a unique pattern of movement over time.
It's as personal as our health records and should be treated with the same respect. A fingerprint generally needs 12 data points to ensure a reasonably accurate identification, whereas location data only needs 4 time-correlated data points to identify one individual from1.5 million with 95%+ accuracy![1]

One unique location/time data point may be enough to identify you. Unlike a fingerprint, changes in our location patterns provide tremendous insight into our personal lives and how they are changing in real-time. How hard is it to find out where we work, go to school or work in todays Internet? That's how easy it is to pick us out from a large location data set.

So location tracking not only provides a detailed definition of who we are in real life, but changes in our regular patterns of movement trigger insight into changes in our lives. Changes that we may wish to keep private or confidential. It's unsurprising that we tend to automatically try and protect our location information.

Our intuitive rejection of location tracking

While the detail of what has just been disclosed through location tracking may not be obvious to many, we instinctively seek to protect ourselves from location tracking because we intuitively comprehend the intrusiveness of this information. A good example was the public backlash when Uber's Gods View tool became public knowledge[2]. Uber had to move fast to mitigate the issue and it still taints them today.

GPS has been around for over 15 years in mobile devices, yet except for mapping services and perhaps hailing a taxi we rarely willingly disclose our location. Even when we do, we tend to minimize the location tracking time. Most of us avoid turning on location services on our mobile devices except when really needed. We even tend to avoid downloading mobile apps with location permissions unless it's obvious why those permissions are needed, even then we tend to explicitly control when location services are used.

Only 11%[3] of us willingly share our precise location in mobile apps with most of us valuing privacy second only to battery life for mobile apps. The latest Mobile Ecosystem Forum Global Consumer Trust Report[4] shows a 30% year on year growth in reluctant sharers of data in mobile apps, with a lack of trust being the single biggest inhibitor to app downloads

Of those nearly half specifically define location or browsing history as their biggest concern. As we will see, some companies highlighted later do both and correlate the data, and it's not the app developers who are the worst offenders.

It is notable that even the most trusted social media platforms are uncommonly used to explicitly disclose location information, while we willingly use them to disclose so much more about our thoughts and opinions. For Twitter for example only 10.3% of users enable the location option explicitly. While detailed data does not publically exist we suspect the majority of these are corporate Twitter accounts, not personal ones, or perhaps inadvertent sharers.

Its scary to learn that turning off location services on your phone has no, none, zero, impact at all on the public Wi-Fi and mobile service providers ability to track you – all the time. And they do, commonly keeping 12 month location histories, some Wi-Fi providers boast they have all their customer movement data since their inception!

Many ways to be location tracked

The majority of us think we are in control of whether our location is being tracked because we define settings in our phone that tell us. On my Android device I have location turned off by default, and in the settings window it tells me "No apps have requested your location recently". This is double-speak. What it should say is that "No apps have used my GPS services to locate me recently." Because I can assure you, you are being location tracked many other ways, consistently.

As a baseline your mobile service provider has to track you so they can route a call to you. They do this by continuously checking for your closest cell tower – but they also keep a history of this data. The fidelity of this information is continuously improving as we move from 2G to 4G services, because more cell towers are needed to cope with changes in technology and density of usage.

There are 52,500 cell towers in the UK; in towns they can be 50m to 500m apart and in the countryside 2-5km[(5)]. So your tracked movements in town are very detailed. This information is required to be stored by law for use by UK security services for 12 months! So every one of us with a mobile phone, even a simple one, is being location tracked all the time.

Unfortunately there are at least two other personal/mobile sources of location tracking information. Bluetooth (these days often referred to as beacons) can be used as can Wi-Fi. They are very often used to track movement within a (geo-located) location as per companies like Navizon and PurpleWiFi[(6)]. Both techniques require us to have turned on those wireless services on our device. However in reality every Wi-Fi hotspot and every Bluetooth beacon is a potential location tracker and if your Wi-Fi is on then its potentially disclosing your actual geo-location without having your GPS turned on. Here's how it works: You may remember the first time you turned on location services on your phone it popped up a message asking if the service could use Wi-Fi to speed up determining your GPS location? This is because GPS needs to locate up to 5 GPS satellites to determine an absolute fix. This can take several minutes to complete. So what the mobile device does is look around at the Wi-Fi hotspots in the vicinity, each one has a unique identity which can be scanned without establishing a separate Internet connection.

Many ways to be location tracked

The service provider (e.g. Google) then looks up the Wi-Fi hotspot in a geo-location Wi-Fi database, for example something like Wigle.net. The mobile device can determine the signal strength to that Wi-Fi, which gives an approximate distance from an absolute hotspot geo-location. When you do this for 3 or more Wi-Fi hotspots, each of which the service provider knows the geo-location for, you can triangulate a very accurate location fix very quickly. The beauty(?) of this approach is that each time you use the service the provider can use your GPS location in combination with the Wi-Fi scanning, to update its database with new or more accurate Wi-Fi hotspot geo-location data! And so the virtuous(?) cycle continues with every Wi-Fi hotspot (public or your home private one) being geo-located by us consumers.

What this means is that every Wi-Fi hotspot is a location tracking device, and most of us walk around with our Wi-Fi turned on most of the time. Just as the unique identity of the hotspot is readily determined by scanning Wi-Fi, so is the unique identity of your phone as it scans for hotspots to connect to. The more technically astute may remember the new iOS feature that scrambles your device identity each time it is Wi-Fi scanned.

This is undoubtedly beneficial to location privacy. However it's not quite the perfect solution, because it only protects your device identity when a connection attempt is made from an unauthorized SSID (hotspot name). If you have authorized your device to connect to say, TheCloud, once, anywhere, then whenever your Apple (or Android) device passes by a hotspot (for example down the high street) with that SSID it makes an authorized connection, which means it provides your actual device identity and thus your actual geo-location and movement is readily determined, via Wi-Fi.

It is also worth noting some companies do work to ensure your privacy is protected, this includes BT, whose Wi-Fi policy[7] takes better actions than most to maintain user privacy by hashing the Wi-Fi device address. They also usually properly inform customers of the tracking being undertaken, although you still opt-in by default.

Very recently (Feb 2016) the ICO issued guidance to public Wi-Fi providers[8], which it is fair to say not a single Public Wi-Fi provider fully complies with; BT being the closet to full compliance.

Many ways to be location tracked

We could go into the surveillance society we live in and the myriad ways in which camera's are tracking us with facial recognition, with a disturbingly high percentage of UK retailers using facial recognition to track our movements around their stores. But these tend to be highly localized sources of location data, which thankfully are not generally aggregated (yet) with wider sources such as public Wi-Fi and mobile operator location tracking information. It is however worth noting that the UK Police Force has access to 22Bn records[9] of number plate recognition, each one tagged with date and time and location, many including pictures of the driver, worse, it seems they are rather too easily hacked[10].

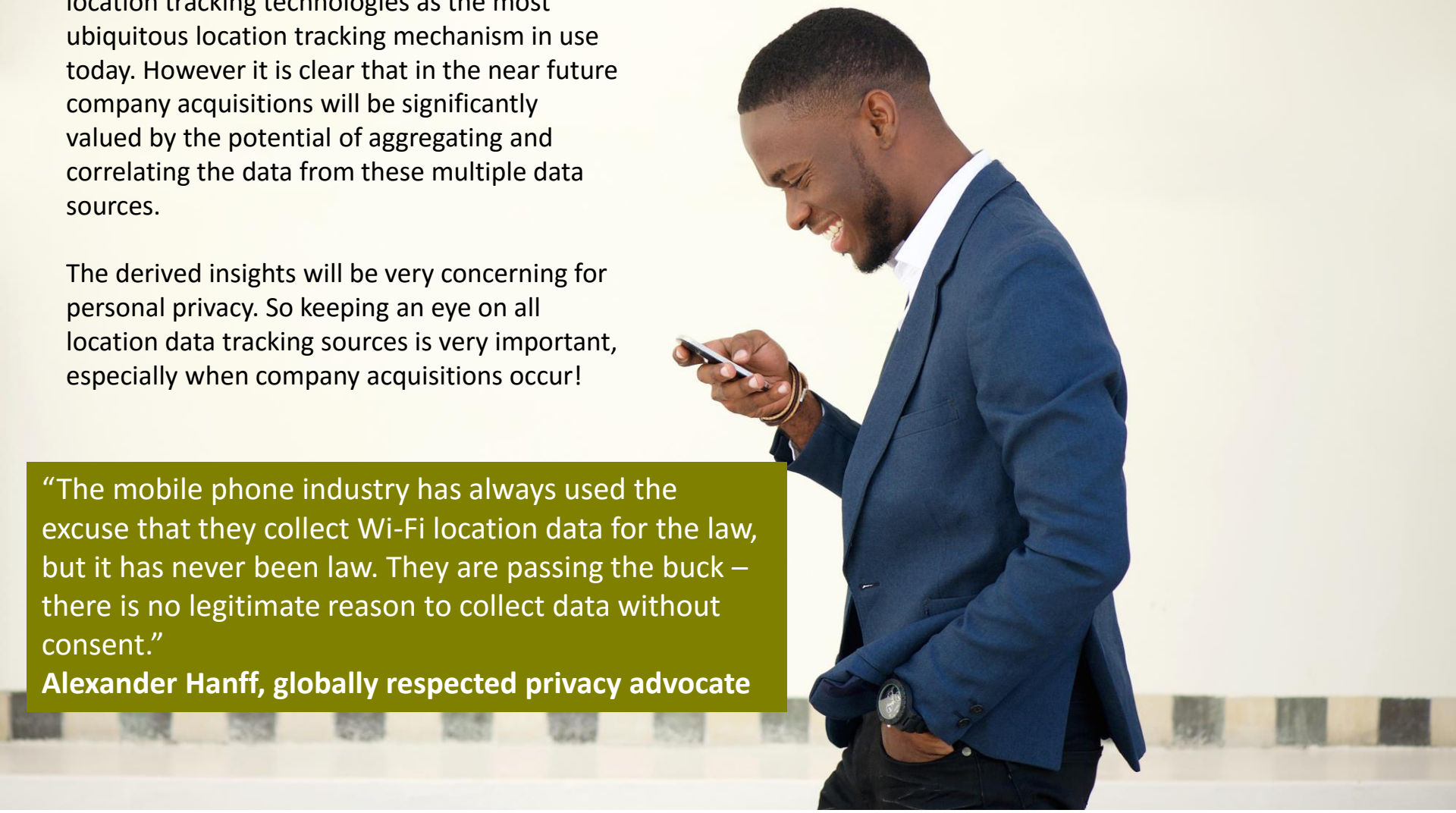
A recent study by researchers at Facebook analyzed the relationship between geographic location of individual users and that of their friends. From this analysis, they were able to create an algorithm to predict the location of an individual user based upon the locations of a small number of friends in their network, with higher accuracy than simply looking at the user's IP address[11]. A worrying issue for those who would prefer not to share location data or have it correlated with friends/follower who do share their location.

It is worth noting one other location tracking mechanism in the context of mobile: Photographs and videos. The digital images created are annotated with information called EXIF. If the location services on your phone are on when a picture is taken then EXIF will include your location with a date/time stamp. If you then post that picture online you have just denoted the absolute location and time of those photographed. A rather amusing, but deadly serious website that captures the essence of the issue is called www.Iknowwhereyourcatlives.com , which scraped many social websites for cat pictures then used the location information contained therein to post the pictures on a geomap. Imagine for a moment if this website was called www.Iknowhereyourchildrenlive.com! As Lt. Andy Norris of the Tuscaloosa County Sheriff's Office stated "This website demonstrates why you should never have your location based services enabled on social media sites. You're just inviting criminals to your home." Although we at Krowdthink would say otherwise – if the social platform was a privacy committed service then they'd strip out all EXIF data before posting the picture publically. If they don't, one has to ask oneself what they might be doing with all that highly sensitive data.

Many ways to be location tracked

This report focuses on wireless and mobile location tracking technologies as the most ubiquitous location tracking mechanism in use today. However it is clear that in the near future company acquisitions will be significantly valued by the potential of aggregating and correlating the data from these multiple data sources.

The derived insights will be very concerning for personal privacy. So keeping an eye on all location data tracking sources is very important, especially when company acquisitions occur!



"The mobile phone industry has always used the excuse that they collect Wi-Fi location data for the law, but it has never been law. They are passing the buck – there is no legitimate reason to collect data without consent."
Alexander Hanff, globally respected privacy advocate

We think we opt out but we opt in by default

It is educational to read the 2004 International Working Group on Data Protection in Telecommunications report on 'Common Position on Privacy and Location Information in mobile communications services'[12] in which location is described as driving "unprecedented threats to privacy', plus the initiatives it outlines for obtaining consent, then read on to make your own judgment as to whether these guidelines are followed. The same group met in Oct 2015 and revised their guidance and added several strengthened perspectives in "Working Paper on Location Tracking from Communications of Mobile Devices" [13]

Mobile Service Providers:

Given the deeply insightful nature of location data and the reticence we have for sharing our location, one might expect that any company or industry or brand that wants our trust would never, and I mean never, track our movements for commercial gain without an explicit, fully understood, opt in on our behalf. Unfortunately the value of location data to industry far outstrips their willingness to play fair with us citizens. Every mobile device owner is having his/her location tracked for commercial gain every day, and apparently we opted in!

How many of us, when buying our mobile phone or sim actually read the paper contract in full? Almost no-one. This is a shame because if you did you'd find that your location data is stored all the time, not just due to government security requirements (e.g. RIPA - Regulation Investigatory Powers Act), but also for marketing purposes! Because we almost all opt in by default to allowing our mobile service provider to use our location data for their commercial marketing purposes, and this includes the right to share that data with 3rd parties (the exception is Three)!

One area, which has not changed from the Data Protection Act (DPA) directive to the new General Data Protection Regulation (GDPR) which comes into force in spring 2016, is the definition of consent. Both state that consent shall be "freely given, specific and informed", although the GDPR adds "unambiguous" to tighten things up a little. So how is it that at multiple events to now over 400 people at live conferences, only two (0.5%) people knew this was happening when polled? As one student put it when I asked about how she felt about having her location being tracked this way, she said "It makes me feel physically sick".

We think we opt out but we opt in by default

In the USA, the President's Council of Advisor's on Science and Technology specifically call for the law to consider location privacy explicitly: "Tracking, stalking, and violations of locational privacy: Today's technologies easily determine an individual's current or prior location. ….. When big data allows such sightings, or other kinds of passive or active data collection, to be assembled into the continuous locational track of an individual's private life, however, many Americans perceive a potential affront to a widely accepted "reasonable expectation of privacy."

Supreme Court Justice Sotomayor[14], stated "I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on." It seems the UK government feel this is fine and our mobile service providers and public Wi-Fi providers are jumping on the opportunity to collate the data too for their commercial gain.

The mobile phone provider contracts used to be very complex and it was very hard indeed to find any reference to location tracking anywhere, but the advent of the GDPR, and its associated harsh fines for non-compliance has forced most of them to clean up their act and their websites (note not their paper contracts as yet) now provide more readable privacy contracts, but how many people visit this part of the phone providers website after starting to use their phone? None clearly state in an unmissable way at the time of contract signature that they track our location and use it for commercial marketing purposes; they tend to separate the clauses about what data is collated from the ones that discuss usage and rarely mention location in both, and they tend to qualify the fact they obtain location as something they need for routing phone calls or meeting the requirements of government security (RIPA). Anyone would think they don't want us to know! Oh…that's exactly what has happened! [15]

So if we are opted in by default can we opt out? The answer is of course yes (in Europe), it's a legal requirement under the DPA and the incoming GDPR. In fact under the GDPR we have the right to have our data deleted – which should be an interesting test case as the UK government requires cell tower location tracking to be stored for 12 months for "security purposes".

We think we opt out but we opt in by default

Any historic data (most mobile service providers 'only' keep up to 12 months, some Wi-Fi operators are far less careful) can be denied use for marketing purposes through the DPA if you opt out. So how do we opt out? Some like O2 and Vodaphone allow specific opt out of location tracking whilst sustaining your ability to remain opted in to marketing generally. So you may want to opt out of both with them.

Others like EE and Three make it a customer service enquiry in which you opt out of marketing services, although its unclear if that also opts you out from location tracking for any purpose other than government security RIPA mandate.

Conversations with Vodaphone and EE customer service indicates it does as both explicitly confirmed that opting out of marketing includes opting out of location tracking for marketing purposes. Three is more opaque in their privacy policy about their use of location data in marketing, but they do clearly state that they do not pass this data to any third parties (that does not mean they don't provide indirect third party access to you via location qualification); they also make it a requirement to correspond to their data protection officer via email to opt out; we have not verified if this works or if they commercialise this location data in any way.

Most other mobile service providers are MVNO's (Mobile Virtual Network Operators) running over the infrastructure of the prime service providers. We suspect they are not privy to the location tracking information, its too valuable to the prime service provider. Tesco as a MVNO over O2's network need to be careful they are not falling foul of the law as currently they don't provide any indication through their mobile privacy policy that users are location tracked through their mobile phone service.

Location information must still be collated by O2 to meet the UK government legal requirements (Tesco does not alert its users to this fact). Tesco user location information should not be collated for marketing purposes by O2 as no informed consent has occurred, not even a cross reference from the Tesco Privacy Policy to O2's. Similarly O2 needs to be aware that it should not be tracking its Tesco customer movements. The potential excuse of anonymization as a legal get out is questionable as we discuss later.

The whole issue of location tracking informed consent via MVNO service providers clearly needs to be looked into legally.

We think we opt out but we opt in by default

To opt out of location tracking and/or marketing services from your mobile service provider use these numbers:

O2 – 1300

This number does not work for Tesco (an O2 MVNO) phone users – another indicator that Tesco phone user location is not tracked for marketing purposes. It would require an opt out mechanism if it was being tracked

GiffGaff (an O2 MVNO) states it collects location data for use its' marketing and via opt-in to 3rd party marketing and you can opt out via email removeme@giffgaff.com. But it offers no method to opt out of location tracking in its privacy policy.

EE – 150 or 0845 412 5150

Make sure you expressly state you wished to halt location tracking as well as marketing

TPO (an EE MVNO) collates location data and offers no specific opt out- but you can express your desire to opt out for location and marketing data collection by calling 0845 225 2505; or by email at help@thepeoplesoperator.com

ASDA mobile (an EE MVNO) tracks location but provides no explicit opt out except to general marketing which you can access by calling 2732 from your Mobile or 0800 952 0393

Vodaphone –

191 or 03333 040 191 to opt out of marketing including location based marketing

Text OPT OUT to 68808 to be removed from their location analytics only

Talkmobile (Carphone Warehouse) is a Vodaphone MVNO. To opt out of marketing services use telephone, letter or email from this web address: http://talkmobile.co.uk/contact-us they do not offer an explicit location tracking opt-out

Three – email: dpa.officer@three.co.uk

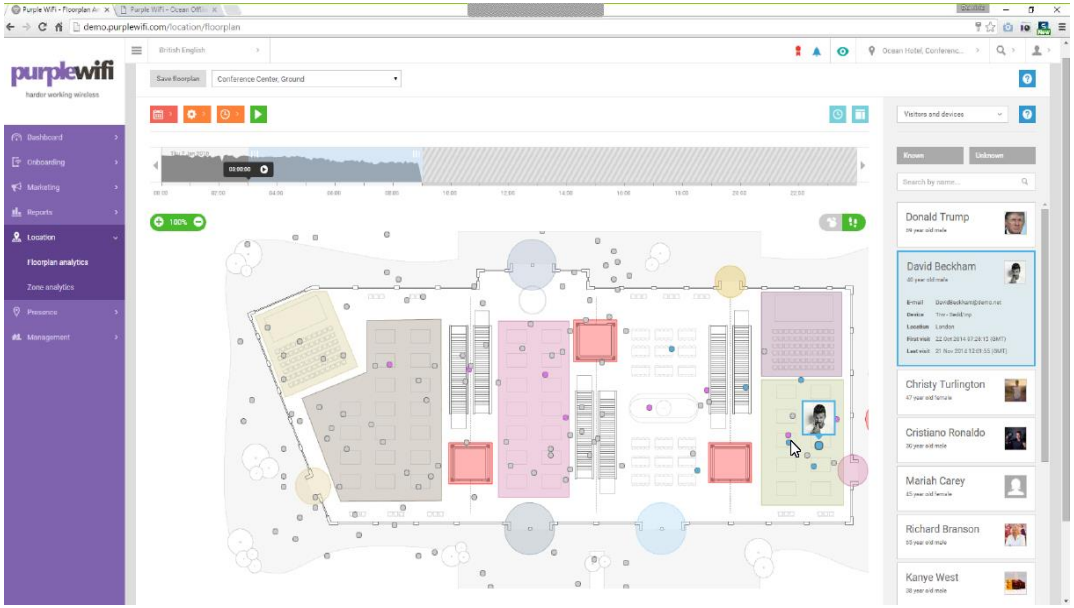
Make sure you expressly state you wished to halt location tracking based marketing as well as marketing generally

The DPA and GDPR requires certain principles for processing, labeled "lawfulness, fairness and transparency". It's well past time the mobile service providers were called out for their lack of transparency under the law regarding their tracking and use of our location information for commercial purposes.

We think we opt out but we opt in by default

Wi-Fi service providers

Many public Wi-Fi service providers specifically opt you into location tracking by default in their privacy policies. Some Wi-Fi service providers are also mobile phone service providers (O2, Vodaphone, Tesco (via BT)).
So they may aggregate the mobile phone location tracking with the Wi-Fi location tracking activities, O2 and Vodaphones privacy contracts certainly allow for that.
This would allow the fidelity of the location tracking to be significantly improved in country areas where cell tower coverage is quite wide as well as within buildings. Both O2 and Vodaphone use the same privacy policy for Wi-Fi as for your mobile phone and are thus contractually enabling themselves to track your location through Wi-Fi as well as cell towers and a Subject Access request with O2 confirmed this.



Individual Tracking within a location by Purple Wi-Fi

We think we opt out but we opt in by default

Growing UK provider Purple WiFi is interesting because they drive users to login via their social media accounts. They then explicitly opt-in[16] users by default to have their precise movement tracked and correlated back to their social media account, they even have real-time access tools as seen above.

So if you thought you had location tracking turned off in your social media account, think again, you may have just opted back in via a Wi-Fi connection. Of course PurpleWiFi masks your device unique ID when sharing your movement data with their retail and other customers whose locations use their service, but their tools graphically show your movement in real-time, along with your name, age, sex and a nice social media picture!

The site owner can record and store this data locally too for their own analytical purposes, in fact this is central to the PurpleWi-Fi business model. Purple Wi-Fi themselves maintains this data (and your device ID) forever! Conversations with PurpleWiFi informs us that they have all the user movement data since they started business 4 years ago. They also confirmed every Wi-Fi hotspot is geo-located to a building or facility and demonstrated historic movements of people within the facility with name-tags from your social media account.

PurpleWiFi is collating the integrated movement and social platform information set across all of their service locations. PurpleWiFi is expanding rapidly and just received a £3.3M investment from Sir Terry Leahy, former Tesco boss[17].

Another example is Aquiva Wi-Fi, they provide public Wi-Fi across Enterprise Inns pubs, Premier Inns, Travelodge and several airports. Their privacy policy, one of the longest I have ever read, also enables them to collect detailed location tracking information and combine it with web browsing habits (something many public Wi-Fi providers do, thus giving highly insightful additional data to correlate with your location).

Local government often engage with this location tracking activity when negotiating public Wi-Fi for their streets. Wi-Fi service providers need permission to locate and maintain their equipment on street lamps or bus stops etc. The service provider can provide detailed insight into peoples movements to the local government departments and this can be tremendously useful. Of course such data is normally provided anonymised. But we'll raise questions on that later.

We think we opt out but we opt in by default

So before you login to the next public Wi-Fi hotspot look into the privacy policy, do a quick search for the words "location" or "where" to find out if they track location, and especially if they give themselves the right to correlate the information with additional information and pass it to 3rd parties.

You can mitigate Wi-Fi location tracking by going to your W-Fi settings and clicking on the very long list of Wi-Fi hotspots that your smartphone maintains and click 'forget' for those larger service providers like TheCloud or O2 or Vodaphone, or just keep Wi-Fi turned off when not really needed to inhibit such tracking entirely.

It might be better if the phone makers turned off Wi-Fi and Bluetooth when the phone was not being used to avoid such inadvertent location sharing, but this would stop push notifications when outside of 3G/4G access. As an aside the Vodaphone Wi-Fi privacy policy for Transport for London (the Tube) makes no mention of location tracking. Maybe TfL protects its customers on their premises?

A few retail stores and public Wi-Fi providers are trying to be conscientious about location tracking of their visitors using their in store W-Fi services by adhering to some reasonably respectful policies managed by a US firm referred to as Smart Places. You can opt out of this sort of location tracking at https://smart-places.org , which you will often only discover if you read the privacy policy(18). The policy they follow is here(19).

It is a good policy if fully adhered to and requires clear notification of location tracking, but exactly what 'clear' means seems a little indeterminate sometimes, how this is policed is not so clear. It is also not clear how rapidly this information is disseminated back to the Wi-Fi service provider to inhibit the kind of real-time tracking PurpleWiFi's tools enable (see below).

But as a minimum it should eventually require the service provider to delete all such data from its historic records and eventually inhibit future real-time tracking. The extent to which this is occurring and how this is policed has not been investigated yet. If more users start to use this service then it will require closer inspection as a privacy service provision.

We think we opt out but we opt in by default

RIPA and Wi-Fi

There seems to be some confusion in some public Wi-Fi operators about their duties under RIPA. In discussions with two separate public Wi-Fi providers they have asserted they need to collate Wi-Fi information as a duty under RIPA for government security purposes.

One sits on a home office committee for RIPA conformance alongside the likes of MI5. However investigations indicate this is not correct at all. RIPA has never explicitly required public Wi-Fi vendors to maintain location tracking information. RIPA has only ever related to Telecommunications providers as per the EU Directive - a Wi-Fi provider is not a telecommunications provider they are a gateway to a telecommunications provider.

RIPA is wholly focused on cell site triangulation data and call metadata. There was an attempt in 2014/15 under DRIP to bring Wi-Fi tracking in, but it was explicitly struck out in 2015 as DRIP was struck down. One obvious reason is this – if anyone with a hotspot opened it up for public access they'd suddenly become subject to RIPA and be required to maintain this data and deliver it to the security authorities. As every mobile phone can be used in this way it would make every citizen potentially liable.

This raises the intriguing question as to whether public Wi-Fi operators are being 'guided' to execute a policy that has not been endorsed in statute, in fact has been explicitly struck down. Certainly the COO of one public Wi-Fi provider was adamant it was a legal requirement. Yet he also never provided reference to the relevant statute to justify his claim. To a public Wi-Fi provider, a RIPA requirement may help them feel justified in also collecting revenue from the collated data as they have to take the cost burden of collection. A case of self-serving justification perhaps?

Those pesky ads

If we did not already need enough reasons to be upset by ads, it is worth noting that a very large number of mobile apps redirect your location information to ad targeting companies like www.placeiq.com or www.xad.com . A quick read of their privacy policies and technology sales pages will highlight the way in which they leverage the location information pathways we highlighted previously to create highly detailed profiles of you based almost solely on location, sometimes in real-time, knowing where you are right now. We have yet to see EU regulators take these US companies practices to task – existing law should be sufficient to inhibit it.

We think we opt out but we opt in by default

Neither company states that they only store this data for limited periods, why would they? It's their business lifeblood. Neither company claims to even attempt to anonymize your data except through the simplest of pseudonymous methods, while retaining your device identifier.

Just to put this into context, at the recent Growth Through Trust event in London Dan Bates, Data Innovation and Privacy Officer, O2, claimed that 47% (~750,000) of iOS apps share location data! (Don't look over here look over there!) Many app developers probably don't even know that happens. App developers are given library code to install in their app if their monetization is advertising, many are too small or legally unaware to review the collection and privacy policies of the 3rd party ad software suppliers.

This does not absolve them, it's just the reality of the app economy. They may also be unaware that location can be tracked by Wi-Fi service providers as previously highlighted. So next time you accept a free app, just make sure you look more closely at the privacy policy and the app permissions. You are handing over far more value than you may comprehend.

It is also worth noting that those mobile operators that sell location as part of their ad services are in effect indirectly allowing the ad vendor to track you. If you click on such an ad that was only sent to you because of where you are, you have just confirmed to the ad company your location, especially if Wi-Fi hotspot data was accessible.

Information they can now store in association with your device identity, building a slower yet just as accurate profile as to your location and movements over time. EE does warn in the depths of their privacy policy of this intrusion potential, but not specifically in the context of location.

"We are doing a lot of work with the next generation of entrepreneurs who are developing social media platforms in terms of them being clear and concise as to what they do with users' data.

"Mobile and Wi-Fi service providers cannot hide behind legalise anymore. If such data gets into the wrong hands, it has huge potential in driving up identity theft and extortion.

Dr Steven McDermott, a Lecturer in media and communications at London College of Communication

The double speak of anonymisation

The big defence thrown up by most location tracking entities is that you have nothing to fear because location is anonymised. It's communicated to the consumer as if this was some form of guarantee. It is not. It is just another layer of security used when sharing with 3rd parties. They still hold the full location data set unanonymized.

We have seen how robust security is on the Internet with 2015 being the year privacy breach records were broken yet again. What is intriguing about 2015 is that it's the first year when significant breaches of data other than financial records were deliberately sought and hacked. 2015 is the year data breaches became intimate[20]. A trend we should be wary of because correlated breaches have the potential to rapidly unravel anonymisation techniques unless extremely well implemented.

For most types of low dimensional data, anonymisation is in fact quite a good security tool. Reasonably low dimension data can be anonymised in a manner that enables a mathematically provable statistical potential that it could be de-anonimised[21].

An explicit percentage chance that data can be de-anonymised can be calculated and in fact US HIPAA Safe Harbor publication/processing of health data usually requires a 0.04% (4 in 10,000) risk of de-anonymization, sometimes they seek even better.

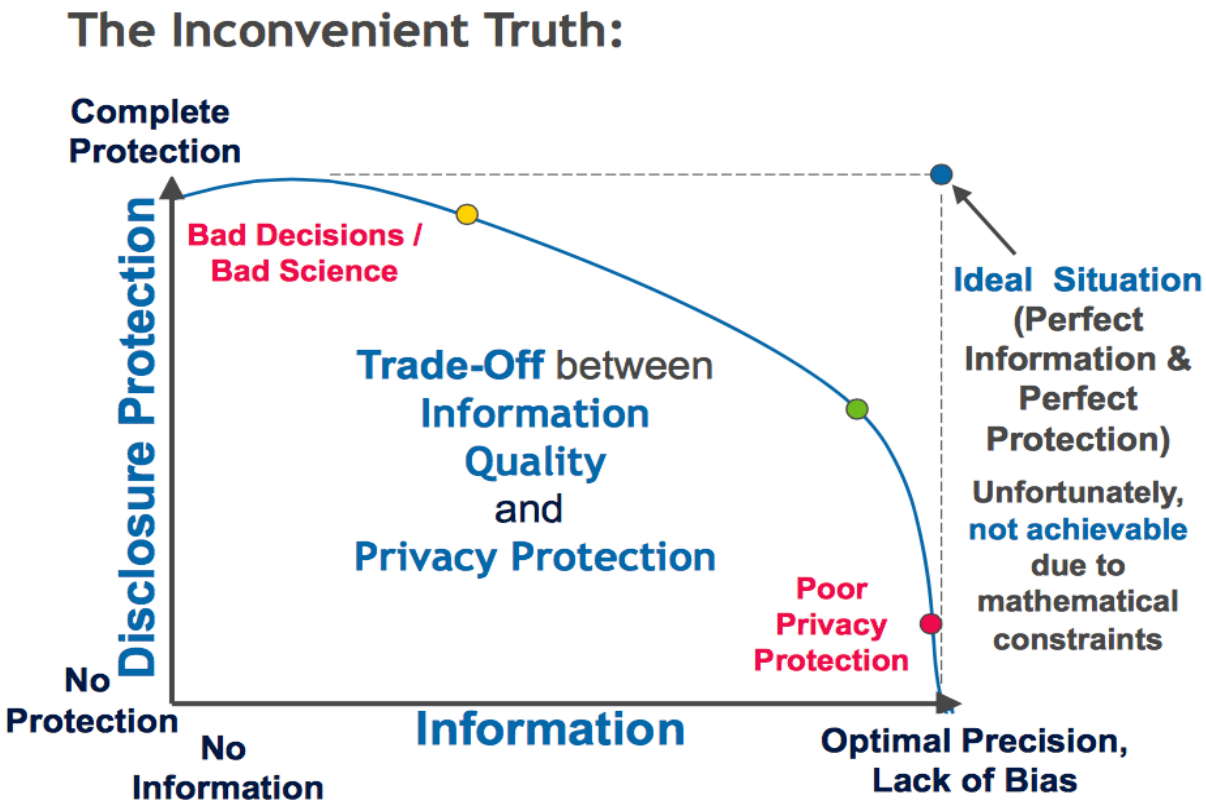
I have yet to find an equivalent level of anonymization in UK NHS guidelines. The point is that the personal privacy risk can be quantified in anonymisation. So why is that not happening with our location data? Why do we not see a quantified privacy risk associated with every claim that data has been anonymised?

The answer is twofold: First, location data is high dimension data and is thus much harder to anonymize, it requires the process to remove a lot of the fidelity of the location in order to safeguard citizen privacy.

The double speak of anonymisation

Secondly, the problem with anonymisation is that the better the anonymisation, the better our privacy protection, but the worse the data set becomes as an informational source. So there is a direct conflict in terms of value to the collector by anonymising the data as shown in D.C. Bart-Jones's diagram. Commercial value is directly degraded as personal privacy is enhanced.

The trade off between privacy and anonymization copyright Daniel C. Barth-Jones



The double speak of anonymisation

The DPA and GDPR understand this trade off and thus require that those using anonymization to protect personal data should be seeking to make the risk of de-anonymization a "negligible" privacy risk to the individual. Exactly what this means has yet to be tested in UK law, but the UK ICO recently published its guidelines[22]. The ICO says "Anonymisation is the process of turning data into a form which does not identify individuals and where identification is not likely to take place." Why 'negligible' became 'likely', and exactly what 'likely' means has yet to be properly tested in UK law – but you can bet the lawyers are lining up to debate the issue in favour of their commercial sponsors, thus sustaining the location data value as high as possible, to our personal privacy detriment[23][24].

Its clear anonymisation can be quantified as a risk to the individual, so why is this risk not being published for location data given its incredible sensitivity?

Worse still, is that our government agencies seem insufficiently aware of the importance of protecting peoples movement data. Transport for London had to backpedal fast in 2014 when they openly published enough of Boris Bikes location data to allow a blogger to de-anonymise 'with ease' who the movement data correlated to[25].

In the US a body called PCAST, President's Council of Advisors on Science and Technology, reported in May 2014[26] that "Anonymization is increasingly easily defeated by the very techniques that are being developed for many legitimate applications of big data. In general, as the size and diversity of available data grows, the likelihood of being able to re-identify individuals (that is, re-associate their records with their names) grows substantially.

While anonymization may remain somewhat useful as an added safeguard in some situations, approaches that deem it, by itself, a sufficient safeguard need updating." Consumers need to be made aware of this unequivocal view of the weakness of anonymization alone to secure our personal information in the long or even medium term. There should be a known de-anonymization risk publication, based on access to the anonymized data source used responsibly and the source data for the anonymization should be deleted as soon as practical in order to protect citizens from the exposure of a hack. Due to advances in technology this risk should be updated annually, taking into context advances in analytics and potential access to new derived data sources. Then a second risk publication based on the data being hacked and aggregated and correlated with other datasets.

Taking Consent for Granted

In both cases the period over which the data is collated should be published with clear reasons why any historic location data at all is needed and to what explicit purpose it is used. It is often not needed to be stored except for personal profiling for marketing purposes – is that really a justifiable reason given its sensitivity and the personal risk it puts upon the person being tracked?

Why should the citizen suffer the privacy loss on behalf of a company making a marketing profit on our data? For them it might mean a short term financial penalty or loss of brand image, but for the millions of individuals whose detailed lives have been laid bare by a location data hack, what is the real cost?

Suicides have already been attributed to the Ashley Madison hack – such consequences are likely from the detailed insights a location data hack could cause. As a minimum we should have the choice to explicitly put ourselves at such risk. Arguably the Data Protection Act as it stands requires this for any data. However it's the The Privacy and Electronic Communications (EC Directive) Regulations 2003[27] that directly addresses location privacy, section 14:

"Prior to obtaining the consent of the user or subscriber under paragraph (2)(b), the public communications provider in question must provide the following information to the user or subscriber to whom the data relate:
(a) the types of location data that will be processed;
(b) the purposes and duration of the processing of those data; and
(c) whether the data will be transmitted to a third party for the purpose of providing the value added service."

As we will discover later, while most telco's are fairly compliant with this directive with respect to (a) and (c), most are not explicit about the purpose. They may provide some examples but they do not limit their purpose by defining it explicitly. This is certainly open to challenge in the courts.

Taking Consent for Granted

However, what was discovered in a subject access request (to be detailed in a separate report) is that W-Fi based location tracking is also collated by O2. Nowhere do they comply with either (a), (b) or (c) with respect to that data in their privacy notice.

So why are the mobile phone providers not leading the charge and informing users that they are being opted in by default to commercial use of their location data? Why is explicit opt in not a specific requirement? This issue will become a lot clearer under the GDPR and the latitude to prevaricate will diminish markedly. So there is hope for us citizens.

"Mobile phone companies should improve the transparency of their operations by making their privacy polices clearer, giving customers' information about what exact data they are collecting, how long they will keep it for, how each particular type of data will be used, who it will be shared with and the risks associated with this.
Javier Ruiz Diaz, Policy Director at Open Rights Group

Location Value without Tracking Location

At Krowdthink we cogitated hard about how to deliver location-based services without putting users at the significant privacy risk. The first step is to understand and accept that it's almost impossible to permanently protect online data forever, whether using security techniques and/or anonymization.

Both should be applied as a matter of principle of course. But it's much more privacy respectful to seek to deliver a location service without storing historic data or even isolating geo-location. In seeking to build a new form of Trust model[28] for digital engagement in a social context we realized a key principle of "how" we develop our application should be to minimize any data, or as Mozilla puts it, follow a 'lean data' development strategy[29].

This means never store anything permanently that is not needed to be stored, never obtain any personal data not really needed to deliver the service and when personal data has to be obtained, minimize the period for which it is held. The right of remedy we have architected in also means that the provenance of stored personal data (this includes any meta-data we create related to the individual) should always be maintained so the individual concerned can readily delete personal stored data at any time (as part of the app not some complex offline legalized process).

When applying this principle to location data it was obvious, given its sensitivity, that we should not store any such data correlated permanently to an individual, however anonymized, ever. This is a simple enough step for GPS based location-based services; use it while the user needs it and don't store it. The problem is that GPS needs to be regularly updated, so the active stream of location data could be hacked in transit too, in real-time. A risk best avoided if possible. Also both iOS and Android maintains historic records of GPS data on your phone, useful to the Police if they catch you and get access to your phone, just as useful to hackers.

Location Value without Tracking Location

We also identified that new users would have no reason to trust we don't store location data, and any social app obtaining location-based service permissions may be naturally suspected by the privacy sensitive. So we decided we needed to build a location service that did not need location! Some lateral thinking led us to the simple insight that digital social interaction in a crowd only needs technical facilitation by knowing people are in the same place at the same time - there was really no need to know where that place was. What we needed was a means to identify that a group of people were co-located in real-time.

We looked at the way wireless communication infrastructure was being deployed – we identified the huge growth of Wi-Fi (within the next 2 years there will be a hotspot for every 18 people in the world), especially in public locations and places where crowds naturally formed - it's needed to enhance the wireless capacity when a high number of people in a dense area need digital communication services.

Wi-Fi was originally a LAN technology, built to connect people in a locality. All we needed to do was re-create that capability in our cloud services when the Wi-Fi was being used as an Internet Access Point

Identifying that people were on the same virtual LAN would be all the information we'd need. In fact we can even reduce the risk of a real-time hacker monitoring our Krowds (a list of Krowd users on the same virtual LAN at the same time) by hashing the LAN (hotspot) identity, because we only need a Wi-Fi/LAN ID that is unique and comparable to deliver our Krowd service to connect people in places. This is important because as previously highlighted it's a simple task to determine geo-location from a Wi-Fi ID. Finally, the list of participants in a Krowd should persist only as long as 2 or more people are connecting in a location. No cloud-based permanent/historic store of who has been co-located with whom is sustained.

We believe this is the most privacy respectful location service we could possibly build that is cloud connected. But it does rely on some of the commercial providers of infrastructure services to be as respectful of peoples location oriented privacy rights. This sort of service does not need the Smart Places opt out tools for location tracking, because no location tracking is occurring. However we cannot control the service provider infrastructure, so we are exposing their current practices in order that consumers can take back a level of control over their location tracked lives.

Next Steps

"There is this very simple equation that we've learnt. People will use a technology if the perceived benefit is larger than the perceived risk."
Elgar Fleisch, deputy dean, ETH Züric[30]

This is what is often referred to as a form of cognitive dissonance. It is explicitly used by many of the world's largest Internet service providers as a critical part of their business model. After all, if you were told up front exactly what data was being collected every time you clicked on an advert or web link, how often would you click?

If you were also told how this contributed to a detailed profile of who you are and shown the profile, and if you were also told that the company is currently passing this information on to 3rd parties, like insurance companies, would you actually click at all? As a minimum it would force those entities to treat your privacy a lot more respectfully.

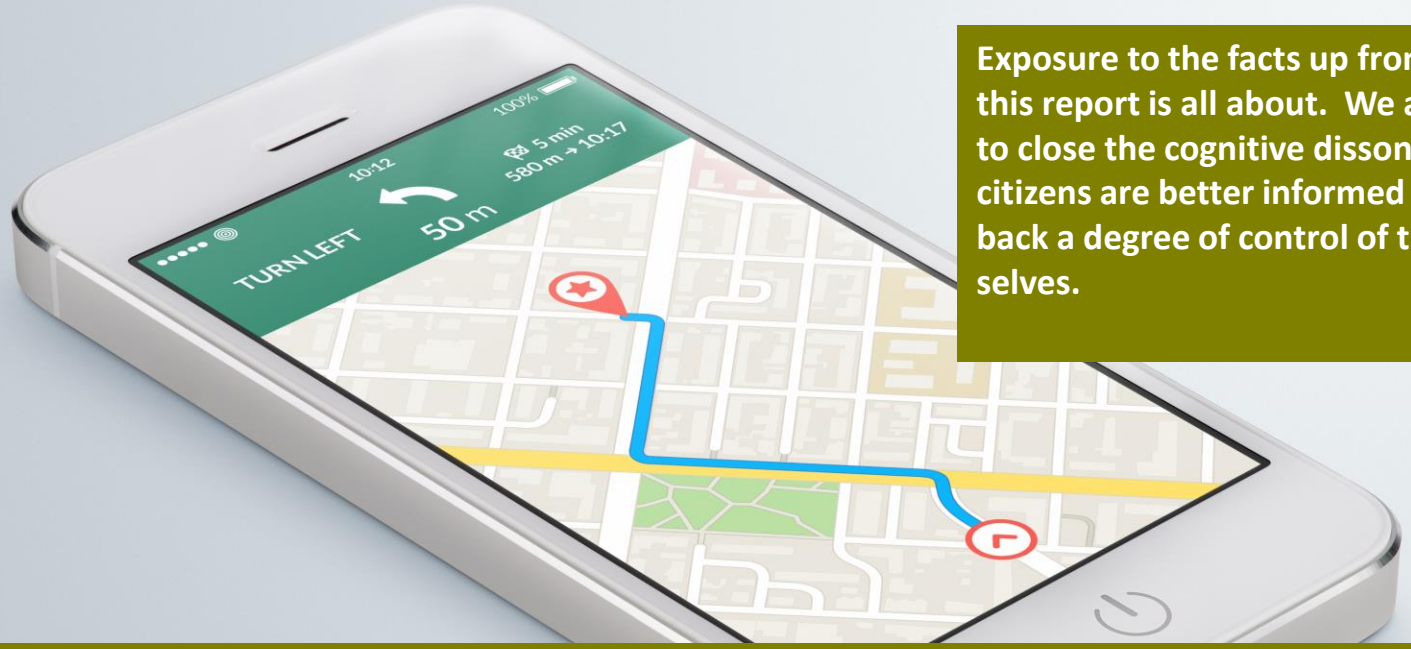
The key word is perception. Over the last 10 years or so we have come to learn what sort of data collection practices many companies are practicing, things we certainly did not understand at the outset.

We reluctantly accept them because we have not suffered a personal consequence and so our lack of early investigation, and thus our implicit trust, was somewhat justified.

However the big race now is to inhibit the data hack which will undermine this implicit trust, hence the UK governments recent £1.9Bn investment in cyber security – because there is so much data about us we are seeing more and more consequences occurring and we are just starting to realize – the corporate suffers only a temporary set back or loss of revenue and almost never with an associated level of personal accountability within the company, whereas the impact on an individual is personal and can be permanent.

2015 became the year of the intimate data hack; nations, individuals and cyber-mafia working to obtain the information they now realize these commercial entities have amassed. It's the citizen that is suffering. So only time and the related consequences for the current status quo of the digital engagement business model will force the fundamental issue to be addressed.

Call to action



Exposure to the facts up front is what this report is all about. We are seeking to close the cognitive dissonance gap so citizens are better informed and can take back a degree of control of their digital selves.

Health data is seen as highly private and in general organisations take great pains to sustain it privately, not just securely. We believe location data is the next largest and most important dataset that needs to protected privately, not just securely. Unlike health data it is not generally needed except as a commercial asset, so it should be a matter of explicit choice as to whether it is collated and stored and its benefits returned to the individual.

We dread to consider the consequences in another 2 to 5 years of large-scale data hacks of the UK's entire population movements.

Call to action

1. Make all mobile phone location tracking entities adhere to best practice in existing law and seek an active, explicit and highly informed opt-in to location tracking for commercial purposes
2. Require location tracking entities to be explicit as to precisely what purposes they put location data to as part of our opt-in
3. Drive government to initiate a program of consumer risk education relating to location information
4. Drive government to create a de-anonymization risk publication for all anonymized location data in a manner that informs the consumer

Research References

1. Unique in the Crowd - http://www.nature.com/articles/srep01376
2. Uber Gods View location Privacy Breach http://www.forbes.com/sites/kashmirhill/2014/10/03/god-view-uber-allegedly-stalked-users-for-party-goers-viewing-pleasure/
3. US 2013 consumer data privacy study, Mobile Edition - http://www.edee.gr/files/WhiteTheClpapers_cases_articles/082613_US_MobileReport.pdf
4. MEF Global Consumer Trust report 2015 – exec summary can be downloaded free http://www.mobileecosystemforum.com/solutions/consumer-trust/global-consumer-trust-report-2016/
5. http://www.mobilemastinfo.com/faqs/
6. https://www.navizon.com/product-navizon-indoors-tracking https://support.purplewifi.net/support/home
7. BT Insights – Wi-Fi policy http://www.btwifi.co.uk/help/common-questions/bt-wifi-insights.jsp
8. ICO Wi-Fi Advice https://ico.org.uk/media/for-organisations/documents/1560691/wi-fi-location-analytics-guidance.pdf
9. Police Force access to 22Bn number plates location tagged http://www.theregister.co.uk/2015/12/30/cops_anpr_database_hold_22bn_records/
10. IT Pro report on hack-ability of speed cameras http://www.itpro.co.uk/security/25510/number-plate-recognition-cameras-can-be-hacked-by-anyone
11. http://cameronmarlow.com/media/backstrom-geographical-prediction_0.pdf Backstrom, Lars et al, "Find me if you can: improving geographical prediction with social and spatial proximity," Proceedings of the 19th international conference on World Wide Web, 2010.
12. International working party in telecoms, common position on location privacy in mobile http://www.datenschutz-berlin.de/attachments/193/local_neu_en.pdf
13. Oct 2015 – revised position by International working party in telecoms on mobile location tracking https://files.acrobat.com/a/preview/8c0c0c03-6d8f-4833-bb5d-76ec654c5eea
14. US Supreme Court ruling on location privacy http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf
15. Mobile service provider privacy contractshttp://ee.co.uk/privacy-policy http://www.o2.co.uk/termsandconditions/privacy-policy http://www.three.co.uk/Privacy_Cookies/Code_of_practice https://www.vodafone.co.uk/about-this-site/our-privacy-policy/
16. PurpleWiFi privacy policy http://purpleportal.net/access/agreement/privacy
17. Sir Terry Leahy invests in Purple Wi-Fi http://www.manchestereveningnews.co.uk/business/sir-terry-leahy-leads-33m-8445716
18. Retail store Wi-Fi tracking opt out http://smart-places.org
19. retail store mobile location tracking code of practice https://fpf.org/wp-content/uploads/10.22.13-FINAL-MLA-Code.pdf

Research References

20. 2015 – The year data breaches became Intimate http://www.govtech.com/blogs/lohrmann-on-cybersecurity/2015-the-year-data-breaches-became-intimate.html
21. Good anonymisation techniques http://www.med.miami.edu/hipaa/public/documents/De-Identification_of_Confidential_Health_Data.pdf
22. UK ICO guidelines on anonymisation https://ico.org.uk/for-organisations/guide-to-data-protection/anonymisation/
23. Lawyers on Anonymsation http://ejlt.org/article/view/378/569
24. Location de-anonymisation debate https://fpf.org/2014/07/24/de-identification-a-critical-debate/
25. Transport for London snafu on Boris Bikes movement data http://www.theinquirer.net/inquirer/news/2339511/boris-bikes-location-data-could-be-used-to-track-you
26. Presidents Council of Advisors on Science and Technology May 2014 report https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf
27. The Privacy and Electronic Communications (EC Directive) Regulations 2003 http://www.legislation.gov.uk/uksi/2003/2426/contents/made
28. Krowdthink Trust Model for 'how' to build a trustworthy digital engagement platform – http://www.krowdthink.com/privacy.php
29. Mozilla lean data priactises guide https://www.mozilla.org/en-US/about/policy/lean-data/
30. The economist – The Internet of Things Business Index http://www.arm.com/files/pdf/EIU_Internet_Business_Index_WEB.PDF