Cashing in on your mobile?

How phone companies are exploiting their customers' data

Open Rights Group (ORG) is the UK's only grassroots campaigning organisation that works to protect your digital rights.

We believe people have the right to control their technology, and oppose the use of technology to control people.

We raise awareness of threats to privacy and free speech and challenge them through public campaigns, legal actions, policy interventions and tech projects.

Research and lead writer: **Javier Ruiz**

Editors: **Pam Cowburn, Jim Killock**

Additional research: **Alexandra Stefano, Ed Johnson-Williams, Ruth Coustick-Deal**

Design: **Avances Comunicación Visual** - www.avances.es

Open Rights Group

www.openrightsgroup.org

+44 20 7096 1079

Open Rights is a non-profit Company Limited by Guarantee,
registered in England and Wales no. 05581537

TABLE OF CONTENTS

CHAPTER 1. INTRODUCTION

The mobile phone market industry in the UK is worth £14 billion[1], with 93% of adults owning a mobile phone, and 61% owning a smartphone[2]. Within this multi-billion pound industry, there is a fast-growing market in services and products created from the data that customers generate when we use our phones.

After we buy a phone, we hand over personal information to our mobile phone providers on a daily basis. From our customer profiles, companies already know our name, address, age, gender and employment status. But from our phone use, they can get a real insight into our behaviour — such as, who we call and text, when we contact them and how frequently. Importantly, they can tell your location throughout the day from the phone masts connected to your handset.

If you have a smartphone, your mobile provider will also have information about your Internet use.

By analysing this data, mobile phone companies can find patterns and insights into customers' behaviour. There is now a rapidly-growing industry in 'secondary products' based on mobile data analytics. These include services such as real-time traffic reports or marketing products, for example tools that could tell website owners how many people are looking at their websites in a particular geographic location.

It is estimated that by 2016 UK mobile operators could be making over half a billion pounds a year just from monetising the location of their customers[3].

Companies need to collect and keep data so that they can bill us for our services. But just because they collect this data, does not mean that they have an automatic right to process that data for other purposes without our consent.

ORG believes that people have the right to control how their data is used. If a company wants to collect and use our data, they should tell us why and ask for our explicit permission. If they don't, they are removing our right to control this data and the risks associated with their use of it. They must also treat this data with care and make sure that it cannot be used to identify us or reveal our personal information to anyone else. Both of these are vital for maintaining trust between customers and companies. In addition, the law must be adequate to allow individuals to fully understand and control what happens to their personal information in the new Big Data world.

About this report

In this report, we examine whether mobile phone users are being given enough information to make informed choices about how their data is used.

We have looked at the policies and contracts of the UK's four main mobile providers: EE, O2, Vodafone and Three UK, and analysed what information they gather, store, analyse and share. We also had several meetings and direct conversations with representatives from these companies as well as officials from the ICO.

ORG's supporters contacted their providers about these practices and requested a copy of the data held about them, which we checked against each company's privacy policy. Finally,

[1] Information Communications Technology (ICT) in the UK: investment opportunities (Feb 2014) https://www.gov.uk/government/publications/information-communications-technology-ict-in-the-uk-investment-opportunities/information-communications-technology-ict-in-the-uk-investment-opportunities

[2] Ofcom Communications Market Report 2014 http://media.ofcom.org.uk/facts/ — 2014, Q1)

[3] http://www.telco2research.com/articles/WP_telco2-making-money-from-location-insights

we carried out mystery shopper visits to the companies' front end shops in the high street to ask about personal data handling.

According to research by the mobile industry association GSMA, 79% of UK mobile Internet users have concerns about sharing their personal information when accessing the Internet or apps from a mobile; and around 90% want to be asked for their permission before 3rd parties use their personal information[4]

We have examined whether these practices, policies and contracts comply with the two main laws that regulate the use of this information: the Data Protection Act 1998 (DPA) and the Privacy and Electronic Communications Regulations (PECR). We also explain where we understand that the letter of the law fails to properly regulate current Big Data practices due to outdated understandings of privacy protection.

Given the sensitive nature of the data we generate when we use our phones, we would like to see mobile companies do more than meet the minimum requirements of the law. Our recommendations reflect what we believe would be best practice when it comes to analysing and using our data.

While this report focuses on mobile companies, they are not the only companies that are collecting and using data. Others, such as app developers can collect vast amounts of data about their customers and are currently under regulated.

Some mobile companies are also involved in providing wireless Internet services at retail locations and use this data in their analytics.

Such convergence of data sources and the tracking of consumers across multiple devices is a growing concern.

The information in this report is based on the information available to us. We welcome feedback and are happy to update this briefing if any of the companies mentioned believe that we have omitted anything. One of our objectives is to stimulate discussions with industry towards the development of best practices that incorporate the concerns of consumers.

Summary of our findings

All four mobile companies say that they are operating within the relevant legislation — Data Protection Act and Privacy of Electronic Communications Regulations — and follow guidance from the Information Commissioner, but we think that there are areas where this is arguable.

Our findings suggest that at best, companies are fulfilling the minimal legal requirements, and at worst could be breaking the law and breaching our right to privacy.

Our key findings are that in most cases:

1. Customers are not being given enough clear information about how their data is being used by their mobile providers.

2. Customers are not being given clear and easy ways to opt-out if they don't want companies to use their data.

3. Companies could be breaking e-privacy law if they process traffic and location data without consent. The mobile phone companies that we spoke to say that they anonymise data, which means that they are not legally obliged to ask for consent to use it. But it appears that in some cases the data is not fully anonymised and should remain classed as personal information requiring consent for reuse.

4. Customers need to understand the risks if they are to give companies permission to use and share their data. But it is currently

[4] http://www.gsma.com/publicpolicy/wp-content/uploads/2014/10/GSMA-Mobile-Privacy-Booklet_WEBv2.pdf

impossible for individuals to work out how effective anonymisation and pseudonymisation techniques are.

5. The law may not be fit for purpose in giving customers control over the risks associated with Big Data.

6. Companies and their clients are potentially getting value from data but it is not clear whether these benefits are being shared with mobile phone customers.

7. The Information Commissioner's Office is doing very little to guide the market or enforce privacy standards and the UK has lower, less protective standards than other parts of the EU despite having the same underlying legal regime.

We have based our analysis on current legislation, but the new EU General Data Protection Regulation (GDPR) that will replace the Data Protection Act later this year places even more stringent demands on consent and transparency on how data is collected and used. Mobile providers need to take urgent action to ensure full compliance with the new laws or risk heavy fines under the beefed up enforcement regime.

Our recommendations

These are our main recommendations, but additional proposals can be found in each chapter.

Consent

- Companies should ask for our permission before they retain and use our traffic and location data for analytics. This should operate on an opt-in basis and start at the point of sale.
- This process should include 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.
- There should be clear and simple ways that customers can opt in and out of different kinds of data sharing from the point of sale onwards.

Anonymisation

- Mobile phone companies should be required to allow independent technical audits by data protection authorities of how they are processing traffic and location data before they share and sell the anonymised outputs. This would reassure customers that their data couldn't be re-identified, and
ensure that companies are not breaching data protection law.
- The ICO should investigate in detail the anonymisation processes of mobile companies and provide clear guidance on compliance with the E-Privacy Regulations. This should cover the creation of pseudonymous profiles combining subscriber information with traffic and location.

Transparency

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.
- Making contracts available before the point of sale, even if they are not legally obliged under commerce legislation;
- Making marketing opt-outs simpler and allowing customers to opt out at the point of sale; and
- Making subject access requests easier to make so that customers can better access, and therefore control, their personal data.
- Clearly explaining how their analytics systems benefit their customers.

Improved transparency requirements will soon be a legal obligation under the new GDPR, and the ICO should ensure mobile companies fully comply.

Regulation

- The Information Commissioner's Office (ICO) should work with industry and civil liberties organisations to develop a Code of Practice for the re-use of mobile data including location. The ICO sets the tone for compliance with e-privacy and general data protection and needs to be proactive in enforcing current and updated standards.
- The Article 29 Working Party should look into the issues raised here and provide guidance to data protection authorities across the EU on how they can understand the law and its current limitations, improve practices and help maintain trust between customers and mobile phone companies.
- Article 29 should consider the development of Big Data analytics based on mobile data in their input towards the next review of the EU E-Privacy Directive, which will take place in 2016.

Legal reforms: review of the EU E-privacy Directive

Although the EU E-Privacy Directive seems clear and designed to give customers control over their data, it has not lived up to expectation. Companies have found ways to push at its limits. The Directive is about to be opened for review in the context of the new General Data Protection Regulation (GDPR), which brings more stringent requirements, including on
consent and transparency.

Data minimisation and purpose limitation

While these principles are already provided for under the GDPR, it is important to spell this out in the revised instrument for sake of clarity, given the increasing use of geographical location data in many different contexts, and the serious intrusions of privacy that can result from the processing of location data.

Geographical information, traffic data, and location data, and any other personal data processed should be reduced to the least-precise (least-granular, least-invasive) type needed for the relevant purpose for which they are used, and deleted as soon as they are no longer needed for the initial or subsequent purpose.

Clarity on traffic and location data

Some data can be both location and traffic, depending on the context. There is a need for more clarity on the particular regime that applies, ensuring maximum protection at any stage.

Derived data

Data derived from traffic, location or subscriber information should also be covered by the confidentiality of communications, in addition to any requirements under the GDPR.

Clarity on anonymisation process

There is need to clarify how and when anonymisation should take place. Particularly concerning is the bundling of subscriber demographics, traffic, and location data into pseudonymous profiles, used for Big Data analytics without consent. Anonymisation of traffic data should take place before any further processing or matching.

Limitations of anonymisation

There are special difficulties in the de-identification of rich data, particularly location data, that were not apparent when the current directive was written. The new instrument must accept these limitations and create a framework for situations where at best location data will likely be pseudonymous.

Billing data

What data is retained for billing and for how long needs tightening. This is currently open to abuse, for example some operators keep detailed web history logs with the argument that they may be challenged on data charges.

There is a need for more consistency and transparency over retention periods.

Value added services

References to "value added services" and "publicly available communication services" need to be reviewed in the light of recent technological developments. There is a need to clarify the difference between value added services and data reuse for the benefit of third parties.

Consent

The e-Privacy Directive allows the processing of traffic and location data for value-added services with consent. However, rules on how this consent needs to be provided (and revoked) should be made more clear. Third parties should be responsible for demonstrating how they have obtained the data.

Bundling of consent and opt outs

Consent and opt outs must not be bundled to cover both marketing communications and value added services in one tick box, as it happens now in some cases. Obligations to provide opt outs should not be watered down because of the challenge of communicating with customers without excessive intrusion. Smart context specific solutions can be found.

CHAPTER 2:

BIG DATA GOES MOBILE

Mobile phone companies have access to a unique set of information that can reveal intimate insights of our life and habits. They know our name, address, age, gender, and employment status from our customer profiles. But they also have data about our behaviour, who we talk to and when, and increasingly with smartphones our Internet history and precise location.

On top of the money we pay in our bills, these businesses can generate revenue by analysing our data, and there is an emerging industry dedicated to creating mobile data 'secondary products'. These include services such as real-time traffic reports or marketing products, for example tools that tell website owners how many people are looking at their websites in a particular geographic location. Much of this is based on the application of tools that allow companies to process very large amounts of information to find "hidden" patterns and insights, generally termed "Big Data".

How do mobile devices collect our data?

Our mobile phones gather data that is used by many different companies.

There are four main points where personal information is collected:

- Communications and infrastructure location data: this is mainly under the control of mobile companies.
- Operating systems: Apple and Google dominate here. Both currently have strong advertising networks, although Apple has announced it's closing down its iAd network in June 2016.[5]
- General web use: there is multiple monitoring from mobile companies to ad networks that track Internet use across all kinds of devices.
- Apps: barely regulated independent developers access huge amounts of personal information, but mobile companies monitor the traffic from apps, mobile adverts and operating system providers and try to control the delivery of adverts to apps and associated data flows.

Mobile operators are in a unique position to access mobile data, and importantly have access to verified demographic data.

In some countries mobile operators have placed unique identifiers called "supercookies" that allow marketeers to track their users' traffic. US provider Verizon has been fined $1.35 million for this practice, and forced to move from an opt-out policy to a more explicit opt-in policy for consumers[6].

Many UK consumers now use Mobile Virtual Network Operators (MVNO's) such as Virgin, Tesco or GiffGaff, which do not own infrastructure but pay for capacity from service providers. These companies do not have access to detailed traffic or location data.

How data is used

Companies compete to obtain and monetise more data from the users in innovative ways. For example, Apple has built a technology called iBeacons into recent versions of Apple's iOS[7], which used Bluetooth to enable the precise location of handsets within a building. The beacons can mine data extracted from users' previously downloaded loyalty applications. Waitrose has trialled the

[5] http://advertising.apple.com

[6] http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0307/DOC-338091A1.pdf

[7] http://www.ibeacon.com/what-is-ibeacon-a-guide-to-beacons/

jnxyz.education CC-BY

technology in its
Swindon store to tailor offers and promotions to its users.

All kind of behavioural data is collected by apps, web browsing monitoring and mobile companies via mobile commerce platforms. The data is then thrown into a very complex global ecosystem of marketing platforms that tries to match potential consumers with the sellers of products. The aim is that every time they visit a website, users will see the most relevant adverts for them in real time, based on whatever data is available and the supposed predictive ability of marketeers to tailor the ads to the viewer. It takes 100 milliseconds for platforms to auction our identity profile (gender, age, web browsing history etc.) to advertisers, who pay around $0.0005[8] per displayed ad.

These advertising exchanges constitute a substantial proportion of all Internet traffic and impair the user experience, leading to growing interest in advert blocking software. Apple now allows apps to block ads in the browser of iPhones and iPads.

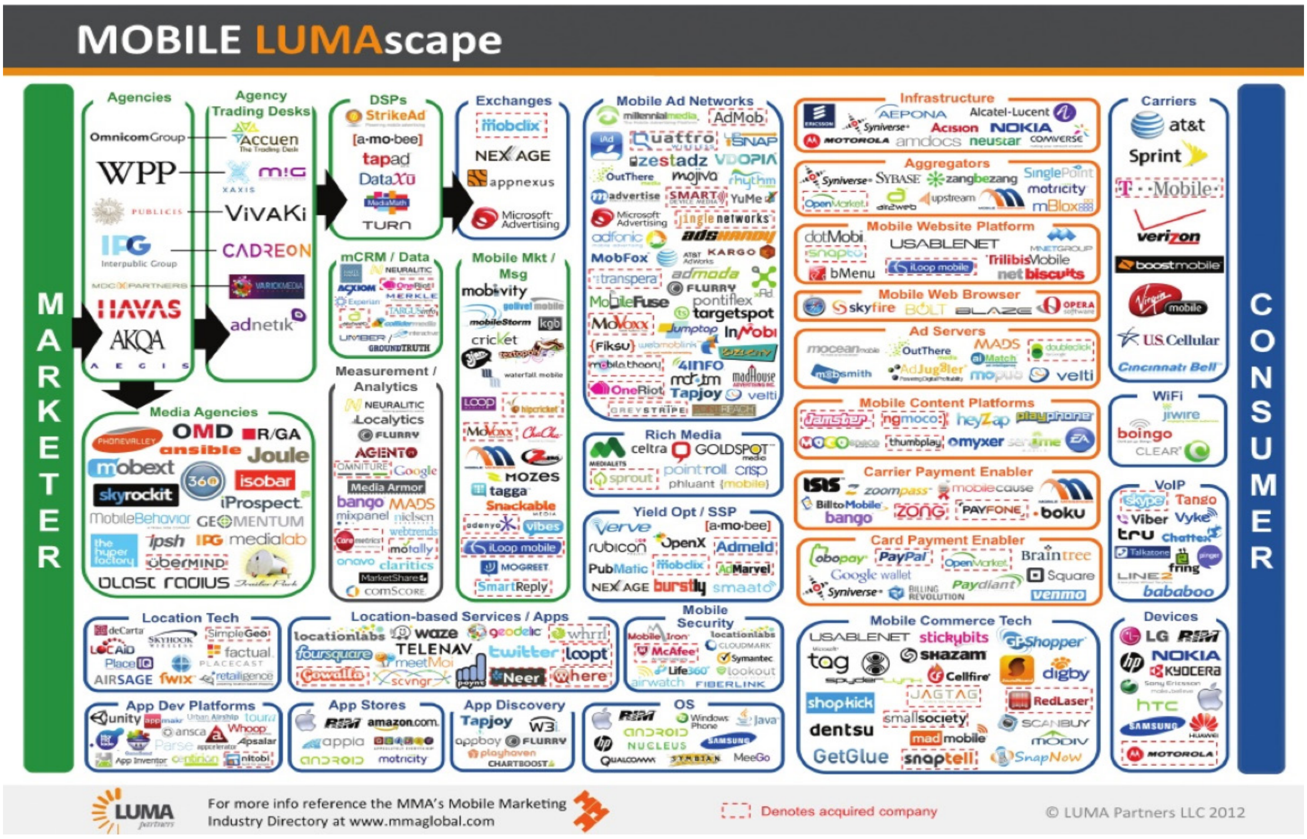
Three UK has started providing an option for network-wide blocking of adverts showing the growing conflicts over data among the players in the mobile world.

The diagram on the following page, kindly made publicly available by Luma Partners[9] gives an excellent overview of the complexity of the mobile advertising industry.

Location services are another major market for mobile users' data. Transport and mobility are a major area. The company INRIX has a location platform called Population Analytics, and has partnered with an unnamed UK mobile operator to receive "aggregate and anonymised data". Their own sponsored research claims that the market for movement analytics could be worth USD$1 billion by

[8] http://www.inrialpes.fr/planete/people/lukasz/rtbdesc.html

[9] http://www.lumapartners.com/lumascapes/mobile-lumascape/



For more info reference the MMA's Mobile Marketing Industry Directory at www.mmaglobal.com

Denotes acquired company

© LUMA Partners LLC 2012

2023 for smart city applications alone[10]. They are offering other mobile companies the opportunity to profit from analytics without having to invest in costly software platforms.[11]

Location based advertising is another area with huge growth. The Internet Advertising Bureau has a Mobile Location Working Group covering issues related to utilising location data for Mobile and Cross-Platform advertising, which developed a guide for publishers, which contains some limited privacy considerations.[12]

Mobile data also ends up being built into larger long term databases and combined with other sources. For example, credit reference agency and major personal data broker Experian promotes its Hitwise service in the following terms:

"Hitwise delivers an in-depth view of consumer behaviour on mobile devices. Using data from desktops, laptops and on-device mobile data from smartphones and tablets captured over both 3G/4G and Wi-Fi networks, marketers are able to see and differentiate between their mobile customers clearly to make better marketing decisions."[13]

The data collected increasingly include the output of sensors which can add completely new insights on our behaviour, such as sleeping patterns, exercise and health.

Mobile companies and telecoms more generally use data extensively for internal purposes, ranging from improving customer service to network planning, but increasingly see external monetisation as an important part of their strategy[14].

There is also growing interest in use of

[10] http://inrix.com/press/movement-analytics-key-unlocking-big-data-revenue-mobile-operators/

[11] http://www.inrix.com/press/2762/

[12] http://www.iab.com/wp-content/uploads/2016/03/IAB-Mobile-Location-Data-Guide-for-Publishers-Final.pdf

[13] http://www.experian.co.uk/assets/marketing-services/white-papers/wp-hitwise-mobile-measurement.pdf

[14] http://www.adlittle.nl/uploads/tx_extthoughtleadership/ADL_BigDataGoldMineforTelcos.pdf

mobile data in developing countries, such as Orange's Data for Development Challenge,[15] which made available trace data for 50,000 customers, and social graphs for 5,000, from Ivory Coast.[16] This allowed analysts propose improvements of
local transport networks.

Mobile data is also used during humanitarian crises. The recent Ebola epidemic saw several West African counties release bulk mobile records to be shared with development agencies. However, such moves have been criticised for ignoring local data protection legislation and not delivering the expected results while violating the privacy rights of millions of citizens.[17]

What do customers think?

According to research by the mobile industry association GSMA, 79% of UK mobile Internet users have concerns about sharing their personal information when accessing the Internet or apps from a mobile; and around 90% want to be asked for their permission before 3rd parties use their personal information.[18]

The same research shows that mobile users are mainly concerned about the explosion of apps collecting information, and actually expect mobile operators to protect them. This is justified by research showing some 82% of mobile apps track their users behaviour and 80% their location.[19]

The Internet Advertising Bureau UK (IAB) carried out research in 2013 that showed

- 75% of smartphone owners want companies to be really clear on the data they hold.
- 91% of smartphone owners say being in control of who gets access to their mobile Internet data is important to them.[20]

Regulation of data collected by apps

Increasingly, location data is also collected by app providers, including social networks such as Facebook. A coordinated global survey of 1200 apps, carried out by 26 privacy authorities worldwide in 2014, found that "85% of the apps surveyed failed to clearly explain how they were collecting, using and disclosing personal information".[21] These companies are not currently regulated in the same way as mobile telecoms because the E-Privacy Directive only covers a narrow definition of Electronic Communications Services.

What kind of data is used in mobile analytics

Personal information

These products may use personal data collected by the companies in their customer profiles, such as gender, address, date of birth and employment status, but it can also include richer details such as spending patterns or lifestyle information obtained via surveys.

The value of personal attributes increases when these are combined and linked with other data that provides behavioural information.

Traffic data

Traffic data[22] is the by-product of providing a communications service, including data that can tell who communicates with whom, for how long and when. Traffic data also includes personal data such as Internet usage, including

[15] http://www.d4d.orange.com/en/Accueil

[16] http://www.cs.usfca.edu/~mfdixon/d4d.pdf

[17] http://cis-india.org/papers/ebola-a-big-data-disaster

[18] http://www.gsma.com/publicpolicy/wp-content/uploads/2014/10/GSMA-Mobile-Privacy-Booklet_WEBv2.pdf

[19] http://www.mcafee.com/us/resources/reports/rp-mobile-security-consumer-trends.pdf?ClickID=anzoznttzosv0zlpzrvls500otk5vra5llro

[20] http://www.iabuk.net/about/press/archive/data-privacy-concerns-for-uk-smartphone-owners-revealed

[21] http://www.bbc.co.uk/news/technology-29143107

[22] http://www.ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/traffic_data

web browsing history, and the data sent by apps installed in smartphones.

Location Data

Location data[23] gives information about the geographical position and time, including direction of travel, where a user or the equipment may be. All mobile phones generate location data when they connect to phone masts in order to work. In addition modern smart phones can also generate large amounts of very accurate location data through the use of GPS satellites. If you enable Wi-Fi, your phone is constantly aware of any wireless networks in its vicinity and this provides further location data via third parties who keep databases of the location of wireless networks across the world. This is different from the use of Wi-Fi by businesses, such as retailers to track their customers movements across buildings and premises.

Location data is collected by a range of companies, including the providers of the phone's basic operating system such as Google, Apple and Microsoft.

Determining whether data is traffic or location data

Sometimes traffic data may also be location data. For example, phone mast data, also known as cell tower ID, could be traffic data when the mast is used for a call or text, as it is required for the delivery of the communications service. But phones are constantly communicating with masts when in stand-by. In this case it is more likely that the dataset that registers which phone masts a mobile has been linked to at different times of the day would not be considered traffic data but location data.

Phone mast references, Cell ID, are normally converted into geographical coordinates and used by EE, Vodafone and Telefónica/O2 in their analytics systems. Once this is done, this data should be classed as location data.

Some mobile companies can use more sophisticated methods to locate mobile devices. Triangulation and measuring precise timings of responses can position a mobile phone much more accurately than using the location of the mast tower. Generally, these kinds of location data would not be considered traffic data, as they are not produced as part of the communication.

It is important to identify whether data is traffic or location data because there are stricter laws regulating the use of location data, as Section 3 shows. The new reviewed e-Privacy Directive should make this distinction easier.

What are the benefits for customers?

It is not clear what benefits, if any, mobile customers get from analytics based on their data. Other methods for collecting data have more obvious benefits for customers. For example, loyalty cards give customers some perks in exchange for providing useful information for marketing purposes. This kind of quid pro quo is well understood and customers can choose to be part of it.

The use of mobile data analytics by supermarkets as an alternative to loyalty cards raises some important questions about how the benefits of Big Data are distributed. Mobile phone customers may not be aware that they are providing the equivalent value of ten years of loyalty card perks for free to companies they may not even use themselves.[24]

Companies need to be clearer about the benefits so that customers can make an informed choice about whether they want their data to be used. The relevant legislation stipulates that data can be used — with consent — to provide "value added services", which implies value for customers, so companies should not rely on this unless they bring benefit to the customer, not just third parties.

[23] http://www.ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/location_data

[24] See case study of the collaboration between Telefonica and Morrison supermarket.

CHAPTER 3:

WHAT UK MOBILE COMPANIES ARE DOING

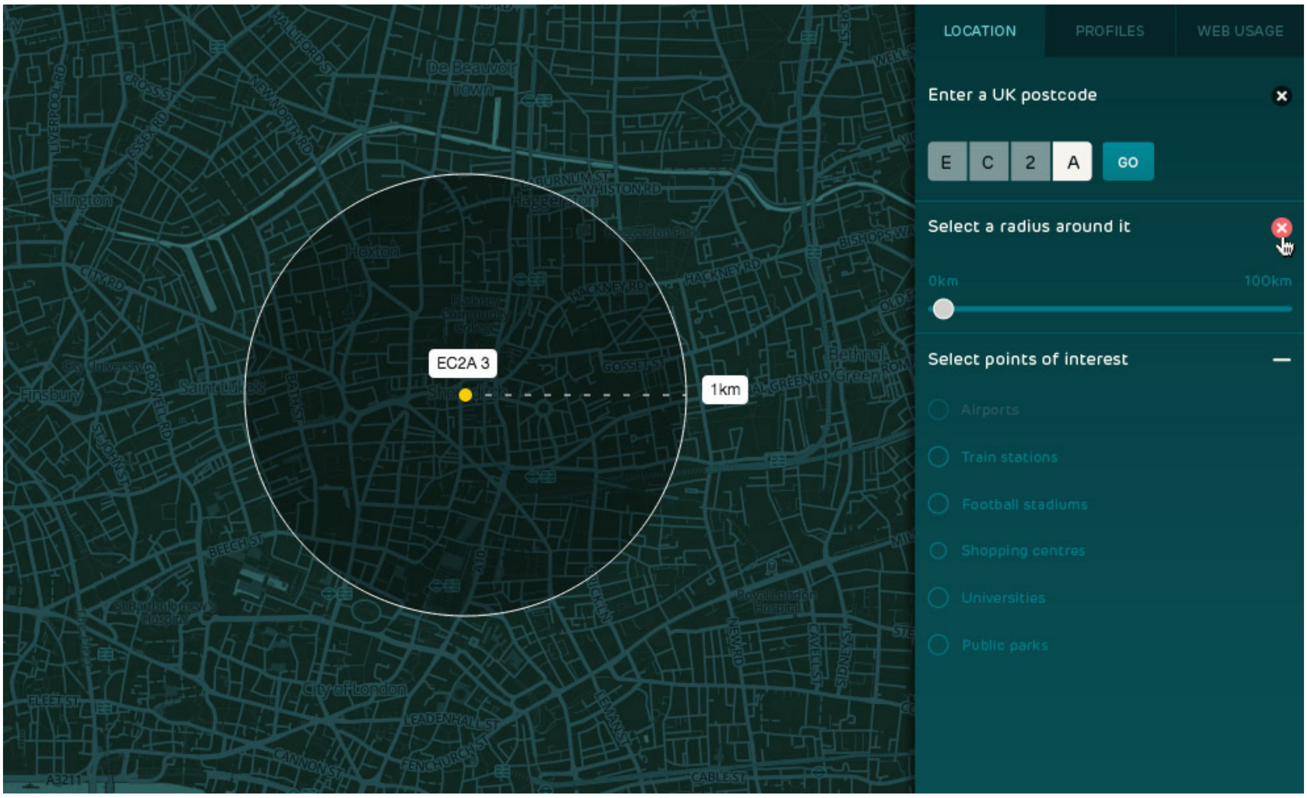
In this chapter, we give an overview of the data analytics businesses of the four main UK mobile providers. We discuss specific activities in the following sections. This is based on meetings and conversations with these representatives. We also looked at their policies and contracts and analysed what information they gather, store, analyse and share.

We also asked ORG supporters to contact their providers about these practices and request a copy of the data held about them, which we checked against the companies' privacy policies. Finally, we carried out mystery shopper visits to the companies' front end shops in the high street to ask about personal data handling.

Everything Everywhere (EE)

EE is one of the largest mobile companies in the UK with some 30 million users. EE has a deep understanding of how people use their mobile phones and they have been using analytics internally to develop their products and manage their infrastructure. Like other similar companies, their main driver is to improve their network EE built its analytics business after an initial partnership with polling and market research company Ipsos Mori, under the brand mData.

EE gained notoriety in the press in 2013 when they were accused of trying to sell their customers' information to the police through a mobile analytics platform. The accusations appeared to be based on some misinterpretation of what the service offered, but they showed the public concern raised by these activities.



Enter a UK postcode: E C 2 A

Select a radius around it: 0km – 100km

EE analyses the location and demographics of their customers to provide a wide range of commercial services in retail, transport, infrastructure and in planning for large events. EE also matches location and profiles to communications data, such as Internet usage, web data and app logs. EE says that insights provided to third parties solely include aggregated information and no information that would identify individuals.

EE worked with Google and Ipsos Mori on a pilot during the Olympics, tracking the Internet use of over 630,000 visitors. They also analysed mobile use at Wembley stadium, including the use of social media during the matches.

Large retail spaces appear to be a major customer of mobile analytics services and EE is no exception. They carried out a pilot work with Westfield shopping centres that used Westfield apps to analyse not just the footfall, but the Internet behaviour of visitors. According to their marketing materials they looked into the apps and websites customers used while at the centres and where they travelled from.

EE works with Posterscope, self-described as "the world's leading Out-of-Home communications agency," which produces billboards and other street advertising platforms. They use mobile Internet data to identify the best locations for different types of adverts and brands, including specific bus stops. EE claims to only use phone mast location data to pinpoint these hotspots, and not any other techniques that would allow them to locate handsets more accurately.

Transport and infrastructure planning is another area of development. EE ran a proof of concept showing how Waterloo station could optimise its entry and exit system by mapping the path of commuters through the station each day, via mobile data.

When we spoke to EE they told us that they are working on other infrastructure contracts, including some for Smart City programmes, but were unable to discuss the details. One known project has involved tracking visitors to London' Hyde Park in order to "inform policing of crowds at large events, tailor amenities to park usage and protect the ecology of the park".[25]

According to Marketing Weekly, EE's mData unit aims, "to offer brands real-time analytics and that this will eventually be able to offer further insights, such as dual-screening, enabling brands to tailor their campaigns during peak TV viewing hours in real-time". EE dispute the article and say that they don't have real time capacity.

Through their Connected Retail initiative, they are also using their analytics capacity to help retailers analyse their own data collected through provided on site WIFI. They have partnered most notably with ASDA, who are building this capacity in some 575 participating stores.

EE recently partnered with Facebook in a project for retailer IKEA, where they used mData to send targeted Facebook ads to potential customers in a "geo-fenced" area near IKEA stores. The aim of the project was to test the "impact and ROI of social media campaigns in the physical world"[26].

EE explained that they are building their internal mData platform using privacy by design principles and have carried out Privacy Impact Assessments, but these are not publicly available so it is difficult to assess how robust they are. The system is meant to have some internal controls and checks with approvals for new projects dependent on privacy considerations.

The mData platform collects location, demographics and, importantly, Internet traffic: website history up to first slash and all http traffic from mobile apps. Secure web connections via https cannot be fully recorded although the company's spokesperson mentioned that there were some unspecified

[25] http://www.theguardian.com/world/2015/dec/25/hyde-park-visitors-tracked-mobile-phone-data-ee

[26] http://ee.co.uk/business-edge-corporate/case-studies/articles/mdata-proves-facebooks-impact-on-ikea-footfall

developments.

EE claims that they do not keep the full web history of customers and certainly not the content, but they aggregate these into profiles for kinds of online activities and the key points of the day for Internet use.

The data is kept at individual level in the platform and includes other customer information such as types of contract, monthly average spend, etc. The phone number itself is converted into a unique code via a hash function.

The company has policies setting out what data is retained and stored and for how long, but these are not publicly available. They regularly review business needs against data retention and the policies have to be agreed by senior stakeholders. Data retained for law enforcement is kept in completely separate databases.

The company applies a principle of purpose limitation, meaning that if a new unit wants to use the data, they have to review the new business cases and match the appropriate levels of data access.

EE's clients get reports using aggregated data but would not be able to access individual customer's data.

The company Signal Noise worked with EE to provide a visually stunning sales tool to promote the mData platform.

According to the Signal Noise website[27], the tool allows, 'users to specify a UK postcode (limited to 5 characters for privacy reasons) and a radius around it'. EE say that this is inaccurate and that the tool is a sales tool and can't be used by external customers.

It is positive that third parties can't manipulate the data independently as that would increase the risk that combined queries could pinpoint groups small enough to be identified with the help of external information.

Telefónica

For some time, the UK leader in analytics services was the Spanish multinational corporation Telefónica (operating in the UK as O2), but EE and Vodafone are now catching up. Telefónica has a very active analytics department, Dynamic Insights,[28] which is based in London. Their website appears to claim that they have access to the information of 309 million customers worldwide, giving them "real data on an incredibly large sample of our society"[29]. But they have confirmed that in practice they only work within three countries — the UK, Spain and Brazil.

O2 also use their customers' location and traffic internally to tailor commercial offers through their internal platform called Vision[30].

Telefónica initially concentrated on location and demographics rather than communications data. They started their analytics by establishing a partnership with German market researchers GfK called Smart Steps[31], which focuses on "the behaviour of crowds". O2 have however recently acquired the marketing platform Weve, with plans to integrate all forms of data such as traffic and marketing profiles, and data from the O2 Wi-Fi network, with the location data from Smart Steps.[32]

Retail appears to be an important client, although overall they appear more interested in population level insights, rather than tracking movement within single premises. The supermarket chain Morrisons used Smart Steps as a cheaper alternative to loyalty card schemes to target marketing promotions of coupons to households in specific postcode areas. According to the supermarket chain, obtaining this kind of data with loyalty cards

[27] http://signal-noise.co.uk/work/ee-mdata-visualisation-tool/

[28] http://dynamicinsights.telefonica.com/

[29] http://dynamicinsights.telefonica.com/479/about-us

[30] http://www.managementtoday.co.uk/go/telefonica

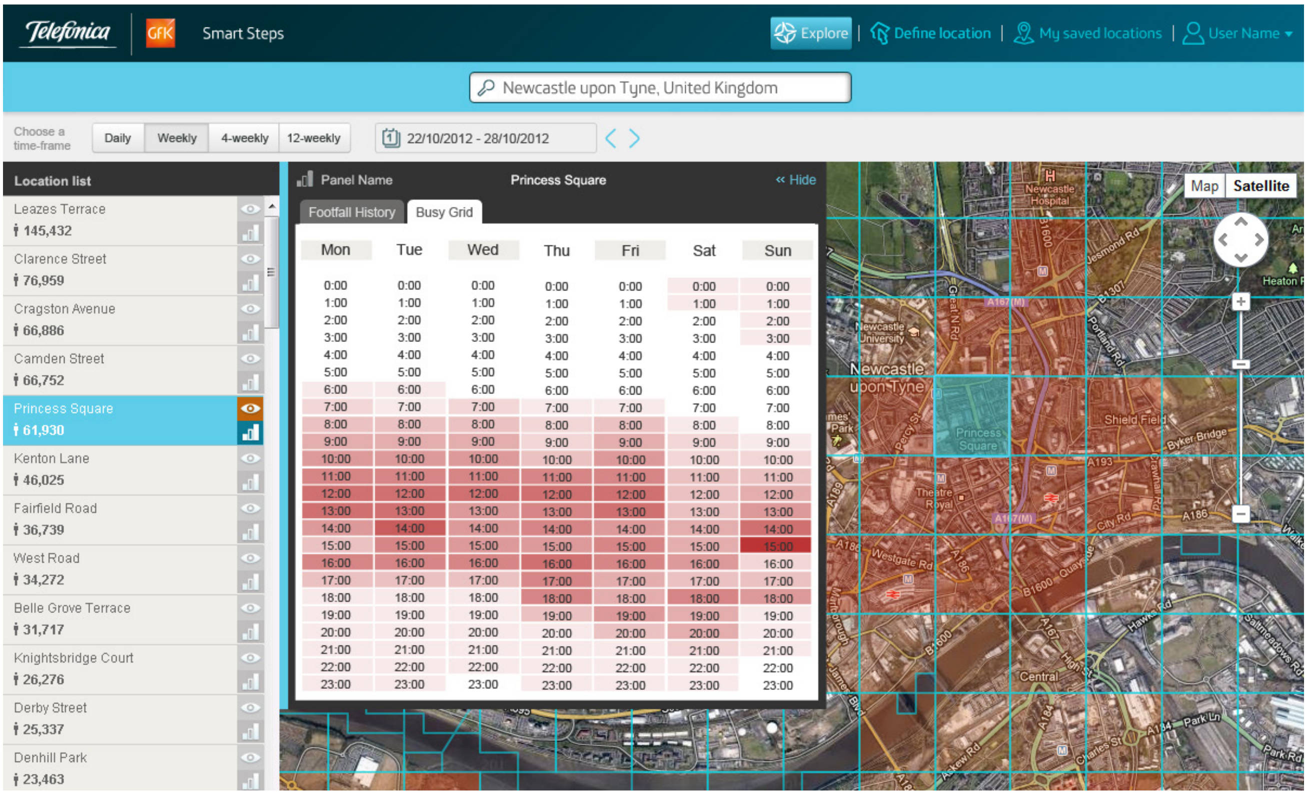
[31] http://blog.digital.Telefónica.com/?press-release=Telefónica-launches-Telefónica-dynamic-insights-a-new-global-big-data-business-unit

[32] http://www.iabuk.net/blog/the-future-of-weve

would take around ten years[33]. They have also worked with the transport sector, including optimising the East Coast Mainline and Newark traffic planning[34].

Telefónica has taken a collaborative approach to building expertise on data and partners with other organisations, including the Open Data Institute (ODI) and the Massachusetts Institute of Technology (MIT). Together they organised a "Datathon for Social Good" at the 2013 London Campus Party, where participants were given access to aggregated mobile data from Telefónica customers. The Mobile Territorial Lab team,[35] based in Italy, won by designing a model to predict crime levels, although the contribution of mobile data to the model was fairly minor.[36]

Telefónica also claim to have a Privacy by Design approach to their system, and like all the other companies have previously been using their data for network optimisation. But they have taken a different approach from the other companies in completely splitting their global analytics division — Dynamic Insights — from their country level mobile telephone businesses, which in the UK is O2.



Newcastle upon Tyne, United Kingdom

Choose a time-frame: Daily | Weekly | 4-weekly | 12-weekly

22/10/2012 - 28/10/2012

Location list

Leazes Terrace	145,432
Clarence Street	76,959
Cragston Avenue	66,886
Camden Street	66,752
Princess Square	61,930
Kenton Lane	46,025
Fairfield Road	36,739
West Road	34,272
Belle Grove Terrace	31,717
Knightsbridge Court	26,276
Derby Street	25,337
Denhill Park	23,463

Panel Name: Princess Square « Hide

Footfall History | Busy Grid

Mon	Tue	Wed	Thu	Fri	Sat	Sun
0:00	0:00	0:00	0:00	0:00	0:00	0:00
1:00	1:00	1:00	1:00	1:00	1:00	1:00
2:00	2:00	2:00	2:00	2:00	2:00	2:00
3:00	3:00	3:00	3:00	3:00	3:00	3:00
4:00	4:00	4:00	4:00	4:00	4:00	4:00
5:00	5:00	5:00	5:00	5:00	5:00	5:00
6:00	6:00	6:00	6:00	6:00	6:00	6:00
7:00	7:00	7:00	7:00	7:00	7:00	7:00
8:00	8:00	8:00	8:00	8:00	8:00	8:00
9:00	9:00	9:00	9:00	9:00	9:00	9:00
10:00	10:00	10:00	10:00	10:00	10:00	10:00
11:00	11:00	11:00	11:00	11:00	11:00	11:00
12:00	12:00	12:00	12:00	12:00	12:00	12:00
13:00	13:00	13:00	13:00	13:00	13:00	13:00
14:00	14:00	14:00	14:00	14:00	14:00	14:00
15:00	15:00	15:00	15:00	15:00	15:00	15:00
16:00	16:00	16:00	16:00	16:00	16:00	16:00
17:00	17:00	17:00	17:00	17:00	17:00	17:00
18:00	18:00	18:00	18:00	18:00	18:00	18:00
19:00	19:00	19:00	19:00	19:00	19:00	19:00
20:00	20:00	20:00	20:00	20:00	20:00	20:00
21:00	21:00	21:00	21:00	21:00	21:00	21:00
22:00	22:00	22:00	22:00	22:00	22:00	22:00
23:00	23:00	23:00	23:00	23:00	23:00	23:00

This creates extra safeguards, as the analytics group does not have access to the fully identifiable data, but it also creates some potential risks around accountability if there are problems downstream.

Their initial strength was being able to understand individual journeys, following

[33] http://dynamicinsights.telefonica.com/1158/a-smart-step-ahead-for-morrisons

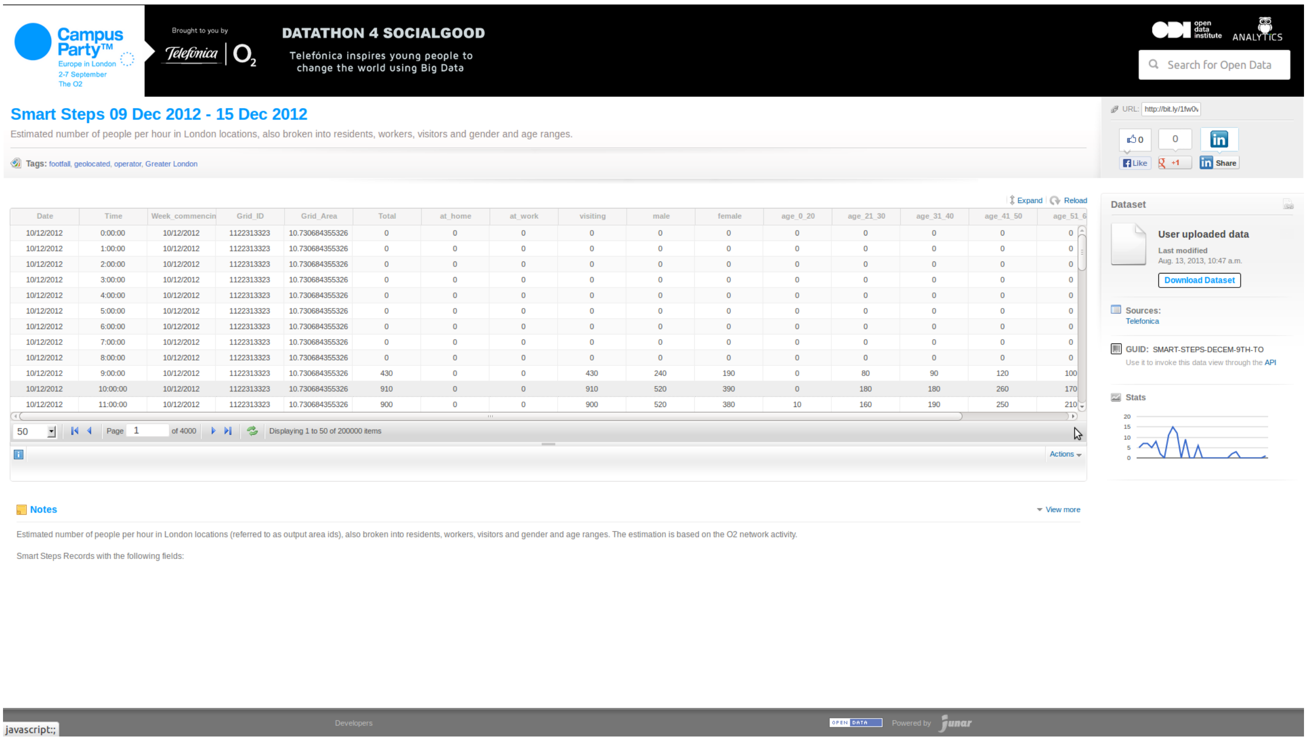
[34] http://dynamicinsights.telefonica.com/blog/1634/smart-steps-saved-newark-from-commuter-lock-down

[35] http://www.mobileterritoriallab.eu/pages/news.html

[36] https://medium.com/the-physics-arxiv-blog/londons-future-crime-hot-spots-predicted-using-mobile-phone-data-ae869a2e67ab

the "breadcrumb trail", in their own words[37]. But their main focus for now is being able to extrapolate their insights — from the data of O2 mobile customers — to the general population with statistical confidence.

They seem to use basic demographic data: year of birth, gender, and the first four digits of the postcode, using some 18 months of historical data in their platform.[38] The age is presented to clients in cohorts of ten years, but the precise grouping is flexible so it can be matched to external datasets.



Smart Steps 09 Dec 2012 - 15 Dec 2012

Estimated number of people per hour in London locations, also broken into residents, workers, visitors and gender and age ranges.

Tags: footfall, geolocated, operator, Greater London

Date	Time	Week_commencin	Grid_ID	Grid_Area	Total	at_home	at_work	visiting	male	female	age_0_20	age_21_30	age_31_40	age_41_50	age_51_6
10/12/2012	0:00:00	10/12/2012	1122313323	10.730684355326	0	0	0	0	0	0	0	0	0	0	0
10/12/2012	1:00:00	10/12/2012	1122313323	10.730684355326	0	0	0	0	0	0	0	0	0	0	0
10/12/2012	2:00:00	10/12/2012	1122313323	10.730684355326	0	0	0	0	0	0	0	0	0	0	0
10/12/2012	3:00:00	10/12/2012	1122313323	10.730684355326	0	0	0	0	0	0	0	0	0	0	0
10/12/2012	4:00:00	10/12/2012	1122313323	10.730684355326	0	0	0	0	0	0	0	0	0	0	0
10/12/2012	5:00:00	10/12/2012	1122313323	10.730684355326	0	0	0	0	0	0	0	0	0	0	0
10/12/2012	6:00:00	10/12/2012	1122313323	10.730684355326	0	0	0	0	0	0	0	0	0	0	0
10/12/2012	7:00:00	10/12/2012	1122313323	10.730684355326	0	0	0	0	0	0	0	0	0	0	0
10/12/2012	8:00:00	10/12/2012	1122313323	10.730684355326	0	0	0	0	0	0	0	0	0	0	0
10/12/2012	9:00:00	10/12/2012	1122313323	10.730684355326	430	0	0	430	240	190	0	80	90	120	100
10/12/2012	10:00:00	10/12/2012	1122313323	10.730684355326	910	0	0	910	520	390	0	180	180	260	170
10/12/2012	11:00:00	10/12/2012	1122313323	10.730684355326	900	0	0	900	520	380	10	160	190	250	210

Displaying 1 to 50 of 200000 items

Dataset

User uploaded data

Last modified
Aug. 13, 2013, 10:47 a.m.

Sources:
Telefonica

GUID: SMART-STEPS-DECEM-9TH-TO
Use it to invoke this data view through the API

Stats

Notes

Estimated number of people per hour in London locations (referred to as output area ids), also broken into residents, workers, visitors and gender and age ranges. The estimation is based on the O2 network activity.

Smart Steps Records with the following fields:

Smart Steps uses the location data from cell masts and may use some micro location techniques that provide more accurate pinpointing of handsets by calculating the distance to the masts. They do not record signals from non O2 customers received by their phone masts.

Their database records the home and work locations of each individual based on the regular day and night movement patterns of the handset, but masks this to a distance of two kilometres. The location data used in the reports is rounded up to the level of postcode sector — the first 4 digits — which roughly translates into areas where some 10,000 people live. However, this varies greatly between rural and high density urban locations.

There are concerns in the relationship between O2 and the marketing company Weve,[39]. which receives supposedly anonymised O2 data and matches it with other data sources to build a mobile advertising platform. Weve claims to have 31 million people in their profiles and can target advertising to mobiles based on demographics, behaviour including both Internet and mobile usage and location, including home[40].

The company's initial plans were to offer clients a graphical way to directly interact with the data, but they explain that this proved less

[37] http://dynamicinsights.telefonica.com/wp-content/uploads/2015/04/Big-Data-Monetization-in-Telecoms-Smart-Steps.pdf

[38] Ibid.

[39] http://weve.com/

[40] http://www.weve.com/products/display/audience-targeting/

useful than expected due to the requirements of interpretation and manipulation. This also had higher privacy risks. Telefónica currently provide graphic reports and aggregated information, and clients cannot get direct access to the data.

Vodafone

Vodafone has been piloting analytics systems for several years and it is starting to implement them in the real world. The company has been using its campus in Newbury, Berkshire, to test some of their location analytics systems on their six thousand employees, and visitors who use Vodafone. The site has no wired telephony and all employees use mobile phones. This means that the buildings have extensive indoor mobile infrastructure that allows for the precise positioning of handsets. The trials have so far looked at ways to ensure a more efficient use of the buildings including energy savings.

There are plans for delivering this kind of location analytics service to shopping malls and similar sites. Negotiations are apparently underway with some of the largest commercial real estate managers in the UK but as far as we are aware these have not been fully implemented yet across the country.

The company is also expanding its analytics services into public infrastructure, working with major civil engineering firms. In one project, Vodafone customers using the main roads crossing from the West of England to Wales saw their journeys measured to inform the planning of future developments.[41]

The company focuses on location and demographics, and does not currently use their clients' Internet usage as part of their Big Data analytics. Vodafone users who visited the centre during their first trials had their demographics analysed: gender, the first three digits of their postcode and age group matched to Experian's Mosaic UK consumer classification. We believe that this is the data they use in their projects.

In a separate trial, users could — on an opt-in basis — also have their Internet traffic data analysed: this involved web use to the first level url and mobile applications. This is apparently in early stages and the company have not fully developed the model. In our communications with the company they have indicated that the current focus of their business development is location services, and not the tracking of communications data.

The location data available depends on the type of handset and customer behaviour. More frequent connections for calls of data will provide a richer location trace. On average they get a location every 15 minutes from the connected mast tower. This information is converted to the coordinates of the cell centroid, the point at the geographical centre of the area covered by the mast, plus a radius. This radius varies from some 300 meters in urban areas to up several kilometres in rural locations.

Vodafone does not use Wi-Fi, MAC addresses or other sophisticated methods to locate GSM handsets based on the timing of signals or power consumption, as are used by some car navigation companies.

Vodafone says its approach to privacy in analytics is based on transparency and choice.

Three UK

Three UK is the smallest of the large mobile operators, with some 8 million customers. When we spoke to the company they told us that they did not use their customers' data to build an analytics business. They use the data to inform upgrades and rollout plans and also in internal marketing and pricing.

Three UK has been using data analytics for internal purposes since 2009, when they started their Network Intelligence project to handle the large volumes of customer and infrastructure data their business was generating. For several years they leveraged

[41] https://www.youtube.com/watch?v=fj353Sj8zdI

technology from IBM but now they are developing their own technology.

In the summer of 2014 the company launched a platform for data analytics and visualisation for its business users. The aim is to get their clients to integrate Three UK’s mobile data with other business intelligence. This does not appear to affect individual customers. But this may change in the future as the company develops more sophisticated data capacities and competitors mature their offers.

Three UK remains the best option for individuals not wishing to see their personal information being reused for Big Data.

CHAPTER 4:

CONSENT AND OPT OUTS

Consent is one of the key avenues in data protection and privacy for the lawful processing of personal information, including analytics. Consent is not always necessary from a legal point of view, but it builds trust between customers and companies as it helps individuals to manage risks and have some control over their data. For consent to be effective, it is important that people understand what happens to their personal information at the time they agree to use a service. There is growing public awareness and concern about how our data is used by companies for advertising and other purposes. Companies may comply with the law by burying requests for consent within contracts or privacy policies. However, we believe that the public wants companies to be up front and tell their customers about how their data is going to be used.

There are limitations when getting consent for the use of mobile data. Nobody can be sure of the new processing activities that will be carried out elsewhere in the complex ecosystem of companies that reuse users' data. This in itself is a reason why mobile companies should explain about how data is used. Customers' should have some rights over their data that cannot be circumvented by removing some identifiers.

ORG believes that the best way to get informed consent is to allow customers to opt in to the use of their data. Opting out is less satisfactory but it would be an improvement on the current situation and ensure legal compliance.

The legal obligation for consent

Under the current UK E-Privacy regulations (section 7 (3)), traffic data can only be used by companies to provide "value-added services" or for marketing purposes with customers' consent. In addition, the Data Protection Act requires "fair processing" of data, and for the ICO this includes being "clear and open with individuals about how their information will be used".[42] The E-Privacy Directive, on which the UK regulations are based, provides further guidance on the information that must be provided before consent is obtained:

> ***PECR 8.*** *(1) Processing of traffic data in accordance with regulation 7(2) or (3) shall not be undertaken by a public communications provider unless the subscriber or user to whom the data relate has been provided with information regarding the types of traffic data which are to be processed and the duration of such processing*

For traffic data, the user has to be notified of the types of data that are retained — and how long this data is kept — in advance of obtaining consent. But in relation to location data, the user also has to be informed of the purposes of the processing and if the data is being sent to a third party.[43]

The UK E-Privacy Regulations introduce extra obligations for information on location data. The DPA does not list location data as one of the types of sensitive personal data that deserves higher protection[44] — such as health, sexuality or religion — but this is not the consensus at the European level. The Article 29 Working Party (composed of the European data protection authorities) has published an opinion on location data[45], which clarifies what constitutes valid consent for the processing of

[42] http://www.ico.org.uk/for_organisations/data_protection/the_guide/principle_1

[43] PECR 14 (3)

[44] http://www.legislation.gov.uk/ukpga/1998/29/section/2

[45] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_en.pdf

location data under the E-Privacy Regulations:

"This definition explicitly rules out consent being given as part of accepting the general terms and conditions for the electronic communications service offered."

The new General Data Protection Regulation coming into force in the next few months will shake up the legal regime and interpretions.

We discuss the laws regulating the use of mobile data in Appendix A.

EE Consent

EE do not believe their analytics system requires consent because they claim there are legitimate business reasons to use the data for analytics. They say they act in accordance with data protection laws and are entitled to rely on other types of justifications to process customer data e.g. for the performance of a contract, for legitimate business interests etc.

This is true for personal information under the Data Protection Act, but as we will see below, under the more restrictive PECR companies are not allowed to use traffic and location data for anything they consider a legitimate business interest.

EE state that they have put in place privacy by design measures to ensure that their customers' data privacy is respected including the fact that the data is anonymised within the platform, and therefore opting out is not necessary.

EE's privacy policy has a section on the use of data, which includes the following:

"*We may use information about your location for research and analytics purposes but we will only retain this information in an anonymised form to ensure that you cannot be identified as an individual."*

EE act in accordance with data protection laws and follow the ICO's guidance on anonymisation but as we show in this report, this guidance may not be sufficient to protect an individual's data.

The company also argue that it is impossible to carry out analytics with an optional system as it would distort the data. During our meetings they expressed very clearly their belief that data analytics will be one of the main driving forces of progress in this century, and mobile companies must be part of it.

In addition, EE argues that these systems benefit customers because the networks perform better and it would be more expensive to run the network without any analytics. This is not our main concern and we don't have a problem with the internal use of data, but we believe that this is quite different from providing services to third parties. EE says there are wider benefits to society in sharing aggregated data with third parties. This is a common argument in the promotion of all kinds of Big Data projects. This may be true to a point in some cases, but we need more transparency about how these benefits are distributed. And arguments about the greater good must still consider individuals' privacy.

During our conversations, EE were adamant that they do not believe their customers are concerned about data analytics.

O2 Consent

Telefónica do not offer any way to opt out of their analytics platform with the argument that the data is fully anonymised by O2 and therefore there is *not* need to consider consent. But this argument appears less clear cut when we look at how the company operates in different countries.

Telefónica announced the launch of Smart Steps in Brazil, Germany and the UK in 2012.[46] The company quickly withdrew the German project due to privacy constraints on the sale of location data.[47] The Brazilian department of consumer protection forced Telefónica's local operator, Vivo, to explain their use of personal

[46] http://www.telecompaper.com/news/Telefónica-to-sell-customer-information-to-companies--901213

[47] http://www.mrweb.com/drno/news16355.htm

data in this venture.[48] Their Brazilian operation publicly stated that customers would be able to opt out[49]. According to the company the opt-out possibility was considered over there because there is no concept of anonymous data for Brazilian authorities.

In the end Smart Steps was only launched in Britain in November 2012. In contrast to Brazil, Telefónica refuses to give their UK customers a choice to opt out. Their argument is that the UK has more robust data protection legislation that allows for the handling of anonymous data.

This appears to be a paradoxical situation, where citizens from a country with a stronger data protection framework, such as the UK, end up with less control over their data than those from less regulated countries in South America.

Vodafone Consent

Vodafone allows customers to opt out of analytics via SMS. In their road traffic project in Wales, the company carried out a publicity campaign on billboards and petrol stations telling people to text a number if they wanted to stop being part of the analytics.

The company put signs on the doors a shopping centre in Leeds informing visitors how to opt out of a project that replicated the campus trial, looking at visitors' movements around the centre and footfall.

ORG queried why they could not use SMS messages to explain that opt outs were available, as this would allow them to target individual customers with more certainty. Vodafone argued that SMS would not be appropriate for an activity so limited in time and geographical scope. Vodafone has committed to communicating more directly to its customers when mAnalytics is rolled out nationally. In their view operational costs and the possibility of consent fatigue make individual notifications more appropriate for a general campaign.

The company explained that they will be informing ten million individuals customers of their analytics programme to give them the option to opt out. They will use various channels in addition to SMS, including email and customer portals. They explained the implications of such operation, including the training of call centre staff to handle customer queries.

The company carefully avoids talking about consent, probably due to the legal implications of the term, and prefers to use the term choice, giving customers the possibility to opt out. Vodafone has a section of its privacy policy online dedicated to data analytics. The webpage contains information about their analytics business, including a project to monitor traffic in London, which is not found elsewhere in their main site. The webpage has information on how to opt out or back in to the analytics systems via SMS.

Overall, it is positive that Vodafone allows for opt outs and acknowledges that customers should have a choice. But we would want to see more proactive consideration of consent, ideally on an opt in basis.

Mobile companies can access their individual customers via SMS, so we cannot see why they do not use this method and instead rely on indirect channels such as webpages and notices. This may lead to more customers opting out, but the overall distribution of these customers pulling out could be diverse enough to maintain the representative nature of their customer base. Given the numbers involved, a smaller sample size of 50% of Vodafone customers may well still be big enough for Big Data.

Opting out of traffic data

At present only one company that engages in Big Data analytics, Vodafone, gives its customers the option not to be part of it.

[48] http://www.telecompaper.com/news/brazilian-govt-questions-vivo-over-use-of-customer-data--903025

[49] http://www1.folha.uol.com.br/fsp/mercado/72850-Telefónica-tera-que-explicar-venda-de-dados-sobre-clientes.shtml

There is no reason why EE and Telefonica/O2 cannot do the same and give their customers a choice about whether they want their data to be used.

Telefónica/O2 does not allow its 23 million UK customers to opt out of its analytics service Smart Steps, because "there is no disclosure of personal information … anonymisation and aggregation protect people's privacy".[50]

Similarly, EE does not allow its customers to opt out with the argument that the data has been anonymised and therefore there is no legal obligation anymore.

But the E-Privacy Directive creates a specific right for subscribers to withdraw their consent to the processing of traffic data. This is in addition to any general obligations under the Data Protection Act.

> *PECR 7 (4) Where a user or subscriber has given his consent in accordance with paragraph (3), he shall be able to withdraw it at any time.*

There is a lack of clarity on how this is meant to work. EE, O2 and Vodafone customers are informed that they can opt out of receiving marketing communications, but the companies may still process their traffic data in their Big Data programmes if they choose to do so.

Mobile companies are not under a strict obligation to provide subscribers with detailed information on how to opt out under either the E-Privacy Directive or the Data Protection Act. ORG believes that this should change and that as best practice, companies should inform their customers about how they can give and withdraw their consent to use traffic data.

Opting out of location data

Users have a specific right to withdraw their consent to the processing of location data using simple means under the E-Privacy Regulations:

> *(4) A user or subscriber who has given his consent to the processing of data under paragraph (2)(b) shall-*
>
> *(a) be able to withdraw such consent at any time, and*
>
> *(b) in respect of each connection to the public electronic communications network in question or each transmission of a communication, be given the opportunity to withdraw such consent, using a simple means and free of charge.*[51]

There is no consensus for what constitutes a proper "opportunity to withdraw" consent at every communication. At the time the Directive was adopted, many mobile location services were delivered via SMS, so this could be easily interpreted as including an opt-out code in messages.

The opinion of Article 29 Working Party is

"that it is a precondition for the exercise of these rights (to withdraw consent by simple means) that individuals are kept informed, not only when they subscribe to a service but also when they use it".[52]

This document also recommends that where the ongoing processing of location data takes place, users are sent regular reminders that their "terminal equipment has been, will be or can be located".[53] This is also recommended by the Mobile Industry Code of Practice for Location services.[54]

The implementation of location opt outs by UK mobile companies is inconsistent.

- **O2** customers can call 1300 to opt out of location services a direct number for a Location Services Privacy Controller, and a specific opt-out for this type of data

[50] http://www.bbc.co.uk/news/technology-19882647

[51] Regulation 14(4)

[52] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_en.pdf (page 7)

[53] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_en.pdf (page 7)

[54] http://www.vodafone.co.uk/cs/groups/public/documents/webcontent/vftst062576.pdf

services, although this does not seem to cover their analytics platform.[55]

- **EE** has some detailed information on location in their privacy policy[56], but no clear simple way to opt out other than contacting their customer services by calling 150 or 0845 412 5150.[57]

- **Vodafone** has a copy of the code of practice in their corporate responsibility website, but no specific information on location and no simple way to opt out specifically for location.[58] They do however allow customers to opt out of data analytics in general by texting OPT OUT to 68808, which includes location.[59]

- **Three UK** told us that customers can opt out of location logging by contacting emailing preferences@3mail.com, or through their online account management website. However, a member of our staff who uses this network could not find any privacy settings in the referred website.[60] Customers can also contact Three's general data protection officer at dpa.officer@three.co.uk

Current guidance from the ICO simply repeats the wording in the legislation,[61] but adding that there is nothing in the law stopping companies from giving customers the option to withdraw their consent for a limited period of time, with automatic reactivation afterwards.

General marketing opt-outs should be easier

Under the E-Privacy Regulations, customers have a right to opt out of marketing but this is not always properly implemented.

In the case of EE, their contract includes a clause giving the option to call a number to opt out after the contract has been signed. But there is no option to opt out on the contract itself. This means that customers will be initially part of a marketing database until they manage to perform the opt-out.

Customers should not be included in marketing databases at any time without consent, even if only for a short period.

The American system of opt outs

American regulators call the bundle of traffic, location and customer data Customer Proprietary Network Information (CPNI). This is classed as personal information in the US, despite the fact that it does not include customers' names, addresses, or mobile phone numbers.

Most mobile companies sell this data for marketing purposes, including advertising placement of the kind we described in the previous sections. CPNI does not cover web browsing, which is also sold to advertisers. Mobile companies in the US appear to engage in more aggressive marketing and analytics practices than their UK counterparts, but at the same time they are forced by law to offer means for opting out.

Verizon Wireless, which is connected with Vodafone, offers several ways to opt out: letter, phone or website.[62]

Sprint offers a detailed yet concise explanation of both its marketing and analytics programmes with an opt in and out default option respectively.[63] This is a good example of

[55] http://www.o2.co.uk/termsandconditions/privacy-policy

[56] http://explore.ee.co.uk/privacy

[57] http://explore.ee.co.uk/privacy

[58] https://www.vodafone.co.uk/about-this-site/our-privacy-policy/index.htm

[59] http://www.vodafone.co.uk/about-this-site/our-privacy-policy/vodafone-analytics/

[60] http://www.three.co.uk/_standalone/Link_Document?content_aid=1220457053001

[61] https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/location-data/

[62] http://www.verizonwireless.com/b2c/globalText?contentType=Legal%20Notice&textId=181

[63] http://newsroom.sprint.com/article_display.cfm?article_id=1623

what UK companies could be doing.

Recommendations

Companies should ask for their customers' explicit consent to use their traffic and location data for Big Data analytics. This should operate on an opt-in basis from point of sale onwards. This should be separate from the general consent to receive marketing communications.

This process should include 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.

Even if a customer has given consent, there should be clear ways that customers can opt out of different kinds of data sharing should they change their minds at any point.

CHAPTER 5:
ANONYMOUS DATA

The E-privacy directive makes very clear that there are only two avenues for an organisation to reuse traffic or location data for purposes that are not related to the original reason the data was collected in the first place: consent — which we discussed above — or anonymisation

In principle, datasets containing personal information are anonymised when they are modified to make it impossible for individuals to be identified. Depending on the data and the context his could involve a simple change, such as removing names and other attributes, or applying complex mathematical processes.

If data is fully anonymised it is generally pulled out of the scope of most privacy legislation and all the accompanying constraints, including the need to obtain consent to reuse it. But it is now accepted by most experts that proper anonymisation of some detailed personal datasets — such as location traces or medical histories — is very difficult, or even impossible without making them useless. In some cases, each record will be so unique to an individual that we cannot guarantee that someone somewhere won't find a way to link it back to him or her.

Defining the line between identifiable and anonymised data is one of the hardest questions in privacy regulation worldwide. European legislators tried to future proof the law against changing technical advancements by introducing the principle that "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person."[64]

In many cases organisations remove any personal attributes that would allow the direct identification of individuals, such as names, and possibly substitute them with some code. But crucially, if those with access to the data are able to link the codes back to the original identities the data remains personal information.[65] In these cases we would be dealing with pseudonymous data, which may look the same as anonymous data but has a very different legal standing. The new GDPR brings more clarity to the regulation of pseudonymous data.

EE Anonymisation

EE uses demographic information but according to the company, all personal identifiers such as name are removed, apart from gender. We are unclear on what happens to the home address postcode, which is typically used in analytics to link to third party demographics data, such as Experian Mosaic. In our initial meetings the company said they included the first three digits of the postcode, but more recently they claimed that there is no direct postcode information in mData. EE explained that each individual profile stores the geographical coordinates of the first three digits of the postcode. But this seems to be quite a similar proposition as it would be trivial to reconstruct the postcodes. The cell ID of the phone masts to which the handset has been connecting are also replaced by the location coordinates (latitude and longitude).

The data is always aggregated in groups of at least 50 when presented to third parties, who sign contracts with clauses prohibiting them from attempting to manipulate the data to work out the identities of EE's customers.

EE told us that in line with the ICO Code of Practice on anonymisation they are now looking at using derived data and banding:

"Derived data is a set of values that reflect the character of the source data, but which hide the exact original values. This is usually

[64] Recital 26 of the Data Protection Directive http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en

[65] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

done by using banding techniques to produce coarser-grained descriptions of values than in the source dataset e.g. replacing dates of birth by ages or years, addresses by areas of residence or wards, using partial postcodes or rounding exact figures so they appear in a normalised form."[66]

Banding applied to data stored in an intermediate stage before disclosure to their clients will reduce re-identification risks. But it would be better if this process is carried out with the source data as early as possible in the process. Banding it would improve the system work better with demographic information, but it will be harder to implement with information about movements location, and particularly traffic Internet use data, which stored at the individual level still pose a privacy risk.

The company says that the platform is not in place yet but but all data within it will be anonymised because all personal identifiers will be removed. But in our view, the data would be pseudonymous. The main personal identifiers may have been removed but it contains unique information that would allow re-identification with the help of some other data.

In further conversations EE admitted that their anonymisation is not perfect and that the process is not irreversible so that the term pseudonymous might be more appropriate. Nevertheless, they think that the risks are acceptable, and that the process fully complies with the law and the recommendations of the ICO.

This divergence of views about risks and anonymisation is a fairly a common situation that can only be remedied with utmost transparency. But in this case we have further concerns. According to EE, one of the possible uses of the system is to support customer enquiries. For example, if a customer were to challenge her Internet bill, the database can show that she has consumed a lot of video, and thus incurred a higher charge. This should not be possible if the data was anonymised.

The company makes the case that this would be limited to a small team and that there would be audit policies and security measures in place. They claim that the process of reverse engineering data back to an individual in restricted circumstances would only happen outside of the mData platform for customer queries, because within the platform reverse engineering is not possible.

We accept that there are organisational measures to prevent abuse. But independently of these measures, this shows that the data is almost certainly pseudonymous and not anonymous because, when combined with other datasets, it can be used to identify an individual. The process is not irreversible.

O2 Anonymisation

The original data is processed by O2 before being sent to Dynamic Insights. Some personal identifiers such as name are removed at source, while other such as quasi-identifiers such as phone numbers are scrambled with a hash. This may provide more effective de-identification in the case of Telefónica than in other companies because the organisational separation between Dynamic Insights and O2 should make it harder to link the pseudonymous data back to the original file. But without a proper technical audit of their systems it is difficult to tell how effective this is in practice.

Telefónica claims this means that the data is "anonymised" but in our view it should be formally treated as pseudonymous data because its richness allows for each individual in the database to be singled out and potentially re-identified.

We agree with Telefónica that the outputs they produce for their clients are fully anonymised, as they are aggregated to numbers above ten with smaller groups getting rounded up to ten. Dynamic Insights teams apply further processing to the data to make it even harder to re-identify individuals.

[66] https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

Customers of Dynamic Insights do not get access to any data, only receiving reports and insights, mainly in the form of footfall heat maps.

Vodafone Anonymisation

The company "anonymises" individual mobile identities, at the source in near-real time, by creating unique codes that allow for a handset to be tracked over space and time, but not to be immediately identifiable. They agree with us that the result is pseudonymous data, which is not truly anonymised data. Individuals had the option to remain identifiable in some of their pilot projects.

Vodafone employ a range of techniques to reduce the risk of re-identification of their customers. The identifiers are hashed with an added code called salt. The salt codes are changed every month, and those who set the codes do not have access to the pseudonymous data, and vice versa, to prevent re-identification. The company tells us that all data is subject to strict organisational, contractual and security standards for handling, anonymisation and encryption, and the company and its vendors destroy the raw data as soon as the analysis is conducted. The analytics software aggregated the individuals in groups of at least ten handsets, and if fewer it would report "fewer than ten". This is intended to lower the risk of identification of individual mobile users.

Bypassing consent through anonymisation

The critical point made by all the three UK mobile companies involved in Big Data analytics is that they rely on the "anonymisation" of their customers' data to bring the data completely outside of any legal obligations in respect of privacy and data protection. Therefore, they don't need to ask their customers for consent. We believe that this is one area where the law has been either too slow or technically circumvented.

The companies rely on their interpretation of the E-Privacy regulations article (7)(1)(b),[67] which allows for traffic data to be processed if it is "modified so that it ceases to constitute personal data of that subscriber or user". This "de-identification" would also remove the data from the remit of the Data Protection Act.

We do not think companies can guarantee that the data they are using is fully anonymised, which means they should not be using it for analytics without asking for our consent. It is very difficult, if not impossible, for individual customers to assess whether their data has been anonymised or pseudonymised. Customers need to be able to trust companies and the ICO should ensure that independent audits are performed on the process.

It is difficult to anonymise rich datasets

There is a growing body of critical evidence questioning whether it is possible to anonymise rich datasets related to individuals.[68] In the case of mobile data analytics, the data being processed could be rich enough to allow for the singling out of individuals, particularly from location data.

We understand that mobile companies remove personal identifiers such as a customers' full names during the earlier stage of processing, or substitute these by a hash code. These "masking" and "pseudonymisation" techniques — as they are respectively called — are not strong protections. The ICO allows these techniques in their Code of Practice on Anonymisation, but cautions that they are "high risk" in terms of the re-identification of individuals.[69]

These techniques may hamper efforts attempts to identify individuals if data is released to

[67] http://www.legislation.gov.uk/uksi/2003/2426/regulation/7/made

[68] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

[69] http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/anonymisation-codev2.pdf

third parties.

Telefónica have created an organisational barrier that would make this re-identification harder, but this does not fully stop the risks from external information sources or analyses.

EE have argued in meetings and correspondence[70] that they do not need consent to produce marketing, research and analytics insights based on personal data because the end products are anonymised and do not involve personal data at that stage. But they also told us that they are able to check individual consumption if there is a query. The fact that the data can be linked back to a named account raises concerns that their "anonymisation" is simply a weak "pseudonymisation". This means that such data should probably be classed as personal data at this stage.

It's very difficult to anonymise location data

A person's location trace over a long period of time is completely unique and very hard to properly anonymise. The risks of re-identification of location data are potentially higher than for other forms of data. Research from MIT shows that four cell points in a mobile trace are enough to uniquely identify 95% of the individuals in a sample of 1.5 million people[71]. So industry claims that consent is not required because data is anonymised are hard to justify for location data.

The E-Privacy Regulations state that location data always requires consent for its processing, unless it is anonymised so the "user or subscriber cannot be identified from such data". The Article 29 Working Party opinion on location data puts it in clearer terms:

"Should service providers wish to keep a record of the locations of their service's users, they must first render the data anonymous"[72].

When the regulations were written, anonymisation was trusted blindly to protect location data. But this position is becoming untenable in the context of advances in both re-identification and Big Data.

Companies create pseudonymous profiles before they anonymise data

We agree that it appears that there is little risk of re-identification for individuals in the outcomes of the analytics provided to third parties we have seen from any of the companies. Companies use this to argue that the data they use for analytics is anonymised and therefore they do not need to ask for consent to use it. It seems very likely that at least in some cases these products and services involve creating databases with data that has not been fully anonymised. This data might include gender, age, postcode, location and traffic data, plus other enriching attributes that help make each dataset more unique to the individual.

There is a lack of clarity from the regulators, including the ICO in the UK, on how the anonymisation process should take place, which allows the companies to claim that they do not need consent and they comply with both the DPA and PECR.

Personal information that is not traffic data can be kept and processed within a company, subject to Data Protection Act principles. In most cases considered under the DPA anonymisation deals with the **disclosure** of personal information.

But PECR place restrictions on the **retention** and **storage** of traffic and location data in the first place. PECR does not explain how exactly should companies modify traffic data "so that they cease to constitute personal data of that subscriber or user". But it seems clear that PECR demand complete anonymisation — or erasure — of traffic data "when no longer

[70] https://wiki.openrightsgroup.org/wiki/Mobile_Provider_Responses_to_Mobile_Privacy_Action

[71] http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html

[72] Regulation 14(2)(a)

required for the purpose of the transmission of a communication", and similarly for location data.

We believe that it is reasonable to interpret this as a requirement that the data must be anonymised as a first step, before being processed any further, including linking it with demographic attributes into a profile without consent. Preventing these kinds of activities appears to be among the chief purposes of the legislation.

The Regulations do not explicitly ban the linking of personal and behavioural attributes with traffic and location data into a profile that is then de-identified through the removal or hashing of personal identifiers. But it is far from clear either that the **creation of pseudonymous profiles** without consent fully complies with PECR.

The role of the Information Commissioner's Office

The Information Commissioner's Office (ICO) has had conversations with the mobile companies about their analytics and so far found no objection to their activities. In relation to Telefónica's Smart Steps service, the ICO has publicly stated that, "so long as individual's (sic) personal information cannot be identified from this service, we don't have any problem with it."[73]

In our discussions with them, they repeated their view that only the identification of individuals in the final product matters not the use of individuals' data without consent before it is "anonymised" or more likely pseudonymised.

This is a very narrow view of the potential issues and fails to capture some of the emergent problems with the current legislation, and Big Data more generally

The ICO had some very sensible proposals in their original draft Code of Practice for Anonymisation, which unfortunately were removed from the final official version. They seem very useful as guidance for how mobile companies should conduct their anonymisation process. This guidance included the following:

> *"neither the anonymisation process — nor the use of the anonymised information — will have any direct detrimental effect on any particular individual;*
>
> *the data controller's privacy policy — or some other form of notification — explains the anonymisation process and its consequences for individuals; and there is a system for taking individuals' objections to the anonymisation process or to the release of their anonymised information into account. Note though that the DPA does not give individuals a general right to prevent the processing (including the anonymisation) of information about them. It is good practice though to respect individuals' objections where possible, and may be a requirement of the DPA where convincing reasons are present."*

Recommendations

E-Privacy legislation on traffic and location data needs to be updated to incorporate new concerns about the risks of anonymisation.

Companies should seek their customers' consent to process location data, even if it is 'anonymised'.

The ICO should look again into concerns with mobile analytics and work with industry and civil liberties organisations to develop a Code of Practice for the re-use of mobile data.

The ICO should investigate in detail the anonymisation processes of mobile companies and provide clear guidance on compliance with the E-Privacy Regulations.

The ICO should update its Code of Practice on anonymisation in the context of Big Data, reinstating the safeguards removed in the current version.

[73] http://www.bbc.co.uk/news/technology-19882647

CHAPTER 6: TRANSPARENCY

Mobile phone companies must be transparent about how they are using their customers' data. This is essential for the "fair processing of personal data" and for customers to be able to consent to the use of their data in an informed way.

All the companies involved in data analytics claim that transparency is critical and that they are informing their customers of what they do with their data. However, we would argue that saying that there is no need for consent undermines this claim.

The new General Data Protection Regulation (GDPR) brings stronger requirements for companies to provide clear information about their data practices

We looked at the information they provide to their customers about how data will be used in general, not just for Big Data analytics services.

We have carried out an analysis of the privacy policies of the major mobile operators, and the full breakdown is in the Appendix 2.

Privacy policies are not detailed enough

Transparency about the use of personal information is generally delivered through privacy policies. They work as part of the most common form of consent, which is to agree to privacy policies at the time of starting a new services or signing a contract.

In general, all of the companies' privacy policies are not detailed enough. Customers are not given enough information about what exact data is collected, and how their different types of personal data are being used. They tend to list a collection of personal data types and a collection of potential processing activities, without linking each type of data to particular activities.[74] See the Appendix for more details.

This is probably not detailed enough to comply with E-Privacy regulations, and it will almost be in breach of the new GDPR. There are similarities to Google's current privacy policy, where a disparate range of data is listed without enough information on what the company does with it. Google has been ordered to change its privacy policy by the ICO, because it is not specific enough to comply with current data protection legislation:

> *"In particular, we believe that the updated policy does not provide sufficient information to enable UK users of Google's services to understand how their data will be used across all the company's products."*[75]

As with the Google case, mobile data deals with a uniquely broad range of data and potential processing activities. Where there is such a lack of information, it is not possible for customers to give fully informed consent.

If privacy policies are not improved to account for the newer re-uses of data, the ICO should investigate, as it did with Google.

It is worth stressing that privacy policies can be both clear and detailed, for example with the layering of information at growing levels of granularity.

Inconsistencies between privacy policies and actual practices

Under the Data Protection Act, individuals have the right to request information that companies and organisations hold about them. These requests are known as Subject Access Requests (SARs). We asked ORG

[74] https://wiki.openrightsgroup.org/wiki/Mobile_Provider_Responses_to_Mobile_Privacy_Action

[75] http://www.ico.org.uk/news/latest_news/2013/ico-update-on-google-privacy-policy-04072013

volunteers to request their information from their mobile providers.

We found inconsistencies between the information the companies say they collect in their privacy policies and the information ORG volunteers received.

For example, Vodafone's privacy policy states that it records the websites you visit:

> *"We'll also get information on how you use our products and services, such as(…) Your website browsing information (which includes information about the websites you visit, and about how you use our website or other Vodafone Group websites on your mobile or a PC"* [76]

But in their response to a Subject Access Request, Vodafone said:

> *"Vodafone does not retain records of websites visited. In respect of websites operated by Vodafone, we do not hold records that can be linked to an identifiable individual or their account via cookies.* [77]

It is unclear whether Vodafone are making their privacy policy as wide as possible or are they failing to respond fully to SAR.

In some cases, the data collected may not match the description in the policy. EE names "types of websites"[78] but, as we understand from our conversations[79] with them, they actually store and process all http Internet traffic, including traffic from third party apps.

Personal data access requests should be easier

All the companies make data requests unnecessarily difficult.

Requests can be initiated via email, but invariably involve sending a letter by post. Mobile companies have online portals that give access to sensitive information, and requests for personal data could be made through these websites. This could include the uploading of identification documents.

Under current legislation SARs normally involve a payment of around £10 to cover the costs, although this is about to end when the new GDPR enters into force. Payments for SARs can only be made by cheque or postal order. Mobile companies can easily add the cost of a new handset to your next bill, so we cannot see why this is not possible with SARs.

The situation should be hugely improved by the GDPR, which in addition to improving access to personal information held by companies also includes a right to data portability. This should be an opportunity for mobile operators to overhaul their practices and not just aim for minimum compliance.

Customers can't see contracts until they have a credit check

ORG carried out a mystery shopper visit to several mobile phone shops. We were not allowed to see copies of any phone contract before we submitted to a credit check. Terms and conditions and privacy policies are generally available online. But the contract is where any opt-outs or explicit consents would be placed before signing up. This makes it harder than it should be to consider privacy when making a decision to join a mobile operator.

There is no legal obligation to provide potential customers with a contract until an offer is made and accepted. But this practice can have a detrimental effect. Credit reference agencies keep a record of such checks. If potential customers approach several mobile companies, the credit reference agencies will record several requests for credit. This is well known to have a negative impact in credit risk assessments.

[76] Found on http://www.vodafone.co.uk/about-this-site/our-privacy-policy/ Date accessed 10/02/2014

[77] Email sent to one of our supporters by Vodafone.

[78] http://explore.ee.co.uk/privacy

[79] Verbal communication during meeting with EE on 31/05/2013

Of course it is reasonable for mobile companies to check the credit status of their likely customers; however, it is also reasonable for customers not to have a list of credit checks just because they are trying to make an informed choice about the phone they want to buy.

Data sharing with third parties

Mobile companies should be transparent about how data is shared with third parties. For example, Weve[80] started a a joint venture of O2 (Telefónica UK), EE and Vodafone UK, which together represent 80% of the UK mobile market. Weve is now wholly owned by O2. Weve collates unspecified data from customers of O2 to produce marketing and research products. For example, they messaged specific demographic groups who lived near IKEA and used location data to check the effect on visits to the stores. This involved monitoring those who did not receive a message.[81]

Weve claim that all the data they use is based on consent, and in their website they provide for mechanisms to opt out of receiving their advertising by opting out of O2 marketing. However, they do not tell customers how to opt out of their data being used.[82] [83]

There is a need for more transparency about data projects like Weve, what they receive from mobile companies and who exactly is responsible for telling customers about them.

Reuse of billing data

Companies should be more transparent about how long they need to keep data for billing purposes.

They may retain traffic data for extended periods for billing purposes under the E-Privacy Regulations.[84]

The ICO guidance is clear that this should only apply to what is truly required for billing: "It does not permit the wholesale retention of such traffic data in every case".[85]

This means that a company does not have an automatic right to process billing data for other purposes — such as marketing products or 'value-added' services — without getting specific consent from customers. It is not clear that some of the companies are complying with this provision.

Using billing data for analytics may contravene principle 2 of the Data Protection Act,[86] which states that data should not be used for purposes incompatible with those it was collected for.

In addition, companies should clarify what kind of traffic data they keep for billing purposes — for example, is it necessary to keep data about browsing history in order to bill their customers.

Recommendations

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.
- Making contracts available before the point of sale;
- making marketing opt-outs simpler and allowing customers to opt out at the point of sale; and

[80] http://weve.com/products/mobile-marketing

[81] http://www.weve.com/showcase/ikea-drive-footfall-by-promoting-summer-sale/

[82] http://www.weve.com/news-views/the-what-how-why-of-our-data/

[83] https://twitter.com/weveuk

[84] http://www.legislation.gov.uk/uksi/2003/2426/made

[85] https://ico.org.uk/for-organisations/guide-to-pecr/traffic-data/

[86] http://www.ico.org.uk/for_organisations/data_protection/the_guide/principle_2

- Making subject access requests easier to make so that customers can better access, and therefore control, their personal data; and

- Clearly explaining how their analytics systems benefit their customers.

- The ICO should look into whether privacy policies account for the newer re-uses of data.

- The ICO should develop best practice guidance for how companies should implement their customers' right to stop their data being used. This guidance should suggest how customers can be given clear, regular and easy ways to opt out and should apply to all uses of location data, including analytics.

- Mobile phone companies should clarify whether they are keeping browsing data for billing purposes. If so, they should be clear about:
  (a) Why they need to keep that traffic data (particularly browsing histories)
  (b) how long they are keeping data for and
  (c) whether they are using that data for any other purposes other than billing.

CONCLUSION

The statement, "Data is the new oil' has been attributed to a number of marketeers, including Clive Humby, whose company Dunnhumby worked with Tesco to create the supermarket's ClubCard.

That was ten years ago. Today, this would be an unremarkable assertion; the importance of data for both businesses and governments is unquestioned. The vast majority of the UK population are carrying devices that are constantly generating data about their location, networks and interests. As frequently reported, this is going to increase exponentially with the expansion of the Internet of Things. We are already living in a world where household objects such as cars, TVs, and even children's toys, also create data that can be analysed and sold.

Marketing commentator Michael Palmer qualified Humby's statement in a 2006 blog: "Data is just like crude. It's valuable, but if unrefined it cannot really be used. It has to be changed into gas, plastic, chemicals, etc., to create a valuable entity that drives profitable activity; so must data be broken down, analyzed for it to have value."[87]

Just as most of us don't understand how crude oil is refined, the processes by which our data is analysed is not common knowledge. Indeed, as this report shows, it is virtually impossible for consumers to fully understand the risks involved in Big Data analysis. For example, it would be very difficult for a customer to gauge whether their data is being properly anonymised before it is being sold to third party organisations. In order for a customer to make an informed choice about this, companies have to make their techniques open and available for computer scientists to test them. As with Volkswagen emissions scandal, independent verification is needed.

Big Data is no longer the next big thing. It is here and now and we are all part of it. With this comes risks and an important new debate about privacy and security. The 2015 Talk Talk hack showed how vulnerable companies are when it comes to keeping our data secure and how much we take their word for it.

This needs to change. It's time for companies to come clean about how they are using and storing our data; it's time that we had a say in this.

The law needs to change and data regulators like the ICO need to step and take action to protect citizens. We urge companies to reognise that this is about more than compliance with the minimum legal requirements.

Companies who want to succeed in the Big Data age need to put consent at the heart of their relationship with customers.

[87] http://ana.blogs.com/maestros/2006/11/data_is_the_new.html

APPENDIX 1: LEGISLATION FOR THE USE OF MOBILE DATA

In the UK the data of mobile phone users is governed mainly by two pieces of legislation.

- The Data Protection Act 1998 (DPA), implements the EU Data Protection Directive 1995, and covers the collection and reuse of all personal data.
- The Directive is being superseded by the new General Data Protection Regulation. Below we set out some of the main changes. In this report we mainly refer to the current legislation under the Directive and DPA.
- The Privacy of Electronic Communications Regulations (PECR)[88] implement the EU E-Privacy Directive in the UK, and are limited to more specific issues such as marketing, location monitoring and surveillance of the use of mobile devices. The PECR treat traffic and location data separately, giving the latter special consideration.
- In the EU, sector specific legislation such as PECR usually takes precedence over more general legislation such as the DPA. But it is expected that all laws applicable should be consistent and do not contradict each other.
- For clarity and consistency, in this report we mostly refer to the legal requirements outlined in the DPA and PECR unless otherwise specified.

E-Privacy is stricter than general Data Protection on what companies can do with traffic data — including mobile phone and web usage — and location data. The general principle in the E-Privacy Directive is confidentiality of communications, where data required for providing a communications service should not be used freely. This data can provide intimate details about the user's life, as it will "contain information on the private life of natural persons and concern the right to respect for their correspondence".[89]

Below we set out how these laws regulate the use of personal, traffic and location data, and how mobile networks are currently complying with these laws.

Regulation of traffic data

Traffic data is automatically generated by electronic communications systems when a service is provided and billed for. This includes call data, such as the time, phone mast used, recipient and duration, and many other types of data generated by the communications equipment. Traffic data also includes Internet usage, such as websites visited and data transmitted by third party apps installed by smartphone users.

Some traffic data will be purely technical data that is used for the basic operation of telecoms equipment, but some, for example phone numbers that you have called, is personal data and should be covered by the DPA.

Personal data has to be processed fairly and lawfully, in accordance with the principles of data protection[90], and should only be used for the reasons it's been collected:

> *Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.*

In addition, all traffic data is specifically covered under Regulation 7[91] and Regulation 8[92] of the PECR. Regulation 7 makes clear that

[88] http://www.legislation.gov.uk/uksi/2003/2426/contents/made

[89] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN

[90] http://www.ico.org.uk/for_organisations/data_protection/the_guide/the_principles

[91] http://www.legislation.gov.uk/uksi/2003/2426/regulation/7/made

[92] http://www.legislation.gov.uk/uksi/2003/2426/regulation/8/made

in principle traffic data should be deleted or anonymised after a communication has taken place except to provide billing:

> *PECR 7. (1) Subject to paragraphs (2) and (3), traffic data relating to subscribers or users which are processed and stored by a public communications provider shall, when no longer required for the purpose of the transmission of a communication, be*
>
> *(a) erased;*
>
> *(b) in the case of an individual, modified so that they cease to constitute personal data of that subscriber or user;*

There are exceptions to this principle, for example, if companies get consent of the user.

Regulation of location data

Location data is more heavily regulated than traffic data because there it can reveal a lot about an individual's habits. There is more risk of it identifying someone, particularly when combined with any other information.

Vast amounts of location data are generated automatically as phone handsets constantly communicate with phone masts. Location data includes data that shows where and when a device is located and the direction it is travelling to. It is defined separately from traffic by the EU E-Privacy Directive as[93]:

> *"location data" means any data processed in an electronic communications network indicating the geographical position of the terminal equipment of a user of a public electronic communications service, including data relating to*
>
> *(f) the latitude, longitude or altitude of the terminal equipment;*
>
> *(g) the direction of travel of the user; or*
>
> *(h) the time the location information was recorded;*

The collection and processing of location data related to individuals is regulated by the general principles of the DPA because it is personal data. In addition, the PECR set out a stricter regime for location data that is not also classed as traffic data.

> *PECR 14. (1) This regulation shall not apply to the processing of traffic data.*
>
> *(2) Location data relating to a user or subscriber of a public electronic communications network or a public electronic communications service may only be processed—*
>
> *(a) where that user or subscriber cannot be identified from such data; or*
>
> *(b) where necessary for the provision of a value added service, with the consent of that user or subscriber.*

This is a loophole that a review of the Directive will need to address.[94]

National security and emergencies

The E-Privacy Directive places no restrictions on national governments to legislate for the processing of data for security purposes. Mobile companies can be required to retain communications data for up to 12 months to be accessed by security services, the police and other public bodies. The law does not expressly prohibit the use of this data for Big Data analytics, but companies seem to keep this data separately.

There are also provisions for data, including location, to be provided to emergency call centres. This data normally includes mast location, but in some cases it may include GPS data if the handset is enabled to transmit it.[95]

Data kept for law enforcement or emergencies should be stored separately and not used for analytics without consent.

[93] http://www.legislation.gov.uk/uksi/2003/2426/regulation/2/made

[94] http://neilzone.co.uk/masters/tel_theme_4_report.pdf

[95] http://samathieson.com/sa-mathieson/your-life-in-your-hands-mobile-phone-locating-of-999-calls/

APPENDIX 2: PRIVACY POLICIES

Accounts and Banking Data: Billing data, names, bank details, payment methods, billings history, invoices, credit fraud checks, telephone number, email address

Communications Data: incoming & outgoing calls, incoming & outgoing texts, cost of communications, date/time of communications, email communications, header information for emails, email addresses contacted

Internet & Application Use Data: Amount of data used, websites visited, record of company website visits, record of company services, use of mobile applications

Location Data: mobile's location during calls, location when accessing the Internet, IP address, unique phone identifier

Subscriber Notes: interaction of subscriber with customer service, subscriber's preferences, lifestyle choices, employment status, purchasing habits

This table shows the customer data collected as stated in the privacy policies available on their respective websites

Table 1

	Accounts & Banking Data	Communications Data	Internet & Application Use Data	Location Data	Subscriber Notes (Data)
EE	• Name • Gender • Date of birth • Telephone number • Email • Delivery/billing address • Credit/debit card details • Banking information • Billing history	• Numbers of incoming/ outgoing calls and messages • Date/time/duration/cost of communications • Use of voice messaging • Roaming information	• Browsing history • Browsing history on company's website • Date/time/duration of session on company website • Data usage • WAP/application use	• Phone location at time of incoming and outgoing communication • IP address • Roaming information	• Information on add-on products and services purchased • Preferences and interests ("both when you tell us what they are or when we deduce them from what we know about you") • Channel of device purchase • Purchasing habits and preferences • Demographic information • Information to help decide on products and services

Vodafone	• Name • Date of birth • Phone number • Email address • Address • Credit/debit card information • Bank account details • Other banking information • Dates of payments (owed and received)	• Numbers of incoming/ outgoing calls and messages • Date/time/duration of above communications • Level of network service	• Browsing history • Browsing history on company's and partners' website • Date/time/duration of session	• Phone location at time of incoming and outgoing communication • Phone location during Internet session	• Interactions with customer service • Preferences and interests ("both when you tell us what they are or when we deduce them from what we know about you") • Subscription services used
Three	• Name • Gender • Date of birth • Telephone and fax numbers • Email address • Current and previous address(es) • Credit/ debit card information • Bank information	• Contact history notes • Unique code identifying phone and SIM	Not specified	• Location data (not specified)	• Interactions with customer service
O2	• Name • Gender • Date of birth • Telephone number • Email address • Delivery/billing/ installation address • Debit/ Credit card details	• Call records • Text records • Date/time/cost of above communications	• Browsing history • Date/time of session • Internet use by customer	• Phone location at time of incoming and outgoing communication • GPS phone location when using specific O2 apps	• Activity with O2 account (top up, interaction with customer service, bill payments) • Checks if the subscriber has made changes in a services • Checks for subscriber interest

Table 3

	EE	Vodafone	Three	O2	Giffgaff
Credit Referencing, Identity Checks and Fraud					
Prevention of fraud or other crimes	√	√	√	√	√
Credit checks to process applications		√	√		
Give details to other companies for prevention of fraud			√		√
See if you qualify for credit				√	
Identity checks			√		
Debt tracing and debt recovery			√	√	√
Recover payments owed		√		√	√
Assign debt to debt collection companies			√	√	
Marketing and advertisement of products					
Inform customers of new products and services, changes to products and services	√	√	√	√	√
Inform customers on products of third party	√	√	√	√	√
Inform customers of changes in terms and conditions	√				
Analyse use of services, cookies and others in order to offer tailored services and market specific products to customers	√	√		√	√
Pass on information to third parties for market analysis	√		√		√
Aggregated information on customer usage of services for market analysis of specific company services	√	√	√	√	√
Comply with laws and regulations on the protection of customers and law enforcement	√		√		
General administration of services and products					
To enable the provision of services and general account processes	√	√	√		
Process orders, registrations and deliveries or other services	√	√	√	√	
Investigate complaints or requests	√	√	√	√	√
recover payments		√		√	√
Track location to ensure network coverage or "other services"	√	√	√		

OPEN
RIGHTS
GROUP

Open Rights Group

www.openrightsgroup.org

+44 20 7096 1079

Open Rights is a non-profit Company Limited by Guarantee, registered in England and Wales no. 05581537