**Planning and Interim Report**

**“Research into data retention and how geolocation data could be analysed and visualised”**

**Introduction**

The use of geolocation technology is currently a big thing in the mobile industry, with hugely popular apps like Tinder, Waze and Nike+ Running all purely based on geolocation. With an app like Waze that has over 50 million installs on android alone (Google Play Store, 2015) it can be said that geolocation technology can be a powerful tool. With more and more apps starting to include geolocation technology it appears that soon there will be huge amounts of geolocation data stored about individual users. This provokes me to research into way geolocation data is currently analysed and how it could be analysed. The idea to look into the analysis of geolocation data stems from a TED talk by Malte Spitz (TED, 2012), a German Green Party politician, in 2012. The talk “Your phone company is watching” looks into how cell phone companies are collecting data on their users due to the EU Data Retention Directive commissioned in 2006. I highly recommend spending 10 minutes watching Malte Spitz’s TED talk - [*https://www.ted.com/talks/malte\_spitz\_your\_phone\_company\_is\_watching?language=en*](https://www.ted.com/talks/malte_spitz_your_phone_company_is_watching?language=en).

**“Your phone company is watching”**

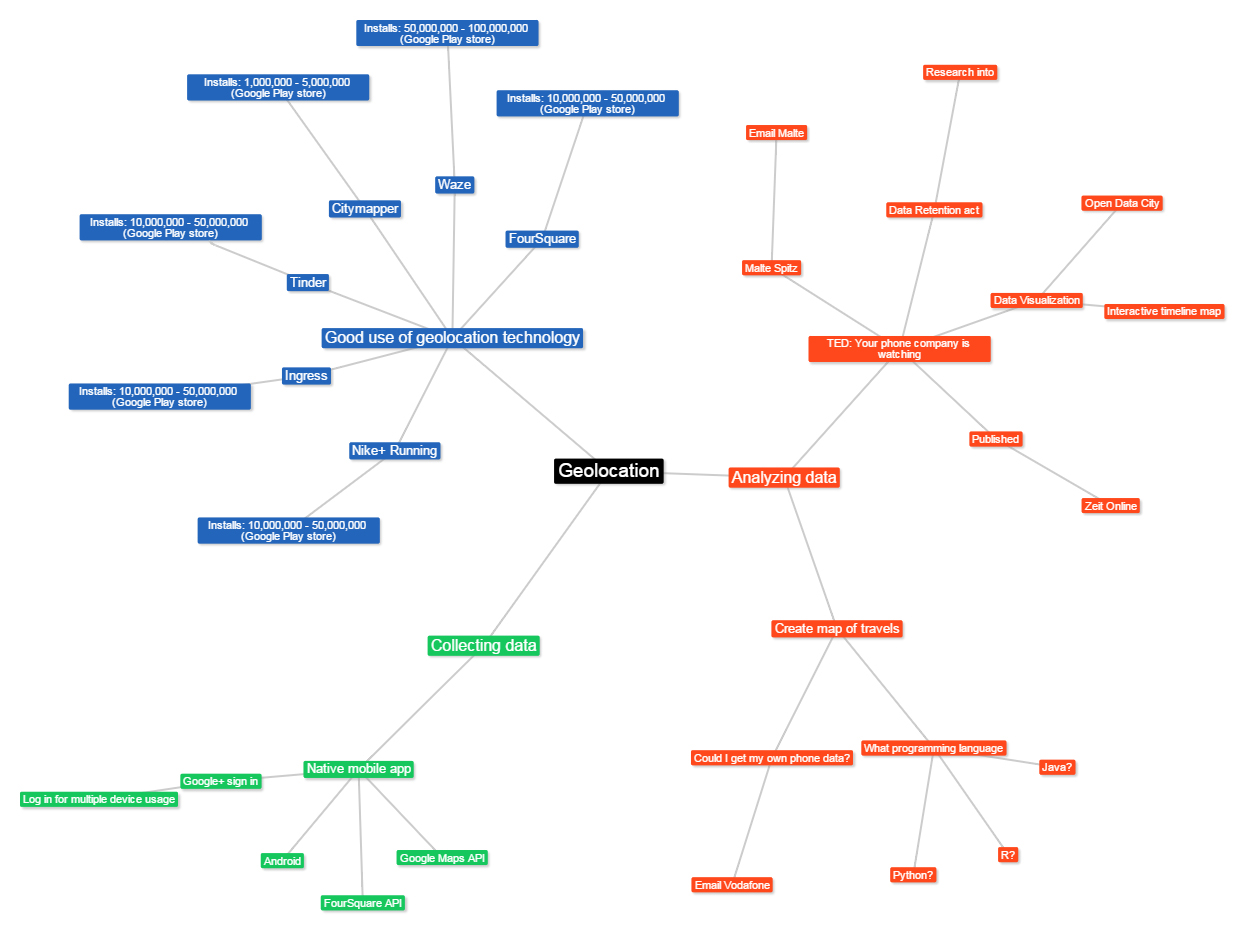
Malte Spitz’s had go to court to gain access to his own data, which was resolved “because in the meantime, the German Constitutional Court ruled that the implementation of this E.U. directive into German law was unconstitutional” (Spitz, 2012) . Spitz received roughly 35,000 lines of data after agreeing to drop the law suit. These 35,000 lines of data were a record of 6 months of Spitz life every single one with geolocation co-ordiantes. Von Kai Biermann, a journalist and author wrote an article about Spitz’ findings for Zeit Online that was titled “Betrayed by our own data” (Biermann, 2011). In this article Biermann talks about the potential power this data could have and how it could be utilised.

*“The real snitch is in our pocket – our own mobile phone betrays us. That’s why the*[*Chaos Computer Club*](http://www.zeit.de/thema/chaos-computer-club)*has rechristened the powerful mini-computers we carry around with us as "tracking devices" revealing where we’ve been and what we’ve been doing.” –* Please see Appendix 1 for more information.

Biermann describes how the consumer of this data could use it to make a profile on Spitz, stating that this kind of profile "reveals an entire life”. Spitz teamed up with Open Data City, a data visualisation company, and Zeit Online, a national news distributor, to produce a visualisation of what the data Spitz received actually showed. In Spitz own words “This is a visualization of six months of my life. You can zoom in and zoom out, you can wind back and fast forward. You can see every step I take. And you can even see how I go from Frankfurt by train to Cologne, and how often I call in between.” You can see the interactive map at <http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten>. This interactive map shows the power in geolocation data, you can see where Spitz was at any moment within those 6 months, when he walked, when he took a train, got on a plane, where he slept, even where he like to spend his leisure time in a beer garden.

**Project Idea**

From Spitz talk I felt inspired to look into geolocation technology and the data it records. This then provoked me to look deeper into geolocation, looking at how it has been utilised, how you can collect it, how it can be analysed, how it can be displayed/visualised. The following mind map shows my thought process of the route in which the project could go down.



First of all I looked into what applications utilise geolocation well and depend on it. For example Tinder that has over 10 million downloads on android alone (Google Play Store, 2014) is primarily a dating mobile application. However it heavily relies geolocation technology as the app would not be able to show people local to you who are also on Tinder, one of the key aspects that made it so successful. Some other apps I researched into were:

* *Ingress*, a mobile game that requires the player to be in a certain location to interact with the game world that is mapped to the real world. It has over 10 million downloads on android alone (Google Play Store, 2014)
* Previously mentioned *Waze* or *Waze Social GPS Maps & Traffic*, is a mobile applicationthat makes a social traffic and GPS network for drivers, allowing you to post hazards, accidents, find best routes, find the cheapest fuel price and inform friends of your location and arrival time. “Waze is all about contributing to the 'common good' out there on the road.” (Waze, 2015). It has over 50 million downloads on android alone (Google Play Store, 2009)
* *CityMapper*, “The Ultimate Transport App - Our mission: Make cities easier to use. We're reinventing the transport app for the world's most complicated cities.” (Citymapper, n.d.) I personally found this app a huge help whilst living in London. It accesses travel API’s to give live data about train and bus arrival times and delays. It also offers directions and various routes from current location to desired location. It has won multiple awards since 2013 including runner up in Apple’s App of the year. The only flaw is it’s only within certain cities but is ever expanded adding the world’s biggest cities. Expect this one to rise in downloads sharply, it has over 1 million downloads on android alone (Google Play Store, n.d.)

My second thought was to make an android mobile application that would collect geolocation data on the user as they travelled the world with their phone, effectively making their phone a GPS tracker. I was set on making an application until I realised I was implementing a mobile application just to access data so I could manipulate it. This then put me on the route of using already collected geolocation data and seeing how it can be analysed and visualised. I then went back to Spitz report and found the data he received is publicly available, (<https://spreadsheets.google.com/ccc?key=0An0YnoiCbFHGdGp3WnJkbE4xWTdDTVV0ZDlQeWZmSXc&hl=en_GB&authkey=COCjw-kG>) I plan to use his data to show different ways this data can be interpreted and visualised. After I realised this I emailed Malte Spitz and I am currently still in contact with him, later in the project I will evaluate mine and his conversation. To see my initial email to Malte Spitz please see appendix 3.

**Aims and Objectives**

My first aim for my final year project is to research what data retention laws are currently or were previously in affect in the United Kingdom, where I live and therefore affect me. I will do this by looking through the various legislations and acts the United Kingdom have passed about data retention. I will also ask my telephone company, Vodafone, in an attempt to attain all the data they have stored on me, if there are any data retention laws in current affect in the United Kingdom.

My next aim is to research into the different methods of big data analysis and data visualisation tools. This will help me to create visualisations of the data Spitz attained, these data visualisations will hopefully go beyond Spitz’s interactive map and expose how powerful the geolocation data can be if analysed in different ways.

**Methodologies**

There are many pieces of software available on the web to create data visualisation. I will need to research into what is capable within these pieces of software, however if they do not meet my requirements I may have to write some code to display the data in the way I need. As I begin to understand these programmes I will be able to make an informed decision on which to use for the project, for now I have a short list of the potential software I could use for data visualisation:

1. InstantAtlas
2. Modestmaps
3. Visualize Free
4. Openlayers 3
5. Google Charts
6. Kartograph
7. CartoDB

**Research**

**So what is Data Retention?**

In the journal “Computer Law & Security Review” Maria Eduarda Gonçalves said:

*“Directive 2006/24/EC aims to harmonize rules on data retention across member states in order to ensure the availability of traffic data for anti-terrorism purposes, in case of investigation, detection and prosecution of this crime. Operators are obliged to retain a broad range of data between 6 and 24 months from the date of communication, and provide to the competent national authorities without undue delay, if requested, incoming and outgoing phone numbers fixed and mobile, the duration of phone calls, IP address, log-in and log-off times and e-mail activity details."* – Please see appendix 2 for more information.

Spitz sums up the directive in a simplified and slightly more direct manner.

*“This directive [is] called Data Retention Directive. This directive says that each phone company in Europe, each Internet service company all over Europe, has to store a wide range of information about the users. Who calls whom? Who sends whom an email? Who sends whom a text message? And if you use your mobile phone, where you are. All this information is stored for at least six months, up to two years by your phone company or your Internet service provider.”* (Spitz, 2012)

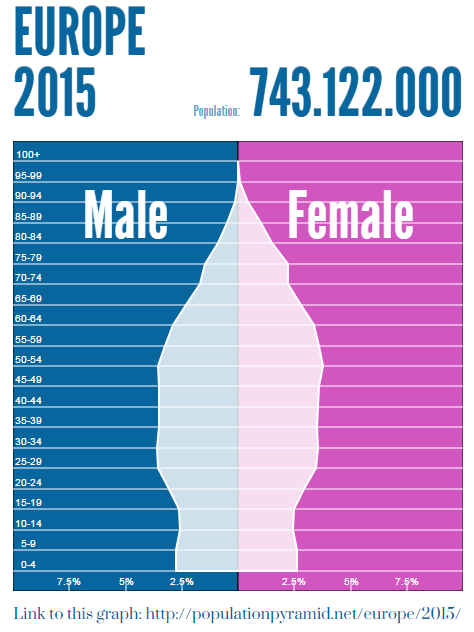
Both Gonçalves and Spitz are referring to the Data Retention (EC Directive) commissioned by the EU on the 15th March 2006 (EUR-LEX, 2006), the United Kingdom passed their Data Retention Regulations in 2007 (Legislation.gov.uk, 2007). The German law implementing the Directive was passed in 2008 and put into immediate effect. Then in 2010 “The German Federal Constitution Court ruled, that the law passed violates the rights to privacy that citizens are guaranteed under the German constitution” (Out Law, 2010). This meaning the law implementing the Directive was ruled unconstitutional by the Court, this is what helped Spitz attain his data before it was deleted. Then in 2014 the Court of Justice of the European Union declared the Data Retention Directive to be invalid (Court of Justice of the European Union, 2014). In the annulment of an EU Directive it is down to each individual nation/state to evaluate the case at hand and then decide on changing the laws they have in current affect.

“A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods” (EUR-Lex.europa.eu, n.d.)

At current, November 2015 the German parliament passed a law “requiring telecoms and Internet companies to store customers' metadata and to make it available to law enforcement agencies investigating "severe crimes.” (arstechnica, 2015), which sounds incredibly similar to that of the first law back in 2008. The main changes to this new law are the time limits the data is held and what must be required to access this data. The law is expected to have the length the data is stored greatly reduced from previously 6 - 24 months to 10 weeks for all most information stored, however geolocation data will only be stored for only 4 weeks. Also the law is stating the information must be stored on German soil. This second bid for data retention in German shows that the government still want this data but understand the first laws for data retention were too generic leaving them open to interpretation. Now the laws are being more explicit and the increase in the security of this data and the length it’s stored for have all been addressed I could see data retention coming back to German in the very near future.

**Who was affected by the Data Retention Directive commissioned in 2006?**

Let’s step back to 2010 when Spitz was trying to attain his data. At that time this type of data was being stored on everyone in Europe as the Court of Justice of the European Union had not yet declared the Data Retention Directive to be invalid. The scariest thing about this data retention was not constricted to smartphone users but all mobile phone users. As the data stored was geolocation of calls, texts and internet access this means even phones like the Nokia 3310, which was released in the year 2000, could have this information tracked by the phone service provider. This means that everyone in Europe with a mobile phone will be having this information tracked and stored about them by their phone companies. Now if we apply the directive from 2010 to current time, 2015. There are currently 743,122,000 people that live in Europe (Pyramids, 2015). What’s the average age a child owns a mobile phone? This data is not the easiest to attain but back in 2013 the Mirror posted an article saying the average age a child owns a mobile phone is 11 years old (Mirror, 2013). If anything in the last 2 years the digital age has furthered itself and the increase in handheld devices the average age is more likely to be around 9 years old. Next we have the older generation, how many adults over the year of 65 own a mobile phone? Pew Research Center in April 2012 reported that “77% of older adults have a cell phone” (Pew Research Center, 2014). Below shows the population pyramid of Europe as of this year, 2015. Using that we can see the percentage of the population within certain age ranges.



We’ve estimated the age a child owns their first phone is 9 years old. Looking at the graph under 9 years old is roughly 5% for boys and the same for girls so 10% overall for children under 9 years old. Next you have the over 65 year olds. I see it as the following table:

|  |  |  |  |
| --- | --- | --- | --- |
| Male | | Female | |
| 65-69 | 2.25% | 65-69 | 2.3% |
| 70-74 | 2% | 70-74 | 2.2% |
| 75-79 | 1.5% | 75-79 | 1.8% |
| 85-89 | 0.75% | 85-89 | 1.3% |
| 90-99 | 0.1% | 90-99 | .5% |
| Total | 6.6% | Total | 8.1% |

So of the total population we have 6.6% males and 8.1% females over 65 years old, combining them to be 14.7% of over 65 year olds in Europe. Now we take into account the Pew Research Center report that states “77% of older adults have a cell phone”. So let’s calculate how many over 65 year olds do not own a phone, 23% of over 65 year olds. 14.1/100\*23 = 3.243 rounded up to 3.25% of over 65 year olds that don’t own a phone.

As I stated earlier this is not exclusive to smart phones but any phone, including house phones not just mobiles. Because of this I am assuming that everyone between the ages of 9 and 65 own a phone. So we have 10% under 9 year olds and 3.25% over 65 years old meaning 13.25% of Europe’s population don’t own mobile phone. So the remaining 86.75% which as of 2015 is equal to **644,658,335** people would have their geolocation data being stored about them every time they send/receive a call/text, every time they tweet, post, share or access the internet. Now that’s a lot of information on majority of Europeans.

Now you might be thinking that this is not relevant since the Court of Justice of the European Union declared the Data Retention Directive to be invalid. However as I mentioned before after the annulment of an EU Directive it is down to each individual nation/state to evaluate the case at hand and then decide on changing the laws they have in current affect.

**Final thoughts**

It seems to me that data retention will in the near future be affecting large amounts of the world population if it is not already affecting them. Therefore for my final year project I plan to continue researching into data retention and how it affects me as a United Kingdom citizen. I will also take the data Spitz attained and use it to show the power in geolocation data, which I will do with data visualisation. I will also look at what kind of visualisation could be possible with only subsets of the data, again showing the value of geolocation data even if it is just on its own. I will research into data visualisation tools to gain knowledge on which tools will be most productive for the task at hand. Overall this should allow me to produce an in-depth report on data retention laws, how they affect the general public and the geolocation data the laws allow governments to collect on their citizens.

**SCHOOL OF COMPUTING, ENGINEERING & MATHEMATICS ETHICS FORM**

This ethics form is designed to help you quickly and easily identify how you should approach any ethical issues raised by your project or dissertation. It should be completed for ALL research projects and dissertations prior to the commencement of the project. Please do not approach any participants involved in the research until this have been completed and discussed with your supervisor or member of the CEM ethics committee (if appropriate).

This form must be completed by the project student or researcher responsible for the project. Once completed, you should discuss it with your supervisor to ensure that you take the right follow-up actions.

**If you answer ‘No’ to all questions** **in this form and this is confirmed with your supervisor (if appropriate) then no further action is required.** Please note that in signing this form you accept that it is still your responsibility for your project or dissertation module to follow the **University’s Guidance on Good Practice in Research Ethics and Governance**, available on StudentCentral. Any significant change in the question, design or conduct of your project or dissertation that would alter your answers on this form must be notified to your supervisor who will advise you on whether you need further action.

**If you have answered ‘yes’ to *any* of the questions in Section B of the Student Checklist your supervisor will need to make a judgment as to whether or not the research includes more than a minimum level of risk. If this is the case then your supervisor will need to email this form to the CEM ethics committee (**[**CEMethics@brighton.ac.uk**](file:///C:\Users\jmc21.UNIVERSITY\Documents\NEW\Modules\CI301\Handbook%20current\CEMethics@brighton.ac.uk)**) for discussion prior to the commencement of research**.This does not mean that you will not be able to do the research, but it will need to be considered by the School Research Ethics and Governance Committee.

Ethics forms, example consent forms/participant information sheets and supporting guidance are available on the ***Research Ethics for Projects – CEM*** area of StudentCentral.

**Signed copies of this completed ethics form must be submitted with your project or dissertation. Note: the project or dissertation will not be marked if the completed checklist is not included.**

**PROJECT DETAILS**

1. Name of researcher: **Philip Lee**

2. Name of supervisor: **Gerard Alsop**

3. Title of project:

**Research into data retention and how geolocation data could be analysed and visualised**

4. Outline of the research (up to 100 words):

**A study** **into data retention laws and legislations and how they affect me as a United Kingdom citizen. A look into what data retention actually means. Research into how much information geolocation data can reveal and how this geolocation data can be analysed and visualised.**

5. Location of research: **On campus**

8. Email address: **P.lee6@uni.brighton.ac.uk**

9. Contact address: **Jubilee Villa, Playden, Rye, East Sussex, TN31 7PN**

10. Telephone number: **07540960156**

| **Please tick the appropriate box and answer the questions where appropriate.** | Yes | No |
| --- | --- | --- |
| 1. Does the study involve **participants who might be considered vulnerable** due to age or to a social, psychological or medical condition? (*e.g. children, people with learning disabilities or mental health problems, but participants who may be considered vulnerable are not confined to these groups).*   If yes then provide details of any such participants. See the University’s ‘Guidance on Good Practice in Research Ethics and Governance’ for more details.  ……………………..……………………..……………………..……………………..………..……………………..………..  ……………………..……………………..……………………..……………………..………..……………………..………..  Note: proposals involving vulnerable participants are often likely to require ethical approval from the Faculty of Science & Engineering Research Ethics and Governance Committee (FREGC). |  | x |
| 1. Will **photographic or video recordings** of research participants be collected as part of the research?   If yes then please outline consent and data protection procedures *(e.g. interviews cannot be overheard, details will not be accessible to others),* for the use of participants’ images. Example consent and information forms can be found on StudentCentral and see guidance on data collection at the end of this document.  ……………………..……………………..……………………..……………………..………..……………………..………..  ……………………..……………………..……………………..……………………..………..……………………..………..  If your data will not be confidential and anonymous then outline the justification for this decision here and procedures for mitigating against potential harm.  ……………………..……………………..……………………..……………………..………..……………………..………..  ……………………..……………………..……………………..……………………..………..……………………..……….. |  | x |
| 1. Does the study require the **co-operation of an individual to gain access** to the participants? (*e.g. a teacher at a school or a manager of sheltered housing)*   If yes then describe the procedures that will be put in place to ensure safe and ethical direct involvement of human participants. Where necessary and as appropriate, include comments on obtaining informed consent, reducing harm, providing feedback, and accessing participants through an individual providing information such as a teacher/lecturer, manager, employer etc. Example consent and information forms can be found on StudentCentral.  ……………………..……………………..……………………..……………………..………..……………………..………..  ……………………..……………………..……………………..……………………..………..……………………..……….. |  | x |
| 1. Will the participants be asked to discuss what might be perceived as **sensitive topics** (*e.g. sexual behaviour, drug use, religious belief, detailed financial matters) or* could participants experience psychological stress, anxiety or other negative consequences (beyond what would be expected to be encountered in normal life)?   If yes then describe the procedures that will be put in place to ensure safe and ethical direct involvement of human participants. Where necessary and as appropriate, include comments on obtaining informed consent, reducing harm, providing feedback. Example consent and information forms can be found on StudentCentral.  ……………………..……………………..……………………..……………………..………..……………………..………..  ……………………..……………………..……………………..……………………..………..……………………..……….. |  | x |
| 1. Will individual participants be involved in **repetitive/prolonged testing or vigorous physical activity, experience pain of any kind, or be exposed to dangerous situations, environments or materials** as part of the research?   If yes then describe the procedures that will be put in place to ensure safe and ethical direct involvement of human participants. Where necessary and as appropriate, include comments on obtaining informed consent, reducing harm, providing feedback. Example consent and information forms can be found on StudentCentral.  ……………………..……………………..……………………..……………………..………..……………………..………..  ……………………..……………………..……………………..……………………..………..……………………..……….. |  | x |
| 1. Will members of the public be **indirectly involved** in the research without their knowledge at the time? (*e.g. covert observation of people in non-public places, the use of methods that will affect privacy)*.   If yes then provide brief details here *(e.g. how they will be involved and, where known, the age, gender, ethnicity and location of those who will be indirectly involved).*  ……………………..……………………..……………………..……………………..………..……………………..………..  ……………………..……………………..……………………..……………………..………..……………………..………..  `  Provide details of any negative impacts members of the public will be likely to face and that would not be considered minimal impacts (e.g. invasion of privacy, harm to property, being subject to what an individual perceives to be inappropriate behaviour). Describe the risks and if appropriate explain why you believe they are only minimal.  ……………………..……………………..……………………..……………………..………..……………………..………..  ……………………..……………………..……………………..……………………..………..……………………..………..  Describe any procedures that will be put in place to ensure safe and ethical indirect involvement of members of the public (*e.g. providing information and feedback if requested by the public*). Examples of participation information forms can be found on StudentCentral.  ……………………..……………………..……………………..……………………..………..……………………..………..  ……………………..……………………..……………………..……………………..………..……………………..………..  Describe how you will ensure data collection is confidential and anonymous (*e.g. people will not be able to be identified by photographs or notes taken by observers*), how data will be stored and who will have access to the data. If the data will not be confidential or anonymous, outline the justification for this decision here and procedures for mitigating against potential harm.  ……………………..……………………..……………………..……………………..………..……………………..………..  ……………………..……………………..……………………..……………………..………..……………………..……….. |  | x |
| 1. Does this research include **secondary data** that may carry personal or sensitive organisational information? *(Secondary data refers to any data you plan to use that you did not collect yourself, e.g. datasets held by organisations, patient records, confidential minutes of meetings, personal diary entrie).*   If yes then provide details regarding any secondary data to be used that may carry sensitive personal or organisational information.  ……………………..……………………..……………………..……………………..………..……………………..………..  ……………………..……………………..……………………..……………………..………..……………………..………..  If secondary data CEMs containing sensitive personal or organisational information are to be used, outline how such use will be ethically managed *(e.g. details such as anonymising data CEMs, ensuring protection of source agency, gaining consent of data owners, and how the data will be stored)*. See guidance on data collection at the end of this document.  ……………………..……………………..……………………..……………………..………..……………………..………..  ……………………..……………………..……………………..……………………..………..……………………..……….. |  | x |
| 1. Is this research likely to have significant **negative impacts on the environment**? (*For example, the release of dangerous substances or damaging intrusions into protected habitats.)*   If yes then provide details of these impacts here (for example the release of dangerous substances or damaging intrusions into protected habitats) and  ……………………..……………………..……………………..……………………..  ……………………..……………………..……………………..……………………..  Describe how you will mitigate against significant environmental harm and manage risks.  ……………………..……………………..……………………..……………………..  ……………………..……………………..……………………..…………………….. |  | x |
| 1. Will any participants receive **financial reimbursement** for their time? (*excluding reasonable expenses to cover travel and other costs*).   If yes then provide details and a short justification (e.g. amounts and form of reimbursement).  ……………………..……………………..……………………..……………………..………..……………………..………..  ……………………..……………………..……………………..……………………..………..……………………..……….. |  | x |
| 1. Are there any **other ethical concerns** associated with the research that are not covered in the questions above?   If yes then give details here.  ……………………..……………………..……………………..……………………..………..……………………..………..  ……………………..……………………..……………………..……………………..………..……………………..……….. |  | x |

**All Undergraduate and Masters level projects or dissertations in the School of CEM must adhere to the following procedures on data storage and confidentiality.**

All data should be encrypted and stored securely. Documentation should be kept in a locked cabinet or desk, and electronic data should preferably be kept on a removable disk or data stick which can be locked away, or if this is not possible on a password protected computer. Confidential and sensitive data should not be emailed unless it is encrypted or password protected since emails are centrally archived.

For Undergraduate/Masters projects, normally only the student and supervisor will have access to the data (see the University’s ‘Guidance on Good Practice in Research Ethics and Governance for further details).Once a mark for the project or dissertation has been published, all data must be removed from personal computers, and original questionnaires and consent forms should be destroyed unless the research is likely to be published or data re-used. If this is the case a justification for this should be included where appropriate in this form and in the relevant consent and participant information forms.

**Student:** Please sign below to confirm that you have completed the Ethics form and will adhere to these procedures on data storage and confidentiality.

Signed (**Student**): P J LEE

Date: 19/11/2015

**Supervisor**: I confirm that the research ***does/does not*** (delete as applicable) include more than a **minimum level of risk**.

Signed (**Supervisor**): ………………..………..……………………..…….

Date: ………………..………..……………………..………..

Note: If the **supervisor judges** that there is more than the **minimum level of risk** then your supervisor will need to email this form to the CEM ethics committee ([CEMethics@brighton.ac.uk](file:///C:\Users\jmc21.UNIVERSITY\Documents\NEW\Modules\CI301\Handbook%20current\CEMethics@brighton.ac.uk)) for discussion prior to the commencement of research.

**Appendix 1**

“The seminal electronic band Kraftwerk was well ahead of the curve musically, but even the lyrics to their 1981 song "Computerwelt" can seem uncannily prescient. "Interpol and Deutsche Bank, FBI and Scotland Yard, [Flensburg](http://www.zeit.de/thema/flensburg) and the BKA, they’ve got all our data squirreled away." What was unimaginable 30 years ago later sounded rather threatening. But today, the words are downright silly.

While government authorities like the BKA, Germany’s Federal Office of Criminal Investigation, (and the country’s database of traffic violations in Flensburg) do indeed have a trove of information about us, the greatest source of data about our lives is much more banal. The real snitch is in our pocket – our own mobile phone betrays us. That’s why the [Chaos Computer Club](http://www.zeit.de/thema/chaos-computer-club) has rechristened the powerful mini-computers we carry around with us as "tracking devices" revealing where we’ve been and what we’ve been doing.

In a [report prepared for Germany’s Constitutional Court in July 2009](http://www.ccc.de/vds/VDSfinal18.pdf) , the hacker group described what kind of information could in theory be collected according to the country’s data retention (Vorratsdatenspeicherung) rules and what could be gleaned from it. The court later stopped data retention as it was practiced at the time, but law enforcement officials and the government have by no means abandoned the concept. The possibilities offered by such seemingly harmless data are just too seductive. In the next few weeks, the German government is set to decide on new data retention rules.

Most people’s understanding of what can actually be done with the data provided by our mobile phones is theoretical; there were few real-world examples. That is why Malte Spitz from the German Green party decided to publish his own data collected from August 2009 to February 2010. However, to even access the information, he had to file a suit against telecommunications giant Deutsche Telekom.”

(Biermann, 2011)

**Appendix 2**

# Security policies and the weakening of personal data protection in the European Union

“Directive 2006/24/EC (the Data Retention Directive) imposing strengthened obligations on telecommunications operators to collect and store data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.[11](http://www.sciencedirect.com.ezproxy.brighton.ac.uk/science/article/pii/S0267364913000629#fn11)

Directive 2006/24/EC aims to harmonize rules on data retention across member states in order to ensure the availability of traffic data for anti-terrorism purposes, in case of investigation, detection and prosecution of this crime. Operators are obliged to retain a broad range of data between 6 and 24 months from the date of communication, and provide to the competent national authorities without undue delay, if requested, incoming and outgoing phone numbers fixed and mobile, the duration of phone calls, IP address, log-in and log-off times and e-mail activity details.

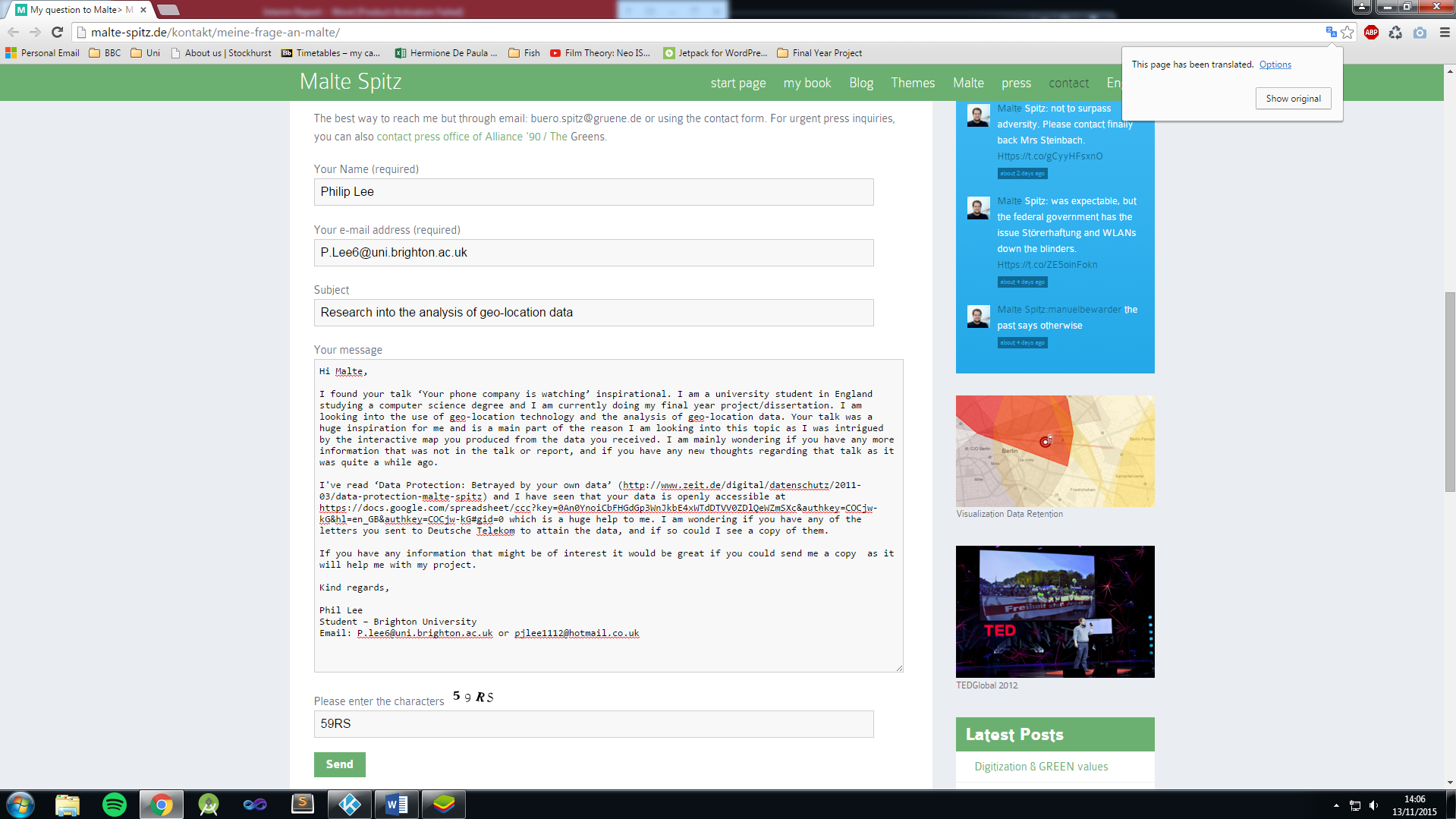
In sum, personal data are more and more recorded, exchanged and retrieved at a European and at an international scale involving police and security systems as well as private entities such as telecommunications operators and aircraft companies.[12](http://www.sciencedirect.com.ezproxy.brighton.ac.uk/science/article/pii/S0267364913000629#fn12)

In fact, all the legal acts mentioned above have been adopted with security interests in mind. They display a widespread trend in Europe for preventive storage of personal data of all individuals, independently of any suspicion of committing a crime, with clear detrimental effects on the effectiveness of personal data protection principles and rights.”

(Gonçalves, 2013)

**Appendix 3**

**Email to Malte Spitz –** [**http://malte-spitz.de/kontakt/meine-frage-an-malte/**](http://malte-spitz.de/kontakt/meine-frage-an-malte/)



Email transcribe

Hi Malte,

I found your talk ‘Your phone company is watching’ inspirational. I am a university student in England studying a computer science degree and I am currently doing my final year project/dissertation. I am looking into the use of geo-location technology and the analysis of geo-location data. Your talk was a huge inspiration for me and is a main part of the reason I am looking into this topic as I was intrigued by the interactive map you produced from the data you received. I am mainly wondering if you have any more information that was not in the talk or report, and if you have any new thoughts regarding that talk as it was quite a while ago.

I've read ‘Data Protection: Betrayed by your own data’ (http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz) and I have seen that your data is openly accessible at https://docs.google.com/spreadsheet/ccc?key=0An0YnoiCbFHGdGp3WnJkbE4xWTdDTVV0ZDlQeWZmSXc&authkey=COCjw-kG&hl=en\_GB&authkey=COCjw-kG#gid=0 which is a huge help to me. I am wondering if you have any of the letters you sent to Deutsche Telekom to attain the data, and if so could I see a copy of them.

If you have any information that might be of interest it would be great if you could send me a copy as it will help me with my project.

Kind regards,

Phil Lee

Student – Brighton University

Email: P.lee6@uni.brighton.ac.uk or pjlee1112@hotmail.co.uk

**Bibliography**

arstechnica, 2015. *German parliament passes new, comprehensive data retention law.* [Online]   
Available at: http://arstechnica.co.uk/tech-policy/2015/10/german-parliament-passes-new-comprehensive-data-retention-law/  
[Accessed 16 November 2015].

Biermann, V. K., 2011. *Zeit Online - Betrayed by our own data.* [Online]   
Available at: http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz  
[Accessed 10 November 2015].

Citymapper, n.d. *Citymapper.* [Online]   
Available at: https://citymapper.com/london/about  
[Accessed 1 November 2015].

Court of Justice of the European Union, 2014. *The Court of Justice declares the Data Retention Directive to be invalid.* [Online]   
Available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf  
[Accessed 16 Novemeber 2015].

EUR-Lex.europa.eu, n.d. [Online]   
Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12002E249:EN:HTML  
[Accessed 16 Novemeber 2015].

EUR-LEX, 2006. *EUR-LEX.* [Online]   
Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006L0024  
[Accessed 13 November 2015].

Gonçalves, M. E., 2013. Security policies and the weakening of personal data protection in the European Union. *Computer Law & Security Review,* 29(3), pp. 255-263.

Google Play Store, 2009. *Google Play.* [Online]   
Available at: https://play.google.com/store/apps/details?id=com.waze&hl=en\_GB  
[Accessed 1 November 2015].

Google Play Store, 2014. *Google Play.* [Online]   
Available at: https://play.google.com/store/apps/details?id=com.tinder&hl=en\_GB  
[Accessed 1 Novemeber 2015].

Google Play Store, 2014. *Google Play.* [Online]   
Available at: https://play.google.com/store/apps/details?id=com.nianticproject.ingress&hl=en\_GB  
[Accessed 1 Novemeber 2015].

Google Play Store, 2015. *Google Play Store.* [Online]   
Available at: https://play.google.com/store/apps/details?id=com.waze  
[Accessed 3 November 2015].

Google Play Store, n.d. *Google Play.* [Online]   
Available at: https://play.google.com/store/apps/details?id=com.citymapper.app.release  
[Accessed 1 November 2015].

Legislation.gov.uk, 2007. *The Data Retention (EC Directive) Regulations 2007.* [Online]   
Available at: http://www.legislation.gov.uk/uksi/2007/2199/contents/made  
[Accessed 3 November 2015].

Mirror, 2013. *Children given mobile phones at average age of 11 but some get them at FIVE.* [Online]   
Available at: http://www.mirror.co.uk/news/uk-news/children-given-mobile-phones-age-2208432  
[Accessed 7 November 2015].

Out Law, 2010. *Germany's data retention law ruled unconstitutional over privacy concerns.* [Online]   
Available at: http://www.out-law.com/page-10807  
[Accessed 5 November 2015].

Pew Research Center, 2014. *Older Adults and Technology Use.* [Online]   
Available at: http://www.pewinternet.org/2014/04/03/older-adults-and-technology-use/  
[Accessed 7 November 2015].

Pyramids, P., 2015. *Europe 2015.* [Online]   
Available at: http://populationpyramid.net/europe/2015/  
[Accessed 7 November 2015].

Spitz, M., 2012. *TED - Your Phone Company is Watching.* [Online]   
Available at: https://www.ted.com/talks/malte\_spitz\_your\_phone\_company\_is\_watching/transcript?language=en#t-278329  
[Accessed 1 Novemeber 2015].

Spitz, M., 2012. *Your phone company is watching.* Edinburgh, Scotland, TED.

TED, 2012. *TED - Ideas Worth Sharing.* [Online]   
Available at: https://www.ted.com/talks/malte\_spitz\_your\_phone\_company\_is\_watching?language=en  
[Accessed 1 November 2015].

UK Government, 2007. *The Data Retention (EC Directive) Regulations 2007.* [Online]   
Available at: http://www.legislation.gov.uk/uksi/2007/2199/regulation/5/made  
[Accessed 16 November 2015].

Waze, 2015. *Waze - About.* [Online]   
Available at: https://www.waze.com/about  
[Accessed 1 Novemeber 2015].