**‘ROAM: A mobile app for the storing and sharing of live geolocation data’**

**Abstract**

An in depth investigation focusing on geolocation, cloud computing and secure handling and analysis of big data. An overview into how a combination of these topics will help me to produce a mobile application that tracks and stores geo-location data across multiple devices.

Emphasis on the ethical issues surrounding personal data focusing on the handling and security of this sensitive data. how to successfully

As location data about an individual is very sensitive information the research into secure data handling will A look into

Introduction

In June 2012 Malte Spitz a politician for the German Green party gave a talk for TED in which he showed the data his phone company, by law, had stored about him. Spitz went to court to gain access to his own data and won receiving roughly 35,000 lines of data. Von Kai Biermann, a journalist and author wrote an article about Spitz’ findings for Zeit Online that was titled “Betrayed by our own data”. In this article Biermann talks about the potential power this data could have and the fact it could allow the consumer of this data to make a profile on Spitz, stating on this kind of profile “All in all, it reveals an entire life”. Spitz teamed up with Open Data City, a data visualisation company, 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.” I agree with Spitz that this is “a little bit scary” but however scary it is to think the government have access to this kind of data on an individual however I was more intrigued by the data Spitz had received.

The mobile app market is currently one of the biggest markets worldwide. With the market expecting to generate 45 billion dollars revenue in 2015 it’s safe to say it’s a good market to be in.

App’s that use GPS successfully

* Ingress – 12 million downloads
* Citymapper
* Untapped + Ted talk – was inspiration
* Pozzr
* Foursquare
* Loads of apps to (track/find someone else)

Similar apps

* Nike+ Running
* My Tracks (google)
* Trip Journal
* Field Trip
* Topo Maps

Project Scope

* Project propsal
* What language, what software, why android, what hardware

*I intend to make an android application that will use geo-location technology to collect live location data before storing it. The main use of the application will be to store location data to show a user where they have explored within the world. It will use google api’s to generate it’s maps which will then become an unexplored world which the user will unlock as the user begins to travel. Storing this data will then become a mapped out journey of their life where the user can unlock achievements and goals. This all stems from a 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)*) that talks about how much information your phone provider has on you as a consumer. In the talk Malte Spitz talks about this data as a bad thing as the government have access to this information. I agree with him that it’s scary that the government have access to this data but personally I’d be interested to see my personal data. Imagine a timeline of your life not just in chorological Facebook posts but geographically mapped out in the real world. Memories become easily stored; a true record of your travels.*

*Obviously this data is very sensitive and you would not want it getting in the wrong hands. This provokes me to look into big data ethics especially with the power and money big data can bring to a business. Also away from the ethics of sensitive data this will allow me to research into database security, who actually owns the data and separately how new scalable web storage such as AWS can be implemented.*

*I could potentially then use foursquare’s developer api to generate data of businesses within the user’s current area, which will then allow users to check in what they are doing. This could then be shared socially to create a social map of memories, events and user activities.*

*With both foursquare and google api’s then combined with geo-location technology will allow me to make an application that could make recommendations for things to do based on previous user check in’s and current location. However this could make the task of building the application too much for the time available so might just be a future idea for the next steps in this application.*

I plan to create a native android application that uses geo-location data to track and store a user’s location data.

Aim and Objectives

Methodologies

* UML
* Gant Charts
* TDD
* Agile

Project Planning

* Use cases
* Class diagrams
* Relationship diagrams
* Gant charts
* User experience

Literature Review

Conclusion

Quotes/Bibliography

“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.” - <http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz>

“This profile reveals when Spitz walked down the street, when he took a train, when he was in an airplane. It shows where he was in the cities he visited. It shows when he worked and when he slept, when he could be reached by phone and when was unavailable. It shows when he preferred to talk on his phone and when he preferred to send a text message. It shows which beer gardens he liked to visit in his free time. All in all, it reveals an entire life.”

* <http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz>

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.

* <http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz>

“If you have access to this information, you can see what your society is doing,” says Spitz. “If you have access to this information, you can control your country.”

Curious what information is being collected on you? After the jump, some surprising tidbits.

**Your internet search habits are recorded**

Journalist Alexis Madrigal sought to find out the extent to which companies collected data about his search habits, for the purpose of targeted advertising, in an article in [*The Atlantic*](http://www.theatlantic.com/technology/archive/2012/02/im-being-followed-how-google-151-and-104-other-companies-151-are-tracking-me-on-the-web/253758/)in February 2012. Madrigal had expected to see about 10 companies following his every click, but was surprised to find that the list totaled up to 105 companies, ranging from Google, Microsoft and Yahoo! to smaller advertising businesses. [*Note: TED uses DoubleClick, an industry-standard ad tracker.*]

**You can get caught in a “filter bubble”**

Online organizer Eli Pariser explains [in a fascinating talk at TED2012](https://www.ted.com/talks/lang/en/eli_pariser_beware_online_filter_bubbles.html) that search engines are smart, learning from what you click in the past to determine which results to give you in the future. Pariser warns that this process of data collection may be encasing people in a “filter bubble.” Sounds great, but there is a dangerous unintended consequence: We don’t get exposed to information that could challenge or broaden our worldviews.

**Your phone’s address book can be collected**

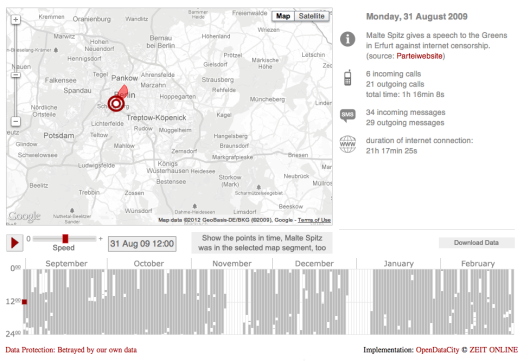
In February 2012, [*the New York Times*](http://bits.blogs.nytimes.com/2012/02/15/google-and-mobile-apps-take-data-books-without-permission/)reported that mobile apps like Twitter, Foursquare, Instagram, Yelp, Gowalla and Foodspotting were mining address books in smartphones and, in some cases, storing data on their own computers. In fact, the mobile security company Lookout found that 11 percent of free apps in Apple’s iTunes store collected address book data. At the time, the issue was beginning to be discussed by members of Congress. Meanwhile, Apple stated that apps storing address book data were violating guidelines, and assured users that permission would be asked in future software releases.

**The government can request your data**

In a [talk given at TEDxSanJoseCA](http://www.youtube.com/watch?v=esA9RFO1Pcw), privacy researcher and [TED Fellow Christopher Soghoian](http://fellows.ted.com/profiles/christopher-soghoian) reveals that telecommunication companies like Google and Facebook, as well as phone companies, have entire departments dedicated to responding to government surveillance requests. And these departments are very busy. Soghoian explains that Sprint set up a website in 2009 allowing law enforcement to log in and track users’ GPS location information. In the first year, the site had been used 8 million times. Meanwhile, Verizon revealed in 2007 that they got 80,000 requests per year for data on users from law enforcement agencies.

Want to protect your privacy? Here, some resources:

* [Collusion](http://www.mozilla.org/en-US/collusion/). This Firefox tool, which Mozilla CEO Gary Kovacs introduced in the TEDTalk “[Tracking the Trackers](https://www.ted.com/talks/lang/en/gary_kovacs_tracking_the_trackers.html),” records the breadth of companies capturing data about you as you search. Collusion developer Atul Varma [spoke to the TED blog](http://blog.ted.com/2012/02/28/meet-collusion-announced-today-onstage-at-ted-u/) in February about the tool, its uses, and what inspired it.
* [Tor Project](https://www.torproject.org/). This free software protects your privacy by bouncing communications all around the world, via a network run by volunteers.
* [Do Not Track Plus](https://addons.mozilla.org/en-US/firefox/addon/donottrackplus/?src=search). This app goes beyond browser-based controls and blocks data collection as you search.
* [Lookout](https://www.mylookout.com/). A mobile security app that is available for Android and iPhones.
* [European Digital Rights](http://www.edri.org/issues/privacy/dataretention). Founded in 2002, this organization is a clearinghouse of news when it comes to digital civil rights, including telecommunication data retention.
* [American Civil Liberties Union](http://www.aclu.org/protecting-civil-liberties-digital-age). This organization is dedicated to protecting rights in the United States, and considers civil liberties in the digital age one of their key issues.

[](http://www.zeit.de/datenschutz/malte-spitz-data-retention/)

And take a moment to play with Malte Spitz’s data map on [Zeit Online](http://www.zeit.de/datenschutz/malte-spitz-data-retention/), to see what kind of data phone companies regularly collect on users.

- <http://blog.ted.com/what-data-is-being-collected-on-you-some-shocking-info/>

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.

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

* <http://www.sciencedirect.com.ezproxy.brighton.ac.uk/science/article/pii/S0267364913000629>

Based on the above review, we infer that it is far from certain that EU security policy and the ensuing legislative acts are passing the appropriate tests of necessity and proportionality. Indeed, this drawback is being acknowledged both in academic work and within the EU system itself. For example, commenting on the Data Retention Directive, Rodotà alerted, “no real debate or analysis of the necessity or proportionality of measures taken for fighting terrorism and no real evaluation of the balancing vis-à-vis fundamental rights” occurred. [46](http://www.sciencedirect.com.ezproxy.brighton.ac.uk/science/article/pii/S0267364913000629#fn46) - Rodotà, S. (2006), La Conservación de los Datos de Tráfico en las Comunicaciones Electrónicas, IDP Revista de Internet, Derecho y Política, Numero 3, p. 57.

* <http://www.sciencedirect.com.ezproxy.brighton.ac.uk/science/article/pii/S0267364913000629>

## **5. Conclusion**

Protection of personal data is one of the key legal issues facing the present-day information society. In the last decade, though, the reinforcement of security policies alongside the expansion of information systems and databases designed for law enforcement and prevention of crime and terrorism entailed growing restrictions to data protection principles and procedural rights construed since the 1980s, in particular in Europe.

By the same token, concerns with the weakening of personal data protection principles and procedural rights have been accentuated in the European Union by the seeming lack of empirically-based demonstration of the necessity and proportionality of such restrictions.

Surprisingly, the EU institutional discourse has commonly presented security, data protection and privacy as values easily amenable to balancing. However, the balancing approach is visibly contradicted by the ways in which EU security policies have been impacting upon the protection of personal data regimes.

The adoption of the EU Charter of Fundamental Rights, that includes a new fundamental right to the protection of personal data, opened up reasonable expectations for a rebalancing of the requirements of EU security policies against the legal protection of personal data, and paved the way for the reform of EU data protection regimes launched by the European Commission in January 2012. To what extent balancing and proportionality are actually guiding this reform is open to question.

Balancing and proportionality involve the idea of weighting up different, opposing values, suggesting some form of equilibrium, therefore, an equitable solution, grounded on an evaluation of the values at stake. Going beyond Alexy's thesis of fundamental rights as optimization requirements, and accepting the moral force of a fundamental right such as the right to the protection of personal data, we deduce that guaranteeing this right should imply reinforcing data protection by the means of more exigent tests of necessity and proportionality of restrictive measures. This includes a more careful defence of the essential nucleus of the right, particularly the privacy and intimacy components involved; ultimately preventing further instrumentalization of personal data to the aims of security policy.

In face of the inconsistency of the EU's balancing and proportionality discourse and EU's institutional practice in this domain, one is left with little other choice than to interpret the present balancing discourse as part of a political or institutional tactic to render a somewhat contentious EU policy more acceptable to European public opinion. Nevertheless, balancing and proportionality maintain their potential as guidelines for arbitrating conflicting values or fundamental rights in ways that could better match security policies with the fundamental human values at issue in personal data protection.

**LOOK AT The legality of the data retention directive in light of the fundamental rights to privacy and data protection**