**Brain dump Final year project**

* 2006 directive
* 2007 legislation
* 2009 legislation
* 2014 annulment of EU directive
* 2014 Dripa legislation passed
* 2015 Dripa legislation revoked
* What’s next?

As I live in the United Kingdom I’ve looked into what this Directive means to me as a UK citizen. Regulation 5, shown below, states the data that must be retained about me as a mobile phone user.

**Data to be retained**

**5.**—(1) The following data concerning fixed network telephony and mobile telephony generated in the United Kingdom must be retained in accordance with regulation 4(1):

1. the telephone number from which the telephone call was made and the name and address of the subscriber and registered user of that telephone;
2. the telephone number dialled and, in cases involving supplementary services such as call forwarding or call transfer, any telephone number to which the call is forwarded or transferred, and the name and address of the subscriber and registered user of such telephone;
3. the date and time of the start and end of the call; and
4. the telephone service used.

(2) The following data concerning mobile telephony must be retained in accordance with regulation 4(1):

1. the International Mobile Subscriber Identity (IMSI) and the International Mobile Equipment Identity (IMEI) of the telephone from which a telephone call is made;
2. the IMSI and the IMEI of the telephone dialled;
3. in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the cell ID from which the service was activated;
4. the cell ID at the start of the communication; and
5. data identifying the geographic location of cells by reference to their cell ID.

(UK Government, 2007)

READ - <http://www.out-law.com/topics/tmt--sourcing/data-protection/data-retention-laws-what-they-mean-for-communication-service-providers/>

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

“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**

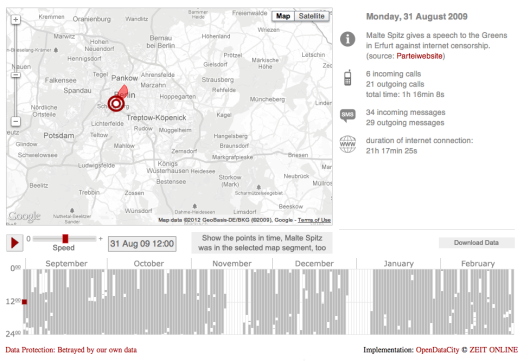
In February 2012, [*the New York Times*](http://bits.blogs.nytimes.com/2012/02/15/google-and-mobile-apps-take-data-books-without-permission/)reported that mobile apps like Twitter, Foursquare, Instagram, Yelp, Gowalla and Foodspotting were mining address books in smartphones and, in some cases, storing 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/>

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.