Location privacy in the European data protection legal framework: when your smart phone is getting "too" smart

K.U.Leuven privacy course

Eleni Kosta

eleni.kosta@law.kuleuven.be

28 June 2011

Got an iPhone or 3G iPad? Apple is recording your moves

Print
Listen

A hidden file in iOS 4 is regularly recording the position of devices.

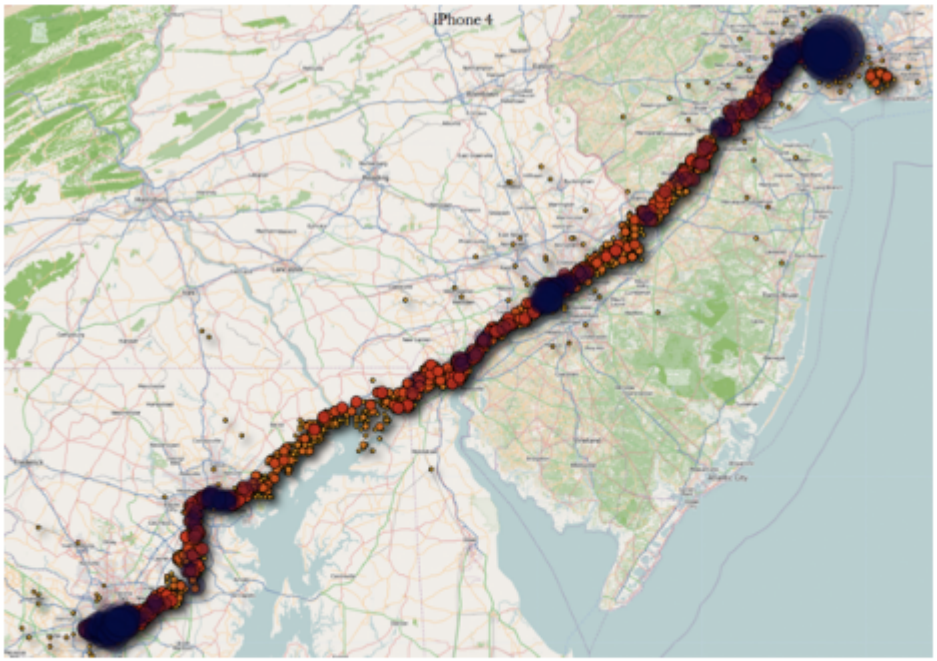
by Alasdair Allan | @aallan | Comments: 230 | 20 April 2011

Tweet 5,174 +1 1 Like 12K

Update, 4/27/11 — Apple has posted a response to questions raised in this report and others.

By Alasdair Allan and Pete Warden

Today at Where 2.0 Pete Warden and I will announce the discovery that your iPhone, and your 3G iPad, is regularly recording the position of your device into a hidden file. Ever since iOS 4 arrived, your device has been storing a long list of locations and time stamps. We're not sure why Apple is gathering this data, but it's clearly intentional, as the database is being restored across backups, and even device migrations.



A visualization of iPhone location data. Click to enlarge.

The presence of this data on your iPhone, your iPad, and your backups has security and privacy implications. We've contacted Apple's Product Security team, but we haven't heard back.

egister®

Networks Security Public Sector Business Science

Spam ID

Alert

isn't harmless and here's why

eing tapped by cops

• Get more from this author

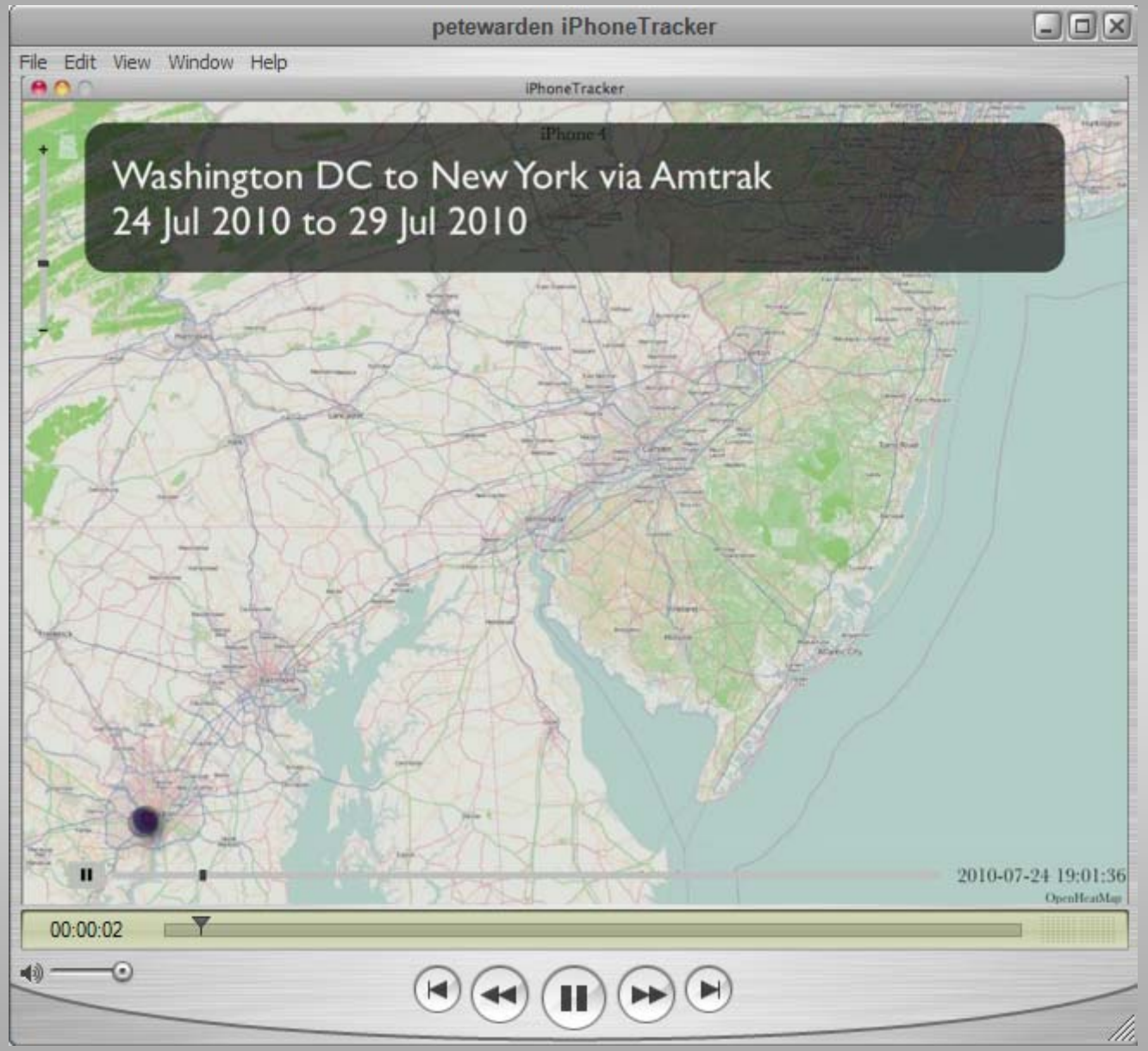
IT

logosphere to pooh pooh research presented on
ple iPhones and iPads unknown to the vast majority of
ir time-stamped locations, sometimes with alarming

sells software to law enforcement agencies gave a
e location-tracking database is crucial. We'll get to that
mpling of the rampant naysaying.

the contents of the SQLite file, which is stored on the
s, were wildly imprecise. Blogger and web developer
searchers' freely available software to map the
one during a recent round-trip bike tour he took from
e compared the results to the actual route, he found that

some of the points on the resulting map were as much
, away from his true location.


petewarden iPhoneTracker
File Edit View Window Help
iPhoneTracker
iPhone 4
Washington DC to New York via Amtrak
24 Jul 2010 to 29 Jul 2010
2010-07-24 19:01:36
OpenHeatMap
00:00:02

Overview

1. Introduction
2. Location data
3. Mining of location data
4. Processing of location data/traffic data
5. Processing of location data other than traffic data
6. Retention of location data

icri

European legislation regarding the protection of personal data

European directives

- ✓ Data protection directive (95/46/EC)
  - ❖ Protection of natural persons
  - ❖ Allows free flow of personal data

European legislation regarding the protection of personal data

European directives

- ✓ Data protection directive (95/46/EC)
- ✓ ePrivacy directive (2002/58/EC)
  - ❖ Protection of natural and legal persons
  - ❖ Application to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks

European legislation regarding the protection of personal data

European directives

- ✓ Data protection directive (95/46/EC)
- ✓ ePrivacy directive (2002/58/EC)
- ✓ Data retention directive (2006/24/EC)

  - ❖ Harmonisation of obligations of providers of publicly available electronic communications services or public communications networks with respect to the retention of certain data.

European legislation regarding the protection of personal data

- General rules in the data protection directive

- Specific rules for electronic communications sector in the ePrivacy directive. For what is not specifically covered by the ePrivacy directive, applies the data protection directive.

- Retention of traffic and location data in the data retention directive.

European ePrivacy Directive

Directive 2002/58/EC (ePrivacy Directive)

concerning the processing of personal data and the protection of privacy in the electronic communications sector

The **ePrivacy Directive** was recently reviewed in the frame of the reform of the regulatory framework on electronic communications by the **Citizens' Rights Directive** (2009/136/EC)

Scope of application

- Article 3: Services concerned

"This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices."

…the fact that provisions of the ePrivacy Directive only apply to provision of publicly available electronic communications services in public communication networks is regrettable because private networks are gaining an increasing importance in everyday life, with risks increasing accordingly

…the tendency of services to increasingly become a mixture of private and public ones.

should be explained in more details in order to allow for a clear and unambiguous

…both definitions 'electronic communications services', and 'to provide an electronic communications network' are still not very clear and both terms should be explained in more details in order to allow for a clear and unambiguous interpretation by data controllers and users alike.

(3) Furthermore, the Article 29 Working party in its previous Opinion 7/2000 referred to Recital 25 of the ePrivacy Directive, regarding the use of cookies. In Recital 25 it is mentioned that the users should have the possibility to refuse the storage of a cookie on their personal computers. The Article 29 Working party fully supported this point of view. However, the last paragraph of Recital 25, stipulating that access to specific website content may be made conditional on the acceptance of a cookie, might be contradictory with the position that the users should have the possibility to refuse the storage of a cookie on their personal computers and therefore may need clarification or revision.

Art. 29 WP, 126, Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive

Scope of application

- PSTN
- Mobile phones
- Internet
- Telex
- Video on demand
- …

Scope of application

BUT: does NOT apply to **broadcasting service** provided over a **public communications network**, intended for a **potentially unlimited** audience

- TV
- Radio
- Near video on demand
- Private networks

Scope of application

Check:

1. Whether there is an electronic communications service,
2. whether this service is offered in an electronic communications network and
3. whether the aforementioned service and network are public.

Overview

1	Introduction
2	Location data
3	Mining of location data
4	Processing of location data/traffic data
5	Processing of location data other than traffic data
6	Retention of location data

Location data

"Location data means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service"

Location data

Location data is limited to the information that relates to the geographic position of the terminal equipment of a user of a publicly available electronic communications service

Overview

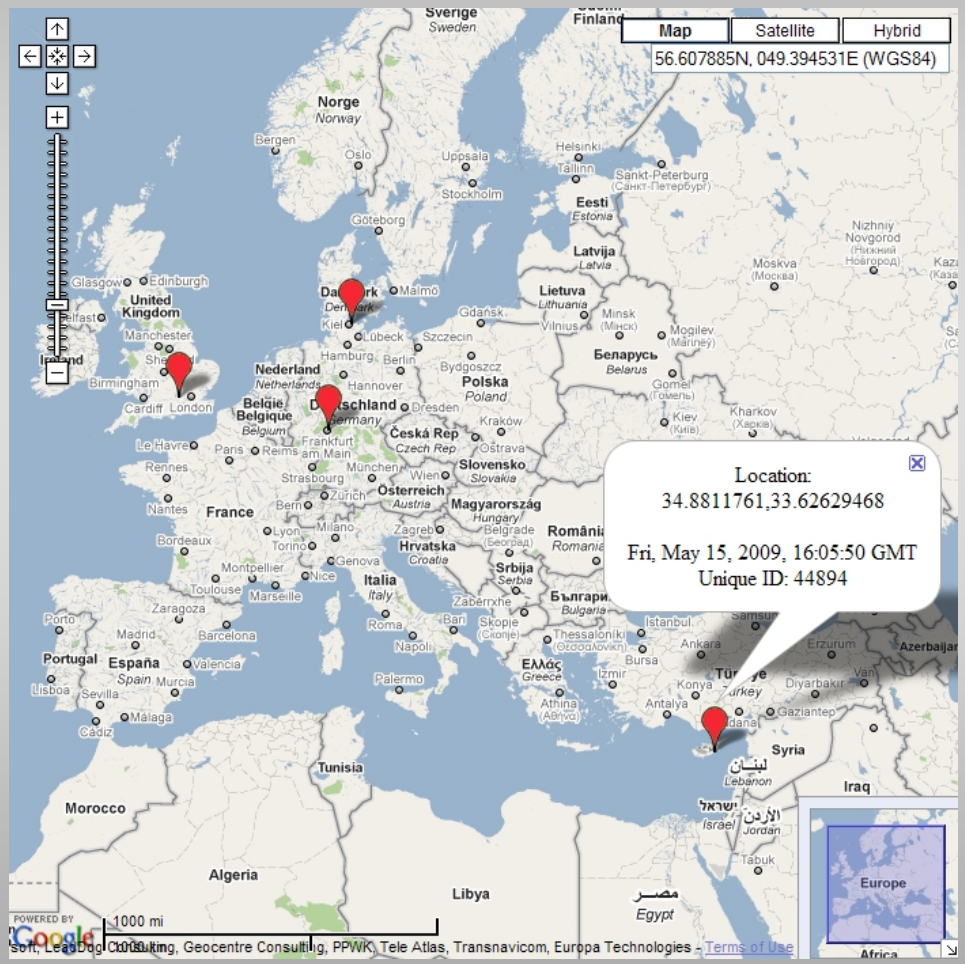
1	Introduction
2	Location data
3	Mining of location data
4	Processing of location data/traffic data
5	Processing of location data other than traffic data
6	Retention of location data

Location Mining Case Study

Short case study tracking four people, in three European Member States, persistently for six weeks using mobile handsets.

FIDIS NoE (www.fidis.net)

Location Mining Case Study

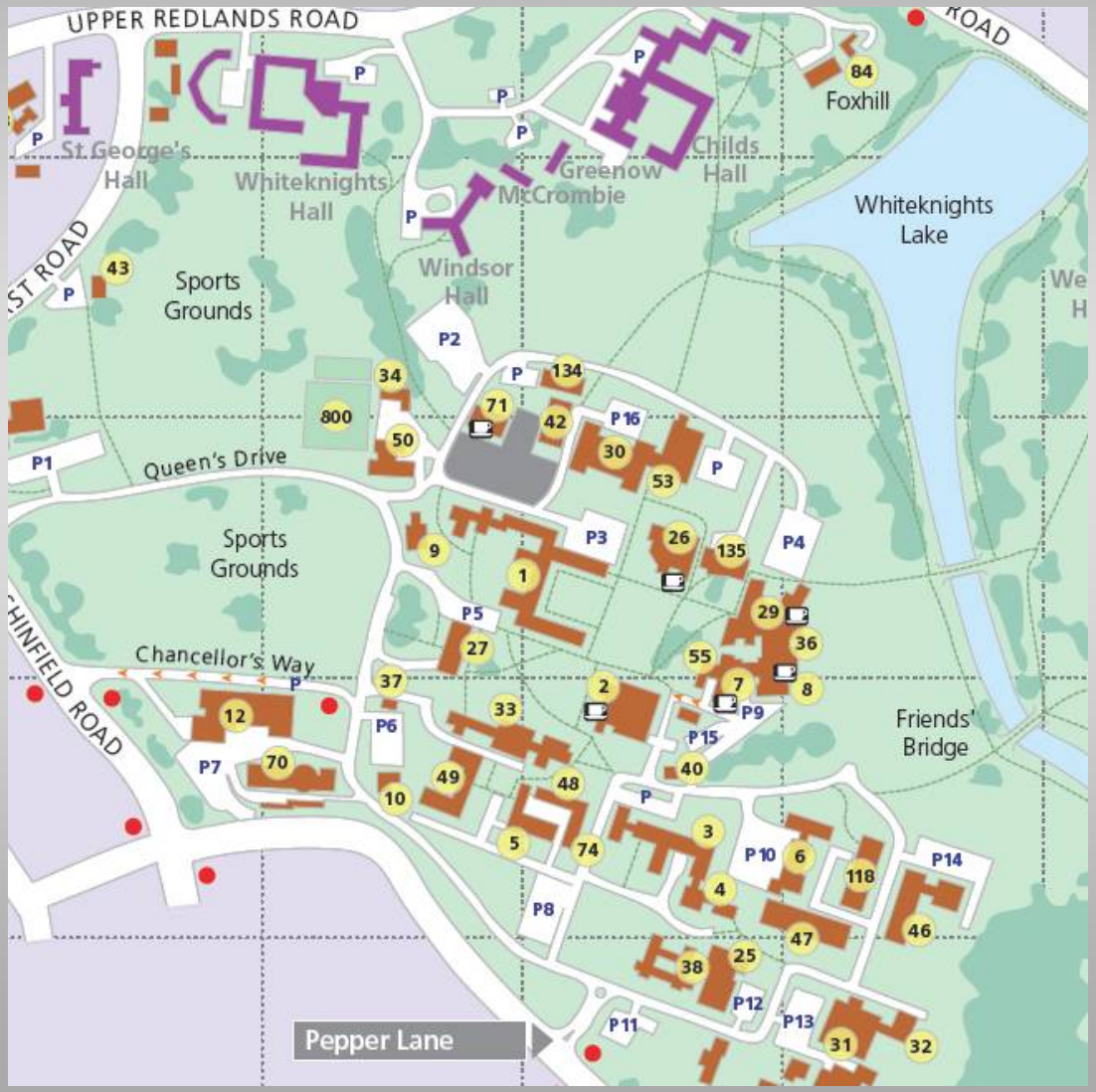


Location Mining Case Study

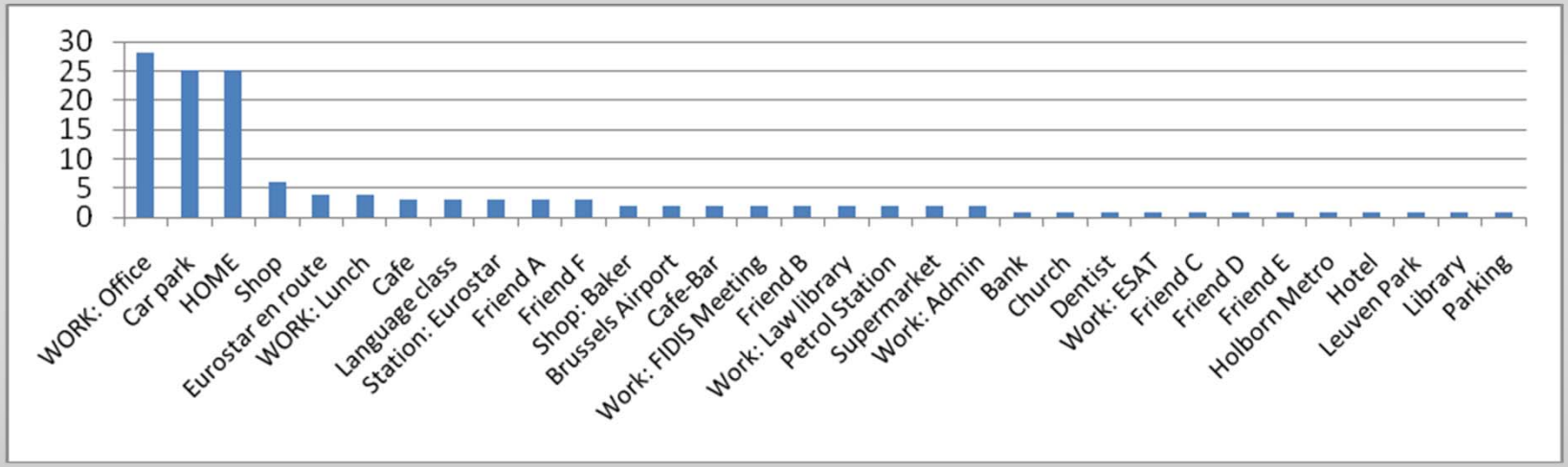
- The GPS locations of these people have been mined to reveal places of interest and to create simple profiles.

- One of the key tools for initial mining is the generation of 'Points of Interest' (PoI) from the data

Points of Interest (PoI)

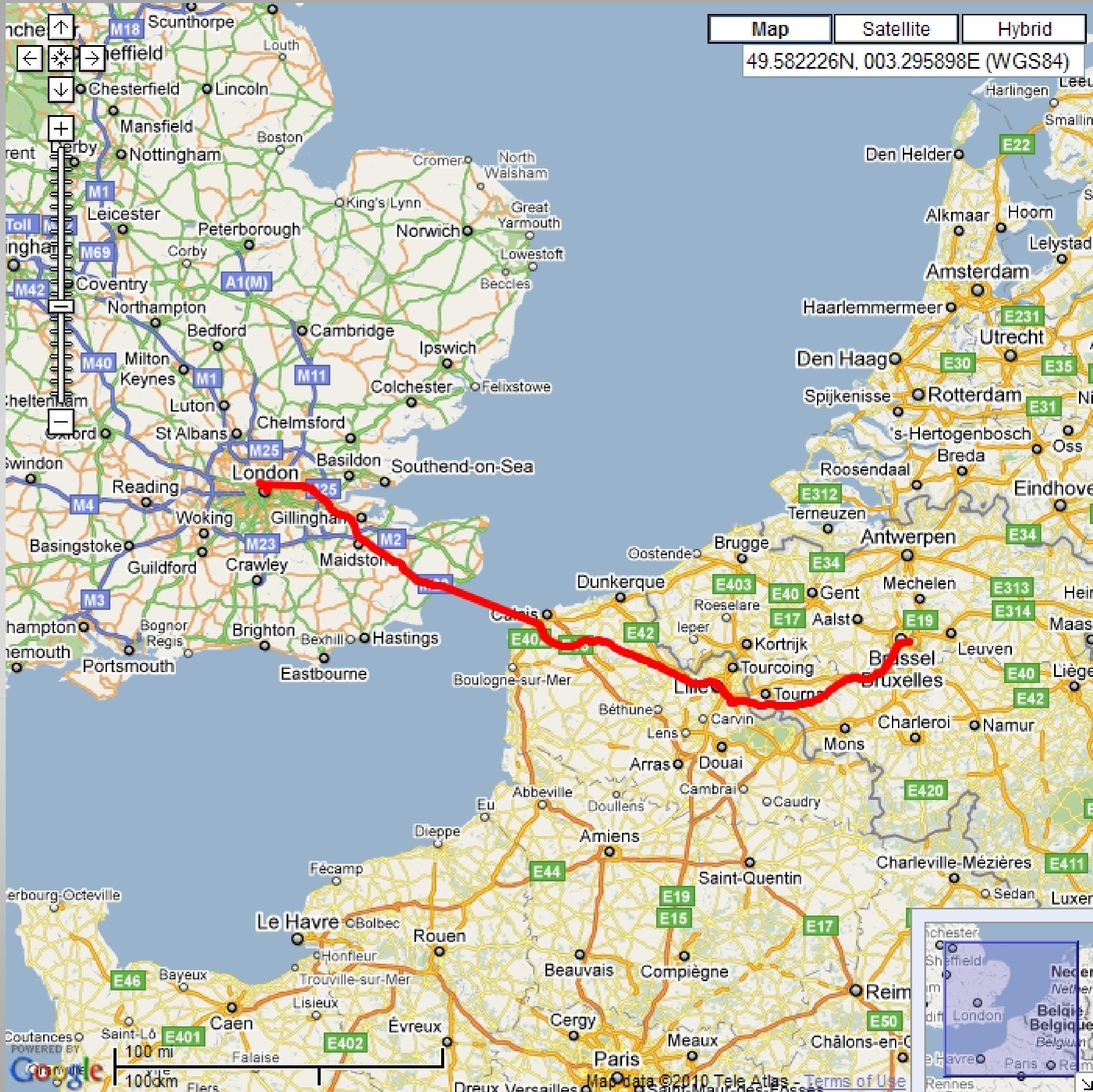


PoIs at identified locations collected from each user



Frequency of PoIs

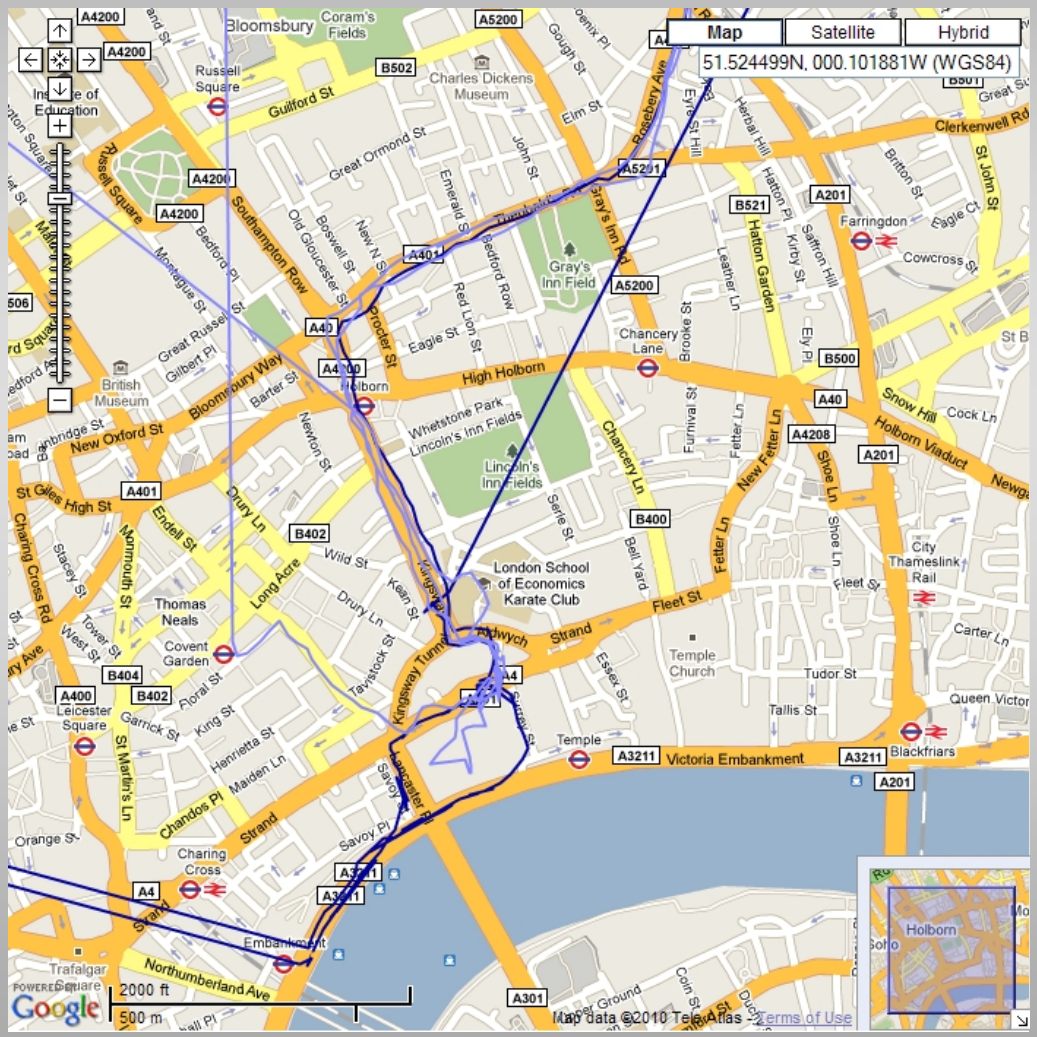
icri



Map
Satellite
Hybrid
49.582226N, 003.295898E (WGS84)
Scunthorpe
Louth
Chesterfield
Lincoln
Mansfield
Boston
Nottingham
Leicester
Peterborough
Corby
Coventry
Northampton
Bedford
Cambridge
Ipswich
Milton Keynes
Luton
Colchester
Felixstowe
Chelmsford
St Albans
Basildon
Southend-on-Sea
London
Reading
Woking
Gillingham
Basingstoke
Guildford
Crawley
Maidstone
Brighton
Hastings
Eastbourne
Portsmouth
Cromer
North Walsham
King's Lynn
Norwich
Great Yarmouth
Lowestoft
Beccles
Den Helder
Alkmaar
Hoorn
Lelystad
Amsterdam
Haarlemmermeer
Utrecht
Den Haag
Rotterdam
Spijkenisse
's-Hertogenbosch
Breda
Oss
Roosendaal
Eindhoven
Terneuzen
Antwerpen
Brugge
Oostende
Dunkerque
Gent
Mechelen
Roeselare
Aalst
Kortrijk
Tourcoing
Leuven
Calais
Boulogne-sur-Mer
Béthune
Lens
Carvin
Arras
Douai
Cambrai
Caudry
Mons
Charleroi
Namur
Liège
Abbeville
Doullens
Amiens
Dieppe
Saint-Quentin
Charleville-Mézières
Sedan
Fécamp
Le Havre
Bolbec
Rouen
Honfleur
Trouville-sur-Mer
Lisieux
Bayeux
Caen
Beauvais
Compiègne
Évreux
Cergy
Paris
Meaux
Châlons-en-C
Falaise
100 mi
100 km
Map data ©2010 Tele Atlas - Terms of Use

icri

Inferring relation



icri

Tracking study:

GASSON Mark, KOSTA Eleni, ROYER Denis, MEINTS Martin & WARWICK Kevin (2011) Normality Mining: Privacy Implications of Behavioral Profiles Drawn from GPS Enabled Mobile Phones, IEEE Transactions on Systems, Man, and Cybernetics--Part C: Applications and Reviews, Vol.41(2), p. 251-261

Overview

1	Introduction
2	Location data
3	Mining of location data
4	Processing of location data/traffic data
5	Processing of location data other than traffic data
6	Retention of location data

Traffic data

"Traffic data means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof"

►► Location data that are processed for the purpose of the conveyance of an electronic communications network are also traffic data !

Location data

"Location data means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service"

Processing of location/traffic data

- ✓Traffic data must be
  - ➢erased or
  - ➢made anonymous

  when they are no longer needed for the purpose of the transmission of a communication

- ✓Billing or interconnection payments

Processing of location/traffic data

Prior consent of subscriber or user for

- purpose of marketing electronic communications services or
- for the provision of value added services

Overview

1	Introduction
2	Location data
3	Mining of location data
4	Processing of location data/traffic data
5	Processing of location data other than traffic data
6	Retention of location data

Location data other than traffic data

Location data other than traffic data that are not processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof

►► for the provision of a value added service

Value added service

"Value added service means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof"

►► "Location Based Services" broad term going beyond the ePrivacy Directive

Value added service

Location data other than traffic data may only be processed

- when they are made anonymous, or
- with the consent of the users or subscribers

to the extent and for the duration necessary for the provision of a value added service.

Technologies for offering LBS

- Cell-based mobile communication networks such as GSM and UMTS;
- Satellite-based positioning systems such as the Global Positioning System (GPS);
- WiFi or Bluetooth;
- Wireless technologies, such as Radio Frequency Identification (RFID);
- Sensor-based systems such as face recognition systems and license-plate scanners for vehicles;
- Chip-card-based systems, such as credit cards

Challenge…

Which of the technologies that offer Location Based Services are covered by the ePrivacy Directive?

Article 29 Working Party

Opinion 13/2011 on Geolocation services on smart mobile devices

Overview

1	Introduction
2	Location data
3	Mining of location data
4	Processing of location data/traffic data
5	Processing of location data other than traffic data
6	Retention of location data

Data retention directive

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the **retention of 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

Campaign against data retention

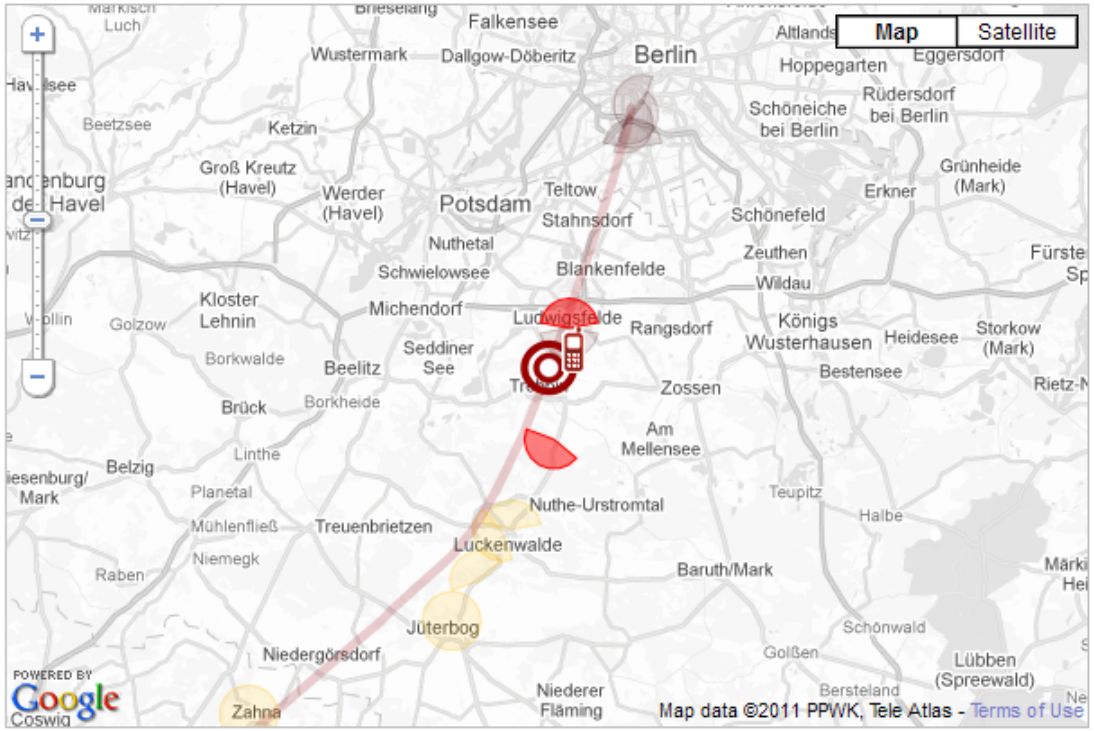
- Civil Rights Organisations, Industry Members etc.:

"Data retention is no solution"

- Petition signed by 58265 people until 14.12.2005.

icri

German politician Malte Spitz put profiling to the test using his own data

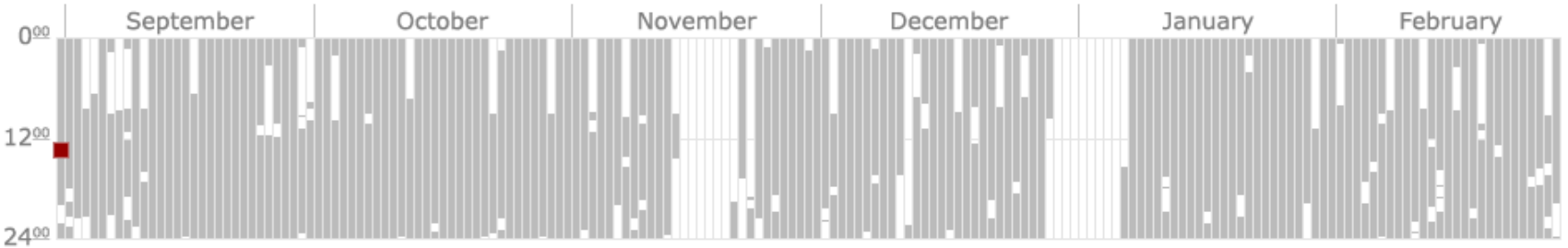


0 Speed +

31 Aug 09 13:18

Show the points in time, Malte Spitz was in the selected map segment, too

Download Data



Monday, 31 August 2009

Malte Spitz gives a speech to the Greens in Erfurt against internet censorship.
(source: Parteiwebsite)

6 incoming calls
21 outgoing calls
total time: 1h 16min 8s

34 incoming messages
29 outgoing messages

duration of internet connection:
21h 17min 25s

Data Protection: Betrayed by our own data

Implementation: OpenDataCity © ZEIT ONLINE

Scope

[Harmonisation] of Member States' provisions concerning the **obligations** of the providers of publicly available electronic communications services or of public communications networks with respect to the **retention of certain data** which are **generated or processed by them**, in order to ensure that the data are available for the purpose of the **investigation**, **detection** and **prosecution** of **serious crime**, as defined by each Member State in its national law

Serious Crime?

- Statement by the Council concerning Article 1:

  "In defining 'serious crime' in national law Member States shall have due regard to the crimes listed in Article 2(2) of the Framework Decision on the European Arrest Warrant (2002/584/JHA) and crime involving telecommunication".

Serious Crime?

Such as…

- participation in a criminal organisation,
- terrorism,
- sexual exploitation of children and child pornography,
- illicit trafficking in narcotic drugs and psychotropic substances,
- illicit trafficking in weapons, munitions and explosives,
- corruption,
- trafficking in stolen vehicles,
- racism and xenophobia,
- Etc…

Who shall retain the data?

Providers

- of publicly available electronic communications services or
- of public communications networks

💣No definition

Who shall retain the data?

- Telecommunications operators
- Internet Service Providers
- Cable TV operators
- …

What data are to be retained?

- **Traffic and location data** on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user.
- Including data relating to **unsuccessful call attempts**
- **No data relating to unconnected calls**
- **No content data**

What data are to be retained?

Art. 3(1) DRD:

> "[T]he data specified in Article 5 DRD are retained in accordance with the provisions thereof, to the extent that those data are **generated or processed** by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned."

What data are to be retained?

Art. 5 DRD

a) Data necessary to trace and identify the source of a communication;
b) Data necessary to identify the destination of a communication;
c) Data necessary to identify the date, time and duration of a communication;
d) Data necessary to identify the type of communication;
e) Data necessary to identify users' communication equipment or what purports to be their equipment;
f) Data necessary to identify the location of mobile equipment.

Review of the Directive

EUROPEAN COMMISSION

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor

on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)

REPO

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Article 7 and 8 thereof,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1],

icri

Thank you for your attention!

Eleni KOSTA
eleni.kosta@law.kuleuven.be

Interdisciplinary Centre for Law & ICT – ICRI
Katholieke Universiteit Leuven

Interdisciplinary Institute for BroadBand Technology

icri

Cookies, spyware and similar… | 1

Article 5(3) 2002 ePrivacy Dir.

3. Member States shall ensure that the use of electronic communications networks to store information or to gain

"use of electronic communications networks"

"to store information or gain access to information stored in the terminal equipment of a subscriber or user"

controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

icri

Cookies, spyware and similar… | 2

✓ An “electronic communications network” was required

✓ Left spyware and similar programmes outside when installed from an “off-line” source

Cookies, spyware and similar… | 3

Article 5(3) ePrivacy Dir.

'3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is

"the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user "

processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.';

icri

Cookies, spyware and similar… | 4

Recital 65 Citizens' Rights Dir.

(65) Software that surreptitiously monitors the actions of the user or subverts the operation of the user's terminal equipment to the benefit of a third party (spyware) poses a serious threat to the privacy of users, as do viruses. A high and

"Unwanted spying programmes or viruses are **inadvertently downloaded** via electronic communications networks or are **delivered** and **installed** in software distributed on other **external data storage media**, such as CDs, CD-ROMs or USB keys"

of information to end-users about available precautions, and should encourage them to take the necessary steps to protect their terminal equipment against viruses and spyware.

icri

Right to object vs. consent | 1

Article 5(3) 2002 ePrivacy Dir.

3. Member States shall ensure that the use of electronic communications networks to store information or to gain

"use of electronic communications networks"

"to store information or gain access to information stored in the terminal equipment of a subscriber or user"

controller. This shall not prevent any technical storage or access

"only when the subscriber or the user is provided with clear and comprehensive information [...] and is given the right to refuse"

user.

Right to object vs. consent | 2

Recital 25 2002 ePrivacy Dir.

some Member States only prohibits intentional unauthorised access to communications.

The prohibition of storage of communications and the related traffic data by persons other than the users or

(25) However, such devices, for instance so-called 'cookies', can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal

"Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose."

confidentiality remains guaranteed. Where this is necessary for making more efficient the onward transmission of any publicly accessible information to other recipients of the service upon their request, this Directive should not prevent such information from being further stored, provided that this information would in any case be accessible to the public without restriction and that any data referring to the individual subscribers or users requesting such information are erased.

on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.

icri

Right to object vs. consent | 3

monitoring employee behaviour by means of traffic data). Another development that calls for reconsideration of the scope of the Directive is the tendency of services to increasingly become a mixture of private and public ones.

The Working Party notes that both definitions 'electronic communications services', and 'to provide an electronic communications network' are still not very clear and both terms should be explained in more details in order to allow for a clear and unambiguous

Recital 25 [...] might be contradictory with the position that the users should have the possibility to refuse the storage of a cookie on their personal computers and therefore may need clarification or revision.

computers. The Article 29 Working party fully supported this point of view. However, the last paragraph of Recital 25, stipulating that access to specific website content may be made conditional on the acceptance of a cookie, might be contradictory with the position that the users should have the possibility to refuse the storage of a cookie on their personal computers and therefore may need clarification or revision.

Art. 29 WP, 126, Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive

Right to object vs. consent | 4

Article 5(3) ePrivacy Dir.

'3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is

"the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user "

processing. This shall not prevent any technical storage or

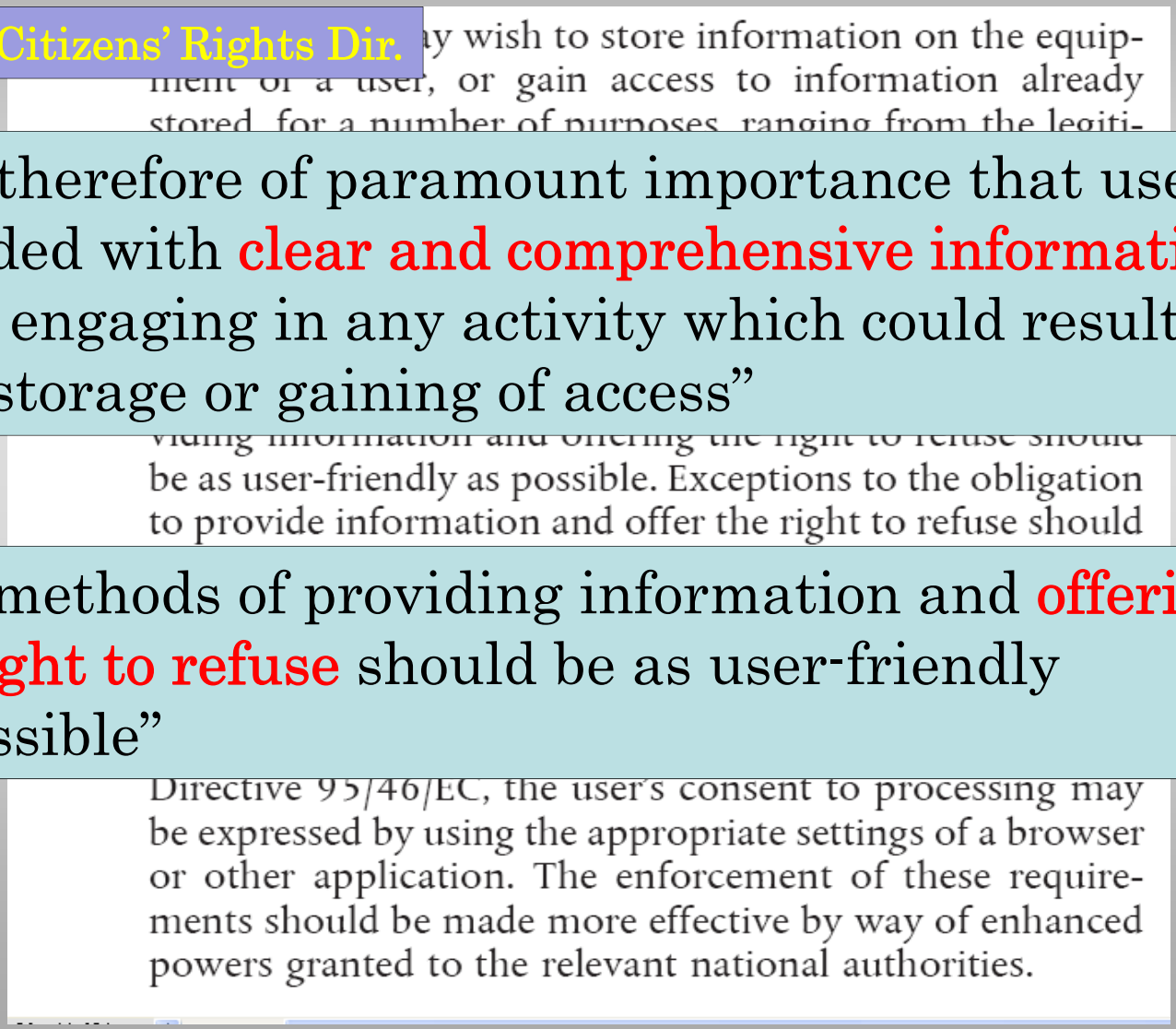
"has given his or her consent, having been provided with clear and comprehensive information"

information society service explicitly requested by the subscriber or user to provide the service.';

icri

Right to object vs. consent | 5

Recital 66 Citizens' Rights Dir.



...y wish to store information on the equip-
...ment of a user, or gain access to information already
stored, for a number of purposes, ranging from the legiti-

"It is therefore of paramount importance that users be provided with clear and comprehensive information when engaging in any activity which could result in such storage or gaining of access"

...viding information and offering the right to refuse should
be as user-friendly as possible. Exceptions to the obligation
to provide information and offer the right to refuse should

"The methods of providing information and offering the right to refuse should be as user-friendly as possible"

Directive 95/46/EC, the user's consent to processing may
be expressed by using the appropriate settings of a browser
or other application. The enforcement of these require-
ments should be made more effective by way of enhanced
powers granted to the relevant national authorities.

icri

Right to object vs. consent |6

Statement by Austria, Belgium, Estonia, Finland, Germany, Ireland, Latvia, Malta, Poland, Romania, Slovakia, Spain and United Kingdom on the "Citizens Rights Directive, E-Privacy Directive" (19 November 2009)

Right to object vs. consent | 7

and the Better Regulation Directive, which was adopted by Council on 20th November.

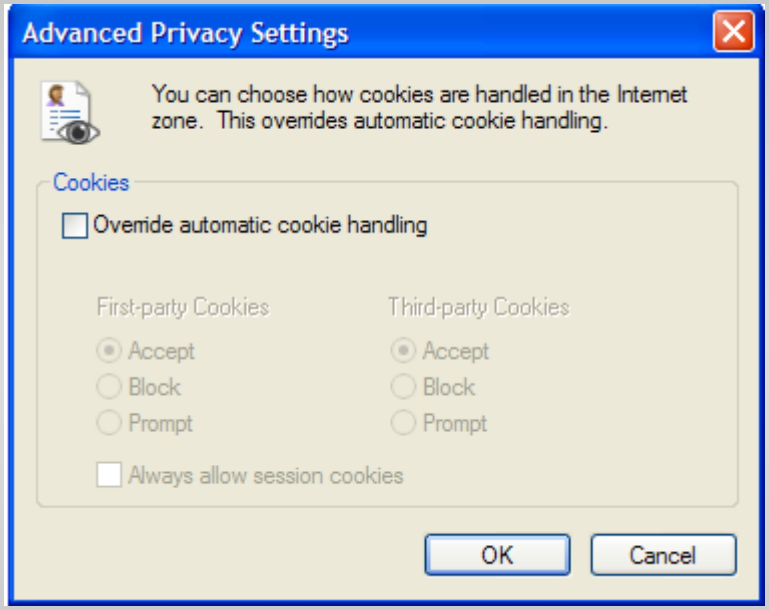
The aim of Directive 2002/58/EC and of the Citizen's Rights Directive is to protect fundamental rights and freedoms with respect to the processing of personal data in the electronic communications sector, and in particular the right to privacy, and to ensure the free movement of

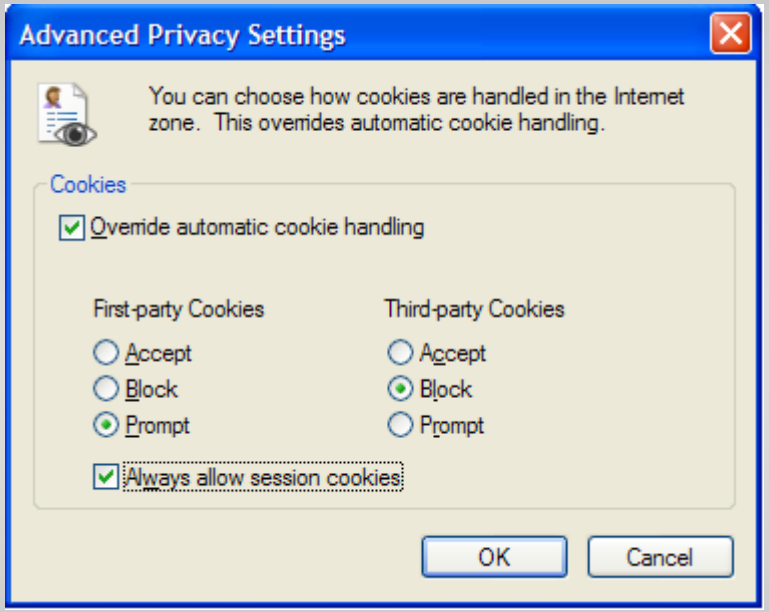
"These Member States recognise that this clarification may require the modification of some national laws. However, as indicated in recital 66, amended Article 5(3) is **not intended to alter the existing requirement that such consent be exercised as a right to refuse the use of cookies or similar technologies used for legitimate purposes**."."

to alter the existing requirement that such consent be exercised as a right to refuse the use of cookies or similar technologies used for legitimate purposes.

These Member States also stress that the methods of providing information and offering the right to refuse should be as user-friendly as possible.

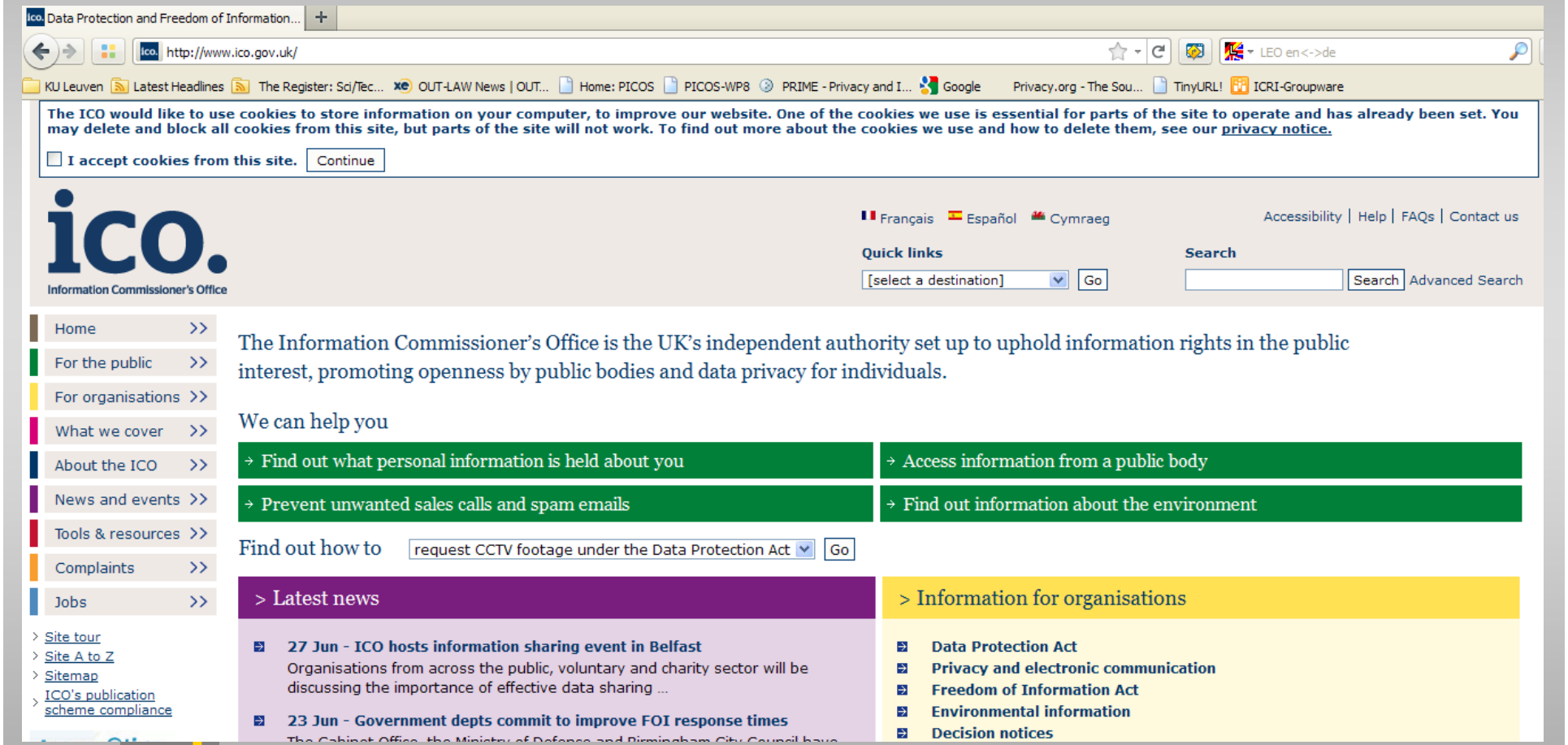
icri


Advanced Privacy Settings
You can choose how cookies are handled in the Internet zone. This overrides automatic cookie handling.
Cookies
Override automatic cookie handling
First-party Cookies
Accept
Block
Prompt
Third-party Cookies
Accept
Block
Prompt
Always allow session cookies
OK
Cancel


Advanced Privacy Settings
You can choose how cookies are handled in the Internet zone. This overrides automatic cookie handling.
Cookies
Override automatic cookie handling
First-party Cookies
Accept
Block
Prompt
Third-party Cookies
Accept
Block
Prompt
Always allow session cookies
OK
Cancel

icri

The way forward?



Or as Obelix would say…

Thank you for your attention!

Eleni KOSTA
eleni.kosta@law.kuleuven.be

Interdisciplinary Centre for Law & ICT – ICRI
Katholieke Universiteit Leuven

Interdisciplinary Institute for BroadBand Technology