Privacy in the electronic communications sector: recent developments

Eleni Kosta

eleni.kosta@law.kuleuven.be

11 June 2009



http://www.icri.be

"We live in a world shaped by technology and fuelled by information"

D. Solove



A man's home is his castle.

BBC NEWS

Watch One-Minute World News

News services
Your news when you want it

News Front Page

Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science/Nature
Technology
Entertainment
Also in the news

Video and Audio

Have Your Say
In Pictures
Country Profiles
Special Reports

RELATED BBC SITES
SPORT
WEATHER
ON THIS DAY
EDITORS' BLOG

Last Updated: Monday, 7 January 2008, 11:56 GMT

E-mail this to a friend Printable version

Clarkson stung after bank prank

TV presenter Jeremy Clarkson has lost money after publishing his bank details in his newspaper column.


Jeremy Clarkson found himself unexpectedly donating to charity

The Top Gear host revealed his account numbers after rubbishing the furore over the loss of 25 million people's personal details on two computer discs.

He wanted to prove the story was a fuss about nothin

But Clarkson admitted he was "wrong"
reader had used the details t
the charity Diabetes

Clarkso
his Barc
Sun new
account
code. He
to find ou

"All you'll be them is put money into my account. No ke it out. Honestly, I've never known such a palaver about nothing," he told readers.

"I was wrong and I have been punished"

Jeremy Clarkson

SEE ALSO
- Clarkson quizzed over gang ordeal
  06 Dec 07 | England
- More firms 'admit disc failings'
  04 Dec 07 | UK Politics
- Brown apologises for records loss
  21 Nov 07 | UK Politics

RELATED BBC LINKS
- Top Gear

RELATED INTERNET LINKS
- Diabetes UK
- emy Clarkson

BBC is not responsible for the nt of external internet sites

TERTAINMENT STORIES
- g arrives for Potter case
- ars' Baker 'a lot better'
- Speight was found

ws feeds

MOST POPULAR STORIES NOW

MOST E-MAILED | MOST READ

1. TV host Speight was found hanged
2. Day in pictures
3. Lonely Planet rebuts 'fake' claim

icri

A short introduction



www.icri.be

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.



http://www.icri.be

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.

Directive 2002/58/EC - ePrivacy directive



http://www.icri.be

The Directive is under review in the frame of the reform of the regulatory framework on electronic communications.



http://www.icri.be

What is covered?

- Publicly available electronic communications services
- in public communications networks



http://www.icri.be

What is covered?

- PSTN
- Mobile phones
- Internet
- Telex
- Video on demand
- Cable TV network
- …



http://www.icri.be

What is covered?

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



Applicability

Check:

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



…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

Security

- Appropriate technical and organisational measures shall be taken to safeguard security

- The subscribers shall be informed about breaches of security of the network, such as viruses, hacking of a database etc.



http://www.icri.be

Confidentiality of the communications

- Prohibition of listening, tapping, storage or other kinds of interception or surveillance of communications

Unless: consent or legal authorisation

Exception: technically necessary for the conveyance of a communication

& data retention for specific reasons



http://www.icri.be

Spyware and Cookies

Spyware is allowed only when the user knows and for legitimate purposes

Cookies: Information to the user and right to refuse the installation



http://www.icri.be

(1) In the mentioned Opinion the Working Party 29 emphasised that 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, in particular because such networks are becoming more specific (e.g. 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.

(2) 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 interpretation by data controllers and users alike. The unclear definitions give rise to several

…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.

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.

However, such considerations can not be pleaded as an excuse for not complying with applicable data protection laws of the Member States. Moreover, search engine providers cannot claim that their purpose in collecting personal data is the development of new services whose nature is as yet undecided. Fairness demands that data subjects are aware of the extent to which their private life might be intruded upon when their data is obtained. This will not be possible unless purposes are more precisely defined.

Persistent cookies containing a unique user ID are personal data and therefore subject to applicable data protection legislation.

applicable data protection legislation. The responsibility for their processing cannot be reduced to the responsibility of the user for taking or not taking certain precautions in his browser settings. The search engine provider decides if a cookie is stored, what cookie is stored and for what purposes it is used. Finally, expiration dates of cookies set by some search engine providers seem to be excessive. For instance, several companies set cookies that expire after many years. When a cookie is used, an appropriate cookie lifetime should be defined both to allow an improved surfing experience and a limited cookie duration. Especially in view of the default settings of browsers, it is very important that users are fully informed about the use and effect of cookies. This information should be more prominent than simply being part of a search engine's privacy policy, which may not be immediately apparent.

Anonymisation

If there is no legitimate ground for processing, or for use beyond the well-specified legitimate purposes, search engine providers must delete personal data. Instead of deletion, search engines may also anonymise data, but such anonymisation must be completely irreversible for the Data Protection Directive to no longer apply.



Art. 29 WP, 148, Opinion on data protection issues related to search engines

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 (Art.2 lit.b ePrivacy dir)
  - Erased or made anonymous
  - Allowed for: billing and interconnection purposes
  - Exception: data retention

Location data

- ✓ **Location data** means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service (Art.2 lit.c ePrivacy dir)
  - Latitude
  - Longitude
  - Altitude
  - Direction of travel
  - Network cell…



http://www.icri.be

Location Based Services



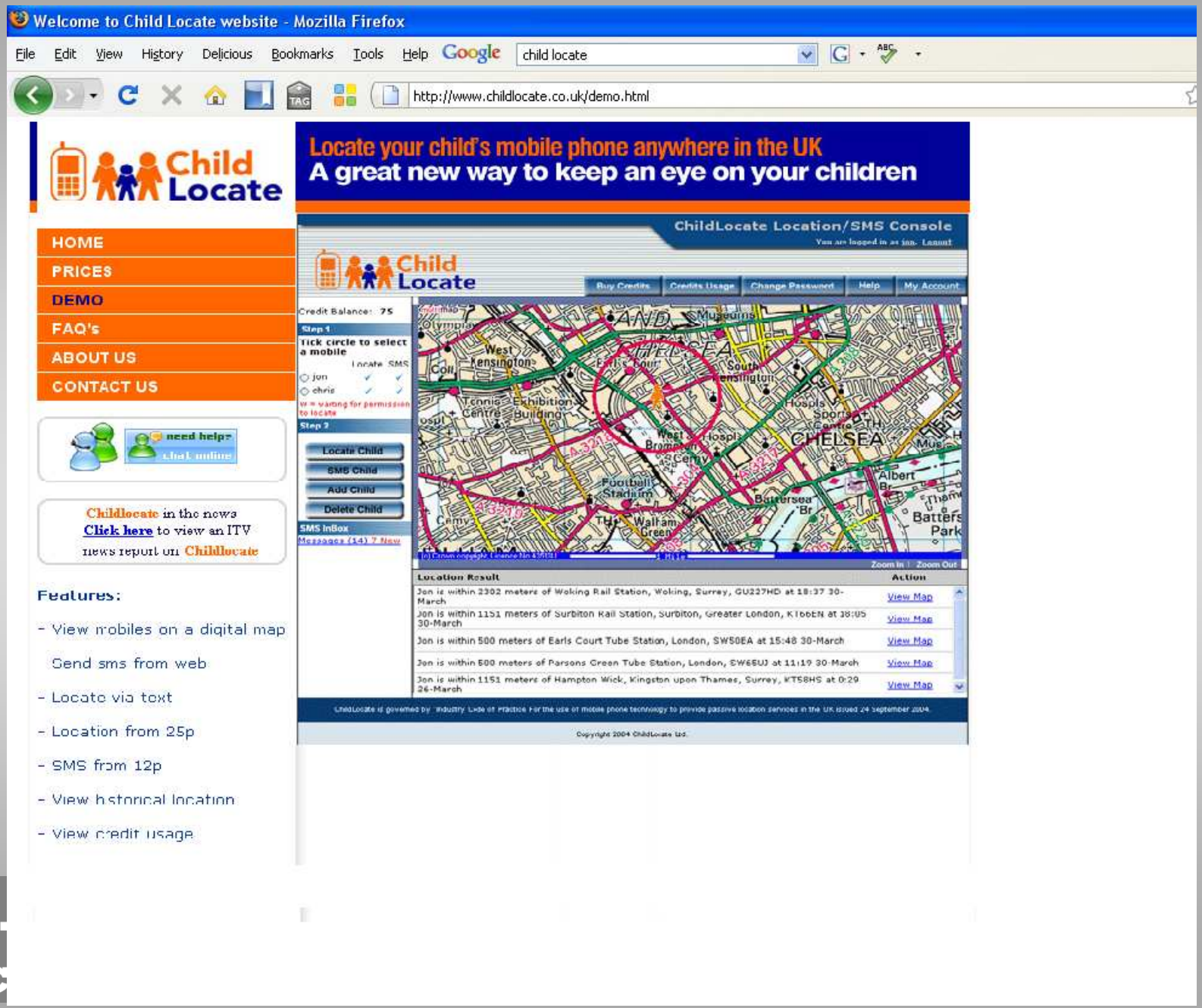
http://www.icri.be

Location Based Services

- ✓ Location Based Service (LBS) is a service provided to a subscriber based on their current geographical location
  - ☆ Where am I?
  - ☆ Find my nearest…
  - ☆ Tracking services
  - ☆ Find a friend
  - ☆ Directory services
  - ☆ ……



http://www.icri.be


Welcome to Child Locate website - Mozilla Firefox
File Edit View History Delicious Bookmarks Tools Help Google child locate
http://www.childlocate.co.uk/demo.html
Child Locate
Locate your child's mobile phone anywhere in the UK
A great new way to keep an eye on your children
HOME
PRICES
DEMO
FAQ's
ABOUT US
CONTACT US
need help? chat online
Childlocate in the news
Click here to view an ITV news report on Childlocate
Features:
- View mobiles on a digital map
Send sms from web
- Locate via text
- Location from 25p
- SMS from 12p
- View historical location
- View credit usage
ChildLocate Location/SMS Console
Buy Credits
Credits Usage
Change Password
Help
My Account
Credit Balance: 75
Step 1
Tick circle to select a mobile
Locate SMS
jon
chris
Step 2
Locate Child
SMS Child
Add Child
Delete Child
SMS InBox
Location Result
Action
Jon is within 2302 meters of Woking Rail Station, Woking, Surrey, GU227HD at 18:37 30-March
View Map
Jon is within 1151 meters of Surbiton Rail Station, Surbiton, Greater London, KT66EN at 18:05 30-March
View Map
Jon is within 500 meters of Earls Court Tube Station, London, SW50EA at 15:48 30-March
View Map
Jon is within 500 meters of Parsons Green Tube Station, London, SW65UJ at 11:19 30-March
View Map
Jon is within 1151 meters of Hampton Wick, Kingston upon Thames, Surrey, KT58HS at 0:29 26-March
View Map
Copyright 2004 ChildLocate Ltd.

Quartix vehicle tracking system, gps vehicle tracking, satellite tracking system and vehicle tracking devices - Mozilla Firefox

File Edit View History Delicious Bookmarks Tools Help Google

http://www.quartix.net/

Vehicle Tracker | GPS Tracking Prices | Van Tracking | Tracking System Prices | Vehicle Tracker Systems

QUARTIX

Home | Product Overview | Pricing | Online Demonstration | Brochure Request | Case Studies | News

Registered Users

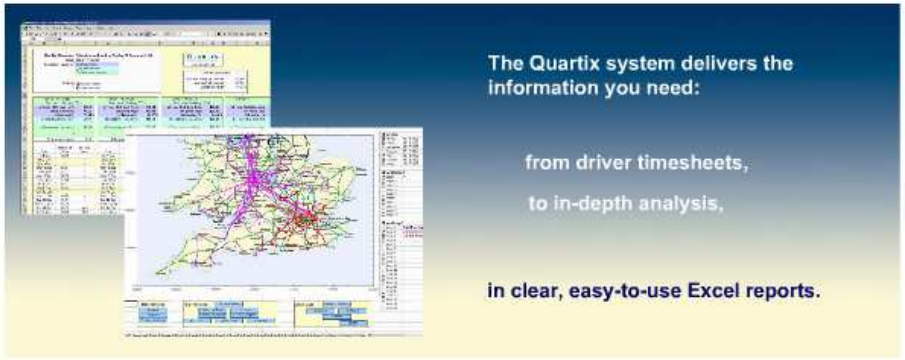
Subscriber ID

Username

Password

Login

For demonstration password details, click here.



Vehicle tracking on the Internet for just 66p per day*

Quartix's vehicle tracking system is both reliable and easy-to-use and it offers considerable financial benefits to commercial fleet operators. GPS satellite and Internet technology are used to deliver vehicle logs to you by e-mail each morning - requiring no special training and very little of your time. If you are considering vehicle tracking, contact us for more information:

request brochure & pricing tel: 0870 013 6663 enquiries@quartix.net



Request brochure

- Clear, easy-to-use timesheet reports **delivered** by e-mail.
- An all-inclusive service, with everything **managed** for you.
- Secure, real-time tracking from **any** PC - **no** software required.
- Weekly management reports sent to you in Excel format.
- Embedded links in location names provide quick access to maps.

New Product Features

Trip Number	Start Location	Departure Time
1	Tilbury Docks, TILBURY, Essex	06:39



Google Mobile | Latitude for your phone - Mozilla Firefox

File Edit View History Delicious Bookmarks Tools Help Google

http://www.google.com/mobile/default/latitude.html

On a mobile device? Click here

Google Mobile

Home Products: Search Maps Gmail YouTube More

Google Latitude

See your friends on a map and get in touch

Get Latitude on your phone

Enter your number or visit **google.com/latitude** on your mobile web browser.

(ex: 123-456-7890) Send a link



With Google Latitude, you can:

- See where your friends are and what they are up to
- Quickly contact them with SMS, IM, or a phone call
- Control what your location is and who gets to see it

Enjoy Google Latitude on your phone, PC, or both.

From your mobile phone - View your friends' locations and status messages and share yours with them. (Supported phones)

From your computer - View your friends' locations and status messages on a full screen even without a compatible phone or data plan. Click here to see your friends from your PC.

Consent

- ✓LBS ⇨ 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 (Art. 9 ePrivacy dir.)

Consent in LBS



Should either the subscriber or the user give their consent?

http://www.icri.be

Consent in LBS

- Enterprise services:
  - employer = subscriber
  - employee = user
- Protection of minors:
  - guardian = subscriber
  - minor = user

Withdrawal of the consent

- ✓Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.(Art.9 ePrivacy Dir)

Exception

- Emergency services

INTERESTING:

- In-vehicle emergency call (eCall) initiative

eCall Toolbox

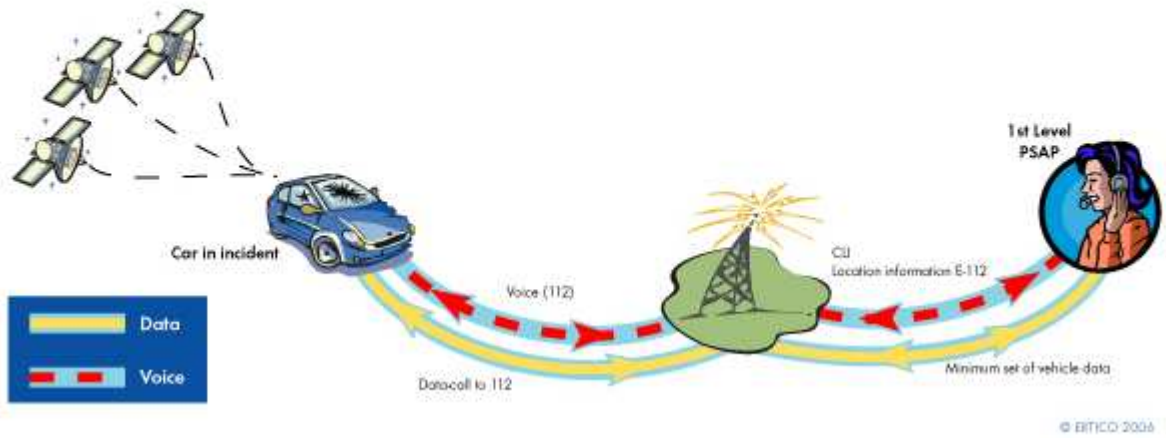
eCall is a high priority area within the European Commission. In order to help stakeholders better understand the aspects and issues surrounding the Emergency Call (eCall) chain, it was decided to create a dedicated eCall Toolbox.

The use of in-vehicle emergency call (eCall) to deploy emergency assistance will save lives and reduce the social burden of road accidents by improving the notification of such accidents, speeding up the emergency service response and lowering the subsequent effects on fatalities, severity of injuries and traffic flows.

eCall is an emergency call either generated manually by vehicle occupants or automatically via activation of in-vehicle sensors when an accident occurs. When activated, the in-vehicle eCall system establishes a 112-voice connection directly with the relevant PSAP (Public Safety Answering Point), which is a public authority or a private eCall centre that operates under the regulation and/or authorisation of a public body. At the same time, a minimum set of data (MSD) - including key information about the accident such as time, location and vehicle description - is sent to the PSAP operator receiving the voice call. The minimum set of data may also contain the link to a potential Service Provider by including its IP address and phone number. If the user is subscribed to a Service Provider, additional information can be sent from the service provider to the PSAP as illustrated below.

The eCall Toolbox is based on existing documents organised into different categories. If you would like to contribute any other information on this subject, please contact us on eCall@eSafetySupport.org

eCall Videos	.
Emege project	.WMV
eCall Video, September 2007 (low resolution)	.wmv



Unsolicited communications

… or simply SPAM



http://www.icri.be

Unsolicited communications

- Sending out e-mails, faxes, SMSs, making phone calls etc. for direct marketing purposes is allowed only with the prior consent ("opt-in" system)

Unsolicited communications

Exception for existing customers

- If a person or a company
- Receives electronic contact details for electronic mail
- From its customers
- In the context of the sale of a product or a service

⇨direct marketing for its own similar products or services is allowed

☺Right to object ("opt-out" system)



http://www.icri.be

Some more rules

- Itemised billing
- Caller ID (right both of calling and called party)
  - Exception: tracing of malicious or nuisance calls & emergency services
- Call forwarding
- Subscribers' directories (prior information & free of charge all changes)



Promusicae v Telefónica (ECJ)

- Judgement 29 January 2008, Case C275/06

- **ECJ**: "Community law does not require the Member States to lay down an obligation to disclose personal data in the context of civil proceedings."

Promusicae v Telefónica (ECJ)

- However MSs **may require** such disclosure and shall **strike a fair balance** between the various fundamental rights they protect when they transpose various directives on **intellectual property**, **e-commerce** and **data protection**, and must respect general principles of Community law, such as the **principle of proportionality** .

Directive 2006/24/EC

-

Data retention directive



http://www.icri.be

Things are not always what they appear to be…



http://www.icri.be

Before the directive…

- Art. 6 ePrivacy Dir.
  - ✓ Traffic data […] must be erased or made anonymous when it is *no longer needed* for the purpose of the transmission of a communication
  - ✓ Some data may be kept and further processed by service and network providers, *for their own business purposes*, such as billing, or after the consumer's *consent*.



Before the directive…

Art. 29 WP 69, Opinion 1/2003:

…"[a] routine storage period for billing [should have the duration of] maximum **3-6 months**, with the exception of particular cases of dispute where the data may be processed for a longer period."



http://www.icri.be

Before the directive…

- Art. 9 ePrivacy Dir.
  - ✓Processing of location data other than traffic data […] must be restricted to what is necessary for the purposes of providing the value added service.



Before the directive…

- Art. 15 ePrivacy Dir.
  - ✓ The measures shall be *legislative* in nature
  - ✓ only for a *limited* period
  - ✓ where *necessary, appropriate* and *proportionate* within a democratic society
  - ✓ to safeguard *national security, defence, public security* and the ***prevention, investigation, detection*** and ***prosecution of criminal offences*** or of *unauthorised use of the electronic communication system*

Campaign against data retention

- Civil Rights Organisations, Industry Members etc.:

"Data retention is no solution"



- Petition signed by 58265 people until 14.12.2005.

http://www.icri.be

Campaign against data retention



http://www.icri.be

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

(O.J. L.105, 13.04.2006, p.54-63)

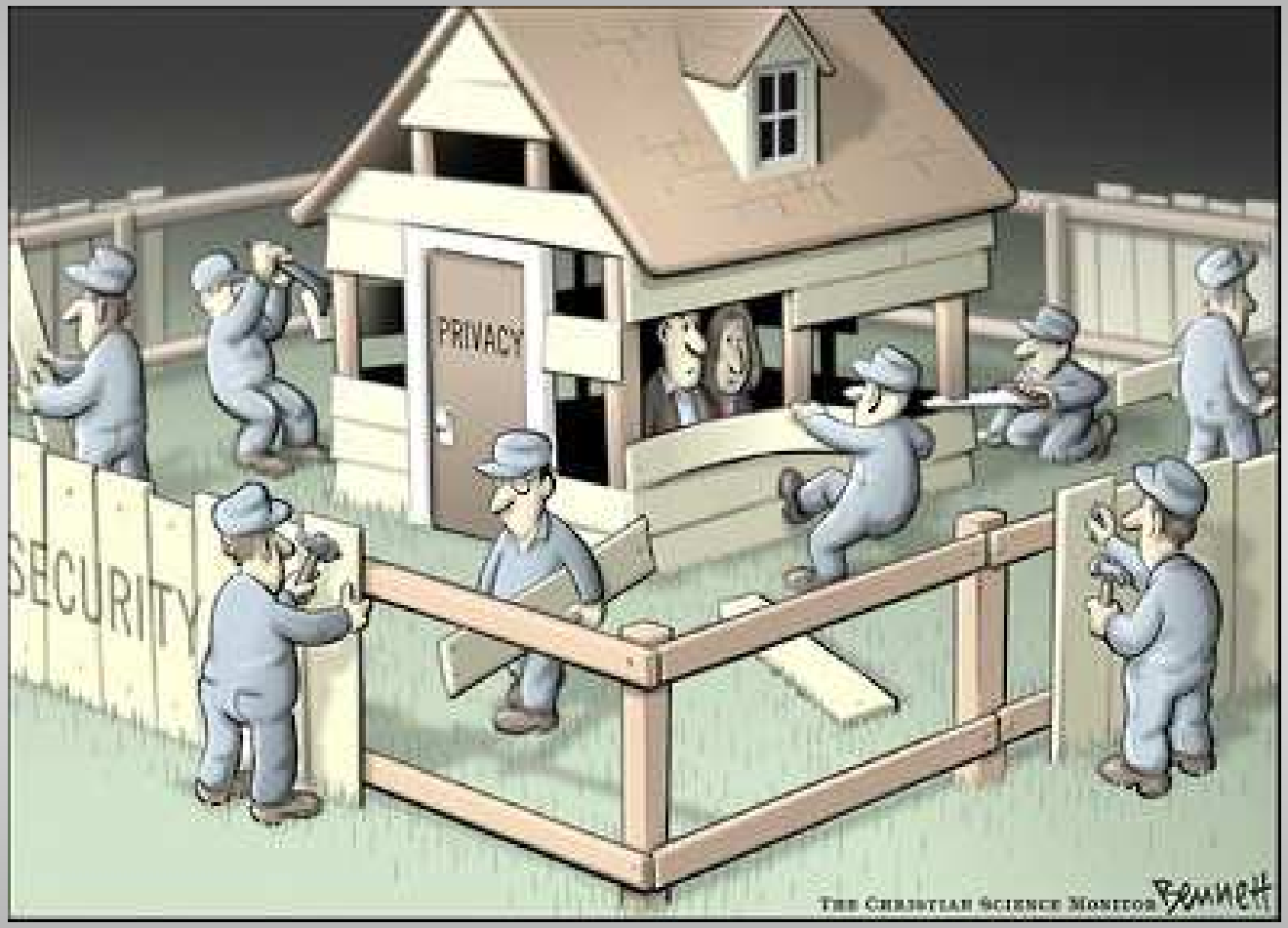


http://www.icri.be

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. (Art. 1(1) DRD)




PRIVACY
SECURITY
The Christian Science Monitor
Bennett

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



http://www.icri.be

Who shall retain the data?

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

Who shall retain the data?

But also…

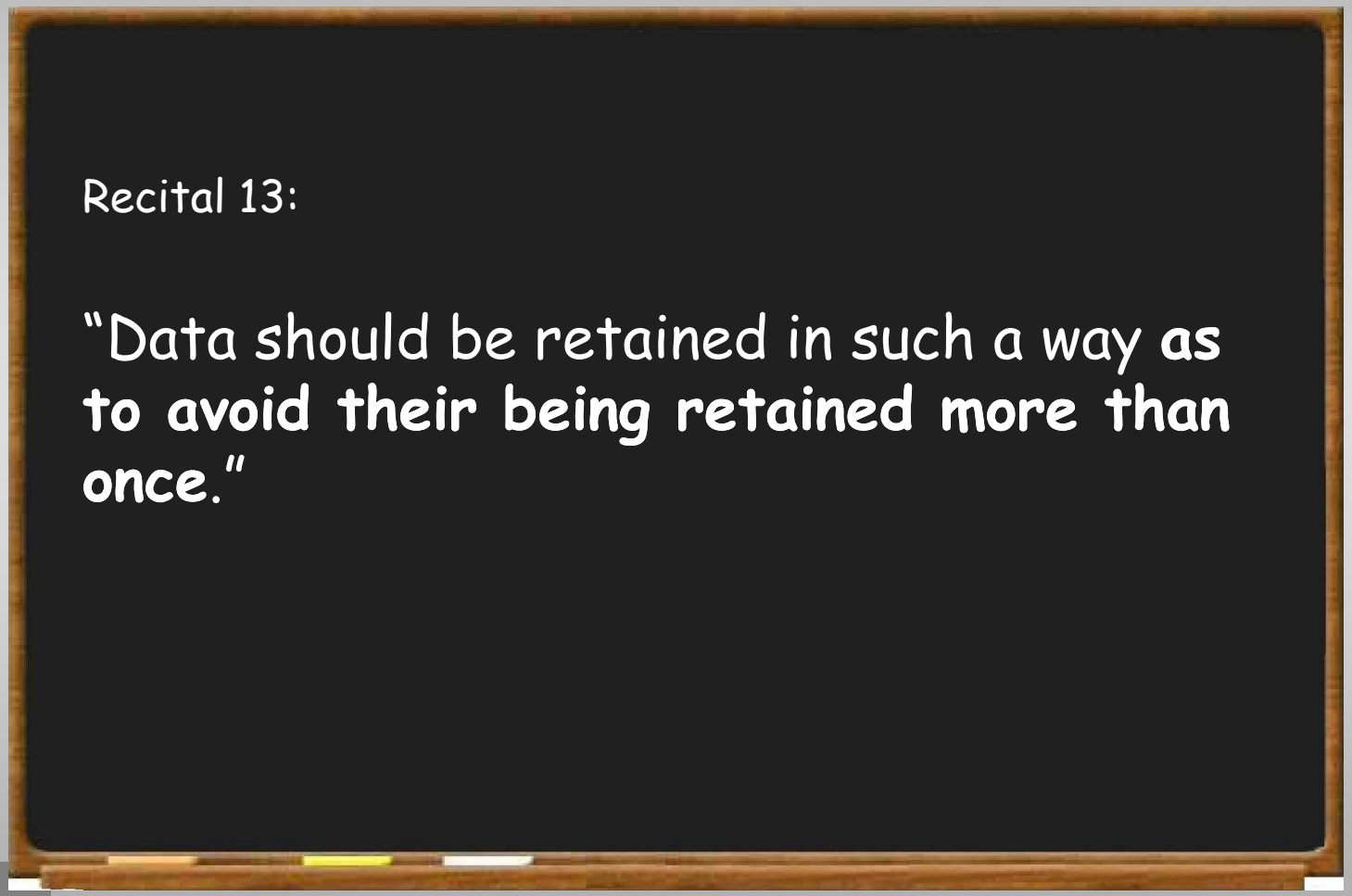
- Internet Cafes?
- Hotels?
- VNOs?
- Friends?

- Germany: anonymisation services



http://www.icri.be

Who shall retain the data?



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**



http://www.icri.be

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?

- A detailed list of data to be retained is included in Art. 5 DRD and not in an Annex, as was initially proposed.
- No "Commitology Procedure" to revise the Annex

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.



What data are to be retained?

Not the URL's of

the web pages we access



http://www.icri.be

What data are to be retained?

Search engines therefore fall outside of the scope of the definition of electronic communication services.

A search engine provider can however offer an additional service that falls under the scope of an electronic communications service such as a publicly accessible email service which would be subject to ePrivacy Directive 2002/58/EC and Data Retention Directive 2006/24/EC.

Article 5(2) of the Data Retention Directive specifically states that "No data revealing the content of the communication may be retained pursuant to this Directive". Search queries themselves would be considered content rather than traffic data and the Directive would

Any reference to the Data Retention Directive in connection with the storage of server logs generated through the offering of a search engine service is not justified.

Article 5 (3) and 13 of the ePrivacy Directive

Certain provisions of the ePrivacy Directive such as Article 5(3)(cookies and spyware) and Article 13 (unsolicited communications) are general provisions which are applicable not only to the electronic communication services but also to any other services when these techniques are used.



http://www.icri.be

Art. 29 WP, 148, Opinion on data protection issues related to search engines

E-mail

- Art. 5(c)(2)(ii) DRD:

  […] data necessary to identify the date, time and duration of a communication, concerning […] Internet e-mail: the date and time of the **log-in** and **log-off** of the **Internet e-mail service**, based on a certain time zone.



E-mail

- That means not the time when an e-mail is sent or received, but the time of logging–in and –off the Internet e-mail Service.

- Quid POP3?



http://www.icri.be

Data retention & ePrivacy Dir.

Art. 11 DRD (amending Art. 15 ePrivacy Dir):

> '1a. Paragraph 1 shall not apply to data specifically required by 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 to be retained for the purposes referred to in Art. 1(1) of that Directive.'



http://www.icri.be

Data retention & ePrivacy Dir.

- Art. 15 ePrivacy Dir.
  - ✓ The measures shall be *legislative* in nature
  - ✓ only for a *limited* period
  - ✓ where *necessary, appropriate* and *proportionate* within a democratic society
  - ✓ to safeguard *national security, defence, public security* and the ***prevention, investigation, detection*** and ***prosecution of criminal offences*** or of *unauthorised use of the electronic communication system*

Data retention & ePrivacy Dir.

- That means that MS's can retain more data according to Art. 15§1 ePrivacy Dir.



http://www.icri.be

No content data

Is it so easy to distinguish?

- eleni.kosta@law.kuleuven.be & peggy.valcke@law.kuleuven.be

- http://www.google.com/search?hl=en&q=gay+bars&btnG=Google+Search&aq=f&oq=

For how long?

- Art. 29 WP 25, Recommendation 3/99 (07 September 1999)

  ⇨ "Telecommunications operators, telecommunications service [providers] and ISP's should not be obliged to keep data for a period of time longer than **necessary for billing purposes.**

- European Data Protection Commissioners (09-11 September 2002)

  ⇨ "Systematic retention of all kinds of traffic data for a period of **one year or more** would be clearly **disproportionate** and therefore **unacceptable** in any case".

For how long?

- Art. 29 WP 69, Opinion 1/2003 (29 January 2003)

  ⇨"A routine storage period for billing of **maximum 3-6 months, with the exception of** particular cases of dispute where the data may be processed for a longer period".
- Art. 29 WP 99, Opinion 9/2004 (9 November 2004)

  ⇨ "Analysis carried out by telecommunication companies in Europe reveal the biggest amount of data demanded by law-enforcement were not older than **six months**. This shows that longer periods of retention are clearly disproportionate".

For how long?

And the directive decided…



http://www.icri.be

For how long?

- The data are to be retained for periods of not less than **six months** and not more than **two years** from the date of the communication. (Art. 6 DRD)



Possible extension of maximum retention period?

Art. 12 DRD:

- ❖ Particular circumstances
- ❖ For a limited time
- ⇨ Take necessary measures

  - ➢ Notify **immediately** the Commission
  - ➢ Inform the other MS's



http://www.icri.be

Possible extension of maximum retention period?

- Commission shall approve or reject the measure within **six months** after the notification
- Otherwise: It is rendered approved

Possible extension of maximum retention period?

!!! Art. 12§3:

"Where, pursuant to paragraph 2, the national measures of a Member State derogating from the provisions of this Directive are approved, the Commission **may consider** whether to propose an **amendment** to this Directive."

Who can have access to these data?

- Art. 4 DRD: Data are provided only to the **competent national authorities** in specific cases and in accordance with national law.

- Quid **competent national authorities**??
- List?? (Art. 29 WP asks for a list of designated law enforcement authorities)



When shall access be allowed?

- Decision of the provider?
- Court order?



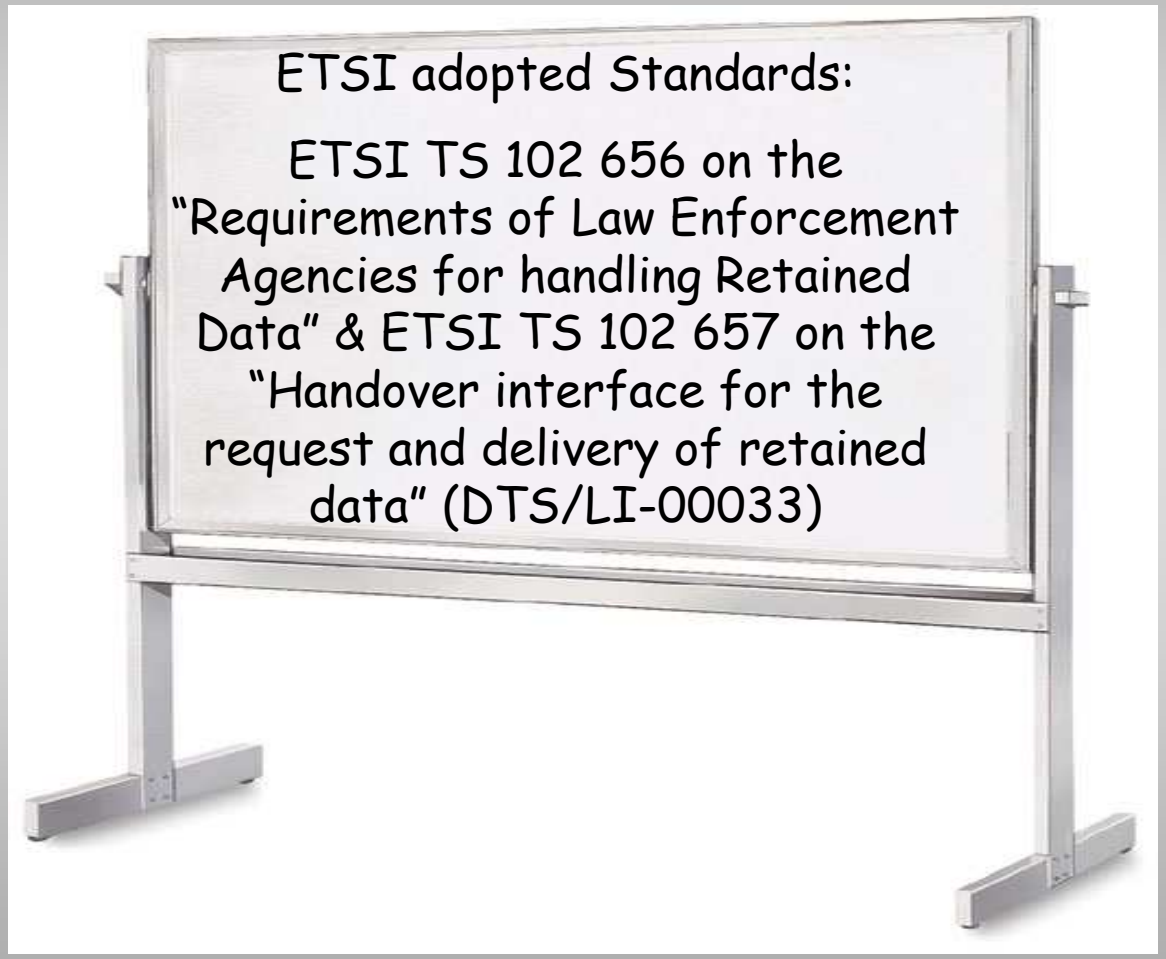
http://www.icri.be

How will data be transferred?

- Raw data?
- Concrete information?

…'in order to ensure that the data are **available** for the purpose of the investigation, detection and prosecution of serious crime'

How will data be transferred?



Response time

- Not foreseen
- In general: ‘without delay’



Cost reimbursement

Not included in the directive



Transposition

- No later than 15 September 2007 (15 (1) DRD)



Transposition

- Each Member State **may** postpone application of this Directive to the retention of communications data relating to **Internet Access, Internet telephony** and **Internet e-mail** until **15 March 2009**. (15(3) DRD)

Transposition

* MS's shall notify the Council and the Commission to that effect by way of a **declaration** upon adoption of the Directive

* 16 MS's filed such declaration
* Bulgaria & Romania



http://www.icri.be

Impact on the industry



ALLE DIENSTEN | INTERNET TOEGANG | WEBSITE/E-MAIL | EIGEN SERVER

XS4ALL

STOP DE BEWAARPLICHT

NIEUWS | OVER XS4ALL | CONTACT | VEILIGHEID | WEBMAIL | SERVICE CENTRE | HELPDESK

TELLER DATAVERKEER XS4ALL

De hoeveelheid dataverkeer uitgedrukt in datapakketten die XS4ALL in totaal heeft vervoerd sinds:
5 september 2005

	Hoeveelheid datapakketten	Uitgedrukt in CD's
Inkomend	59.827.954.638.403	52.410.367
Uitgaand	59.827.952.842.363	52.410.366
Totaal	119.655.907.480.770	104.820.733

De eerste kolom laat de hoeveelheid data in IP pakketten zien, de tweede toont diezelfde hoeveelheid data uitgedrukt in Compact Discs van 700 MB. De datapakketten hebben een gemiddelde grootte van ongeveer 630 bytes.

De teller wordt automatisch door uw browser opgehoogd maar wordt periodiek gesynchroniseerd met de actuele tellers van het XS4ALL netwerk.

icri

http://www.icri.be

http://www.xs4all.nl/bewaarplicht/

Impact on the industry

Data security obligations (Art. 7 DRD)

The retained data shall be:

- ✓ of the same **quality** and subject to the same security and protection as those data on the network;
- ✓ subject to appropriate technical and organisational measures to **protect** the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;



http://www.icri.be

Impact on the industry

- ✓ subject to appropriate technical and organisational measures to ensure that they can be accessed by **specially authorised personnel only**;
- ✓ the data, except those that have been accessed and preserved, shall be **destroyed** at the end of the period of retention.



http://www.icri.be

Experts Group

Experts Group on the transposition of the Data Retention Directive:

- Web Mail
- Spam e-mail
- Internet transit providers
- VoIP/ "Internet Telephony"
- Centralised Data Storage within EU
- Data Security issues
- …

Implementation status

- A few countries had data retention legislation prior to the directive and they will now have to amend it in order to comply with the directive
- Many Member States have transposed the directive, while others are still working on the national legislation



Ireland v Council of the European Union, European Parliament

- Case C-301/06
  - Ireland asked the annulment of the directive on the grounds that it was not adopted on an appropriate legal basis.



http://www.icri.be

Ireland v Council of the European Union, European Parliament

- The ECJ on its judgment on 10 February 2009 found that the Data Retention Directive relates predominantly to the functioning of the **internal market** and was correctly adopted on the basis of Article 95 EC.



http://www.icri.be

ECHR Case: Copland v. U.K.

- Judgement 3 April 2007, Application no. 62617/00
- ECHR: "the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8."



http://www.icri.be

BVerfG – German Constitutional Court

- Interim ruling 1BvR 256/08, 11.03.2008
- BVerfG: found that data retention is not as such unconstitutional. However, it ruled that the German Law transposing the Data Retention Directive did not provide sufficient guarantees concerning the access to the data and the crimes for which data retention may be used.



BVerfG – German Constitutional Court

- **BVerfG:** It also repeated that data retention may only be used for serious crimes and when a judicial warrant is present and concluded that §113b of the Telecommunications Act (TKG) should be revised.

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