# Tracking trends: Location Tracking and Do Not Track

IFIP Summer School

Thursday, 08 September 2011

Dr Eleni Kosta

ICRI – K.U.Leuven



# Overview

1. Location data: location mining
2. Processing of location data/traffic data
3. Cookies
4. Do Not Track



# 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.**

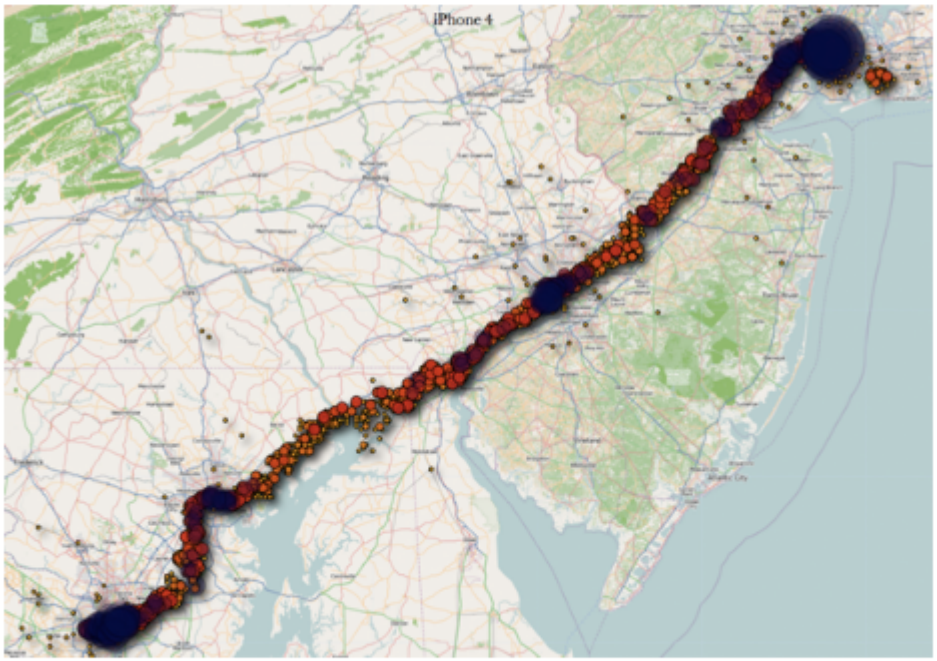
by Alasdair Allan | @aallan | Comments: 230 | 20 April 2011

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

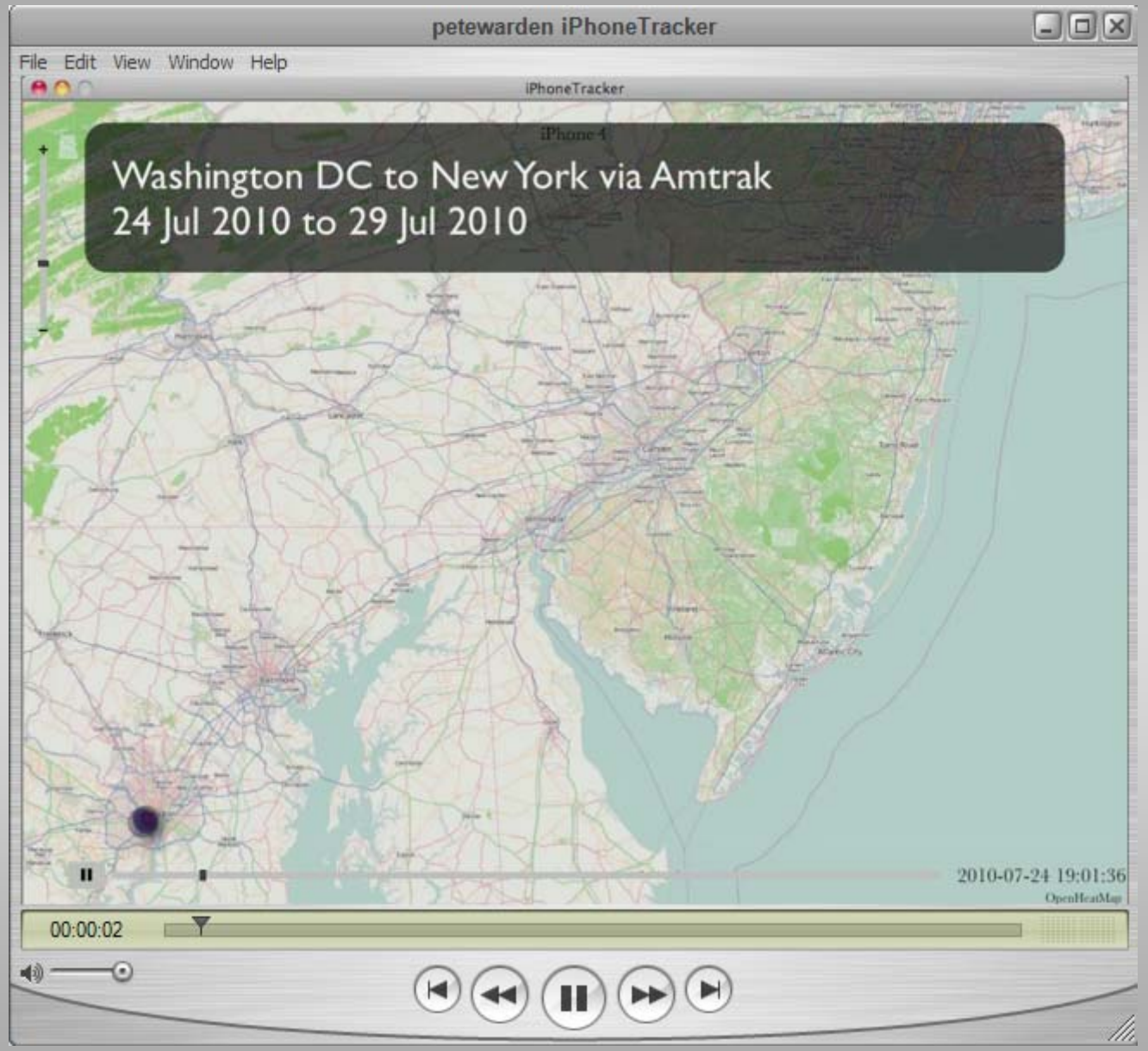
IT

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

# 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



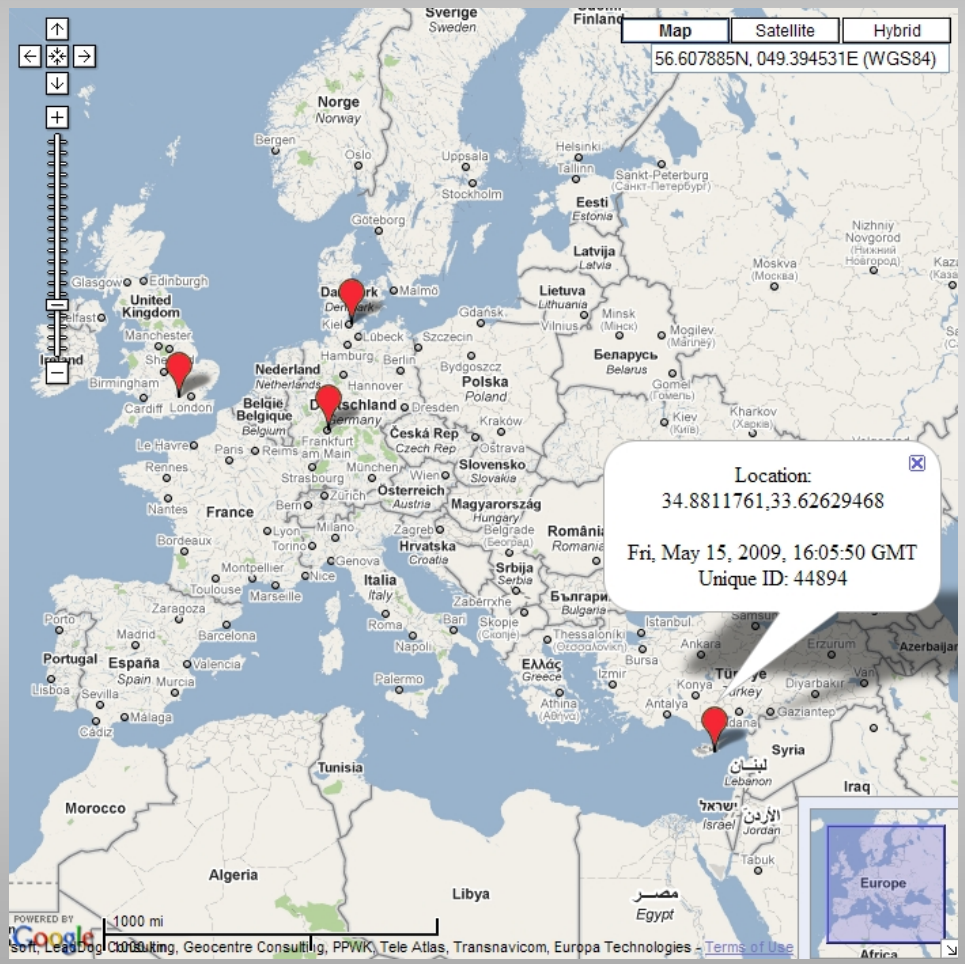
# Location Mining Case Study

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





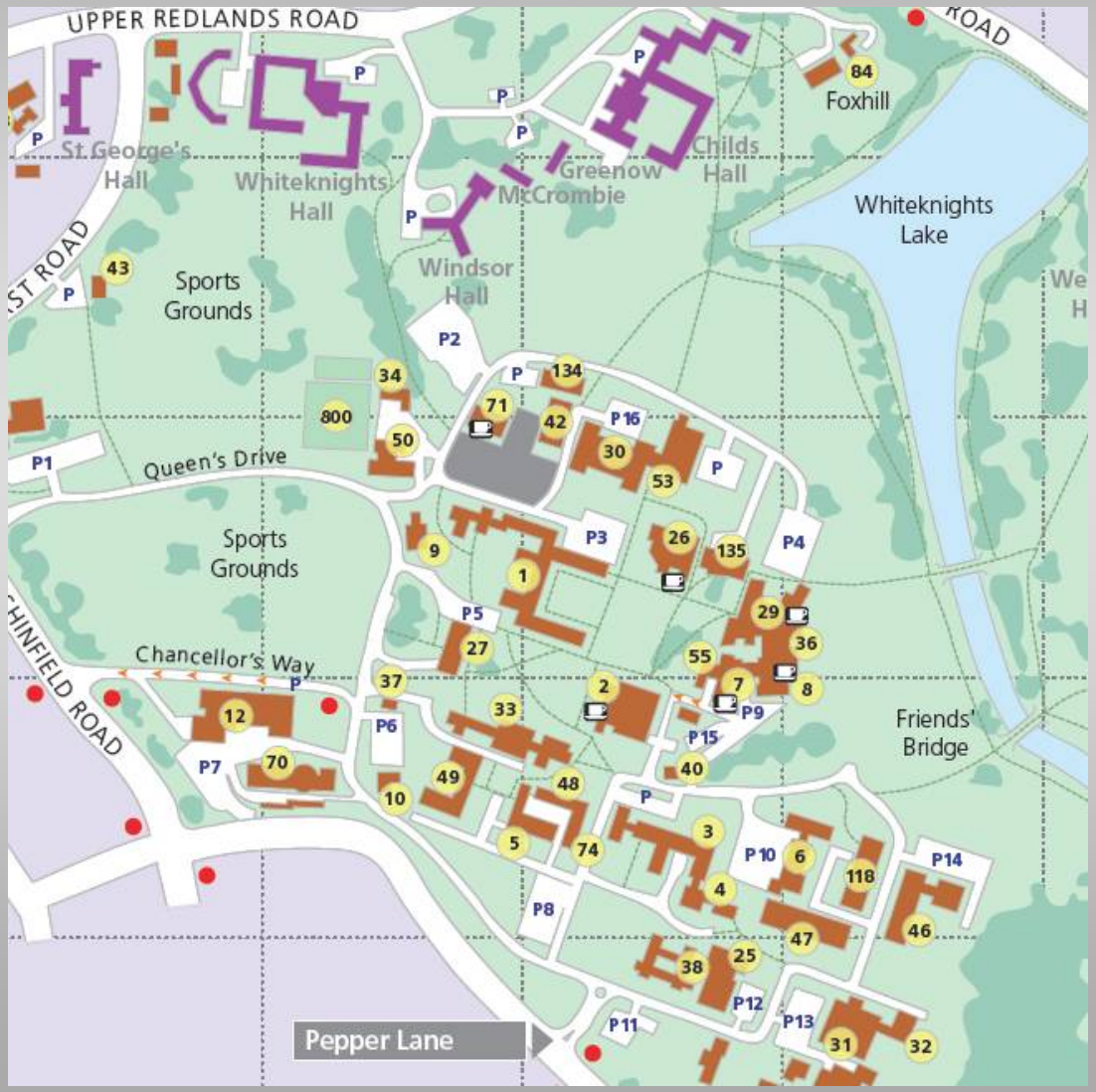

# Location Mining Case Study

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

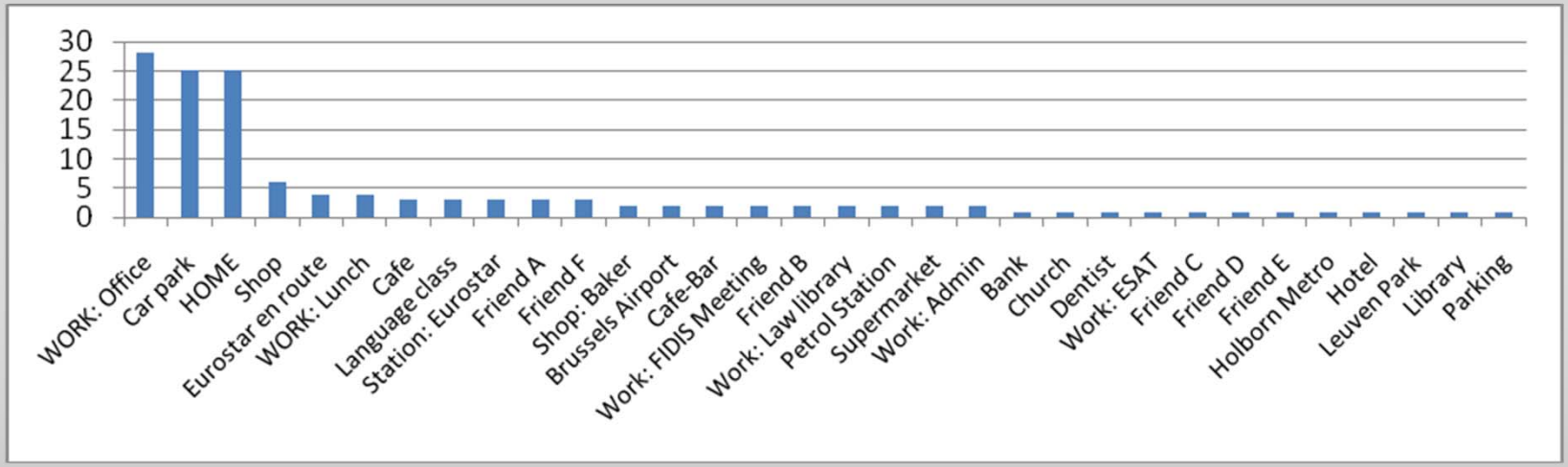
- One of the key tools for initial mining is the generation of 'Points of Interest' (PoI) from the data



# Points of Interest (PoI)



# PoIs at identified locations collected from each user

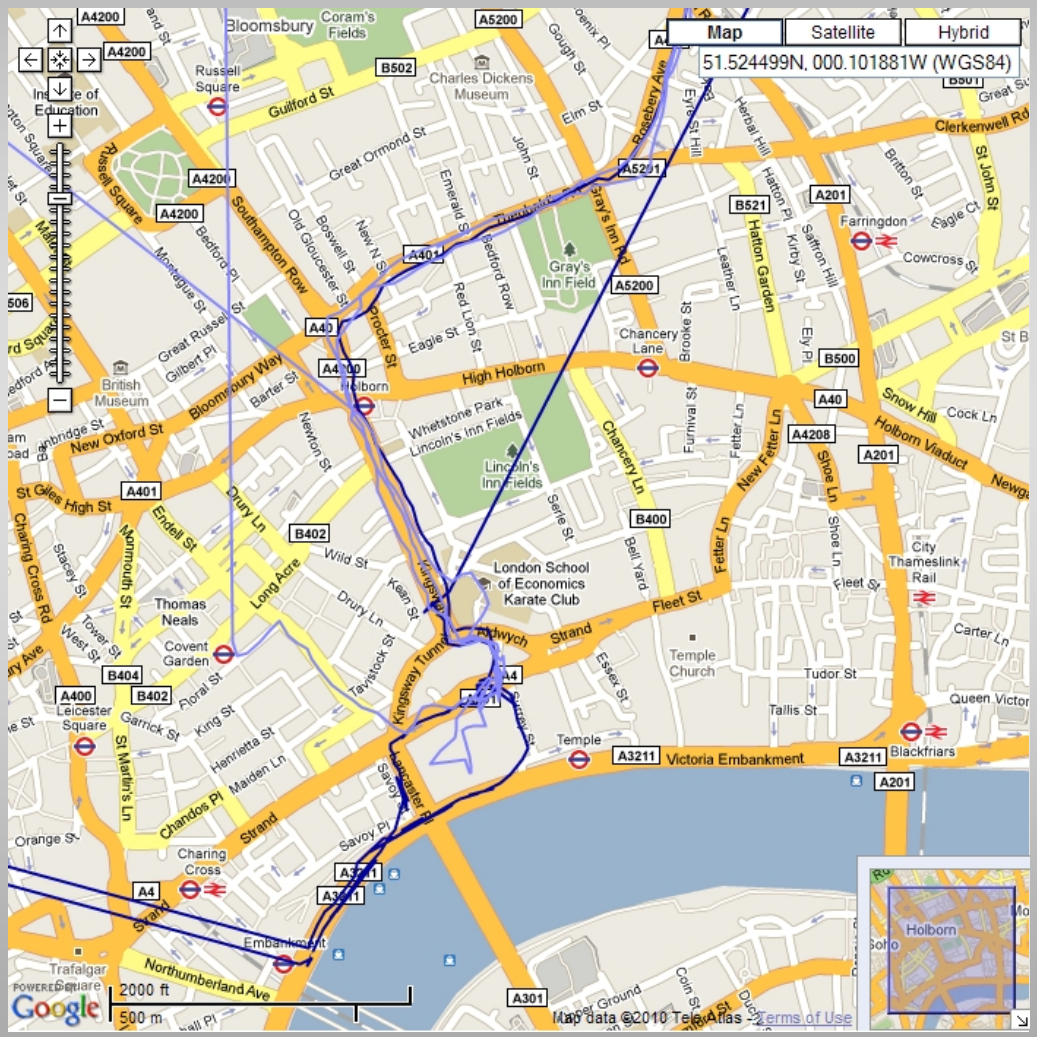



Frequency of PoIs

icri


Map
Satellite
Hybrid
49.582226N, 003.295898E (WGS84)
London
Paris
Amsterdam
Brussel
Bruxelles
Antwerpen
Rotterdam
Den Haag
Utrecht
Eindhoven
Le Havre
Rouen
Amiens
Caen
Évreux
Beauvais
Compiègne
Saint-Quentin
Lille
Dunkerque
Calais
Boulogne-sur-Mer
Brugge
Gent
Mechelen
Leuven
Tourcoing
Kortrijk
Roeselare
Ieper
Oostende
Terneuzen
Roosendaal
Breda
Den Helder
Alkmaar
Hoorn
Lelystad
Haarlemmermeer
Spijkenisse
's-Hertogenbosch
Oss
Charleroi
Namur
Mons
Tournai
Béthune
Lens
Carvin
Arras
Douai
Cambrai
Caudry
Abbeville
Doullens
Eu
Dieppe
Fécamp
Bolbec
Honfleur
Trouville-sur-Mer
Lisieux
Bayeux
Coutances
Saint-Lô
Falaise
Cergy
Meaux
Châlons-en-C
Reim
Charleville-Mézières
Sedan
Luxer
Aalst
Maas
Liège
Namur
Harlingen
Smallin
Lelystad
Amersfoort
Oss
Eindhove
Neder
Belgique
Belgium
Rennes
Paris
Havre
Sheffield
Chester
London
Scunthorpe
Louth
Lincoln
Chesterfield
Mansfield
Nottingham
Boston
Cromer
North Walsham
King's Lynn
Great Yarmouth
Norwich
Lowestoft
Beccles
Peterborough
Corby
Leicester
Coventry
Northampton
Bedford
Cambridge
Ipswich
Colchester
Felixstowe
Milton Keynes
Luton
Chelmsford
St Albans
Basildon
Southend-on-Sea
Reading
Woking
Gillingham
Maidstone
Basingstoke
Guildford
Crawley
Brighton
Bognor Regis
Bexhill
Hastings
Eastbourne
Portsmouth
Swindon
Cheltenham
Oxford
Hampton
Bournemouth
Weymouth
Cherbourg-Octeville
Toll
M1
M2
M3
M4
M11
M18
M23
M25
M40
M42
M69
A1(M)
E22
E30
E31
E34
E35
E40
E42
E44
E46
E50
E15
E17
E19
E231
E312
E313
E314
E403
E401
E402
E411
E420
100 mi
100km
Map data ©2010 Tele Atlas
Terms of Use

# 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 | Location data: location mining |
| 2 | Processing of location data/traffic data |
| 3 | Cookies |
| 4 | Do Not Track |

# 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
- ✓Data retention



# 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

# 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 | Location data: location mining |
| 2 | Processing of location data/traffic data |
| 3 | Cookies |
| 4 | Do Not Track |



icri

# Confidentiality

- 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



# 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

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

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.

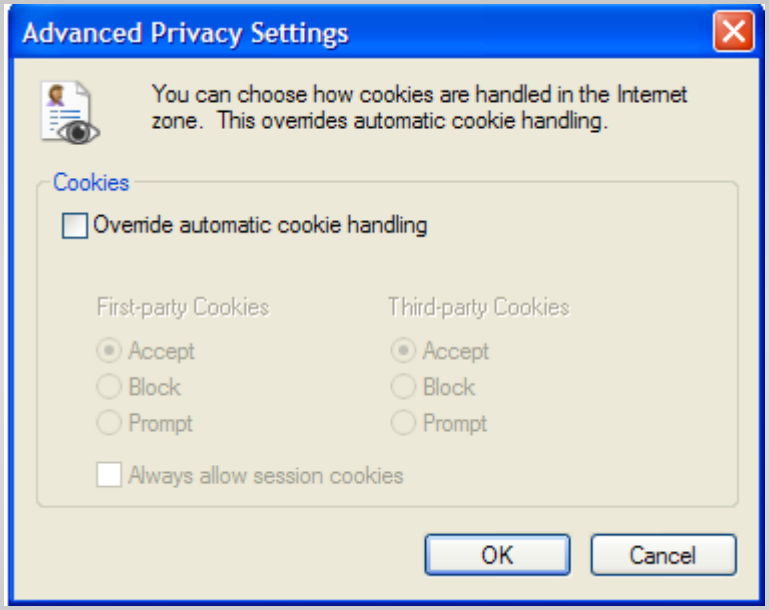
The Working Party notes that both definitions 'electronic communications services', and 'to provide an electronic communications network' are still not very clear and both terms should be explained in more details in order to allow for a clear and unambiguous

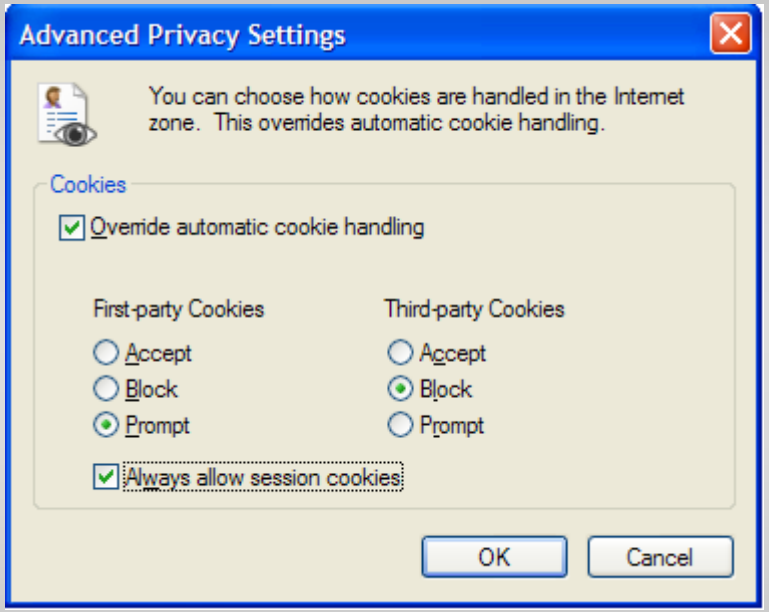
Recital 25 [...] might be contradictory with the position that the users should have the possibility to refuse the storage of a cookie on their personal computers and therefore may need clarification or revision.

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




icri

# Right to object vs. consent | 5

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

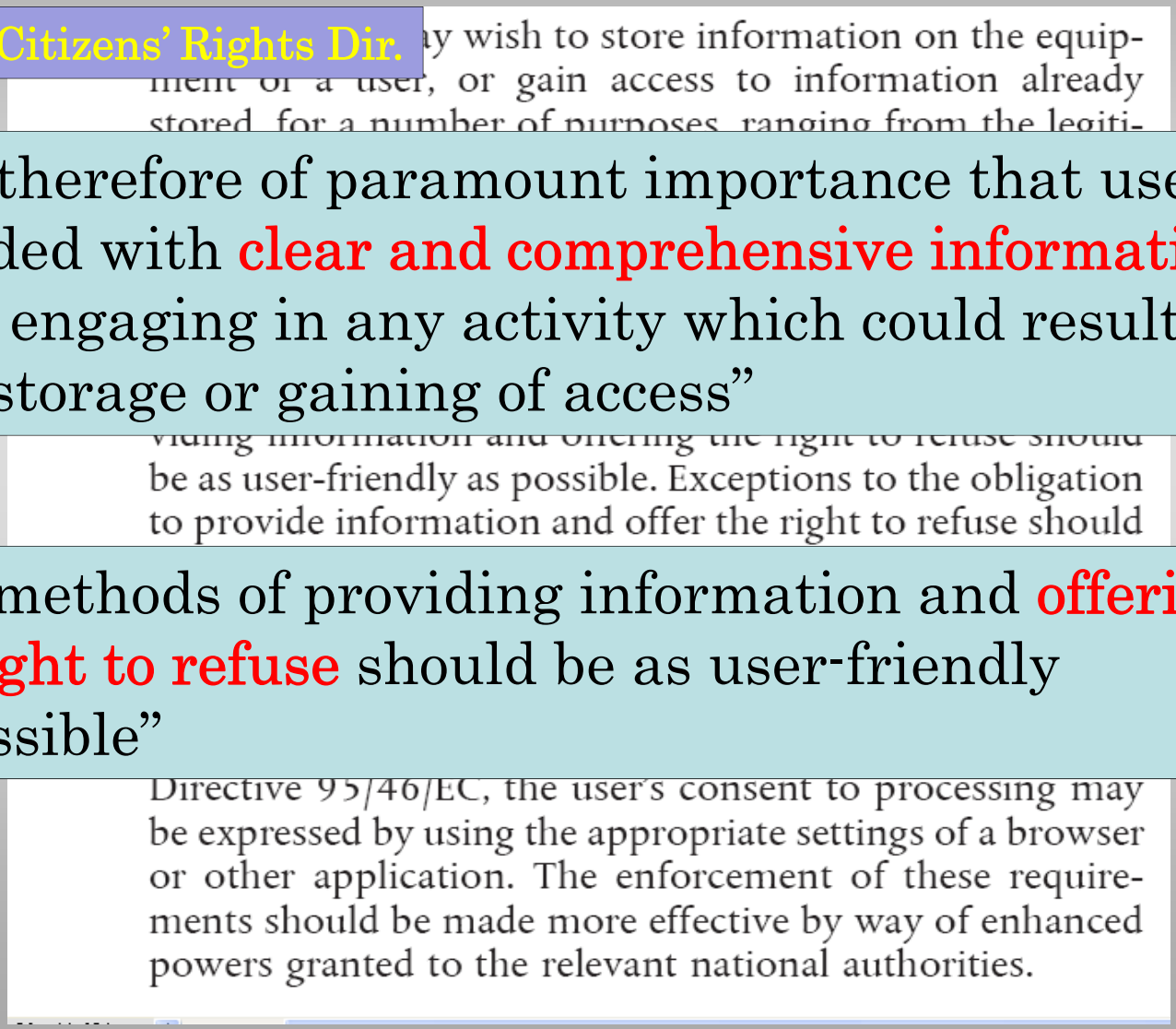
"has given his or her consent, having been provided with clear and comprehensive information"

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

icri

# Right to object vs. consent |6

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 | 7

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 |8

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

# UK

**What do the new rules say?**

The new requirement is essentially that cookies can only be placed on machines where the user or subscriber has given their consent.

> *6 (1) Subject to paragraph (4), a person shall not store or gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met.*
>
> *(2) The requirements are that the subscriber or user of that terminal equipment--*
>
> *(a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and*
>
> *(b) has given his or her consent.*

**UK PECR 2011**
**UK ICO 09.05.2011 advice on cookies**

# France

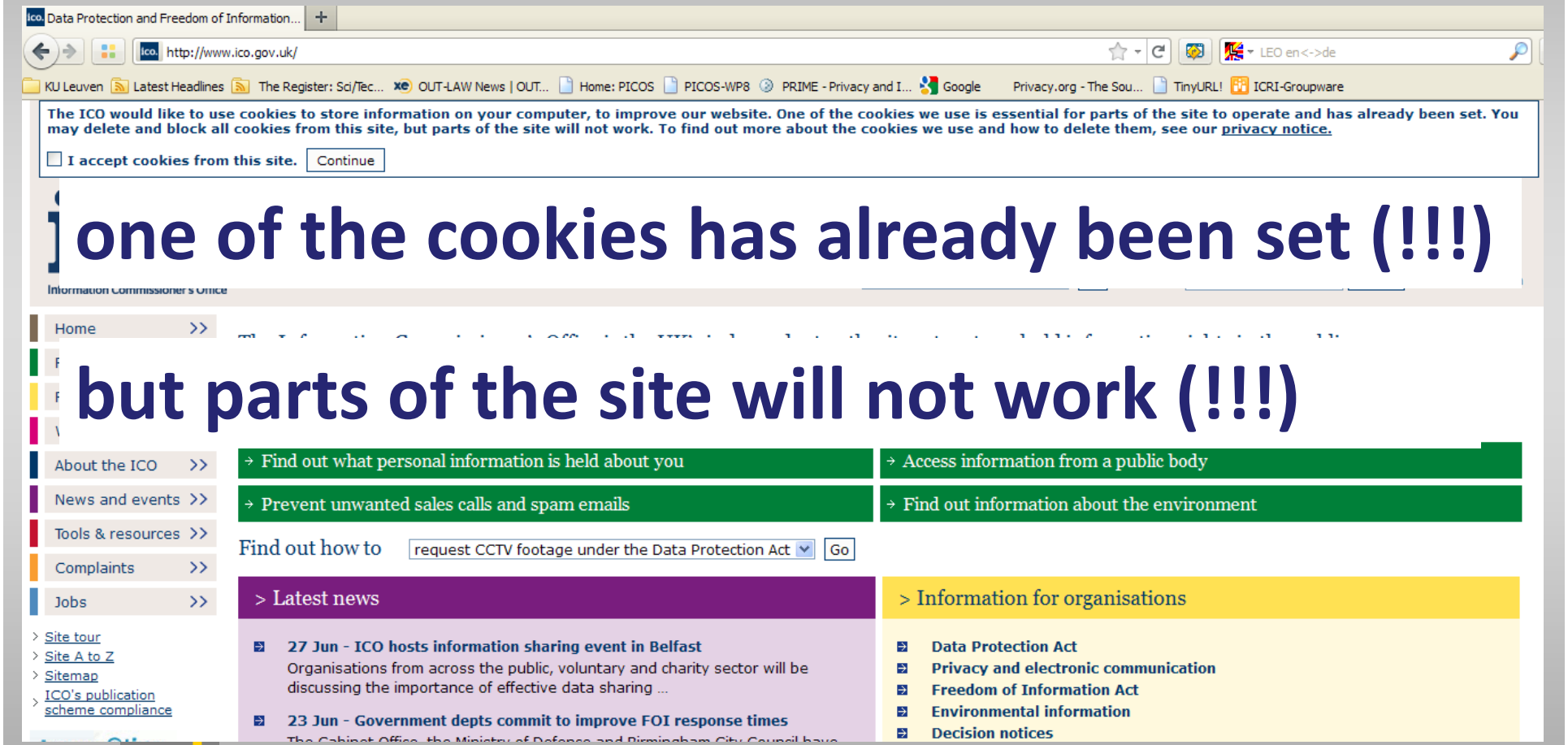
Consent for cookies may be obtained via user-controlled settings on the relevant device.

- No requirement for the user to amend or set the settings!

Ordonnance n° 2011-1012 du 24 août 2011
relative aux communications électroniques



# The way forward?





First-party cookies

Third-party cookies

icri

The next sub-sections analyse whether consent by the way of browser settings and opt-out options provided by ad network providers meet the requirements of Article 5(3).

**4.1.1. Consent by the way of browser settings**

Given the importance that browser settings play in ensuring that data subjects effectively give their consent to the storage of cookies and the processing of their information, it seems of paramount importance for **browsers to be provided with default privacy-protective settings**. In other words to be provided with the setting of 'non-acceptance and non-transmission of third party cookies'

expressed by using the appropriate settings of a browser or other application, "*where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC*". This is not an exception to Article 5(3) but rather a reminder that, in this technological environment, consent can be given in different ways - where technically possible, effective and in accordance with the other relevant requirements for valid consent.

Art. 29 WP, 171, Opinion 2/2010 on online behavioural advertising

THE WALL STREET JOURNAL.

Get 2 weeks to WSJ.com FREE!
SUBSCRIBE NOW ▸

Europe Edition Home ▾ | Today's Paper ▪ Video ▪ Blogs ▪ Journal Community ▪ Mobile ▪ Tablet
Subscribe | Log In

World ▾ | Europe ▾ | U.K. ▾ | U.S. ▾ | Business ▾ | Markets ▾ | Market Data ▾ | Tech ▾ | Life & Style ▾ | Opinion ▾ | Jobs ▾

# What They Know

Like 211 Ser + More

**Marketers are spying** on Internet users -- observing and remembering people's clicks, and building and selling detailed dossiers of their activities and interests. The Wall Street Journal's What They Know series documents the new, cutting-edge uses of this Internet-tracking technology. The Journal analyzed the tracking files installed on people's computers by the 50 most popular U.S. websites, plus WSJ.com. The Journal also built an "exposure index" -- to determine the degree to which each site exposes visitors to monitoring -- by studying the tracking technologies they install and the privacy policies that guide their use.

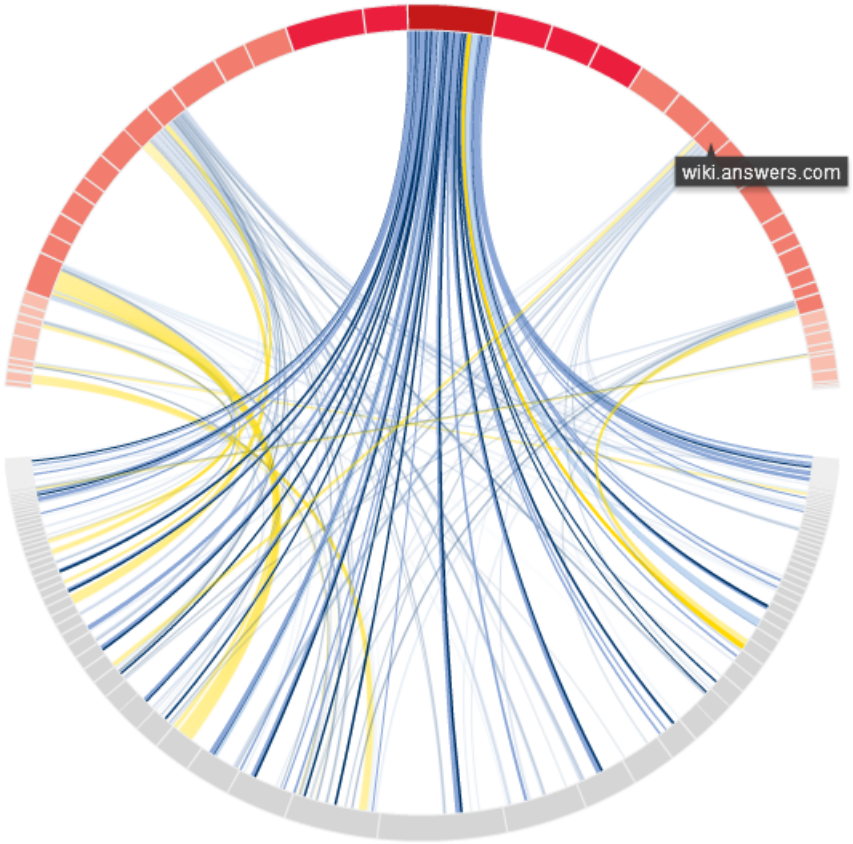
## Recent Stories

- The Web's New Gold Mine: Your Secrets
- Personal Details Exposed Via Biggest U.S. Websites
- Microsoft Quashed Bid to Boost Web Privacy

More views of the data »
APPS
KIDS
THE TOP 50 SITES

Begin introduction

Explore the data




Credits


YOU CAN CLICK
BUT YOU
CAN'T HIDE

# Overview

1. Location data: location mining
2. Processing of location data/traffic data
3. Cookies
4. Do Not Track

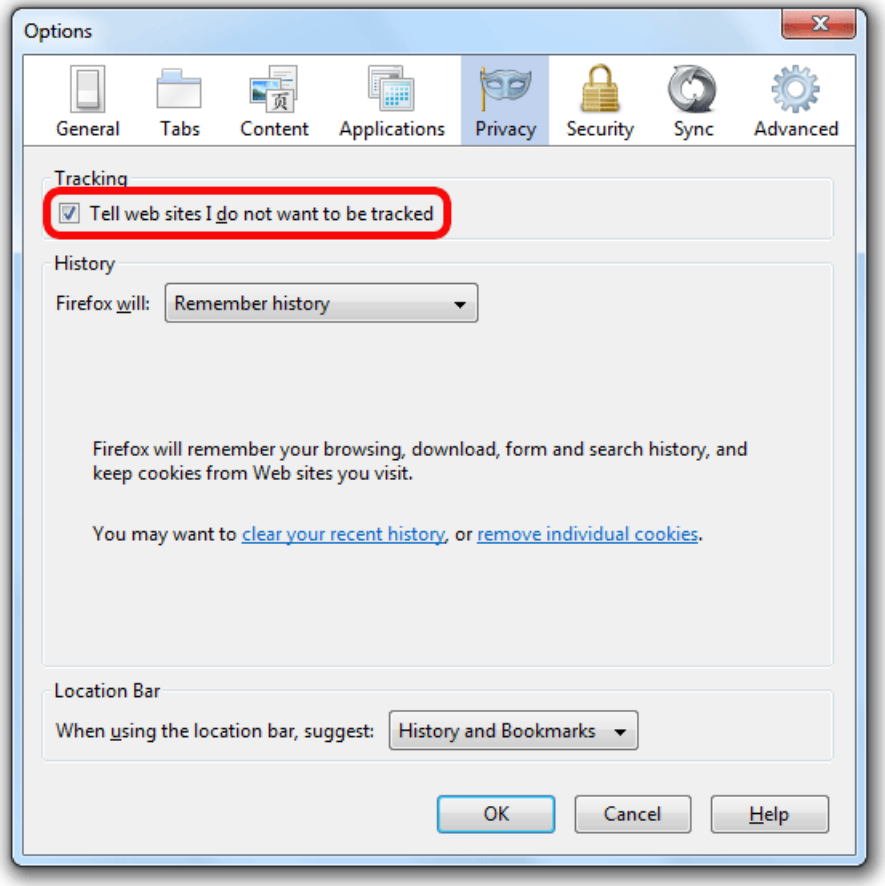

mozilla
Firefox
» Do Not Track FAQ
DO NOT TRACK
Mozilla is a global, nonprofit organization dedicated to making the Web better. We emphasize principle over profit, and believe that the Web is a shared public resource to be cared for, not a commodity to be sold. We answer to no one but you and believe it is crucial to put you in control of your online experience. We are aiming to give you better insight and control into the ways your personal information is collected, used, stored and shared online.
Mozilla Firefox offers a Do Not Track feature that lets you express a preference not to be tracked by websites. When the feature is enabled, Firefox will tell advertising networks and other websites and applications that you want to opt-out of tracking for purposes like behavioral advertising.

icri

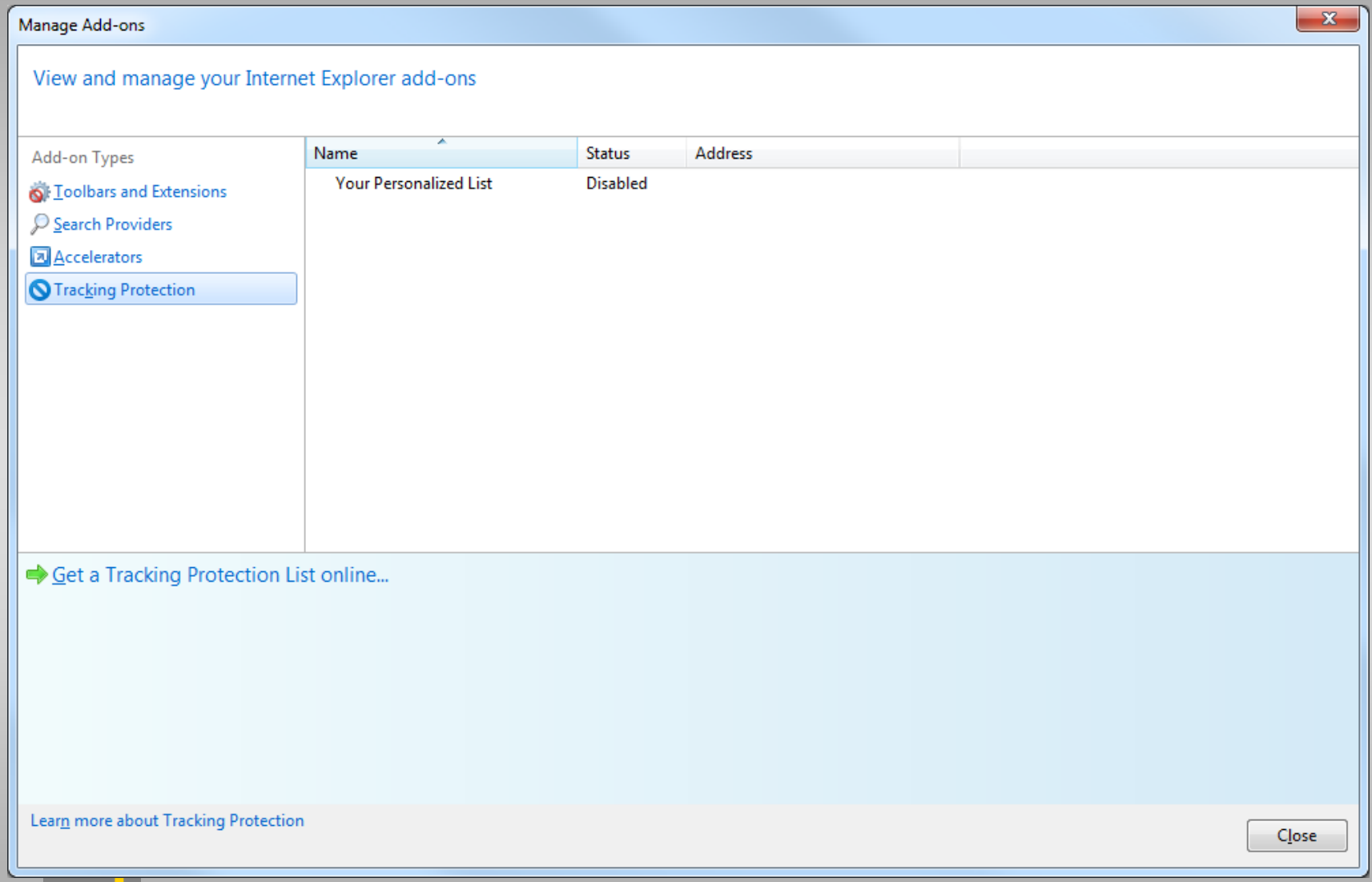
# How do I turn the Do-not-track feature on?

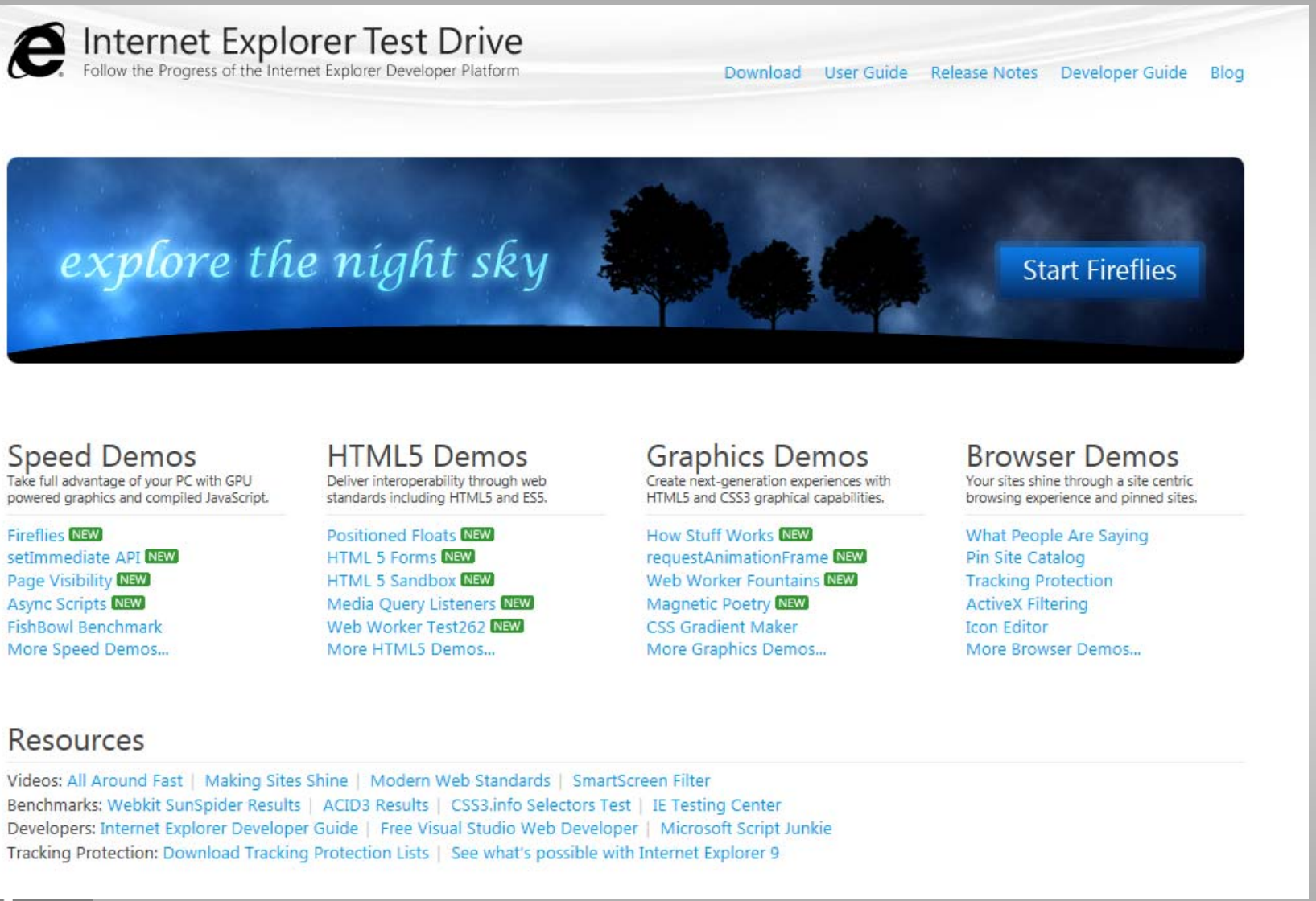
The Do-not-track feature is turned off by default. To turn it on:

1. At the top of the Firefox window, click on the Firefox button ( Tools menu in Windows XP) and then click Options . .
2. Select the Privacy panel.




3. Check **Tell websites I do not want to be tracked.**
4. Click OK to close the Options window.


Manage Add-ons
View and manage your Internet Explorer add-ons
Add-on Types
Toolbars and Extensions
Search Providers
Accelerators
Tracking Protection
Name
Status
Address
Your Personalized List
Disabled
Get a Tracking Protection List online...
Learn more about Tracking Protection
Close


Internet Explorer Test Drive
Follow the Progress of the Internet Explorer Developer Platform
Download
User Guide
Release Notes
Developer Guide
Blog
explore the night sky
Start Fireflies
Speed Demos
Take full advantage of your PC with GPU powered graphics and compiled JavaScript.
Fireflies NEW
setImmediate API NEW
Page Visibility NEW
Async Scripts NEW
FishBowl Benchmark
More Speed Demos...
HTML5 Demos
Deliver interoperability through web standards including HTML5 and ES5.
Positioned Floats NEW
HTML 5 Forms NEW
HTML 5 Sandbox NEW
Media Query Listeners NEW
Web Worker Test262 NEW
More HTML5 Demos...
Graphics Demos
Create next-generation experiences with HTML5 and CSS3 graphical capabilities.
How Stuff Works NEW
requestAnimationFrame NEW
Web Worker Fountains NEW
Magnetic Poetry NEW
CSS Gradient Maker
More Graphics Demos...
Browser Demos
Your sites shine through a site centric browsing experience and pinned sites.
What People Are Saying
Pin Site Catalog
Tracking Protection
ActiveX Filtering
Icon Editor
More Browser Demos...
Resources
Videos: All Around Fast | Making Sites Shine | Modern Web Standards | SmartScreen Filter
Benchmarks: Webkit SunSpider Results | ACID3 Results | CSS3.info Selectors Test | IE Testing Center
Developers: Internet Explorer Developer Guide | Free Visual Studio Web Developer | Microsoft Script Junkie
Tracking Protection: Download Tracking Protection Lists | See what's possible with Internet Explorer 9


icri

# Tracking Protection Lists

Below are several Tracking Protection Lists (also called TPLs) created by companies and organizations that want to help consumers understand and make choices about their online privacy. You can add individual lists by clicking the "Add TPL" links on the right side of the page. To manage your lists, click on the **Tools** button, point to **Safety**, then click **Tracking Protection**. These tracking protection lists were created by their respective authors, who are solely responsible for maintaining the lists and for their content. Microsoft does not control any of these lists. Click here for answers to commonly asked questions about TPLs.




Abine, The Online Privacy Company, is the leading provider of online privacy solutions for consumers. Abine's products and services allow regular people to regain control over their personal information while continuing to browse, interact, and shop online.

Add TPL

Abine's Tracking Protection List blocks many online advertising and marketing technologies that can track and profile you as you browse the Web. This list is updated weekly to keep you safer and more private.

Visit the Abine website for more information about this Tracking Protection List.




EasyPrivacy Tracking Protection List is based on the popular EasyPrivacy subscription for Adblock Plus and is managed by the well-known EasyList project, which serves nearly ten million daily users and has a large support forum with dozens of experienced members able to assist resolving any issues that may arise.

Add TPL

Visit the EasyList website for more information about this Tracking Protection List.




PrivacyChoice maintains a comprehensive database of tracking companies, including domains used by nearly 300 ad networks and platforms, tracking methods, summaries of key policies, oversight, and opt-out and opt-in processes.

Add TPL 1

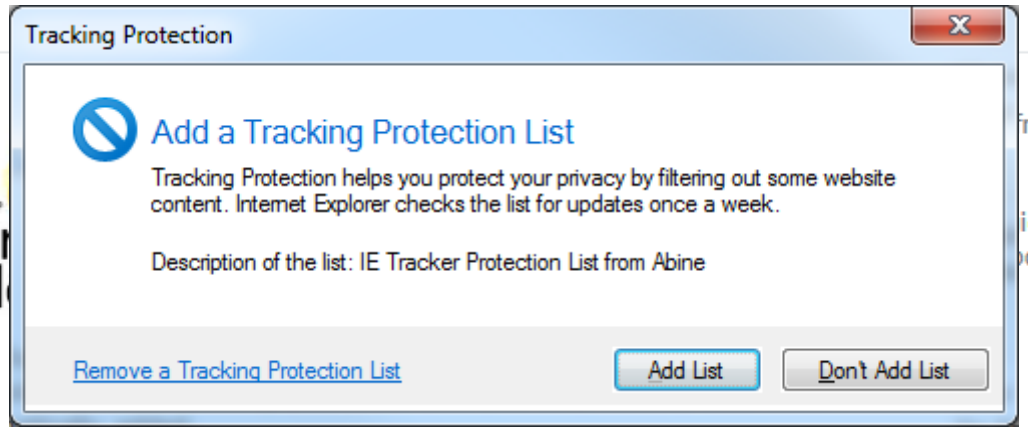
PrivacyChoice has created Tracking Protection Lists based on this data. You have the option of installing two lists. The first list blocks companies that are not subject to oversight by the NAI and the second list blocks all tracking company domains in the PrivacyChoice database. These lists will be automatically updated with new tracking domains discovered through continuous website scanning and user panels.

Add TPL 2

Visit the PrivacyChoice website for more information about this Tracking Protection List.



ABINE

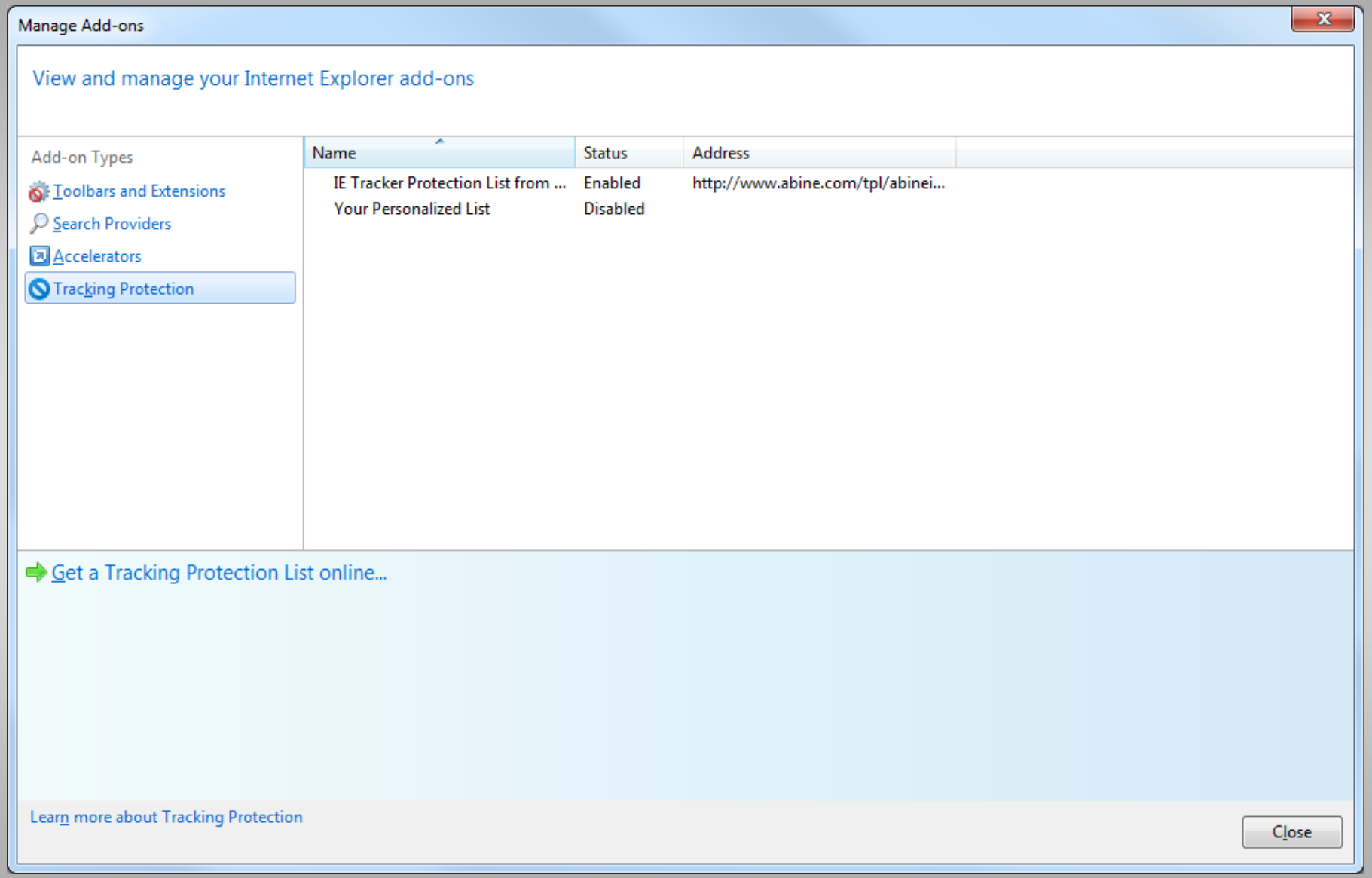



Using your IE9 Browser, click here and the list will be automatically added.

Get a Tracking Protection list focused on the top websites used by kids and teens. You can use this list alone, or add it alongside other IE tracking protection lists you may already use. Click here and the list will be automatically added.

For more information, a detailed description of the trackers in our latest list, or questions on other privacy enhancing technologies and services, visit out support page anytime.

icri


Manage Add-ons
View and manage your Internet Explorer add-ons
Add-on Types
Toolbars and Extensions
Search Providers
Accelerators
Tracking Protection
Name
Status
Address
IE Tracker Protection List from ...
Enabled
http://www.abine.com/tpl/abinei...
Your Personalized List
Disabled
Get a Tracking Protection List online...
Learn more about Tracking Protection
Close

"If you are not paying for it, you're not the customer; you're the product being sold"

blue_beetle (Discussion on MetaFilter)



# Thank you for your attention!

Dr Eleni KOSTA
eleni.kosta@law.kuleuven.be

Interdisciplinary Centre for Law & ICT (ICRI)
Katholieke Universiteit Leuven

Interdisciplinary Institute for BroadBand Technology






# Postgraduate Studies in ICT & Media Law

- High-level postgraduate studies programme offering
  - advanced knowledge of European ICT & Media Law;
  - interdisciplinary insights (technology, economy, media studies);
  - practical skills training.

- We welcome applications from:
  - Graduate students aspiring to
    - A professional career in the public / private sector
    - An academic / research career;
  - Professionals who want to update & expand their knowledge and skills.

More information:

http://www.law.kuleuven.be/icri/psiml.php

Questions:

eva.lievens@law.kuleuven.be