Press Release

FIDIS urges mobile users to be aware of data disclosure

...Research from Future of Identity in the Information Society highlights the information many of us may unknowingly give away on a day-to-day basis...

LONDON, Saturday 16 May 2009: At a time when privacy issues are higher on the news agenda than ever, the EU-funded Network of Excellence FIDIS (Future of Identity in the Information Society) is urging users to safeguard their digital identity and privacy, especially when using mobile technologies. With their research, announced today, revealing the staggering amount of information that can be concluded about a person simply by knowing their location via devices such as GPS enabled mobile phones, FIDIS warns that your future job applications, car insurance, and even health insurance could be in jeopardy depending on what information you give away when signing new contracts and downloading the latest applications. The team is particularly concerned that, in the wake of Apple's 'Thanks a Billion' campaign to celebrate the billionth download from the App Store, consumers are still not aware of the potential privacy issues involved with these technologies.

For five years, the EU-sponsored Network of Excellence FIDIS has been investigating the implications of the ‘new era of information disclosure’ that technology is making possible. To discover the kind of information that can be revealed about a person just by knowing their location, FIDIS researchers based in the UK, Germany and Belgium, led by Dr Mark Gasson of the University of Reading, were fitted with GPS enabled tracking devices, which have recorded their every move since March. Having observed the results, the team is concerned that the data does not simply reveal where you have been, but also exposes aspects of you and your private life that you may not realise. While data-share issues with mobile phones have been noted by privacy campaigners, FIDIS is concerned that consumers are still not aware of growing concerns over the trend of GPS-enabled mobile phones.

FIDIS report that the smaller pieces of information gathered via mobile GPS devices – like where you live, when you go to work, how often you socialise or who you go for coffee with – can be aggregated to create a fuller ‘behavioural profile’ of the user. By revealing whether you go to the gym, how often you exercise, where you eat and how often you go to bars and pubs, it’s possible to put together a picture of the lifestyle you lead, even calculating your risk of heart disease – information that, if passed on to third parties such as health insurance companies, could be used against you. With Nokia forecasting that 50% of its phones shipped this year will be equipped with GPS*, and Apple reaching a billion downloads on its App store after only nine months**, consumers are embracing the trend of GPS-enabled mobiles, without ensuring that their information is safe.

‘This information is of course extremely useful for companies aiming to produce targeted advertising, and of course many of us would gladly receive customised drinks offers when we’re heading to a local coffee shop,’ says study participant and researcher Denis Royer from the Chair of Mobile Business and Multilateral Security at Goethe University Frankfurt. ‘However, if users are targeted based on their inferred lifestyle, which restaurants they visit, or how much alcohol they seem to drink, their own information could potentially be used against them’.

The behavioural profiling based on GPS data can also produce estimates of how safe a driver you are, your social status, and even the type of shopper you are – do you always go to the same petrol station, even if it means a long wait, rather than going to a more

expensive one? If third parties use this data to build a comprehensive picture of who you are, you may find it being used in a way that is detrimental to you – for example, by car insurers, current or potential employers. And it's all because mobile users don't always check the terms and conditions when they're signing a new contract or downloading new software and applications.

'Location information isn't considered sensitive data, and as such it's possible for companies to use it as long as you give consent,' notes Legal Researcher and study participant Eleni Kosta from the Katholieke Universiteit Leuven. 'The trouble is that when you're downloading the latest application to your phone that will tell you where the best restaurants or busiest clubs that you may like are based on the type of places you've been before, you may not read the terms and conditions but simply tick the 'OK' box. This puts you at risk.'

'We want mobile users to be aware of the wealth of information they can potentially give away just by agreeing to disclose their location,' says Gasson. 'Real-time commercial and social networking services which use location history to better understand the user are coming very soon, and these will offer very real benefits to the user. However we can't stress enough the need to be aware of what services you're using on your phone and exactly what further uses of the information you might be consenting to when you agree to use the service. Nobody wants to read the legal text, but it's there to defend your privacy – and while this data isn't yet being used, developments in the mobile technology industry including user customised services, and everything that comes with it, suggest that this isn't far away.'

For the full report, please visit http://mobile.fidis.net/

To download a broadcast quality interview with Dr Mark Gasson, please visit
http://www.reading.ac.uk/research/media/res-markgasson-19537.asp

This can also be viewed on the University of Reading's Youtube channel here
http://www.youtube.com/watch?v=bxO_bhx2qso

- ends -

*http://uk.biz.yahoo.com/04022009/323/update-2-asustek-garmin-join-gps-phone-market-foray.html

**Apple Advertising Campaign

Editor's Notes.

About FIDIS

The Future of Identity in the Information Society (FIDIS) is a large EU-sponsored NoE (Network of Excellence) targeting various aspects of digital identity and privacy. The 24 partners of the project are universities and companies working in areas related to digital identity. FIDIS areas of interest include new forms of ID cards, usage of identifiers in information systems, emerging technologies used for citizen's identification and profiling.

About Dr Mark Gasson

Dr Mark Gasson is a senior research fellow at the School of Systems Engineering, University of Reading, UK. He obtained his first degree in Cybernetics and Control Engineering in 1998 from the Department of Cybernetics at Reading where he also obtained his Ph.D. for work on interfacing the nervous system of a human to a computer system in 2002. His current research predominantly focuses on user-centric applications of emerging technologies, with specific focus on pushing the envelope of Human-Machine interaction.

Dr Gasson is active in research concerning technical, social and security aspects of 'ambient intelligence' and its underlying enabling technologies such as RFID and data mining. This has been pursued in the interdisciplinary FIDIS project (www.fidis.net) where, among other activities, he has investigated the privacy implications of convergence of technologies, especially in relation to the combination of biometrics with technologies such as RFID, for example in the European ePassport. Dr Gasson is also an associate editor of the academic journal IDIS.

About Eleni Kosta

Eleni Kosta obtained her law degree at the University of Athens in 2002 (magna cum laude) and in 2004 she obtained a Masters degree in Public Law (summa cum laude) at the same University. In the academic year 2004-2005 she participated in the Postgraduate Study Programme in Legal Informatics (Rechtsinformatik) at the University of Hanover (EULISP) with a scholarship from the Greek State Scholarships Foundation (IKY) and she obtained her LL.M. (magna cum laude).

Since 2005, she has been working as a legal researcher at ICRI – K.U.Leuven, where she conducts research in the field of privacy and identity management, specialising in new technologies. She worked on the European Project PRIME (Privacy and Identity Management for Europe), which finished in May 2008. She is currently working on the European Project PICOS (Privacy and Identity Management for Community Services) and is also involved in the Network of Excellence FIDIS (Future of Identity in the Information Society) and the Thematic Network PrivacyOS. Eleni is also preparing a PhD on "Consent as a legitimate ground for data processing in electronic communications" under the supervision of Prof. Dr. Jos Dumortier.

About Denis Royer

Denis Royer completed his diploma in business informatics at the Technical Institute in Braunschweig (Germany) in 2003. From 2000 to 2001 he studied information systems and business administration at the University of Nebraska in Omaha, Nebraska (USA). Since 2004 he has been a researcher and executive project coordinator of the FIDIS NoE (Future of Identity in the Information Society Network of Excellence) at Johann Wolfgang Goethe University in Frankfurt, Germany. As the Chair for Mobile Business and Multilateral Security, he is working on the evaluation of investments into enterprise identity management systems (EIdMS), decision support systems for the introduction of EIdMS in organisations, and enterprise identity management (EIdM) process models, in the context of the European research project FIDIS. Furthermore, he is active in the GenericIAM Group of NIFIS, working on the creation of generic process models for identity and access management (IAM) systems.

Press Contacts:

Jane Leah, Andy Stafford or Kate Baxter

Beam Agency, 1 Rosoman Place, Exmouth Market, London EC1R 0JY

T: + 44 (0) 20 7833 9595, 07795 654 326, 07949 379 974

E: jane@beamagency.com, andy@beamagency.com or kate@beamagency.com