ENISA
Update 7 December 2012

Υποστηρίζοντας την επανεξέταση και εφαρμογή της νομοθεσίας της Ε.Ε. για την Προστασία των Δεδομένων

Demosthenes.Ikonomou@enisa.europa.eu

Privacy and Trust – definitions

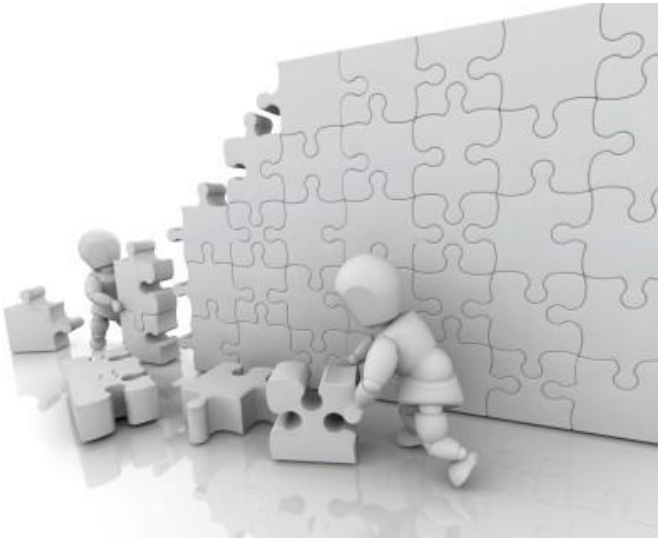
- Privacy is about handling of data about or of persons according to accepted social norms,
  - valid in a particular context;
- Privacy & Trust need joint consideration of technology with
  - social science;
  - economics, ethics;
  - law and other disciplines;
- Needs to be addressed from a pan-European perspective;

The 'problem'

- Internet is open and distributed without authoritative control;
- In many cases, service providers need to collect **some** data in order to better dimension their services;
- In terms of privacy a number of challenges are posed:
  1. Data 'pollution'
     - Data are disseminated without control and
     - **Replicated** on multiple servers and Peers;
  2. Contrary to humans, data lives forever
     - emails (not only web mail), social networking sites, online collaborative spaces (e.g. Google docs);

Privacy & Trust – current context

- EU citizens right: "*Everyone has the right to the protection of personal data concerning them*". Article 16, The Treaty of Lisbon;
- EU legislation reform
  - Data Protection
    - The directive (1995) to be replaced
    - the new regulation for data protection
      - Personal data protection by design and by default
      - Right to be forgotten
      - sanctions
  - Data retention reform (ePrivacy Directive??)
  - EC proposal for a Regulation on electronic identification and trusted services for electronic transactions in the internal market (June 2012);
- Many actors at EU level (DGJUS, DGINFSO, EDPS, ART29);



New virtual world (I)

- No national borders
- No uniform legal system
- Divergent approaches
  - Personal data protection vs. data retention;
- Difference of perception across countries/regions
  - Privacy – human right in EU or consumer right in US;
- Not a level playing field for EU online service providers
- Policy framework reactive instead of proactive;
- ***Towards forming an EU approach in the area of privacy.***

New virtual world (II)

- A new currency: personal data
- Contradictory expectations and practice
  - Privacy - fundamental human right in the EU
  - Users concerned about privacy
    - 93% of participants in recent ENISA study
  - Users wiling to disclose more personal data for discounts
    - up to 87% of participants, in some cases, for 0.5 € discount in the study
- ★ A **gap** is observed between
  - ★ what is possible at technological level, and
  - ★ what is available at market place and proposed by policy makers;

Areas of (possible) intervention

- Information/Education
  - People have to be aware and educated!
  - However, remember the example of the car industry (100+ years)
    - Safety as a competitive advantage;
    - Defamation, Liability;
- Policy maker
  - Order to remove contents;
  - Promote availability of subscription based services in addition to free;
  - Avoid online service providers lock-in by fostering user profile portability;
  - Implement Data Breach Notification;
- Technology
  - Limit data pollution (e.g. minimal disclosure);
  - Limit content's lifetime (e.g. ephemeral communication);
  - Limit data leakage by design (privacy by design) by introducing more traceability;

enisa
European Network and Information Security Agency

New York 66° | 56°

THE WALL STREET JOURNAL. | BUSINESS

U.S. Edition Home ▾ | Today's Paper ▪ People In The News ▪ Video ▪ Blogs ▪ Journal Community

World ▾ | U.S. ▾ | New York ▾ | Business ▾ | Markets ▾ | Tech ▾ | Personal Finance ▾ | Life

Small Business ▾

Asia | Europe | Earnings | Economy | Health | Law | Autos | Management | Media & Marketing

TOP STORIES IN Business

1 of 12 BlackBerry Maker in Turmoil

2 of Best Buy Rethinks Stores

BUSINESS | Updated March 30, 2012, 3:12 p.m. ET

Breach Hits Card Processor Global Payments

Article | Video | Stock Quotes | Comments (59)

Save | +1 26 | Tweet 714 | A A

By ROBIN SIDEL And ANDREW R. JOHNSON

Global Payments Inc., GPN -9.06% which processes credit cards and debit cards for banks and merchants, has been hit by a security breach that has put some 50,000 cardholders at risk, according to people with knowledge of the situation.

CBS Boston WBZ .com

Home | News | Sports | Boston's Best | Watch + Listen | Traffic

Latest News | Local | Consumer News | Politics | Business | Health

NEWS

Local Restaurants Fined Over Ongoing Data Breach

By Anthony Silva, WBZ NewsRadio 1030

March 28, 2011 6:31 PM

Got Visa or Mastercard? Your Data May Have Leaked

March 30, 2012 by Alex Fitzpatrick

4

The personal data of thousands of customers — from all major credit card brands — has been leaked from a third-party processing company.

The massive leak was first reported by the security news blog Krebs on Security, following reports that MasterCard and Visa were warning banks of a possible breach.

According to a follow-up story from *The Wall Street Journal*, the breach came from the Atlanta-based payment processing firm Global Payments, not from a credit card company. Global Payments works with debit cards, credit cards and gift cards.

theguardian

News | Sport | Comment | Culture | Business | Money | London 2012

News › Technology › PlayStation

PlayStation Network users fear identity theft after major data leak

Sony issues worldwide alert after personal details of 77 million PlayStation users, including 3 million Britons, stolen by hackers

Charles Arthur and Keith Stuart

guardian.co.uk, Wednesday 27 April 2011 20.59 BST

Comments (12)

Data breach notifications

- Review of ePrivacy Directive (2002/58/EC)
  - Article 4

*In the case of a **personal data breach**, the provider of publicly available electronic communications services shall, **without undue delay**, notify the personal data breach to the **competent national authority**.*

*When the personal data breach is likely to adversely affect the **personal data or privacy** of a subscriber or individual, the provider shall also notify the **subscriber** or individual of the breach **without undue delay**.*

*Notification of a personal data breach to a subscriber or individual concerned **shall not be required** if the provider has demonstrated to the satisfaction of the competent authority that it has implemented **appropriate technological protection** measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the **data unintelligible** to any person who is not authorised to access it.*

Implementing the notifications

- Differences between Member States
- Concerns of competent authorities
  - Lack of resources
- Concerns of industry
  - Confidence in internal procedures
  - Need of support in interpretation of law
  - Feeling of injustice in the telecom sector
- Impact of Data Breach Notifications
  - Short term: DBN will ensure information is given and actions taken
  - Long term: contribution in data protection in general
- Problems are not country-specific (cloud!)
- Recommendations for technical implementation: ENISA 2011/12
- **Close collaboration with EU DPAs and Art29TS;**

Severity of a data breach

Estimation of the magnitude of potential impacts on the individuals' privacy and data protection

Low	Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	Data subjects may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).
Very High	Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

‘The right to be forgotten’ - between expectations and practice

- Included in the proposed regulation on data protection published by the EC in Jan 2012.
- ENISA addressed the technical means of assisting the enforcement of the right to be forgotten.
- A purely technical and comprehensive solution to enforce the right in the open Internet is generally not possible.
- Technologies do exist that minimize the amount of personal data collected and stored online.

Electronic identification

- eSignatures Directive (1999/93/EC)
  - a degree of harmonisation to practices on electronic signatures across Europe.
  - its benefits are achieved to a small degree, especially as regards cross-border transactions.
- EC proposal for a Regulation on electronic identification and trusted services for electronic transactions in the internal market (June 2012);
- Article 15: *trust service providers have to undertake extensive security measures and notify competent bodies of any breach of security and loss of integrity with significant impact on the trust service provided and on personal data maintained therein.*

Contact

European Network and Information Security Agency

Science and Technology Park of Crete

P.O. Box 1309

71001 Heraklion - Crete – Greece

http://www.enisa.europa.eu