

Security Breach Notification Symposium
UC Berkeley School of Law
March 6, 2009

Breach Notification in the EU

*Daniel P. Cooper, Partner
Covington & Burling LLP*

COVINGTON & BURLING LLP

BEIJING BRUSSELS LONDON NEW YORK SAN DIEGO SAN FRANCISCO SILICON VALLEY WASHINGTON

Current State of Play

- Some EU Member States recommend breach notice (more on this later).
- Legislation under consideration at EU level would require Member States to establish mandatory rules.
 - The e-Privacy Directive.
 - Negotiations underway among the Council, Commission and Parliament on key issues.

Which Entities Should be Covered by Breach Notice?

- The e-Privacy Directive generally only applies to public electronic communications services and network operators (*i.e.*, ISPs, telco companies, and some web-based communication providers).
- Parliament, the Article 29 Working Party, and the European Data Protection Supervisor would like breach notice to also cover information society services (web page operators).
- Extension to all businesses possible through additional legislation (amendment of the Framework Privacy Directive or a new Breach Notice Directive).

Who Should Determine if Notice is Necessary?

- Self-assessment is favored by Council, Commission, Article 29 WP, and EDPS.
- Parliament believes NRAs should evaluate breaches, but many question if they have the resources.

Should There be an Exception for Encrypted Data?

- All three Institutions favor a carve-out, but the Council's version would not be mandatory.
- The Article 29 Working Party opposes such an exception.
- Many companies would like a broader exception, covering data that is either encrypted or rendered unusable.

Should the Commission be Empowered to Harmonize Member State Rules?

- Industry is concerned that diverging Member State notification requirements could make compliance unduly burdensome.
- The Commission wants the authority to harmonize such rules; the Council and the Parliament would limit the Commission's role to recommendations.

Next Steps

- Parliament is considering the proposal in second reading; a vote is likely this spring.
- “Triialogue” negotiations are continuing.

Current Member State Practices (I)

- There is currently no statutory requirement at European or national level requiring industry to release breach notifications.
- A number of Member States have published non-binding guidance on steps that should be taken following a data breach. The UK, for example, recommends that a breach management plan include:
 - 1) containment and recovery;
 - 2) assessment of ongoing risk;
 - 3) notification of breach; and
 - 4) evaluation and response.

Current Member State Practices (II)

- Germany is the only Member State considering legislation for compulsory notification, but only for:
 - significant violations of data protection laws;
 - involving especially sensitive personal data.