

Comments on the Commission Staff Working Document on the Review of the EU Regulatory Framework for electronic communications networks and services {COM(2006) 334 final} Proposed Changes (29 June 2006)

October 27, 2006

The European Privacy Officers' Forum (EPOF) is composed of European-based data protection compliance officers and corporate legal counsel in charge of data protection from approximately thirty companies. As such, EPOF members deal on a daily basis with the compliance challenges presented by the EU Framework for electronic networks and services, and welcome this opportunity to comment to the European Commission on its review.

The EPOF comments here only concern the recommendation of the Commission Staff that electronic communications service providers give notice to regulatory authorities and individuals in the event of a breach of security that results in the loss, modification or destruction of, or unauthorized access to, personal information ("PI") (collectively "compromise" of data). But before addressing the issue of notification itself, it would be useful for the Commission to clarify the term "electronic communication service providers" in its review of the regulatory framework. Currently, the regulatory framework does not provide for a definition that allows companies to assess whether for example email networks provided and operated by companies would fall under this definition. In principle, the EPOF supports notice to both regulatory authorities and affected individuals when there is a significant risk that a breach of security may result in a compromise of data or loss of PI. It would also be useful to obtain confirmation from the Commission that the responsibilities of data processors in light of security breach notifications are different to those of a data controller. A data processor should have an obligation to notify the data controller in case of a suspected compromise of personal data, but this notification obligation for data processors should not be extended to include the regulators and affected individuals as well. The critical questions in formulating such a rule, however, go unanswered here – what types of PI if compromised trigger the notice obligation, when must notice be given and when may it be delayed, what form of notice is sufficient, and what the content of such a notice should consist of as a minimum.¹

¹ The EPOF understands that this is the first step for the Commission in addressing a comprehensive, multi-faceted approach to security. That is wise, because while the proposals here address ISPs and network access providers, the greater risk for users for data loss or compromise lies with data processors that store, use or make PI available for various applications. Even a cursory review of reported breaches of security

As written, the proposal would require notice for *any* compromise of PI. As the Commission Staff no doubt is aware, breach notification laws in the several of the United States apply only to the compromise of PI where there is a material risk of harm to the consumer such as identity theft or financial loss.² Thus, the mere compromise of a name or an email address alone would not trigger notice, but loss of a full name in combination with financial account information and access codes would require it.

The EPOF supports a similar standard here. As the Commission Staff notes generally, the “level of security [must be] appropriate to the risk.” (p.28). When the risk of harm to an individual is small, notice should not be required. To do otherwise might overwhelm individuals with notices, raise anxiety, or worse, render notices so commonplace that they are ignored. Accordingly, the EPOF recommends that notice be required when, for example, sensitive PI is compromised, or in the event of compromise of those PI elements that alone or in combination can result in financial or other material harm to individuals.

The timing of any notice likewise is an issue. The proposal does not address the timing of any notice. Notice must be sufficiently prompt to afford individuals a meaningful opportunity to take steps to avoid harm. But, companies likewise need to investigate the cause of the breach, take remedial action, and prepare for notification as well.

Giving notice is the easy part; responding to subsequent inquiries, however, takes planning. For example, companies that have been through the breach notification process have commented on the need to establish call center support to respond to customer inquiries that arise after receipt of a notification. Many companies also arrange for fraud protection insurance coverage and take steps to notify credit reporting agencies, banks and card issuers. These customer-friendly steps are important to ensuring a complete and accurate notification and for the protection of the customer.

around the world reveals that lost laptops, insecure databases, and poor security procedures account for the vast majority of loss or compromise of PI. In contrast, the access link to PI generally is secure, relies on encryption such as SSL connections and user control of passwords for access, and in corporate environments, uses virtual private networks or other tunneling technology for secure access. Thus, the Commission Staff’s recommendations, if adopted, likely will not have a significant impact on access providers or improve user security; yet the recommendations have the virtue of spurring on discussion of the appropriate framework and scope for a breach notice regime.

² For a list of security breach notice laws and their requirements, *see* <http://www.perkinscoie.com/statebreachchart/chart.pdf>

Similarly, companies often quickly complete their investigation and determine that the compromise is the result of the illegal acts of a third party. In those cases, referral is often made to law enforcement agencies. In some instances, law enforcement requests the service provider to refrain from giving notice or publicly disclosing the incident in an effort to further investigate the crime and find the perpetrator. Service providers should be able to delay notice at the request of law enforcement if doing so is in the public interest. The Commission Staff proposed that NRAs, once informed of a breach, have the power to notify individuals if they deem it to be in the public interest to do so. The same standards should apply to private entities working with law enforcement.

The proposal does not address the form of notice that is required. The EPOF recommends that the form of notice be flexible but one most calculated to lead to actual notice. The Commission Staff may know that in the United States, the form of notice is either a writing or publication in a newspaper of record if enough individuals have been affected. Some state laws also recognize alternative notice if the service provider has established notice procedures as part of an information security program. Alternative forms of notice might include electronic mail, prominent posting on the service provider's Web site or any other form reasonably calculated to provide actual notice.

The EPOF also stresses the need to have harmonized implementation among of the Member States of any breach notification provisions. Because of the difficulty of determining the law that would apply to breaches, harmonized rules as to breach notification are vital. The EPOF welcomes the fact that the Commission seems to favor a comitology procedure that would encourage harmonization, but it is critical that, if breach notification rules are adopted, they apply at an EU level rather than at a national level.

The Commission Staff should recognize that in an electronic world, much of the relationship between a user and a service provider persists only in electronic media. These users expect to receive their communications electronically. In this light, the business world might also benefit from the Commission's review of the current art 13 on the regime for unsolicited marketing communications. The current "unsolicited marketing" regime as set out in article 13 of the E-communications Directive has seen various interpretations throughout the European Union. In particular Member States seem to have different views on b2b marketing communications. We feel that it would be useful for the European Commission to review the current regime as set out in art 13 of the Directive and clarify specifically the scope of b2b marketing communications. Currently both b2b and b2c electronic marketing communications require a positive opt-in for new contacts. In practice this means is that in some jurisdictions it is prohibited to

The logo for the European Privacy Officers Forum, featuring the text "European Privacy Officers Forum" in a bold, black, sans-serif font. On either side of the text is a small, square icon of the European Union flag, which consists of twelve gold stars arranged in a circle on a blue background.

Hunton & Williams
326 Avenue Louise
B-1000 Brussels, Belgium
Tel. +32-2-643 5800
Fax +32-2-643 5822

send an electronic message to marketing leads and in this message request consent before being able to send further marketing materials. A firm step towards a more business friendly approach would help organizations target more prospects without needing to obtain a positive opt-in. With email having become the most common form of communication in the work place, requiring opt-in for these communications without being able to send an email requesting an opt-in response, is in our opinion highly unrealistic in the business world.

The Commission could consider whether a Europe-wide approach mirroring the CNIL's view would constitute a more commercially friendly marketing environment. CNIL has made a clear distinction between b2b and b2c electronic marketing communications and requires businesses wishing to communicate to new customers to include an opt-out in the communication.

The EPOF commends the Commission Staff for opening this important dialogue. When service providers and data controllers or processors are entrusted with user PI, they are required under Article 17 of Directive 95/46/EC to take "appropriate technical and organisational measures" to safeguard the information. The EPOF takes this obligation seriously. We also recognized the reality that things can and do go wrong, that bad people exist who will use force or guile to gain access to valuable PI, and that no system is or can be made completely secure. Thus, it is appropriate to notify users whenever a compromise may result in disclosure of sensitive PI or material harm to any person.

Submitted on behalf of EPOF
Christopher Kuner
Chairman
ckuner@hunton.com