International Working Group
on Data Protection
in Telecommunications

675.40.12

Working Paper on privacy risks in the re-use of email accounts and similar information society services

46th meeting, 7-8 September 2009, Berlin (Germany)
Revised and updated at the 47th meeting, 15-16 April 2010, Granada (Spain)

Introduction

For many people, email has become the primary means of communication, superseding traditional mail for both domestic and business purposes. An email account which can identify an individual and can be used for personal communications is universally regarded by data protection and privacy authorities as constituting personal data.

An individual may have one or many email accounts, which may have been provided via a free or a paid-for service; an employee may also be permitted by his employer to use a business email address for personal purposes. Apparently "free" email accounts may be packaged in with information services such as broadband services and cable TV.

So what happens if an individual needs to change his email service provider?

The real-world analogy is with moving house. Normally, when someone moves house, they send out letters to all their business and personal contacts informing them of the new address. In addition, the person will normally arrange with the postal services for all of their mail to be redirected to their new address – not a simple matter as nowadays there may be many postal delivery services involved. The 'backstop' is to give the new occupants re-address labels to use for any residual mail that arrives.

If we translate this real-world analogy into cyberspace then we need to consider any information society service that involves identifying an individual by name. This can include the increasingly popular social networking services and cyber-trading accounts which use an email address for validation purposes and to which electronically delivered goods and invoices, etc. may be sent. The problem may also manifest itself in the case of SMS messaging associated with mobile phones.

Changing an email address or information society service account

If an email address or cyber-account is terminated, the possibility arises that a new user may be able to reuse the username and then inherit its history. This possibility is fairly remote in the case of free "email-for-life" services (such as gmail or hotmail), as such service providers would rarely reallocate ceased accounts.

Unless the individual has paid for a personal domain, the likelihood is that the email domain name will be associated with the service provider and not be transferrable from one provider to another.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

By way of example, consider someone with a common name, such as Joe Doe, who lives in Portugal, uses gmail, subscribes to a cable TV channel and works for a company called Xpto; Joe may have a number of email accounts, such as **joedoe99@gmail.com**, **joedoe@cabletv.pt**, or **joedoe@xpto.pt**. Additionally, he may have purchased or use a personal domain for his family, such as **doe.pt** and use the email address **joe@doe.pt**.

If he wishes to cease his gmail account, he can be fairly confident that the account **joedoe99@gmail.com** will not be reallocated, but if he terminates his cable TV subscription or moves his employment, then he may discover that he is no longer able to access his email from the addresses **joedoe@cabletv.pt** or **joedoe@xpto.pt**.

On the other hand, the personal domain **doe.pt** should be readily portable from one service provider to another, provided that he or his family continues to pay for it.

However, if his former cable TV supplier has a new customer or his former employer has a new employee also called Joe Doe, they may decide to reallocate his previous email address to this new person. In such a case, the new 'owner' of the email address may well inherit email messages and personal information intended for its former owner.

Similarly, any new owner of a reallocated personal domain where the payment has lapsed may inherit email traffic intended for the former owner.

Possible adverse consequences

There could be several adverse consequences:

- if the user did not cancel newsletter subscriptions or inform all his contacts of the change to his address, the new owner of the address will start to receive information intended for the former owner, leading to a potential disclosure of personal data;
- If the user uses the "forgot-password option" of a third party where he registered under the old mail-address, the new owner would receive his username and personal password to use the site;
- in the case of leaving employment, the new employee could receive personal messages intended for the former employee as well as business email intended for whoever replaced the former employee;
- in the case of terminating a contract with an ISP, the new costumer could impersonate, on purpose or by coincidence, the former owner of the e-mail address.

Similar considerations apply to other Information Society services such as instant messaging, VoIP internet phone services and social networking services, especially where email addresses may additionally be used for authentication. If a subscriber wishes to cease a service, then the new subscriber may receive messages intended for the former subscriber, or more seriously, attempt to impersonate the former subscriber.

Whilst MNP, mobile number portability, may reduce the possibility of this problem occurring with SMS messages associated with mobile phones, the opportunity for MNP may not always be available (e.g. in case of lack of awareness, moving to a different country, death of a subscriber, or with some forms of anonymous or pay-as-you go services), so again there is the possibility that someone else may inherit a recently used mobile number and the SMS heritage that is associated with it.

This is particularly problematic as SMS messaging is commonly used in particularly confidential areas such as online banking, e-ticketing, etc.

Although the portability of mobile telephone numbers has helped to address these problems, the subscriber may feel that he needs to keep an e-mail address or mobile number with a certain ISP or mobile service provider just in order to protect his privacy and personal security.

Recommendations

The Working Group has previously considered privacy and security aspects of telecommunications services[1], internet services[2] and social network services[3].

The Working Group considers that a provider of Information Society Services (referred to below as "the ISP") should provide facilities that would enable a subscriber to a service to mitigate any damaging consequences of terminating their contract, and makes the following recommendations:

1. The ISP should impose a "suspense period" of at least three months before anyone could take over the e-mail address, personal domain name or telephone number of a former subscriber.

2. The ISP should provide the subscriber with an opportunity, for the duration of the suspense period, to have messages sent to a suspended e-mail address or telephone number to be rerouted or auto-responded with a suitable message.

3. The ISP should provide a warning text alerting subscribers of the risk of losing their email address when terminating a contract and the potential consequences of data disclosure.

4. The ISP could offer a feature such as a roaming folder, where the subscriber could archive the login information that is used for web services where he registered using his e-mail-address or mobile telephone number. If the account is cancelled or contract not renewed then the user could transfer this folder to another service or at least would have a list of all third party services connected to this email-address or mobile number and could change the email-address or mobile number there. This would require that the user keeps such information up to date.

5. Services which use SMS authentication (e.g. in online banking) should display the number to which the message was sent. If the service does not receive any feedback from the user to continue a transaction within a certain time limit, the mobile number should be considered compromised and suspended until the owner of the account confirms once again the number of the mobile phone to be used.

6. In case of premium services via SMS or similar services, a time-to-time message, free of charge, should be sent by the service provider to verify if the user still wants to continue subscribing the service. In a case of bank account, it can be confirmed by the introduction of part of a credential that only the real-user knows and has access to, for example.

---

[1] Common Position on the incorporation of telecommunications-specific principles in multi-lateral privacy agreements (Berlin 13/14.09.2000); http://www.datenschutz-berlin.de/attachments/216/tc_en.pdf?1200658742

[2] Working Paper on privacy and security in Internet telephony (Berlin 5/6.09.2006); http://www.datenschutz-berlin.de/attachments/102/WP_VoIP_en.pdf?1201702629

[3] Report and Guidance on Privacy in Social Network Services- "Rome Memorandum" (Rome 3/4.04.2008); http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491

7. Individuals (Employees) should avoid using email addresses which can be subject to reallocation (e.g. business email address) for subscription and/or registration to services of personal interest, e.g. mailing lists, e-shops, social networking services, etc.

8. An individual wishing to have a permanent email address should register a personal domain name, which can be used as homepage, weblog, etc. However, a personal domain normally requires renewing annually otherwise it may be lost and reassigned to another individual.

9. Employers and other organizations which allocate business related e-mail addresses should clarify the procedure to be used when an employee leaves or changes his role within the organization. Messages directed to such an address should be redirected or auto-responded such that the sender is aware that the employee's address may have changed or have been discontinued. It is recommended not to re-use identifiers for personal e-mail-addresses of future employees, when they had already been assigned previously to former employees.