Revoking Personal Data in the Digital World

Gina Kounga, Pete Bramhall

HP Laboratories
HPL-2009-362

Keyword(s):
Privacy, Security and Privacy Protection

Abstract:

Requiring data subjects to authorise organisations, from which they request some services, to use their personal data in order for these services be provided has become common practice. This, partly because in order to provide a service to the right individual, an organization needs to know who that individual is. But also, because personal data are an asset that organisations have an interest in keeping. In this context, individuals are in situations where they are constrained to give away their personal data without being capable of stopping these data to be used for operations that are not necessary profitable to them. In this paper, we discuss the revocation of the consent to use or access personal data. We study the technical challenges that need to be overcome in order to allow data subjects to revoke their consent as well as the requirements that should be fulfilled to provide such a revocation.

External Posting Date: November 21, 2009 [Fulltext] Approved for External Publication
Internal Posting Date: November 21, 2009 [Fulltext]

Revoking Personal Data in the Digital World

Gina Kounga and Pete Bramhall

***Abstract*—Requiring data subjects to authorise organisations, from which they request some services, to use their personal data in order for these services be provided has become common practice. This, partly because in order to provide a service to the right individual, an organisation needs to know who that individual is. But also, because personal data are an asset that organisations have an interest in keeping. In this context, individuals are in situations where they are constrained to give away their personal data without being capable of stopping these data to be used for operations that are not necessary profitable to them. In this paper, we discuss the revocation of the consent to use or access personal data. We study the technical challenges that need to be overcome in order to allow data subjects to revoke their consent as well as the requirements that should be fulfilled to provide such a revocation.**

***Index Terms*—Privacy, Security and Privacy Protection**

I. Introduction

Is it not paradoxical that in the United Kingdom (UK) and elsewhere, individuals can easily purchase some products in shops and return them back in order to be refunded, but can hardly avoid some organisations using the personal data – i.e. "*data which relate to a living individual who can be identified*" [1] – that they disclosed to them in order to be provided some services? Why is it that for material goods, that are not inherently linked to them, individuals are authorised to change their mind and reverse a transaction, but, for immaterial quantities that are inherently linked to them, as they define what or who they are, individuals are not authorised to change their mind? Then, should data subjects use or request online services if this requires giving up control over their personal data?

These questions illustrate the dilemma that data subjects face each time that they request to be provided services. No approach have been proposed in the literature that makes it possible for data subjects to fully control their personal data by giving data subjects the possibility to effectively revoke some previously given consent to use their personal data. This is as much surprising as some European laws and regulations, such as the European directive on data protection [2], define privacy as a human right. Then, could a country, in which individuals are forced to give up their human rights in order to be provided some mercantile services, considered as a democracy? If no, then, is it acceptable that in many European democratic countries individuals are not able to revoke the consent given to organisations to use their personal data?

In this paper, we focus on personal data stored by organisations in their databases. We study the technical challenges that need to be overcome in order to allow data subjects to revoke the consent they gave to some organisations to use or access to their personal data. Our paper is organised as follows[1]. In Section II, we discuss the approaches proposed in the literature to provide revocation. This allows to identify their limitations. Then, in Section III, we discuss the problems that need to be solved in order to permit data subjects to revoke their consent. We identify the requirements that suitable solutions should fulfil in Sections IV and V. We discuss our paper in Section VI and conclude our work in Section VII.

II. Related work

A. Definition

The term revocation designates the process of terminating the validity of a resource before its otherwise due date. This term is frequently used to designate the invalidation of a passport or a credit card after it has been declared lost by its legitimate owner. In information security, it is used to designate the process that makes it possible to invalidate a public key certificate [3], [4].

Applied to consent, revocation designates the termination of the validity of some previously given consent.

B. Standardised revocation techniques

Different mechanisms have been defined in the literature to manage revocation. These revocation mechanisms

Gina Kounga and Pete Bramhall are with the Systems Security Lab of Hewlett-Packard Laboratories Bristol, UK.
E-mail: name.surname@hp.com

[1]In the remainder of this paper "*to some organisations to use or access to personal data*" is sometimes implicit when we refer to the *revocation of the consent given to some organisations to use or access to personal data*. For practical reasons, we use "*revocation of consent*", "*revoke consent*" or expressions derived from these two.

most often initially require the entity wishing to terminate the validity period of a given resource to request the revocation of that resource to a trusted authority. These trusted authorities can, for instance, be the banks that issued some credit cards or the governmental body that issued some passports.

Similarly, the revocation of a public key certificate $Cert_B$ requires Bob, the legitimate owner of $Cert_B$, to inform a trusted authority, the certification authority (CA), that $Cert_B$ needs to be revoked. The CA, verifies that the claim has been made by the legitimate owner of $Cert_B$. If it is the case, then the CA propagates the revocation information to allow any entity that is about to use $Cert_B$ to know that $Cert_B$ is not valid anymore. Two propagation mechanisms have been standardised by the Internet Engineering Task Force (IETF). The first, requires the CA to regularly generate a Certification Revocation List (CRL) [4] where are listed the certificates that have been revoked. CRLs are digitally signed by the CA and stored in CRL repositories. The second, requires the CA to send the information that $Cert_B$ has been revoked to a Online Certificate Status Protocol (OCSP) responder [3]. Revocation mechanisms are only useful in a context where entities using some resources, whose validity can be changed, do check the revocation status of these resources before using them.

In the case of the revocation of the consent to use or access some personal data, the data collector – i.e. the organisation that has collected Bob's personal data – does not necessarily need to run a specific process to verify that Bob's personal data are still valid in order to properly provide the services that it advertises. This, because if Bob needs to be provided a service, Bob will most probably assure that the personal data, that he has disclosed to the data collector and that are necessary to the proper provision of the requested service, are valid. Bob has, for instance, no honest and legitimate interest in giving a wrong name, wrong credit card details and address when he is buying a product online, since this would avoid any of his transactions to be validated. For the same reason, Bob will most probably take the initiative to update the previous details, if they have changed. Therefore, data controllers are able to identify the personal data items, collected from data subjects, that have a high probability of being valid. Then, if revocation mechanisms, as described for public key certificates, were to be used, they would mainly benefit the data subject. Consequently, such revocation mechanisms, if they were to be established for consent, may not be used by the data controller. The foregoing highlights that standardised revocation mechanisms alone do not suffice to guarantee that revocation of consent is provided.

C. Revocation of access and use of personal data

Solutions have been proposed in the literature to give data subjects more control of their personal data. The World Wide Web Consortium (W3C), for instance, has defined the Platform for Privacy Preferences (P3P) standard [5]. P3P automates the negotiation, between organisations and a data subjects agent, of the manner in which personal data, to be disclosed by the data subject to a collecting organisation, are to be used by that collecting organisation. However, collecting data subjects preferences regarding the manner in which they want their personal data to be used is not sufficient to guarantee that data subjects will be able to revoke the use or access to their personal data.

Pöhls proposes in [6] a solution that relies on Merkle's hash tree [7] to bind a data subject's consent to a specific use of his personal data within a public key certificate. Revocation of the consent to the use of these personal data is provided by revoking the certificate using the previously described IETF standardised mechanisms. However, as explained by Pöhls in [6], the solution does not protect "*against unconsented data processing*". Therefore, the proposed approach alone is not sufficient to guarantee to data subjects that once they have revoked their consent, these personal data will not be accessed anymore by that organisation. Further mechanisms need to be put into place at the organisation side to enforce revocation of consent.

In the remainder of this paper we identify the problems that need to be solved in order a suitable solution be defined to enforce revocation of the consent and we specify the requirements that should be met by such a solution.

III. Problems

Enforcing revocation of consent to use and access to personal data requires several problems to be solved. In this section, we discuss these problems.

A. Data are an asset

Many organisations do need personal data in order to provide properly the services that they advertise. E-shops, for instance, can need data subjects' names, surnames and addresses to guarantee that some products, bought online, will be delivered to the right address.

For these organisations, personal data are an asset. The more they collect, the more customers they can reach. This can also permit these organisations to improve the services they provide by using data subjects' contact details to request these subjects feedbacks, improvements

wish lists or preferences regarding the way in which they would like to be provided some specific services.

The capability to anticipate individuals needs plays a major role in advertising and advertising is a major income source for most organisations that do collect personal data. Data that can allow to understand data subjects' consuming habits is therefore a key to the definition of advertising campaigns that will reach the targeted individuals. Then, collected behavioural data about data subjects are also an asset, as it allows collecting organisations to sell the capability to reach specific individuals to companies for which these individuals constitute a target. This can encourage organisations to use a pro-active approach consisting in collecting as much personal data as possible, even if they are not useful for their business in the short therm, since they might be useful in the long term.

The foregoing highlights that the establishment of mechanisms allowing data subjects to revoke the consent they gave, to organisations, can go against some of these organisations interests. Therefore, it does not create any incentive for these organisations to use techniques that would allow the enforcement of revocation.

B. No regulatory and legal requirements exists for providing revocation

In the UK and perhaps elsewhere, organisations have less reason to put into place revocation mechanisms as there is, to the best of our knowledge, no regulation that imposes them to enforce revocation. Most of the legislation dealing with the use of personal data focuses on their collection [1], [2]. It for instance specifies the conditions in which personal data should be collected and stored, but does not require anything for allowing revocation. Furthermore, the legislation – see [1] – does authorise, the "*fair processing*" of personal data, by organisations, if it does not go against the data subjects' interest. Therefore, even if data subjects were able to effectively revoke their consent to use or access to their personal data, organisations could, under certain conditions, still be able to use these data.

However, even if all use of and access to all data are not revocable, there is still the need to provide revocation of consent for some use and access. An illustration of this need comes from a case that happened in 2009 in the UK. In 2009, a company advertised a service allowing anybody to get anybody's else private telephone number, previously obtained from third parties. This has raised many concerns, among which, the fear that this service may expose children's safety [8]. To avoid individuals to have their telephone numbers in this company's database against their will, a public campaign was launched. This campaign has lead to thousands of individuals requesting their telephone number not to be disclosed to this company's customers. This episode highlights that some organisations can lawfully obtained some personal data from third parties and use them for a purpose to which the corresponding data subjects did not consent. It also highlights that in such cases, data subjects do want to be able to revoke their consent. Another illustration of that need is the frequently observed case where members of some social network websites decide to close their accounts and express the need that their personal data, such as their photos, be removed from these websites' databases.

IV. Non-technical requirements to be fulfilled to provide revocation

A. Filling the regulatory void

The lack of regulations dealing with revocation of consent can be understood given the fact that, in the UK at least, data cannot be owned and therefore personal data do not belong to their data subjects. Therefore, allowing a data subject to revoke an organisation's right to use or access to personal data that relates to him, but do not belong to him, can appear as a nonsense. However, if this is true, it should also apply to consent. But, it is not the case. Regulations indeed do specify that organisations do need to obtain data subjects' consent in order to collect and process their personal data. Then, why what seems logical for consent becomes illogical for revocation? If regulations do cover consent it could also be expected that they do cover revocation of consent.

Then, if regulations were to be put into place to cover revocation of consent, they should take into account both: organisations' needs to process personal data for their business interests and data subjects' needs to control that their personal data are not used in a way that can be penalising for them. This may appear contradictory. However, this has already been done in [1] for consent. Further, there are situations where both of the previous aspects are not in contradiction. If we consider, for instance, photos or discussion traces, there are most probably some that are of no interest for the social networking websites thats store them. Then, why not allow the data subjects, that uploaded them, to revoke the consent to use these photos? This would free up some space in the websites' databases and satisfy the data subjects.

The regulatory measures to be put into place should create an incentive for organisations to manage the revocation of consent. Indeed, as data controllers do

not gain much by allowing revocation of consent – as revocation can lead to the loss of information that could have been traded for money, there is no reason to expect data controllers to enforce revocation of consent. Among the regulatory measures that could increase organisations incentive to manage revocation of consent, there is the establishment of auditing processes to verify that data controllers enforce revocation of consent.

B. Introducing pro-active Behaviour

To allow a data subject to exercise a right to revoke consent, it should be made sure that data subjects are indeed aware of this right. Different means are used nowadays to achieve the previous. One of these is the organisation of information campaigns targeting the individuals that are less likely to be aware of their rights.

Then, once data subjects are aware of their rights, allowing them to revoke the consent they have given to an organisation implies that the data subject is able to remember that he has disclosed some personal data to that organisation. However, nowadays data subjects have a large number of online interactions, during which many personal data items are disclosed. Therefore, revoking consent for a specific use of their personal data requires data subjects to keep track of:

1) **The data they disclose**;
2) **The entity to which these data are disclosed**;
3) **The term and conditions that have been consented to**.

After the data subject has decided that he or she needs to revoke some previously given consent, a communication channel must be available that does allow him or her to reach the organisation in order to request the revocation. As revocation may happen at anytime, organisations need to maintain online communication channels allowing the reception of revocation request at anytime. Such channels are already in use to allow, for instance, the revocation of credit or debit cards and can be, for instance, telephone hotlines.

In the organisations, guidelines should be specified to raise awareness of the good practices regarding the management of revocation of consent.

V. Technical requirements to be fulfilled to provide revocation

The process, that makes it possible for a data subject to revoke his consent and for an organisation to enforce that revocation, can be decomposed into the following three phases:

1) **The transmission, by the data subject to an organisation, of a revocation statement**;
2) **The reception and validation of a revocation statement by that organisation**;
3) **The enforcement of revocation**.

In each of these phases, specific security requirements need to be fulfilled in order to provide revocation of consent. In the remainder of this section, we study and discuss these requirements.

A. Transmission of revocation statements

A revocation statement should allow a data subject to inform an organisation that he or she revokes some previously given consent to use his personal data for a specific purpose. Therefore, a revocation statement should contain all the information that would allow the targeted organisation to identify, which data and rights are concerned by the statement. This information should be provided by the `TermsID`, `ConcernedDataItems` and `RevokedConsentParams` fields of the revocation statement (see figure 1).

Since a successful revocation of consent can lead to the suppression of a right to access data, it can alter the manner in which other data related to a data subject are managed by an organisation. It can further alter the services that are provided by the organisation to a data subject. To avoid an attacker to revoke the consent that some customers gave to the organisation in order to disrupt the services provided by the organisation to these customers, no other entity than the data subject, to which some personal data relate, should be authorised to revoke the consent to use or access to these data. Achieving this, requires the revocation statement to contain the information that would allow the targeted organisation to verify that the received statement is authentic. This information should be provided by the `DataSubjectId` and `Authenticator` fields of the revocation statement (see figure 1).

Data subjects frequently do disclose the same personal data to different organisations. The same names and contact details can, for instance, be stored by different entities at the same time. Then, to avoid the case where, because of a mistake, an organisation enforces revocation after having received a statement that was not targeted to her, a unique identifier of the organisation targeted by a revocation statement should be explicitly appear in the revocation statement. The `OrganisationID` field of the revocation should achieve this.

Since a data subject may need to "re-disclose" to an organisation some data that he revoked in the past, a data subject can also be in a situation where he needs to revoke again a consent that he previously revoked. The following example illustrates the previous:

Fig. 1. Required field of a revocation statement.

Bob has registered to an airline company X to buy online plane tickets for his private trips and receive promotional offers. Bob was required to disclose his contact details and credit card details during the registration process. After a while, Bob decides to change air company and to unregister from the current one. To guarantee that his data will not be used anymore by the the company X, Bob revokes his consent to allow the company X to access and use his personal data. However, later, Bob is constrained, by his employer, to use the company X to book plane tickets for his business trips. Bob must, therefore, re-disclose his personal data to the company X. Some of which, he already revoked in the past. After many years passed working in his company, Bob has been offered a better job position in another company. Before leaving his current company, Bob revokes the consent he as given to company X as he knows that he will not have to use it anymore in the future.

The previous example highlights that the revocation statement, sent by a data subject to an organisation, should also contain some information that would allow the targeted organisation to uniquely identify the time when the statement was issued by the data subject. This, to allow the organisation to differentiate revocation statements that may concern the same personal data, the same data subject, the same type of consent but that have been issued at different times. This information should be provided by the `DateAndTime` field of the revocation statement (see figure 1).

The fields that should compose a revocation statement are represented in Figure 1.

Remark:

To protect their privacy, revocation statements could be encrypted with the destination's public key.

B. Reception of revocation statements

When an organisation receives a revocation statement, it needs to verify that it is indeed the expected destination of the statement. Then, it must verify the authenticity of the revocation statement thanks to the `Authenticator` field contained in it. If the statement is valid, the organisation knows that the message was sent by the data subject identified by the `DataSubjectID` in the statement.

In order to allow the enforcement of revocation, after the reception of the statement, the organisation must advertise this revocation statement both internally and to all the organisations to which it has disclosed, in the past, the data concerned by the revocation. Indeed, as some organisations may need to share personal data with business partners, revocation statements may not only impact their internal operations but also their business partners' operations. Performing the previous requires that the organisation to be equipped with a registry component, as described by Casassa Mont et al. in [9], that makes in possible to keep track of the location of personal data items. As previously discussed for the transmission of revocation statements, communications between an organisation and its business partners about a revocation statement should be secure.

The internal advertising of a revocation statement should allow internal business processes to be aware of the revocation status associated to a specific use or access to some personal data. Therefore, this advertising mechanisms should consist in putting the revocation statements in a location accessible by all authorised entities of the organisations. Similarly to what is done to manage the revocation of public key certificates, authenticated Consent Revocation Lists (CoRLs) could be generated by the organisation and stored in CoRL repositories or Online Consent Status Responders (OCoSRs) could be used. The CoRL repositories do not need to be trusted, as CoRLs need to be authenticated by the organisation that issued them, but OCoSRs do need to be trusted since, as OCSP responders, they are expected to return the requested consent revocation status (CoRS) for a specified data item.

C. The enforcement of revocation

Enforcing revocation of consent requires that, each time that an entity, within the organisation, needs to perform an action that requires the access to some given

personal data, the access to the data be only granted if the corresponding consent to access to these data has not been revoked. This means that CoRS should be used during the access control decision process to permit or deny the access to personal data. This may require to modify existing access control frameworks to allow the access to CoRS for the decision making process.

Enforcing revocation also requires to put mechanisms into place that make it possible, for the organisation, to not allow the access to some personal data received from a business partner if the corresponding data subject has previously revoked the organisation's right to use these personal data. It can require storing data subjects' revocation statements over a long period of time and therefore make the organisation store a large amount of information that can be useless – if it is considered that the organisation may never ever receive any personal data corresponding to some stored revocation statements. Therefore, mechanisms should be defined that mitigate this. A solution can be to make organisations specify, in their terms and conditions, the time during which they are able to guarantee that revocation of consent will be enforced to personal data received from third parties. This would allow data subject to know what to expect when they revoke the consent given to organisations to allow the use or access to their personal data.

VI. Discussion

Some of the previously identified requirements may appear contradictory. Allowing data subjects to revoke their consent and requiring organisations to keep revocation statements, for instance, can seem in contradiction as revocation statement can be linked to the data subject that issued them and therefore can be considered as personal data. However, depending on the form under which revocation statements are to be stored and the technologies that are to be used to generate these statements, it may be possible to recognise that some personal data received from a third party are linked to a stored revocation statement without knowing which data subject has sent this statement. Identifying which technologies can allow to achieve the previous is among the technological challenges that need to be addressed in order to provide revocation of consent.

Most of the requirements specified in this paper will be addressed by the EnCoRe project [10] that aims at allowing individuals to "*grant and, more importantly, revoke their consent to the use, storage and sharing of their personal data by others*". Prototypes will be build that do implement these requirements and provide revocation of consent to use or access to personal data.

VII. Conclusion

Nowadays, individuals are often in situations where they are constrained to give away their personal data without being able of stopping these data from being used for operations that are not necessary profitable to them. However, no approach that makes it possible for data subjects to fully control their personal data by giving data subjects the possibility to effectively revoke some previously given consent to use their personal data, has been proposed in the literature.

In this paper, we have studied and discussed the problems that need to be solved, identified the challenges that need to be overcome and the requirements that need to be fulfilled in order to allow the previous. As personal data represent an asset that can allow organisations to generate revenue, enforcing revocation of consent is not necessarily in these organisations' interests. Therefore, among the non-technical requirements that need to be fulfilled, there is the need to establish regulations that increase organisations' incentive to put into place mechanisms allowing revocation of consent. This, in a way that takes into account both the organisations' interests and the data subject interests. Such regulation should also specify mechanisms for verifying that organisations properly manage revocation of consent. The technical requirements to be fulfilled must make it possible to enforce revocation of consent. This requires, among others, technologies to be put into place that provide access to up-to-date Consent Revocation Status (CoRS) information and allow CoRS to be used to make access authorisation decisions. The future work will consist in defining the technologies and implementing a prototype allowing organisations to enforce revocation of consent.

References

[1] UK Parliament, "Data Protection Act 1998," 1998, accessed the 1 October 2009. [Online]. Available: http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

[2] The European Parliament and the Council of 24 October 1995, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," 1995, accessed the 1 October 2009. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

[3] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP," RFC 2560 (Proposed Standard), Internet Engineering Task Force, Jun. 1999. [Online]. Available: http://www.ietf.org/rfc/rfc2560.txt

[4] R. Housley, W. Polk, W. Ford, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 3280 (Proposed Standard), Internet Engineering Task Force, Apr. 2002, obsoleted by RFC 5280, updated by RFCs 4325, 4630. [Online]. Available: http://www.ietf.org/rfc/rfc3280.txt

[5] W3C, "The Platform for Privacy Preferences 1.0 (P3P1.0) Specification," 2002, accessed on 02 October 2009. [Online]. Available: http://www.w3.org/TR/P3P/

[6] H. C. Pöhls, "Verifiable and Revocable Expression of Consent to Processing of Aggregated Personal Data," in *ICICS '08: Proceedings of the 10th International Conference on Information and Communications Security*. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 279–293.

[7] R. C. Merkle, "Secrecy, authentication, and public key systems." Ph.D. dissertation, Stanford, CA, USA, 1979.

[8] BBC, "Mobile phone directory to launch," Jun 2009, accessed on October 19. [Online]. Available: http://news.bbc.co.uk/1/hi/programmes/working_lunch/8091621.stm

[9] M. C. Mont, S. Pearson, G. Kounga, Y. Shen, and P. Bramhall, "On the Management of Consent and Revocation in Enterprises: Setting the Context," 2009, accessed on 21 October 2009. [Online]. Available: http://www.hpl.hp.com/techreports/2009/HPL-2009-49.pdf

[10] EnCoRe Project, "EnCoRe prject website," accessed on 26 October 2009. [Online]. Available: http://www.encore-project.info/