

Reverse Privacy Engineering

Julien Pierre

▶ **To cite this version:**

Julien Pierre. Reverse Privacy Engineering. 2013. hal-00825801

HAL Id: hal-00825801
https://hal.science/hal-00825801

Submitted on 24 May 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Reverse Privacy Engineering

Julien Pierre
Université de Grenoble Alpes
GRESEC
Avenue du 8 mai 1945
F-38130 Echirolles

Introduction

Facing the problems of personal data industrialization, many technical and legal solutions have been proposed. Pro-privacy legislation and new design patterns try to make engineers and merchants more responsible. Although these efforts must be maintained from these actors, we believe that such a consideration for privacy, focused on commercial transactions, leaves the individual subjects and their social interactions at the deadlock. We suggest reversing privacy engineering by empowering users in context. Thus we propose to model privacy among the concept of "privatory framework" [11], then compare face-to-face and computer-mediated privatory frames, mainly in social network sites (SNS). From these results, we can discuss technical potential allowing the user to completely define privatory framework of her computer-mediated social interactions.

The privatory framework

How a private conversation is set up? Moreover, how what belongs to private life (such as family rituals) is set up? We define as "holder" the one who owns and shares her own personal data (in a very extensive way, like her thoughts, her nudity, and her behaviors, everything that makes her identity). Holder could be any kind of entity, a monad like individual or an organization like a family, a group of friends, a business company, and so on. In case of groups, it is still reduced to individuals: a child or an employee who can tell outside what happens in their group. Therefore, we think that the "holder" has to be considered as a single subject. We also define as "recipient" the one who receives the holder's personal data: lover and friends as clerk or doctor. Observing such private conversation among any kind of population (between teenagers, parents, family, employees) leads us to model a first layer in the "privatory framework". We go back to the concept of Goffman's "participatory framework" for this kind of microsocial interactions [5]. In this first layer, the holder identifies the ones she wants as recipients (Goffman talks about "attendees"). There are so many people excluded from the privatory framework (Goffman's "bystanders"). The sociologist also mentions "overhearers" who are identified while listening to the conversation (or having access to a private interaction), and "eavesdroppers" who stay hidden (like neighbors or spies). Identity is thus fundamental in privatory framework: its concerns both holder (because she shares what defines her) and recipients (because it's the key to participate in holder's privatory framework and access/own parts of her identity). Indeed we build our messages according to identity, we do not say anything to anybody, especially when they are information concerning privacy.

In face-to-face private interactions, privatory framework can be "arranged" by the sole holder, especially when she excludes everyone, by gestures or words ("That is none of your business"), or by locking herself in a room. It's the "right to be let alone" of Warren & Brandeis, claimed by the famous Watzlawick's airplane passengers (One cannot not communicate). Here, silence acts like the Bateson's framing message meaning privacy. Beside this "arranged frame", the "negotiated privatory framework" is conclude between holder and recipients, at the one or the other's request: there is a

promise that is made not to disclose personal data or a contract that is concluded to delegate these personal contents to third parties (other single recipient as friend, family member, close acquaintance, other doctor). Therefore, a trust is in the respect of the privatory framework, and in the non disclosure of private contents. This is both a social trust ("it's easier", Luhmann could say [7]) and a cognitive trust ("I know you", as Louis Quéré could say too [12]). Arranged and negotiated instances of the privatory framework are ad hoc, lapsed, context-dependant, only valid for each private situation of communication. Thus, even if holder and recipients meet again, the privatory framework is still explicit.

The dual level of trust can also be found in the privatory framework's second layer. This one is dedicated to mediated social interactions (mail and email, phone, web services). There is initially an "instrumented" framework, set by the one we call "operator" of the mediation (like Post office, phone or Internet provider). It is more or less complex, from a simple envelop to tunneling encrypted bytes. But in this latter case, the complexity of socio-technical processes hides stakeholders which reduces trust in such devices (with Foucault, we will now call theses devices "dispositif"). Specifically, free service is the base of the operator's economic model, mostly acting online (i.e. SNS). Likewise, the editorial model of the operators involved in the mediation of personal contents includes technical partners. These ones require making profit for their service supply (providing servers, bandwidth optimization, etc.). Finally, economic and editorial models from the advertising industry require an access to these personal contents, and also need to identify their holders. So many eavesdroppers are present in the instrumented privatory framework: we call them "beneficiaries". It is obvious, after talking with users, that first of all these hidden beneficiaries and secondly the status of operators (beneficiaries or not?) are the cause of distrust in social interaction dispositifs (and moreover any transaction dispositifs, i.e. eCommerce).

Beside this "instrumented" framework, the "instituted privatory framework" means any situation where privacy is set up by social norms. Secrecy is thus defined in confession meeting (see the last of twelve Anonymous Alcoholics' traditions), in professional situations (with her lawyer, in business or diplomatic negotiations, see the Chatham House rule for instance) or in medical consultation (part of the Hippocratic Oath). More with decency or family rituals, respect for privacy is a short-term individual learning, and a long-term socio-historical process, what Norbert Elias named "civilizing process".

The main difference between the first and the second layer of the privatory framework lies in the explicitness degree. Here, we go back to the conversational maxims of Grice, and his theory of "implicature" [6]. The philosopher of language explains that conversation cannot be understood without history of interactions. Both speaker and receiver share references on which they pursue or upon which they build new conversations. A third ignoring these references cannot grasp the interaction he is attending. However, if this implicit dose can be found in private conversation (and this is increasingly the case online), the privatory framework, more than any other social frame, requires explicitness. Sentences like "Keep this for you" are all injunctions defining privatory framework, mainly at the beginning and/or occasionally at the end of personal contents' enunciation. In conclusion of this section, privatory framework – in the case of microsocial daily interactions – requires identification and explicitness, before sharing secretly parts of identity.

Analyzing the privatory framework of computer-mediated communication

We have conducted a survey based on hidden capture of personal contents published by "friends" on Facebook (2009-2011, in the context of our doctoral research [11]). Indeed, "friends" were our students (young apprentices in service sector, a few tens of 18-25 y. o.). We interviewed them too, but main results resort of our immersion in their life: this way, we were able to understand what they mean in their statuses, even when they are implicit. We were authorized as a participant in their privatory framework. The other side of our research is focused on information politics of social network sites (first of all Facebook, plus Google and Twitter): semantic model, interface design, privacy policy, algorithms. With Richard Rogers [13], we divide this politics into front-end information politics (look n' feel, terms of service) and back-end (information architecture, economic strategies). Two main results appear of this survey: 1, a misunderstanding about private situations of communication and 2, tactics implemented by users to maintain a privatory framework.

First of all, there are three bias between what users expect and what dispositifs offer. One concerns the content license: who does really own the personal data published on a SNS to? A post on a social network site is stored in operator's data warehouses. Its country's laws also cover such data. Ultimately, the operator owns holder's data. Her recipients and she are deprived of what makes intersubjective relations. The second bias is close to this dispossession process, not according to economic laws but to data modeling principles. In addition of becoming a merchandise, fragments of identity and social life are atomized and sorted out according to designers' social representations (briefly: in SQL tables). These points of view about real life lead the users' abilities to interact with others [10]: "where's the 'I dislike' button ?". More to regulatory and functional frames, the last bias deals with the audience selector (publish to friends, friends of friend, everybody…). Confronted to the face-to-face privatory framework, the audience selector equals its first step: the identification process. When one joins a SNS, there is a global setting about privacy: friends, friends of friend, lists, circles, etc. Then, in the publication form, the audience selector is spotted after the text editor. Observations, interviews, surveys show us that the audience selector is not praised [1, 8, 11]. However, this is in contradiction with the uniqueness of private communication situations. Notwithstanding, translated in the privatory framework, it means that there is first, content sharing then people filtrating. Holder can "arrange" her privacy setting only among those implemented in the SNS, she can "negotiate" them with recipients (by reading which privacy settings they use), but she is still under the influence of "instrumented" to those that the operator considers as sufficient. In the reception space of shared contents (the Timeline I read), the explicitness level of the audience is minimalized: little areas before post in Google+, after in Facebook, a lock icon in Twitter. We think it is here the most important discrepancy between face-to-face and online privatory framework.

We believe it even more when we look at social uses. Second results of our survey show us that holders, and recipients implement two kind of tactics in their online conversation. First, they play the game of explicitness failure: locutors increase conversational implicature. They elide messages with allusion, deixis, nickname, idiolects, quotes and private joke. So, bystanders cannot understand conversation. Second, holder can appeal friends to pursue conversation outside the public sphere of the SNS: in instant messaging, email or phone, or in real life, within a dispositif they trust, in a place where they can manage a privatory framework. In most cases (that we have observed), recipients respect this framework and do not disclose contents to bystanders, but screen capture (or any kind of decontextualization) is still possible ex post or with wrong friends. We think that this kind of social practices are still under construction (SNS are quiet young) [17], but the intensity of computer-mediated social interactions and their related stakes can lead to the standardization of an "instituted privatory framework".

Privacy's frame of use

Two options then emerge from this observation. Either Government, school, public institutions, families, users build alone this privatory framework; either designers, software engineers and business managers participate together to this social construction. In the first case, the digital world will take more space in self-development and for the construction of social world as Elias conceived. But this will greatly depend on how legislators sustain privatory framework. It can be rough (see US-Europe discussions about "the right to be forgotten"). As constitutional laws affect all entities in privatory framework's actantial model, both current legal and technical regulations primarily focus on operators and beneficiaries (ePrivacy). While it is essential to protect the user right from the operating framework of online socialization dispositifs (Privacy-by-Design), but we think the frame of use must be considered more focally and instrumented more precisely.

Starting from and exceeding the distinction made by Spiekerman & Cranor [15] between privacy-by-notice (labels, opt-in) and privacy-by-architecture (SSL, PETs), we propose to locate several initiatives in the perspective of our "privatory framework". Discussion can begin here about these projects or if any other issues are invented. Helen Nissenbaum talks about the "transparency paradox" of the privacy labels [9]: they struggle to count up the complexity of technical process embedded in computer-mediated communication dispositifs. These labels lead us to another deadlock because designers wrote them and because they only describe the operating frame. It certainly is very useful, but the question is how far it is possible to leave control to the user to describe her privatory framework as she intends to have for her online social interactions. What extent online chat interface can reproduce face-to-face interlocution? How holder can explicit foremost the privatory framework of her self's sharing? Insofar as Facebook, Google, or Twitter, and all SNS will declare to support the construction of the self in its relation to others, the identification process should be first for any single personal content's publicizing. Furthermore, the explicitness level must remain the prerogative of users: it is their interpretation of the speech context of personal contents which sets the boundaries of the privatory framework. With the same ontological freedom as in folksonomies, holder and recipients must have the right to append the metadata that will privatize their exchanges. Online conversation can also be framed like a multi-agents system, one "privacy avatar" per actant, enhanced by interactional history and previous privatory frameworks. Compliance with W3C rigid standards can be discussed, in the perspective of a socio-semantic web, rooted in singular contexts [18]. Thus, as we can see, the two levels of privacy (notice and architecture) are intertwined.

This sociotechnical configuration must also be assessed according to our relationship with brand devices supporting social processes. Appropriating the language (even non-native) allows us to build any kind of conversation, discussion, narration, and so on. But what is the appropriability of SNS? Not only the functional and semantic frames of these dispositifs do not fit with the frame of use, but the socioeconomical model does not frame too. Do conversations belong to the café where they happen in? Privacy is this part of personal life we do not want to share with others, known or not. They are some personal contents and we do not want them to suffer from a "transcontextual syndrome" [16] (like gossip, screen capture or spam). These interactions are linked with persons, social space, time and context; but also, privacy is the experience of otherness, and the result of our abilities to move the boundaries. It is because we can interact in different social spaces we have social life (the opposite is reduced to sectarian life). Starting from this assertion (but G. Tarde, G. Simmel, S. Freud, E. Goffman and many others said the same thing), a holder has different recipients in different social spaces: salt of life is playing within these fringes. In other words, a Facebook user has friends on Twitter, Google+, LinkedIn and all other SNS. Despite the APIs (which remain operators'

property), such a partitioning is contrary to social life. We believe the proprietary logic that is operating computer-mediated privacy must remain attached to the holder and the interactants, and not to operators who are simultaneously beneficiaries. But from the time when there is income generation based on personal data exploitation, holder must build a strong privatory framework. If identification and socialization processes currently take place in different online services, the single crucible in which these processes forge is the web browser, some web apps or OS (separated from any link with beneficiaries), SocialTV, smartphones, cloud-based "bubbles" [14] or "habitele" [2], software that have enough appropriability and hospitality to sustain privatory framework's holder and their intersubjective process. But as soon as hegemonic desire prevails, by economic strategies or universalizing ontologies, operators can not provide the socialization process, and even less privacy.

Acknowledgements

I thank peer-reviewers for their comments and Joanna Ernst for her translation advices.

References

boyd, d., and Hargittai, E. Facebook privacy settings: Who cares? First Monday [Online], 15, 8 (July 27, 2010). URL=http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589

Boullier, D. Habitele: Portable Digital Identities, NSF workshop, New Configurations of the Virtual and the Material, Chicago, (March 19-20, 2011)

Bowker, G. C., and Star, S. L. Sorting things out: classification and its consequences, MIT Press, Cambridge, MA (1999)

Flichy P. Socio-technological Action and Frame of Reference. In: Réseaux. The French journal of communication, 3, 1 (1995), 9-30.

Goffman, E. Forms of Talk. University of Pennsylvania Press, Philadelphia, PA (1981)

Grice P. Studies in the Way of Words, Cambridge, MA: Harvard University Press (1989)

Luhmann, N. Trust and Power, Wiley Press, Chichester, UK ; The Reality of the Mass Media, Stanford University Press, Palo Alto, CA (1979)

Madden. M. 2012. Privacy management on social media sites. Pew Internet Project (Feb. 2012). URL=http://pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx

Nissenbaum, H. Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford University Press, Palo Alto, CA (2010)

Pierre, J. Reconfigurer le réel : performativité des bases de données du web social. In Rojas, E. (ed). 2013. Le social est-il soluble dans le web ? Hermes Science Publishing, London, UK (2013)

Pierre, J. Le cadre privatif : des données aux contextes. Approche inter-dimensionnelle des mediations de la vie privée. Doctoral thesis. Université de Grenoble, France (2013)

Quéré L. La structure cognitive et normative de la confiance, Réseaux, 4, 108 (2001), 125-152

Rogers, R. Information Politics on the Web. MIT Press, Cambridge, MA (2004)

Sloterdijk, P. Sphären III. Surhkamp, Frankfurt a/ Main, Germany (2004)

Spiekerman, S., and Cranor, L.F. Engineering Privacy. Software Engineering, IEEE Transactions, 35, 1, (Jan.-Feb. 2009). DOI=10.1109/TSE.2008.88

Star, S. L., Ruhleder, K. Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces. Information System Research, 7, 1 (1996), 111-134

Stutzman F., Gross R., Acquisti A., Silent Listeners: The Evolution of Privacy and Disclosure on Facebook, Journal of Privacy and Confidentiality, 4, 2 (2012), 7-41

Zacklad, M., et al. Hypertopic: une métasémiotique et un protocole pour le Web socio-sémantique. Actes des 18eme journées francophones d'ingénierie des connaissances, IC2007 (2007). URL= http://www.zacklad.org/articles_web_socio_semantique/zacklad-et-al-ic-2007-8.pdf