A Contrastive Study of Pre- and Post-legislation Interaction Design for Communication and Action About Personal Data Protection in e-Commerce Websites

Clarisse Souza

A contrastive study of pre- and post-legislation interaction design for communication and action about personal data protection in e-commerce websites

Clarisse Sieckenius de Souza [0000-0002-2154-4723]

Departamento de Informática, PUC-Rio
Rio de Janeiro, RJ 22451-900, Brazil
clarisse@inf.puc-rio.br

Abstract. The European General Data Protection Regulation (GDPR) has had a major impact on data collection and processing practices. It has also challenged interaction design aiming to support the effectiveness of data owners' rights, their informed decisions, and their actions regarding how personal information is used by companies, governments, and others. Similar legislation has been issued in various non-European countries, which means that, in this respect, the HCI community has an important role to play for users all over the world. This paper presents the conclusions of a contrastive study with four major e-commerce websites in Portugal, where data protection law has been effective since 2018, and four analogs in Brazil, where the national Data Protection Law (DPL) has been sanctioned but will only be effective in 2020. The purpose of the study is to examine the pre-legislation to post-legislation evolution in the design of interaction for communication and action about personal data protection matters, so as to anticipate some of the threats and opportunities ahead of us. Using concepts and elements of Semiotic Engineering methods and techniques, we found that, within the scope of this study, GDPR seems to have had little impact on what European users can do and experience online, compared to pre-DPL Brazilian users. We discuss some of the possible reasons for this and conclude with thoughts on the role of interaction design in empowering data owners for this new regulation era.

Keywords: General Data Protection Regulation (GDPR), Interaction Design, Semiotic Engineering.

1 Introduction

The European General Data Protection Regulation (GDPR) [1] has had a major impact on data collection and processing practices. It has also challenged the design of interaction aiming to support the effectiveness of data owners' rights, their informed decisions, and action regarding how personal information is used by companies, governments, and others. [2] Similar legislation has been issued in various non-European countries, such as Brazil [3], for example, where part of this research takes place. The HCI community has thus an important role to play in helping users from all over the world to access and exert their rights in this new era of data protection legislation.

E-businesses constitute an interesting domain to evaluate what interaction design currently allows users to do or not do with respect to personal data management. Years ago, when e-commerce started to flourish, one of the major technical challenges was to secure sensitive user data like name and identity, home address, and credit card numbers. Moreover, legislation protecting consumers, sellers, and service providers had to be enforced by online processes. These factors gave rise to important advancements in data security and privacy, as well as to legislation-compliant business process modeling and implementation techniques.

Personal data protection (PDP) legislation does involve security, privacy and legislation-compliant business processes, for which we have decades of successful research and development efforts. But it also involves new complex elements, such as informed consent and the interpretation or justification of algorithmic decision making, about which there is much less available knowledge to support urgently needed solutions.

This paper presents the conclusions of a contrastive study with four major e-commerce websites in Portugal and four analogs in Brazil. As a European country, Portugal must enforce GDPR requirements for all online businesses that collect and process their clients' data. Brazil, however, is at a different stage. The Brazilian Data Protection Law (DPL) has been issued in August 2018, and will become effective only in 2020. We are specifically interested in how interaction design may have changed (or needs to change) in order to ensure the users' ability to know and exert their rights *online*.

Portugal and Brazil are used in the study because both countries speak the same language and share much of their culture. The focus of the contrast is PDP-related interaction communication and action for first-time website visitors. These visitors are the ones who must take the most important step in personal data collection and processing matters, they must give the data collectors and processors their *informed consent*. As a requirement for such consent, they must be able to understand and anticipate their rights, what kinds of decisions they can make, and actions they can take regarding their data. Appropriately informed consent should allow users to infer (even if in very general terms) *how* to act and what kind of response to expect in key situations, such as when exercising the right to be forgotten, or to retrieve their personal data from one provider and transfer it to another.

We used concepts and elements of Semiotic Engineering [4] methods and techniques to capture the content and style of *metacommunication* in the selected websites. Metacommunication, as proposed by Semiotic Engineering, is an especially productive concept for this kind of analysis. Very briefly, according to this semiotic theory of HCI, user interfaces are *communication proxies* that *speak for* interaction designers in dialogs with users, which take place at interaction time. Through their structure and behavior, systems interfaces *tell users* about the modes, the means, the possibilities, and the effects of the kinds of *communication* that they may have with software systems and applications. By so doing, they also communicate one party's *intent* to the other. Hence, human-computer interaction, in Semiotic Engineering terms, is a case of social *metacommunication* between humans, expressing the designers' communication about how, when, where, why, and for what purposes users can, in turn, communicate back with the designed technology.

Compared to user-centered HCI alternatives [5,6,7], for instance, the analysis of metacommunication has the advantage of bringing software designers and users *together* at interaction time [8], that is, of investigating how senders' and receivers' communicative goals are expressed and enabled, how different communicative strategies support interface-mediated meaning negotiations, how artificial interface languages and protocols occasionally create asymmetries of power, and so on, and so forth.

Our findings show that metacommunication design in this particular context is surprisingly poor, both in Portuguese and Brazilian websites. In other words, so far, GDPR seems to have had little impact on what users can do **while interacting** with the analyzed European websites, in comparison with the non-European, pre-legislation ones. Based on our findings, we argue that if nothing changes with respect to *supporting interaction for personal data management and decision making*, we may, against our will, end up contributing to the ineffectiveness of GDPR and similar legislation around the world. Hence the role of interaction designers in this context is critical, as Bus and Nguyen had already concluded following a different line of reasoning. [9]

This paper is organized in five sections, starting with the present introduction. Section 2 is a commentary on related work. Section 3 describes our contrastive study, with special attention to the theory and the methodology that was used. Section 4 presents our findings. Finally, Section 5 discusses our conclusions and contribution, the limitations of this study, and some directions for future research.

2 Related Work

Although GDPR is not just about privacy, this is a central notion in the European regulation. Privacy studies go a long way in HCI. [10] Legally, however, the role of the user after GDPR has changed in important ways. For example, European users are now *legally entitled* to specific privacy management rights, like giving and revoking consent for the collection and processing of their data. To be sure, GDPR is, to a considerable extent, the result of cultural change regarding privacy and information abuse online. But it also raises new questions, like the users' right to monetize their personal data in profitable ways, and the consequences of controlling intelligent agents by learning how they predict user behavior, and then playing the reverse game to evade control. [2]

Users have been long known to agree with terms of services (ToS) and privacy policies (PP), having little understanding (or no understanding at all) of what such terms and policies are saying. [11,12,13,14,15,16] The problem is often traced back to the fact that ToS and PP are contracts, and contracts are typically written by lawyers and for lawyers, even though they regulate the mutual interest and relations of lawyers' clients. [17,18,19]

In a comprehensive analysis of privacy-related empirical research, Acquisti and colleagues [14] have identified three recurring *themes*. First, users are uncertain about what privacy trade-offs entail. Second, privacy decisions and behavior are always dependent on context. The same person can manifest widely different preferences in slightly different situations. Third, people or groups with more insight into the factors that determine privacy decisions can influence the behavior of others (and thus change one's

individually manifest decisions). This perspective sheds light on previous research results suggesting that people neglect privacy issues [20,21,22], or that they control privacy threats by such strategies as falsification, passive reaction, and identity modification. [23].

Earlier GDPR-related research underlines the importance of personal data management tools for users to take actual control of their data. [9] More recent research work discusses the available kinds of solutions, paradigms or technical support for this. In a survey of current technological solutions for processing personal data, Carvalho and co-authors [24] study the ways how consent is affirmatively expressed. These include consent by electronic signature, consent sent by email or SMS, consent by access code, consent by confirmation buttons, and several others. All of them have risks, some more than others. Another study by Politou and co-authors [25], analyzes two high-impact rights defined by GDPR: consent revocation and the right to be forgotten. The authors underline software implementation challenges associated with both, and conclude that one of the main reasons for the fact that very few companies are now capable of complying to GDPR is that GDPR provides "little if any technical guidance for entities that are obliged to implement it." [p. 15] One possible solution, they think, is to develop low-level implementation guidelines and business-wide requirements modelling.

Regarding usability and interaction design in the PDP domain, earlier work by Pettersson and co-authors [26] reports on an extensive study with different user interface paradigms for privacy-enhanced identity management. One paradigm differentiates users' roles (what they are doing), and typically assigns pseudonyms to each role. Users can then choose which role they want to play when privacy decisions must be taken. Another paradigm differentiates users' context relations (with whom they are interacting), which allows for *bookmarking* privacy decisions along with website addresses, for example. Finally, the third paradigm associates privacy preferences with physical locations (it *maps* privacy options). Every paradigm opens up different interaction design solutions and has specific usability testing determinants that researchers must keep in mind while investigating user behavior.

Regarding usability research specifically or more closely related to GDPR, Renaud and Shepherd [27] have compiled a list of previously proposed guidelines that can respond to GDPR compliance requirements. The authors have included some of their own to the list. Moreover, interdisciplinary work taking HCI and legal factors into consideration, address the use of contract visualizations and icons [18,19] to simplify the *legalese* and the complexity of concepts and terms in ToS and PP statements. We should finally note that machine learning and AI techniques have also been explored to face the challenges of usable GDPR compliance. For example, some studies propose to automate the evaluation of published terms and policies. [28,29] Others propose to summarize ToS and PP content, and use it to support question answering dialogs with users. [30]

3 The Contrastive Study

The goal of our contrastive study was to examine the spectrum of evolution in interaction design for PDP communication and action, in actual and comparable online applications. There are different approaches to covering the change from *before* to *after* data protection regulations. One of them is temporal (historical, diachronic). Another is spatial (structural, synchronic). The former analyzes the *same* set of objects as they evolve over time, while the latter analyzes *different* sets of objects, which are at different evolutionary stages, at the same physical point in time. For convenience, we chose the structural, synchronic approach. In addition to avoiding the costs of longitudinal studies with evidence being traced back to two or more years past, this alternative also allowed us to discount the change of cultural attitude toward personal data protection during the historical period comprised by a longitudinal approach. In our synchronic perspective, we used the current cultural context of the two sets of analyzed objects, namely the post-legislation interaction design of European websites, and the pre-legislation design of comparable non-European websites.

3.1 The objects of the study

The objects of our study were four supermarket websites in Portugal – Continente (www.continent.pt), Froiz (www.froiz.pt), Pingo Doce (www.pingodoce.pt), and Jumbo (www.jumbo.pt) – and four equivalent ones in Brazil – Zona Sul (www.zonasul.com.br), Extra (www.deliveryextra.com.br), Super Prix (www.superprix.com.br), and Pão de Açúcar (www.paodeacucar.com). Together they constitute two mutually exclusive subsets of objects. The Portuguese websites were inspected in January 2019, when GDPR had been effective for more than seven months. The Brazilian websites, inspected on the same dates, demonstrate the state of affairs seventeen months before Brazilian businesses had to comply to the national data protection legislation.

The comparability of objects in both subsets was established by the following criteria. First, all objects belong to the same business sector. Second, in all of the websites we could run the same inspection scenario. Third, both countries have current legislation about how businesses collect, control and process their citizens' personal data online. Brazil, however, is not at the same stage of legal enforcement as Portugal. Finally, both countries speak the same language and share much of their cultural characteristics (Brazil has been colonized by Portugal, and has also been the seat of the Portuguese empire from 1808 to 1821).

3.2 Semiotic Engineering

The entire study was informed by Semiotic Engineering [4,31,32]. By looking at social communication mediated by computer programs that *express*, on behalf of participating humans, these participants' communicative intent and content to each other, Semiotic Engineering has the advantage of connecting many points and findings that have been addressed separately by previous research.

Our use of Semiotic Engineering concentrated on the concept of **metacommunication**, (introduced in Section 1) and the three classes of computer-mediated social interaction signs that the theory investigates, namely: **static signs**, **dynamic signs**, and **metalinguistic signs**. They can be used to define different communication strategies, depending on the communication purposes, the context, the means and the modes of interaction made available to the engaged parties.

Before we define each one of the metacommunication sign classes, it is useful to note that in typical communication settings participants alternate between two roles: the role of *senders* and that of *receivers*. The *meaning* of signs that they exchange is rarely (if ever) the *same*. Yet, communication is possible mainly because of two factors. First, participants typically share a considerable volume of world knowledge, sociocultural practices and values, linguistic competence, and so on. Second, inevitable misunderstanding can frequently be prevented, detected, and corrected during communication, by means of strategies that are vastly employed on a daily basis, by virtually every human being. Therefore, when we talk about *the meaning of signs* in metacommunication, we should bear in mind that there are always two human parties involved – the system's designers and the users – in addition to a computational mediator, the system's interface. In the following definitions, when talking about *the* meaning of signs, we refer to the meaning that *humans* (designers or users) assign to them, which may or may not coincide, but still share substantial elements with one another.

Fig. 1. Illustration of a static sign (a side bar menu item magnified for readability)

Static signs are those expressed and interpreted *instantly*. For example, look at **Fig. 1**, depicting a snapshot of the interface mockup for an imaginary e-commerce web application called *The Alchemist Store*. The side bar menu item named "Privacy & Data Protection" (see the magnified portion of the image) probably means different things for interaction designers and application users. When they see the phrase "Privacy & Data Protection" followed by the upward arrow, designers know exactly what they mean by it. Users, however, may look at this sign and have only an incomplete (or even an incorrect) interpretation of what it means. For example, users may interpret this

menu item sign as the equivalent of "the access point to knowing more about or taking action with respect to Privacy & Data Protection." Although this interpretation is correct, it remains incomplete if the users cannot anticipate which actions can be taken, under which circumstances, for which purposes, and so on.

When users assign incomplete or incorrect interpretations to static signs, another class of metacommunication signs is typically used to complete and correct such meanings. **Dynamic signs** are (shorter or longer) sequences of static signs that span over time, most often as the result of user-system interaction. The meaning of the entire sequence cannot be assigned instantly by any static sign present in its initial state. For example, in **Fig. 2** we sketch the expression of an extremely short dynamic sign that a first-time user of *The Alchemist Store* will typically encounter. Its duration spans from the pre-click to the post-click state of the system.

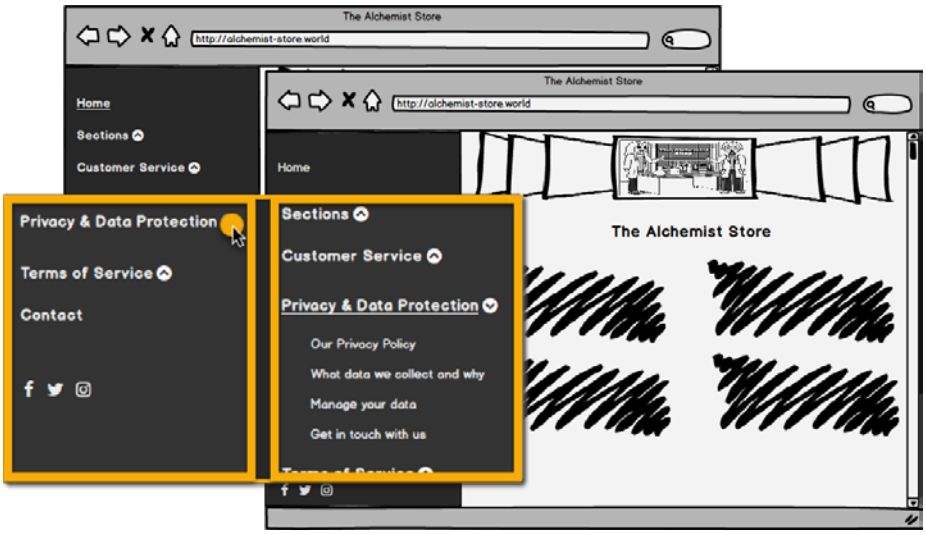

Fig. 2. Illustration of a dynamic sign (side bar menu items magnified for readability)

As already mentioned, the static sign shown in **Fig. 1** gives a first-time user an imprecise (and potentially wrong) idea of what this website's designers mean by "Privacy and Data Protection". However, her *interaction* shown in **Fig. 2** communicates to her new meanings that this system's designers have assigned to the static menu item "Privacy and Data Protection". On the background screen, whose menu entries are seen on the left-hand side of the magnified area of the image, the user *gets the message* that she can click on the arrowhead to learn more about what she can do regarding privacy and data protection, and she does it. Then, comes the foreground screen, whose menu entries are seen on the right-hand side of the magnified area of the image. The system's response to the user's clicking on "Privacy & Data Protection" communicates additional messages intended by the designers, namely: that she can learn about "[The service provider's] Privacy Policy"; "What data [the service] collects and why"; how she can "Manage [her] data"; and finally, how she can "Get in touch with [them]". Thus, at the end of this tiny sequence of interaction – which constitutes the dynamic sign – the

user has new shared meanings with her indirect and asynchronous interlocutors, the system's designers.

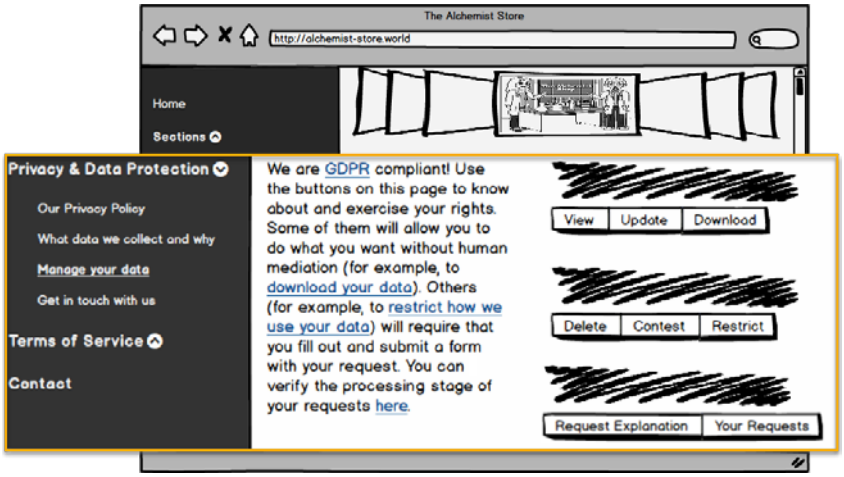

Fig. 3. Illustration of a metalinguistic sign (side bar and page content magnified for readability)

Metalinguistic signs are orthogonal to other signs. Their distinctive feature is to *communicate something about other signs* in the interface language. Typical examples of metalinguistic signs include warnings (with signs that refer to dynamic or static signs shown in other states of interaction), tool tips (with signs that help users understand the meaning of the sign that they are pointing at), and other explanatory or informative help messages that appear during interaction. In **Fig. 3**, we show a different state of the interface for our imaginary website. On the left-hand side of the magnified portion of the image, we see once again the submenu items for the "Privacy & Data Protection" option. The "Manage your data" option is active. On the right-hand side of the magnified portion, we see the sketch of page content accompanied by push buttons, communicating instantly what users can do in order to "Manage [their] data": to View, to Update, to Download, to Delete, to Contest (the use of), to Restrict (the use of), to Request [an] Explanation (about the use or effect of computations upon) their personal data, and to access [their] Requests. The center portion of the image, however, contains text that *communicates about the meaning of interface signs* on the left- and right-hand side of the image. These are **metalinguistic signs**. For example, the text informs that "[some] of [the buttons] will allow you to do what you want without human mediation (for example, to download your data)." This is a sign that *explains* other interface signs. The same occurs with another portion of the text, saying that "[others] (for example, to restrict how we use your data) will require that you fill out and submit a form with your request."

Interaction designers combine static, dynamic and metalinguistic signs to compose several metacommunication strategies with which to get their message across to users. The effect of such strategies can be investigated in depth with specific Semiotic Engi-

neering methods, like the Communicability Evaluation Method. [31] In this paper, however, we are not going to investigate empirically how users receive and interpret the designers' communication. We will only characterize, based on empirical semiotic evidence, how metacommunication is expressed by the designers, then discuss the range of potential effects that can be analytically expected to follow from such expressions. As an example of what we mean by analytical effects, compare the metacommunication message communicated through the mockup in **Fig. 4** with that communicated through the mockup in **Fig. 1**. Regardless of other merits or flaws in each design (which will not be discussed in this paper), even without asking the users, it is analytically evident, by the mere presence and arrangement of static interface signs, as well as their conventional meaning, that data protection is more salient in the communication expressed by the designers of the interface in **Fig. 1** than in metacommunication expressed by the designers of the interface in **Fig. 4**. In particular, regarding the latter, because the design uses static signs that have been long seen on website interfaces prior to GDPR (cf. "Terms of Use" and "Privacy Policy" at the very bottom of the page), the message conveyed by this specific portion of design suggests that there is nothing new in post-GDPR design in this website.

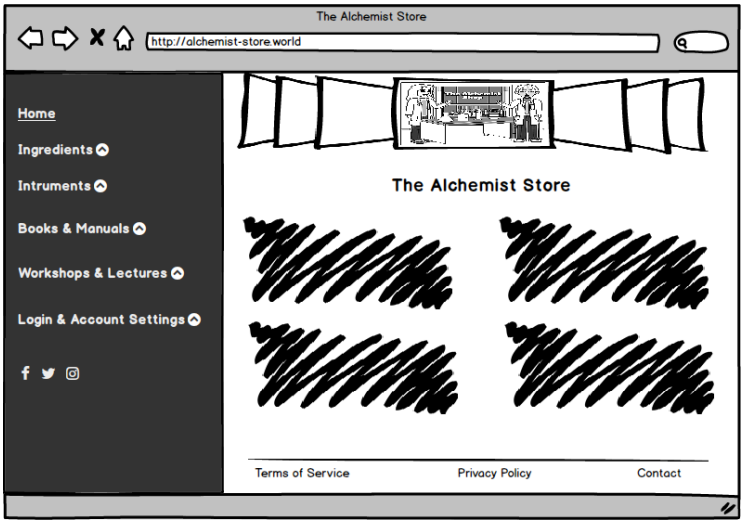

Fig. 4. Alternative entry page design of *The Alchemist Store*

3.3 Method

Semiotic Engineering methods are *interpretive* (qualitative), and explore the meaning of interface and interaction signs for both the producers (designers) and consumers (users) of digital technology. [31,32] The contrast between intended and perceived meanings in metacommunication is one of the richest results that Semiotic Engineering methods can yield. Yet, studies focused solely on the *emission* or the *reception* of metacommunication can also reveal the effects of certain semiotic features of algorithmically-mediated social communication between humans.

In this study we focused on the **emission** of metacommunication, that is, on the designers' **expression** of their message to users. The evidence for semiotic engineering analysis was collected by means of an interactive **walkthrough** of the interface, where the analyst played the role of a first-time visitor to the website, guided by the content of the following inspection scenario:

Antonio, a business administrator in his early fifties, is spending vacations with friends and family in a nice region of his native country that he has never been to in his entire life. Tomorrow, the group will have a barbecue in the front garden of the house they are renting, and Antonio is in charge of buying snacks and drinks for ten people. He decides to buy them online, but immediately realizes that the food chain where he usually shops when at home does not provide services in the place where he is now. He must then use a new online supermarket service.

Antonio is extremely careful with personal data protection when shopping. So, before he starts, he wants to learn what data the company collects, for what purposes, how they handle it, and finally what rights he has as the owner of the data.

The walkthrough focused primarily on interaction required to find answers to three sets of questions:

- **Data Collection**
  - What data is collected? By whom? For what purposes?
- **Data Access, Correction, Portability and Elimination**
  - How can the user access his data? How can he correct it? How can he transfer it to another service provider? How can he delete it (be forgotten)?
- **Consent and Explanations**
  - What does he have to consent to? Can consent be partial or revoked? How? Is there an explanation for how the automatic processing of his data affects him? Can he understand the explanation?

The analysis consisted of four main steps. Firstly, we looked at how content *and* interactions are communicated (expressed) by the designers of the analyzed websites through static, dynamic, and metalinguistic signs (cf. subsection 3.2 to see what this means). Secondly, we looked at the distribution of sign classes and characterized the designers' metacommunication strategy. Thirdly, we made an overall assessment of what consequences the designers' strategy might bring about for the quality and effectiveness of GDPR-related communication and action.

The final step of the analysis was to contrast the findings of post-GDPR Portuguese websites and pre-DPL Brazilian websites. Differences and similarities regarding communication strategies and their consequences for users should allow us to appreciate the evolution of interaction design to support users' decisions and actions for personal data protection. The walkthroughs were carried out using Firefox 64.0.2, with the recommended (default) configurations for cookies and security. The browser's interface language was set to Portuguese, which is also the language of the eight inspected websites.

4 Findings

We begin this presentation of findings by noting that evidence of GDPR-related metacommunication collected during the walkthroughs of all websites is almost entirely made up of **metalinguistic signs** explaining the properties, behavior, policies, and terms of use of *other* interaction signs, namely the website's interface for online shoppers. **Fig. 5** presents one example of massively textual communication from designers to users about the users' personal data protection rights, and what they should do to exert them. Although this might not come as a surprise, given the novelty of the law and data governance practices, the upshot of the virtual *absence* of metacommunication achieved with static and dynamic signs (like, for example, the mockups shown in section 3.2) is that users can do little more than read and navigate through long spans of text, rather than directly access and download collected personal data, request the deletion, limitation, or specific restrictions of personal data usage *online*, as suggested in **Fig. 3**.

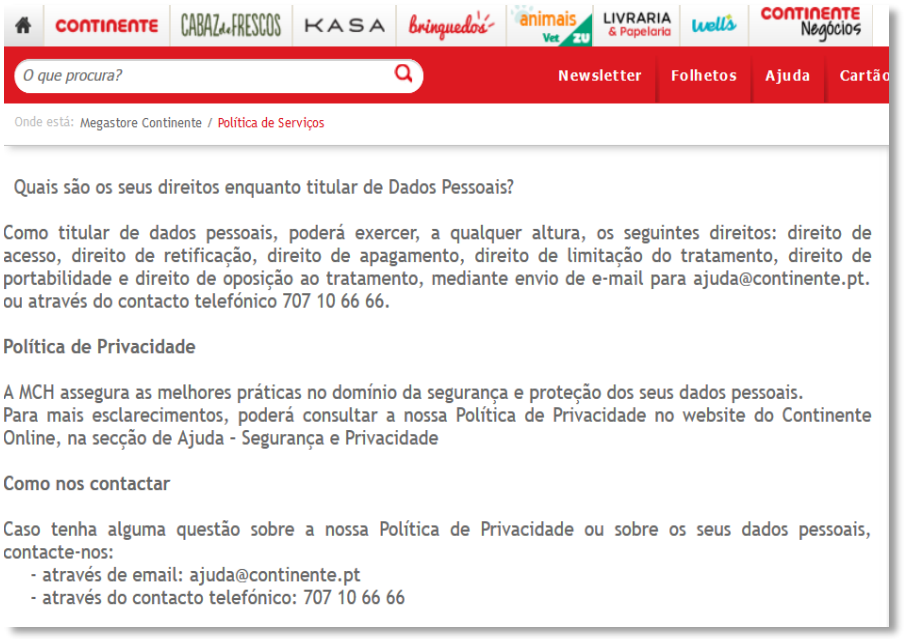

Fig. 5. A typical *interface* to exert personal data protection rights

Moreover, as can also be seen on **Fig. 5**, for a first-time visitor, metacommunication is thoroughly opaque regarding *how* the users' rights are handled by the businesses analyzed in our study. All of the European ones, tell users to send email (**Fig. 5** "mediante envio de e-mail") or call a telephone number (**Fig. 5** "através de contacto telefónico") to make their requests. In other words, most of the GDPR-related tasks cannot be carried out online, through interaction *with the website*. As previous research has

shown [33], since the early days of e-commerce and e-businesses, users seem to perceive the broader social context (especially the 'people') behind interfaces. This has been evident, for example, with the alternate use of "it" (the interface) and "they" (website owners) when verbalizing interaction with websites. The absence of interaction to achieve GDPR-related tasks is, thus, likely to motivate perceptions that although *a website* or *a system* may collect and process users' personal data and online behavior, *it* has nothing to do with the obligations of data controllers and processors obligations (*their* obligations). Websites may then be seen (and possibly used) as a protective shield for legally responsible parties. **Table 1** summarizes our top-level findings.

Table 1. Overview of findings.

Dimensions of Analysis	**Portuguese Websites**	**Brazilian Websites**
Users' Rights to Know, Decide, and Act	All four websites addressed the users' rights.	Two of the websites partially addressed the users' *new* rights.
Interaction Design and Metacommunication Strategies	Very restricted *interaction* (mainly navigation, scrolling); massive textual *communication* to users; most action takes place via email or telephone (*meta-communication* is almost non-existent).	Three of the websites support very restricted *interaction* (mainly navigation, scrolling); massive textual *communication* to users; action takes place via email, chat or telephone (*meta-communication* is almost non-existent). One website provides a presumably *intelligent assistant*. PDP-related Q&A is, however, very poor.
Pre- and Post-Legislation Contrast	Although content (information design) is clearly different before and after PDP law is enforced, interaction design is not different. Moreover, even if legislation empowers users to decide when to share personal data and entitles them to take several actions to manage such data, interaction design does not allow them to do so with the same ease and agility as they can do their online shopping transactions.	

Table 2 summarizes the main features of European websites regarding the use of cookies. This is the most striking post-GDPR difference for first-time users, and also one of the few where simple static and dynamic signs fully achieve a PDP task. The middle column shows that the phrasing of messages (translated by the author) underlines the advantages of using cookies, and in some cases suggests that users can *not accept to use cookies*. Although they can technically do it, if they care to read lengthy textual instructions and follow links to web browsers' documentation on how to block cookies, once they load the current website home page, cookies are *immediately* in use with default browser configurations. Moreover, most cookie notifications are placed at the bottom of a browser's screen laden with animations

advertising products and discounts. These will most likely distract the user's attention away from relevant PDP information.

Table 2. Overview of freely translated communication about cookies in Portuguese websites.

Website	Metacommunication Message and Location on Screen	Further Information / Dialog
Continente (PT)	*"Our website uses cookies to enhance and personalize your navigation experience. As you continue navigation you consent to the use of cookies. Learn more."* **Location:** BOTTOM OF BROWSER'S WINDOW	If the user clicks on "Learn more", a pop-up window is opened with fixed questions about cookies. The answers appear as the user clicks on the arrow control (see **Fig. 6**).
Froiz (PT)	*"This website uses cookies to enhance your experience. As you continue to navigate you agree with such use. If you want to know more, see our Cookies Policy. I understand. More information."* **Location:** BOTTOM OF BROWSER'S WINDOW	If the user clicks on "More information", a new tab is opened, showing a web page with plain textual explanations about cookies. The text contains no active links.
Pingo Doce (PT)	*"This website uses cookies and other tracking technologies to help navigation and [enhance] our ability to provide feedback, analyze the use of our website, [...] present promotional information about our services and products, and provide content for third parties. Check our Cookies Policy. I accept."* **Location:** BOTTOM OF BROWSER'S WINDOW	If the user decides to check the Cookies Policy, a new tab is opened, showing a web page with typographically designed information about cookies. It even includes a link to an independent legal consultancy group's website, where abundant information about cookies is provided.
Jumbo (PT)	*"We use cookies, of our own and third parties, to enhance your navigation experience and to show you publicity oriented to your preferences and navigation habits.* *Click on 'Accept' to confirm that you have read this and that you accept our Cookies Policy. Accept"* **Location:** POP-UP HOVERING ON THE RIGHT-SIDE OF THE BROWSER'S WINDOW	If the user clicks on the "Cookies Policy" link, he navigates to a webpage with typographically organized information about cookies. The problem is that the pop-up can only be closed by clicking on 'Accept'. The pop-up stays in front of the content which should help the user decide (see **Fig. 7**). The practical effect is that of a *nagging splash screen* to persuade users to act as the website owners expect.

Fig. 6. Pop-up window with information about cookies in Continente's website

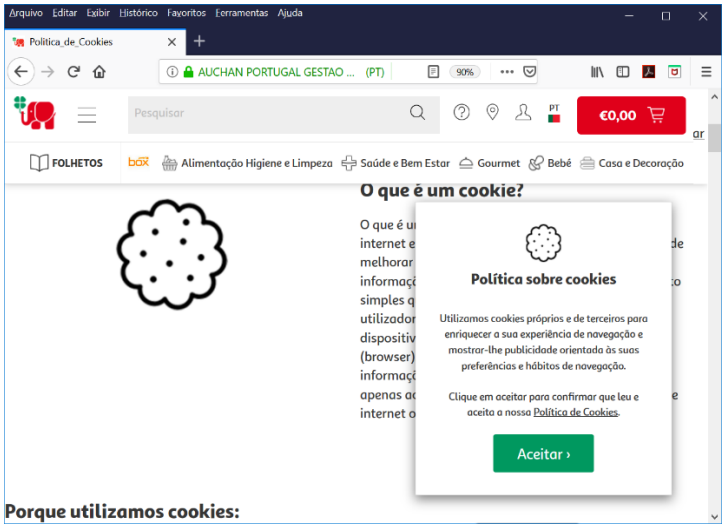

Fig. 7. Encumbered communication about cookies in Jumbo's website

Brazilian websites do not warn the users about the use of cookies (which they all use). The irony is that, even though European websites warn their users about it, users have no option to say "no", at least to the first load of cookies placed when they hit the home page of the analyzed websites. This communication problem has more to it than meets the eye. In these websites, cookie control is the result of interactions with *web browsers*, not *web servers.* Therefore, although metacommunication is carried out in one channel, one context, and with two fairly defined interlocutors (the user and the e-commerce 'website'), a silent third party who is mediating the entire process – a web browser – is the only one that can effectively do something if users do not agree with

the website's terms of cookie use. The consequence for communication and user experience may is that, if users want to communicate with the online shopping website on different terms, they cannot *tell it to the website*. They have to tell it to *a silent mediator*, who suddenly steps into the scene. This situation is very similar to the one presented in **Table 1**, where communication needed to turn the users' rights into full effect is systematically directed to *mediators* that can only be reached by email and telephone.

Further relevant PDP-related evidence comes from a Brazilian website, Super Prix, which uses a different pattern of metacommunication. Instead of the plain navigation-scrolling option to 'learn more' about ToS and PP, Super Prix initially offers interaction with an 'intelligent assistant'. At first, if the user clicks on an ostensive "May I help?" button floating on the side of the page, a pop-up window is shown encouraging users to just *ask* ("Perguntar") what they want to know. The added arrow on the right side of the screenshot image in **Fig. 8** indicates the location and design of the pop-up dialog.

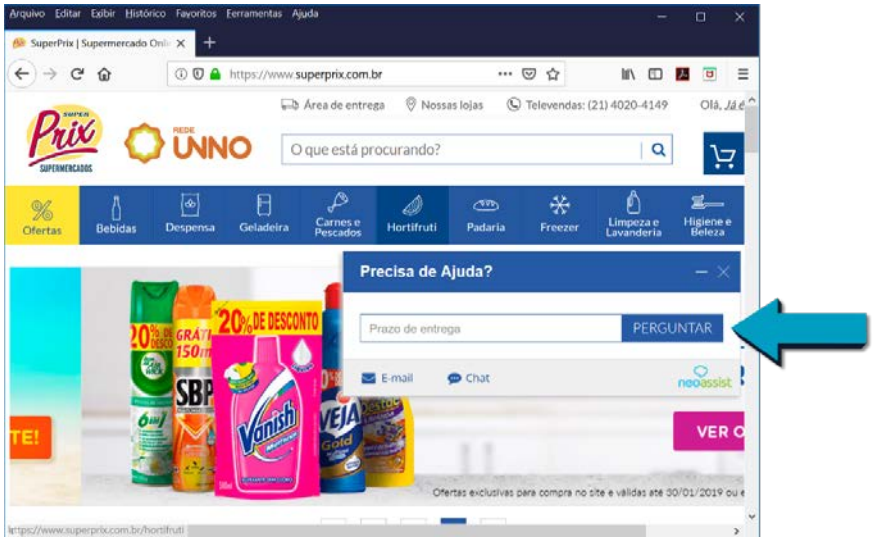

Fig. 8. Brazilian website "free text" interaction when users need help

Intelligent assistance is more explicitly invoked when users follow the link to this website's Privacy Policy. In **Fig. 9**, however, we show an example of the assistant's behavior when asked: "What do you have to offer re: Personal Data Protection" (author's translation from Portuguese). The user gets two links to information: "What happens with my credit card data?" and "What must I do to change my registered data?". These links are the *answer* to several other questions like: "May I erase my data?", "May I see what data you collect?", and so on. Beneath the brittle chatbot cover, **Fig. 9** also demonstrates the tendency to direct conversation to non-algorithmic interaction. The other tabs to the right of "Atendimento Inteligente" (Intelligent Assistance) are: "Fale Conosco" (Contact, via email) and "Atendimento via Chat" (Online Chat), with human intervention.

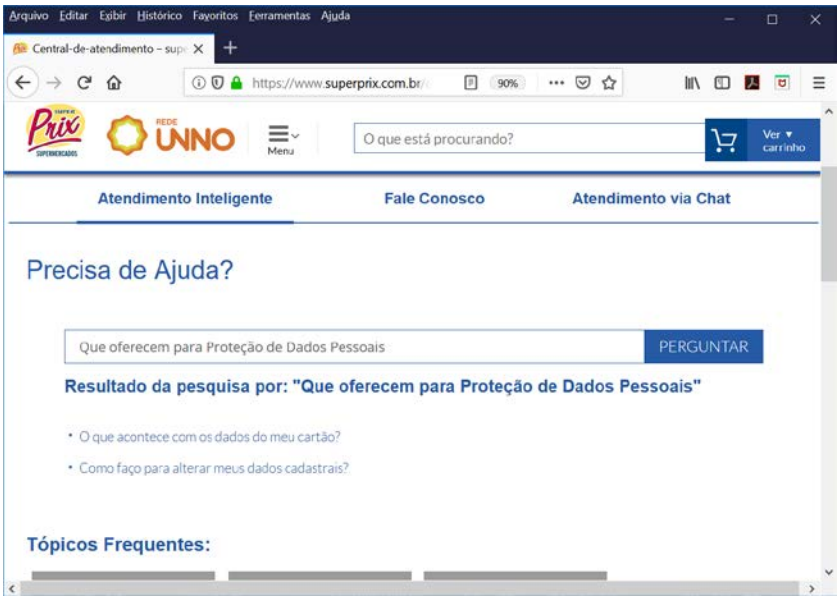

Fig. 9. Super Prix intelligent assistant behavior

The findings of our contrastive study can be grouped in three clusters. The first one refers to **underprovided online opportunities** for users to exert their personal data protection rights *while interacting with the analyzed websites*. In all cases they are instructed to use email and telephone lines to do it. The second refers to the **uncontrolled mediation** of web browsers in metacommunications regarding the use of cookies. Consent conversations between users and websites (speaking for their designers, developers and owners) are only consistent if users *accept* that websites use cookies. If they don't, they *must talk to somebody else* (in this case, their browser's configuration interface). Finally, we also found evidence that **intelligent conversational agents are not yet an option** to inform and guide users in their attempts to know how businesses handle their GDPR obligations. All relevant information, steps and decisions relative to enforcing data protection rights are explicitly directed to human-to-human communication channels like email and telephone lines. Algorithmic mediation, which has long been in place for e-commerce – a comparable data-sensitive and legally ruled application area – is clearly not used. In the next section we will discuss these findings and present our conclusions about the significance of this study.

5 Concluding Remarks

The qualitative study presented in this paper has not been designed to answer questions like "how has interaction design changed after GDPR?", or "how do e-businesses handle their clients' data protection rights online?" in a generalizing sense. The validity of this study is limited by the analysis of only a small set of websites, the contingency of

walkthroughs guided by a specific scenario, and the researcher's inevitable interpretation biases. However, as qualitative methodology requires, the researcher has strived to discount such limitations. The adopted strategy has been to use an explicit orienting theory throughout the process. Semiotic Engineering has provided not only the initial categories of analysis (with the concept of metacommunication and the three classes of signs that are used to compose designer-to-user metacommunication messages), but also a framework to organize sociotechnical relations among parties involved in PDP-related interactions and transaction online. The following paragraphs should show that this study's main contribution is to support the elaboration of *qualified hypotheses* for subsequent predictive (or non-predictive) more general inquiries with larger samples of interactive systems that collect, store, and process their users' personal data.

The findings reported in section 4 are *themselves* part of the meanings that might be inferred from metacommunication by more reflective users. For instance, users might ask what the owners and producers of the analyzed websites mean by declining to engage in PDP-related interactions in the same way as they engage in buying and selling interactions. The just as interesting reverse question could be asked by reflective interaction designers: What might users take this strategy to mean?

The Semiotic Engineering perspective used in the study can also add significant elements to the current debate on privacy by design [34,35] and usability aspects of GDPR-related interactions online. Because it takes *metacommunication* as its object of investigation, and metacommunication involves software producers, software users, and software itself, this theory can shed light on certain aspects of current scientific discussions that are not necessarily framed in connection with one another.

The three classes of signs investigated by the theory (see subsection 3.2) establish different conditions of meaning making in HCI. Static signs support instant meaning making, often associated with intuitiveness and ease of use. Metalinguistic signs, in turn, support indefinitely many levels of referential meaning making, which can augment or correct previous meanings assigned to the interaction objects in reference. It is the class of dynamic signs, however, that creates the most complex and intriguing conditions for meaning making. We will refer to this as *algorithmically-negotiated meaning making*. On the one hand, the expression underlines the fact that dynamic signs are controlled by *algorithms* (computing rules), and are thus inherently akin to what Peircean semioticians refer to as *legi signs*, or signs that are established by some kind of law. [36] On the other, the expression also underlines the fact that human meanings are always *negotiated* in social communication. A communication sender (S) can never be sure that the communication receiver (R) has captured what she (S) means by a single piece of communication. Likewise, a receiver (R) can never be sure that what he (R) takes the sender's (S) communication to mean is actually what she means. As a result, social communication is full of interpretation checkpoints and verifications, adjustments, corrections, redundancy, explanations, and other meaning-negotiation procedures that cannot, unfortunately, ultimately guarantee that senders and receivers share the *same* meanings. Certain semiotic theories actually suggest that they never do. [36]

Computer-mediation, however, creates and enforces meaning stability (or *algorithmic meaning*) that governs metacommunication between human parties. The algorithm that captures a user's click on the "Accept" ('Aceitar') button on Jumbo's cookie use

notification interface (**Fig. 7**) defines the necessary and sufficient technological conditions for a user's explicit consent to having cookies placed on her device. The same will be true of other algorithms defining the necessary and sufficient technological conditions for users to access, modify, delete or transport their personal data. The problem, as **Fig. 7** conveniently demonstrates, is **how interaction design communicates to users the meaning of algorithms**. The rhetorical effect of a pop-up window that will not disappear unless the user clicks on the "Accept" ('Aceitar') button is to rush users into accepting the terms of service. In other words, interaction design may *add* meanings to the algorithmic rule that establishes the technological protocol for consent. On the other hand, the walkthrough has shown that the pop-up window is actually preventing users from reading this website's cookie policy (some portions of it are occluded behind the nagging window). If interaction designers did not mean it to happen, it is now the algorithms that are adding (undesired) meanings to the designers' and possibly the owners' intended message, inducing users to accept personal data usage terms without reading them. The challenge indicated by this piece of evidence is that interaction designers and software engineers do not always negotiate models and implementation meanings with one another. [32] Thus, if algorithms are to be taken as an expression of the law, not only interaction design, but also software development processes may need new meaning-negotiation tools for design and development teams to compose and express their message in unison and accordance with the owners' intent.

Furthermore, dynamic signs may well be the reason why GDPR and DPL matters in the Portuguese and Brazilian websites we analyzed are channeled to and processed by humans, rather than algorithms. This view connects with Politou and colleagues' research [25], as well as with studies coming from other domains. For example, Katsh's analysis [37] of the state of the art in online dispute resolutions (ODR) says that in "the earliest forms of [ODR] […] email seemed an appropriate tool for communication between disputants and between disputants and third parties." [p. 7] Now, however, "the role of software has been recognized in discussions of legal doctrine by the expression *code is the law*." [p.8] Algorithms, as of now, are not ready to *stand for* GDPR or DPL.

Our future work with Semiotic Engineering is to explore the merits of alternative metacommunication strategies for PDP communication, decision-making, and action. GDPR is only a trigger for research that aims to contribute for greater transparency in the digital world [38], striving to enable ethics and fairness in power relations established by algorithmically-mediated metacommunication among humans. This is the call we want to make with this work, that as member of the interaction design community, we *tell* users what is ethically and otherwise important for them to know about their rights, and *help* developers and owners express what they mean to say more effectively.

Acknowledgments

The author thanks the Brazilian National Council for Scientific and Technological Development (CNPq) for partially funding this research, with grant #304224/2017-0. She also thanks anonymous Interact 2019 reviewers, her students, and colleagues for insightful comments and suggestions that improved the original version of this paper.

References

1. The European Parliament and Council General Data Protection Regulation. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 Last Accessed in January 2019
2. Hildebrandt, M.: Slaves to Big Data. Or Are We? *IDP. Revista de Internet, Derecho y Política* 17, 7–44 (2013)
3. Governo Brasileiro LEI 13.709/2018 (LEI ORDINÁRIA) 14/08/2018. http://legislacao.planalto.gov.br/legisla/legislacao.nsf/Viw_Identificacao/lei%2013.709-2018 Last Accessed in January 2019
4. de Souza, C. S.: The semiotic engineering of human-computer interaction. MIT Press (2005)
5. Norman, D. A., Draper, S. W.: User Centered System Design: New Perspectives on Human-Computer Interaction. Lawrence Erlbaum Associates, Hillsdale, NJ (1986)
6. Holtzblatt, K., Wendell, J. B., Wood, S.: Rapid contextual design: a how-to guide to key techniques for user-centered design. Elsevier, Amsterdam (2004)
7. Ritter, F. E., Baxter, G. D., Churchill, E. F.: User-centered systems design: a brief history. In Ritter, F. E., Baxter, G. D., Churchill, E. F. (Eds.) Foundations for designing user-centered systems. pp. 33-54. Springer-Verlag, London (2014)
8. de Souza, C. S.: Semiotic engineering: bringing designers and users together at interaction time. Interacting with Computers 17(3), 317-341 (2005)
9. Bus, J., Nguyen, M.-H. C.: Personal data management – a structured discussion. In Hildebrandt, M., O'Hara, K.: Waidner, M. (Eds.), Digital Enlightenment Yearbook 2013: The Value of Personal Data (Vol. 270) pp. 270–287. IOS Press, Amsterdam (2013)
10. Iachello, G., Hong, J.: End-user Privacy in Human-computer Interaction. Foundations and Trends in Human-Computer Interaction. Vol. 1(1), 1-137. (2007)
11. Obar, J. A., Oeldorf-Hirsch, A.: The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. Information, Communication & Society. pp. 1-20. DOI: 10.1080/1369118X.2018.1486870 (2018)
12. Carolan, E.: The continuing problems with online consent under the EU's emerging data protection principles. Computer Law & Security Review. Vol. 32(3), 462 - 473 (2016)
13. Nguyen, J. H., Vu, K.-P. L.: Does Privacy Information Influence Users' Online Purchasing Behavior? Smith M. J., Salvendy G. (eds.) Human Interface and the Management of Information. Interacting with Information. Human Interface 2011. Lecture Notes in Computer Science, vol 6771. Springer, Berlin, Heidelberg pp. 349-358. Springer-Verlag, Berlin, Heidelberg (2011)
14. Acquisti A, Brandimarte, L., Loewenstein, G.: Privacy and human behavior in the age of information. Science. 347(6221), 509-514 (2015)
15. Angulo J., Ortlieb, M.: "WTH..!?!" Experiences, Reactions, and Expectations Related to Online Privacy Panic Situations. In Cranor, L. F., Biddle, R., Consolvo, S. (Eds.) SOUPS 2015 Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security. pp. 19-38. USENIX Association. (2015)
16. Tsai, J. Y., Egelman, S., Cranor, L. Acquisti, A.: The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. Information Systems Research 22(2), 254-268 (2011)
17. Berger-Walliser, G., Bird, R. C., Haapio, H.: Promoting business success through contract visualization. Journal of Law, Business, and Ethics 17, 55 (2011)
18. Rossi, A., Palmirani, M.: From Words to Images Through Legal Visualization. In Pagallo, U., Palmirani, M., Casanovas, P., Sartor, G., Villata, S. (Eds.) AI Approaches to the Complexity of Legal Systems. pp. 72-85. Springer International Publishing, Cham (2018)

19. Rossi, A., Palmirani, M.: A Visualization Approach for Adaptive Consent in the European Data Protection Framework. In Parycek, P., Edelman, N. (Eds.) Proceedings of the 2017 Conference for E-Democracy and Open Government (CeDEM), pp. 159-170. IEEE Computer Society, Piscataway, NJ. (2017)
20. Zhao, J., Binns, R., van Kleek, M., Shadbolt, N.: Privacy Languages: Are We There Yet to Enable User Controls?. In Proceedings of the 20th International Conference Companion on World Wide Web. pp. 799-806. International World Wide Web Conferences Steering Committee. (2016)
21. Schaub, F., Balebako, R., Durity, A. L., Cranor, L. F.: A Design Space for Effective Privacy Notices. In Cranor, L. F., Biddle, R., Consolvo, S. (Eds.) SOUPS 2015 Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security. pp. 1-17. USENIX Association (2015)
22. Cranor, L. F., Guduru, P., Arjula, M.: User Interfaces for Privacy Agents. ACM Transactions on Computer-Human Interaction 13(2), 135-178 (2006)
23. Chen K and Rea Jr, A. I. Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques. Journal of Computer Information Systems 44(4), 85-92 (2004)
24. Carvalho, A. C., Martins, R., Antunes, L.: How to Express Explicit and Auditable Consent. In McLaughlin, K. et al. (Eds.) Proceedings of the 16th Annual Conference on Privacy, Security and Trust (PST) 2018, pp. 1-5. IEEE Computer Society, Piscataway, NJ. (2018)
25. Politou, E., Alepis, E., Patsakis, C.: Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions". Journal of Cybersecurity. (1), 1-20 (2018)
26. Pettersson, J. S., Fischer-Hübner, S., Danielsson, N., Nilsson, J., Bergmann, M., Clauss, S., Kriegelstein, T., Krasemann, H.: Making PRIME Usable. In Proceedings of SOUPS'05 Proceedings of the 2005 Symposium on Usable Privacy and Security. pp. 53-64. ACM. New York, NY (2005)
27. Renaud, K., Shepherd, L. A.: How to Make Privacy Policies both GDPR-Compliant and Usable. In Creese, S., Renaud, R., Pedersen, J. M., Keane, E. (Eds.) Proceedings of the 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA). pp. 1-8. . IEEE Computer Society, Piscataway, NJ. (2018)
28. Contissa, G., Docter, K., Lagioia, F., Lippi, M., Micklitz, H.-W., Palka, P, Sartor, G., Torroni, P.: Claudette meets GDPR: Automating the evaluation of privacy policies using artificial intelligence. pp. 1-59. Available at SSRN: https://ssrn.com/abstract=3208596 or http://dx.doi.org/10.2139/ssrn.3208596 (2018)
29. Tesfay, W. B., Hofmann, P., Nakamura, T., Kiyomoto, S, Serna, J.: PrivacyGuide: Towards an Implementation of the EU GDPR on Internet Privacy Policy Evaluation. In Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics. pp. 15-21 ACM. New York, NY (2018)
30. Zaeem, R. N., German, R. L., Barber, K. S.: PrivacyCheck: Automatic Summarization of Privacy Policies Using Data Mining. ACM Transactions on Internet Technology 18(4), pp. 53:1-53:18 (2018)
31. de Souza, C. S., Leitão, C. F.: Semiotic engineering methods for scientific research in HCI. Synthesis Lectures on Human-Centered Informatics. Morgan & Claypool. San Rafael, CA. (2009)
32. de Souza, C. S., Cerqueira, R., Afonso, L. M., Brandão, R. R. M., Ferreira, J. S. J.: Software developers as users: semiotic investigations in human-centered software development. Springer, Cham. (2016)
33. Light, A., Wakeman, I.: Beyond the interface: users' perceptions of interaction and audience on websites. Interacting with Computers 13(3), 325-351 (2001)

34. Colesky, M., Hoepman, J., Hillen, C.: A Critical Analysis of Privacy Design Strategies. In 2016 IEEE Security and Privacy Workshops (SPW). pp. 33-40. IEEE Computer Society, Los Alamitos, CA. (2016)
35. Cavoukian, A.: Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D. Identity in the Information Society 3(2), pp. 247-251 (2010)
36. Merrell, F.: Peirce, signs, and meaning. University of Toronto Press, Toronto (1997)
37. Katsh, E.: Online dispute resolution: Some implications for the emergence of law in cyber-space. International Review of Law Computers & Technology 21(2), 97-107 (2007)
38. Edwards, L., Veale, E.: Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking for. Duke Law & Technology Review 16, 18-84 (2017)