V!19
issn 2175-974x | ano 2019 year
semestre 02 semester

André Lemos is a Mechanical Engineer and Ph.D. of Sociology. He is a Full Professor at the Department of Communication, and the Graduate Program in Contemporary Communication and Culture at the Federal University of Bahia, where he coordinates Lab404 - Research Laboratory in Digital Media, Networks and Space. He works in the areas of communication and sociology, in particular on digital culture or cyberculture. He is a member of the Steering Committee of the Brazilian National Institute of Science and Technology in Digital Democracy.

Daniel Marques holds a Bachelor's degree of Design and a Master's degree in Contemporary Communication and Culture. He is an Assistant Professor at the Federal University of Recôncavo da Bahia, Brazil, and a researcher at Lab404-Research Laboratory in Digital Media, Networks and Space, at the Federal University of Bahia. He studies Design, Innovation and Culture, Data Visualization and Mapping Art, Culture, Communication, and Language Systems.

How to quote this text: Lemos, A. and Marques, D., 2019. Malicious Interfaces: strategies for personal data collection in apps.Translated from Portuguese by Colin Richard Bowles. *V!rus*, Sao Carlos, 19. [e-journal]. [online] Available at: <http://www.nomads.usp.br/virus/_virus19/?sec=4&item=2&lang=en>. [Accessed: 13 December 2019].

ARTICLE SUBMITTED ON AUGUST 18, 2019

Abstract

This paper analyzes malicious interfaces (MIs) (dark patterns) in ten apps used by the municipality of Salvador to collect personal data. By mediating different aspects of urban social life, these apps contribute to the construction of the contemporary city and the way it is experienced. This new informational dimension of the city, in turn, poses challenges for citizens' privacy as it fosters the production and collection of as much sensitive personal data as possible. We evaluated the app interfaces with a severity scale (SS) in order to identify the different types of MIs and the level of threat they pose to users' privacy. All the analyzed apps have MIs, most of which are level 1 (minor), and there is a tendency for these to become increasingly commonplace. The MIs in the apps are part of the increasing *platformization* and *datafication* of society and the performative agency of algorithms (PDPA).

Keywords: Dark patterns, Apps, Privacy, Salvador

1 Introduction

The production of social life in the contemporary digital city increasingly overlaps with digital information and communication technologies. Smartphones, virtual assistants, apps, algorithms and social networks, for example, now occupy a significant space in the social fabric and mediate relations of sociability, affect, work, education and leisure. The spread of these mediations takes the idea of an "informational society" to an extreme level, given the central role of the production of information—and its access to increasing amounts of data—in generating value for so-called platform/surveillance capitalism (Zuboff, 2015).

Data has become the new commodity in contemporary capitalism, and citizens and the city have become sources of this commodity. As the value of data increases and becomes more apparent, we begin to see a more significant effort by multiple institutions, whether private or public, to collect and extract value from this information, jeopardizing people's privacy in the process. Given that the production and collection of data is the main objective of surveillance capitalism, there is a raised awareness of strategies and mediations used to domesticate citizens to produce more and more data. Data capitalism involves the "construction of information", putting the privacy of citizens in urban space at risk.

Therefore, this article seeks to discuss what has become known as dark patterns (DPs), namely interfaces that lead users to perform certain actions intended to achieve a variety of purposes. One of such purposes is to collect personal data, which may not be essential to the service initially provided by the app. This collection of data constitutes datafication for commercial or technical purposes. DPs pose a threat to privacy because they persuade users to perform actions that result in personal data capture. Our interest in this subject arose from criticism of these threats found in apps and websites (Ash et al., 2018a, 2018b). We analyze ten apps used by Salvador City Hall. The approach adopted for analyzing these DPs is from a neomaterialist, pragmatic perspective (Fox, Alldred, 2017; Lemos, 2019a). We use a three-level severity scale (SS) to analyze, describe and compare the interfaces. Building upon the original dark patterns framework, we argue in favour of naming these strategies "malicious interfaces" (MIs).

2 Malicious interfaces

The term dark pattern (DP) was proposed by Harry Brignull, a cognitive psychologist who works with user interaction (UI) and user experience (UX) design, in a lecture at UX Brighton in 2010[1]. DPs are design strategies used in digital interfaces (sites, apps, wearables, etc.) and have their origins in the tradition of design patterns[2]. The term, which has gained popularity, has been adopted by academics and professionals in the fields of design and computing, and the issue of DPs has been the subject of recent articles in the Financial Times[3], Gizmodo[4], The New York Times[5] and The Verge[6].

For Brignull (2010), DPs are not merely bad designs. They are anti-patterns, created to trick the user into performing actions of interest to the app/company either unwittingly or because there is no way to avoid them. Unlike bad designs, DPs are characterized by an obscure intention and are developed to achieve specific results without the need to provide any explanations to the user. As he puts it, "this is the dark side of design, and since this kind of design patterns don't have a name, I'm proposing we start calling them Dark Patterns" (Brignull, 2010). These strategies are based on the exploitation of users' cognitive and psychological attributes, so the users do not notice that their behavior is subjected to the agency of the platform. Brignull proposed an initial taxonomy of DPs and catalogued 11 different species[7], a number that subsequently increased as new papers were published.

We propose to change the term "dark patterns" by "malicious interfaces" (MIs). In this article, we discuss MIs in the use of personal data issues and threats to privacy. The development of MIs to maximize the production, collection and processing of personal data is part of a broader context: the PDAP culture (Lemos, 2019a, 2019b), that is, the **platformization** of society (Van Dijck; Poell; De Waal, 2018), **datafication** (Mayer-Schonberger; Cukier, 2013) and **algorithmic performativity** (Bucher, 2017; Danaher, 2016).

PDAP is the phenomena that characterize the current state of digital culture and illustrate how digital platforms are playing an expanding role in the mediation of everyday life. The platformization of society in this sense refers to the growing presence of digital platforms—generally products and services associated with GAFAM[8] —in the mediation and realization of social life. This mediation occurs mainly through the action of performative algorithmic systems, which, as key elements in the design of platforms, have an impact on the organization of social life. As PDAP is developing at the same time as data (or surveillance) capitalism is expanding (Srnicek, 2017; Zuboff, 2015), personal data are considered the principal commodity (Sadowski, 2019) given the need to "datafy" social life, i.e., maximize production, collection and processing of this

commodity. The term PDAP refers to the integration of these phenomena: digital platforms which act and materialize through the implementation of performative algorithms and different processes that collect personal data (datafication).

Since 2010, the literature on MIs has become more diverse and now covers areas and subjects such as game design (Zagal, Björk, Lewis, 2013), proxemic interaction technologies (Greenberg et al., 2014), the violation of privacy and maximization of datafication processes (Bösch et al., 2016; Doty, Gupta, 2013; Fritsch, 2017), ethical implications (Gray et al., 2018), activism in digital platforms (Trice, Potts, 2018) and physical and voice interfaces (Lacey, Caudwell, 2019). And, as some authors have noted, developers are using MIs as a competitive strategy (Lewis, 2014; Nodder, 2013).

We highlight four central issues found in the current literature on the subject: (a) the problem of intentionality; (b) the focus on the observation of micro-interactions; (c) ethical aspects; (d) psychological factors. The problem of intentionality is the most widely discussed issue, and much of the literature acknowledges that MIs are implemented by companies as deliberate strategies. The focus of the present study was, therefore, to consider what the intentions that lie behind the MIs used in the apps analyzed here might be. From a pragmatic perspective, as we have adopted here, it seems somewhat subjective to declare that intentionality is present; instead, it would be more productive to analyze the concrete effects of MIs. MIs comply with the letter but not the spirit of the prevailing legislation (Doty, Gupta, 2013), and usually, the user is not aware of the agency to which she or he is being subjected.

Psychological and subjective factors vary from user to user, and they also come into play (Bösch et al., 2016, Zagal et al., 2013). The user's understanding undoubtedly has a role in this process, but it is not the only factor in the same way as noticing a malicious strategy is not sufficient to avoid interaction. In many cases negotiation is not possible, and the only alternative is to opt-out. For Bosch et al. (2016), MIs affect users regardless of their level of literacy because of our increasing dependence on apps. It is almost impossible to live nowadays in Western capitalist societies without the services offered by GAFAM.

Many people now experience the "privacy paradox" (Williams, Nurse, Creese, 2016). When assessing whether it is worthwhile releasing personal data in exchange for goods and services, users concerned with privacy end up giving in. This paradox becomes more complex as users are rarely able to determine what their data are worth and the consequences of supplying them to someone else. The asymmetry between the power wielded by platforms and users' limited ability to negotiate leads to a process in which MIs are becoming increasingly common as the hegemonic paradigm of interaction design. The existence of literature that encourages and offers support for the implementation of MIs corroborate this fact (Lewis, 2014, Nodder, 2013).

We shall consider two examples of MIs before we take a more detailed look at our empirical corpus: the Mi Fit and Bike Itaú apps.

Mi Fit use smart bands made by the Chinese company Xiaomi. In this app, it is challenging to verify relevant documents such as the User Agreement and Privacy Policies, as shown in Figure 1. In the Settings screen there is no indication that User Agreement and Privacy Policies are in the About section. In addition to this, even if the user manages to find the documents, no efforts have been made to adapt the long, complicated legal text to make it readable on a smartphone screen. These documents are compulsory, and including them is considered good privacy practice (Colesky, Hoepman, Hillen, 2016; Hoepman, 2012; Patrick, Kenny, 2003). The user must give his consent even though it is difficult to locate these documents to use this app. The alienation in the app is materialized in the MI. As with all MIs, this MI is produced in an asymmetric negotiating space (Ash, 2018b). The immediate effect is that users become more lenient about data collection by Xiaomi.

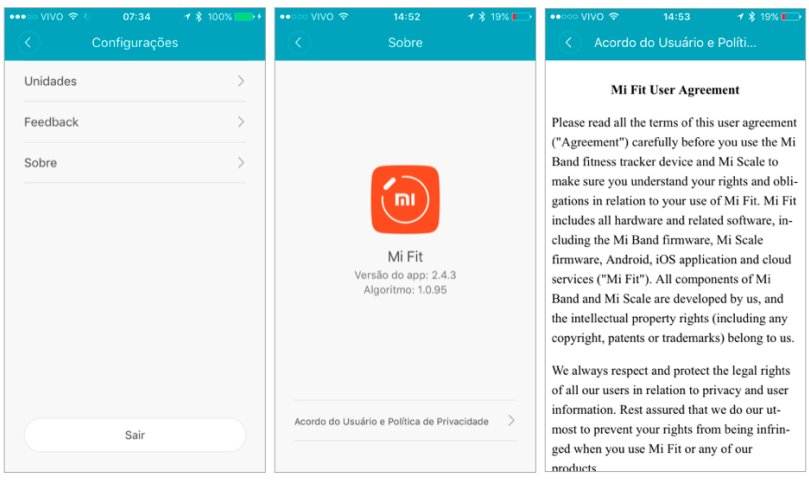


Fig. 1: Example of a MI in the Mi Fit app. Source: Lemos, Marques, 2019.

Furthermore, a MI frequently found in apps is Confirmshaming, a discursive strategy intended to shame the user into giving up data. In the Bike Itaú example in Figure 2, the first screen asks for real-time access to the user's location while the second encourages the user to complete registration, telling him that the data will be collected "only to show the locations nearest to you where bikes can be collected and returned." Ironically, the privacy policy[9] states that the data collected can be shared with third parties explicitly. In the second screen, the tone of the text is punitive as it informs the user that leaving the registration process will result in more work in the future as the information will not be saved.

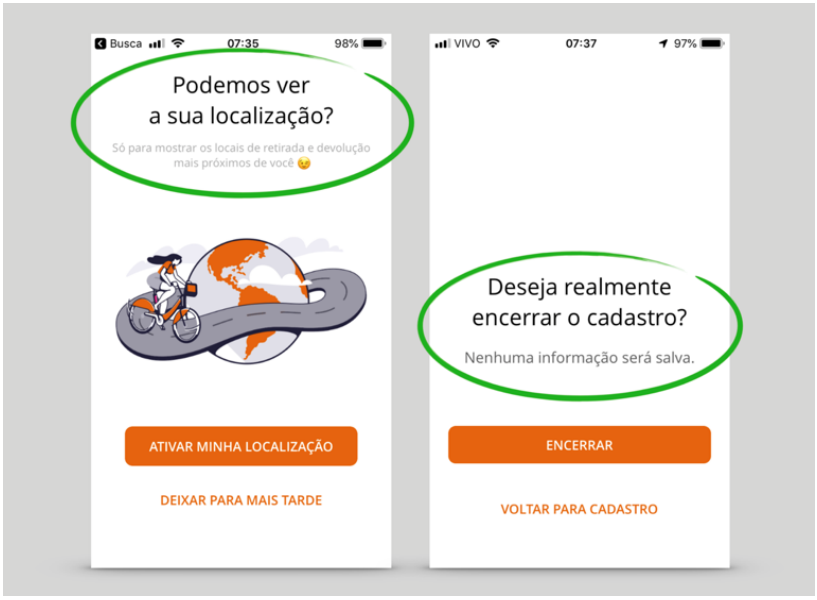


Fig. 2: Confirmshaming in the Bike Itaú app. Source: Lemos, Marques, 2019.

3 Methodology

In light of the scenario described above, we sought to identify whether the ten apps shown in Table 1 contain MIs and represent a threat to privacy. The apps, which were developed by private and state companies, were chosen because they offered services of interest to the general public in the capital of the state of Bahia. Apps intended for niche users, such as government employees, were excluded. The main screens of each app (the screens that ask the user to provide some type of personal data, both in a formal request—e.g., forms, registration, consent requests—and through interaction with the functionality of the app) were analyzed using ATLAS.ti[10]. An average of 8.1 screens was analyzed for each app. The apps with the most and fewest screens analyzed were Bike Itaú (15) and SAC BA (4), respectively.

	APP	PURPOSE
01	**Bike Itaú**	Short-term bicycle hire
02	**CittaMobi**	Monitoring of bus routes and bus stops
03	**Coleta Seletiva**	Information about selective garbage collection
04	**Detran.BA**	Requesting and following up Detran-BA services
05	**Fácil Estacionar**	Blue Zone parking
06	**FAZ Salvador**	Blue Zone parking
07	**NOA Cidadão**	Channel for reporting and following up problems on public highways in Salvador
08	**Rotativo Digital**	Blue Zone parking
09	**Rotativo Salvador**	Blue Zone parking
10	**SAC BA**	Requesting and following up SAC-BA services

Table 1: Apps analyzed. Source: Lemos, Marques, 2019.

After the MIs had been coded for the first time, we created different levels of privacy threats on a severity scale (SS), as required by the comparative analysis. We used the following SS: 1 - minor; 2 – moderate; and 3 - severe. Level 1 corresponds to MIs that require the collection of personal data that are not needed for the task in question but have some connection with the functionality of the app. Level 2 corresponds to MIs that allow personal data to be shared with third parties; the data requested are in one way or another directly connected with the purpose of the service. Level 3 corresponds to MIs that collect data that are irrelevant to the task in hand and share them with third parties while keeping the user unaware of, or alienated from, the data collection process. An app can be level 3 without being levels 1 or 2; level 2 without being levels 1 or 3; and level 1 without being levels 2 or 3. The classification scheme is shown in Figure 3.

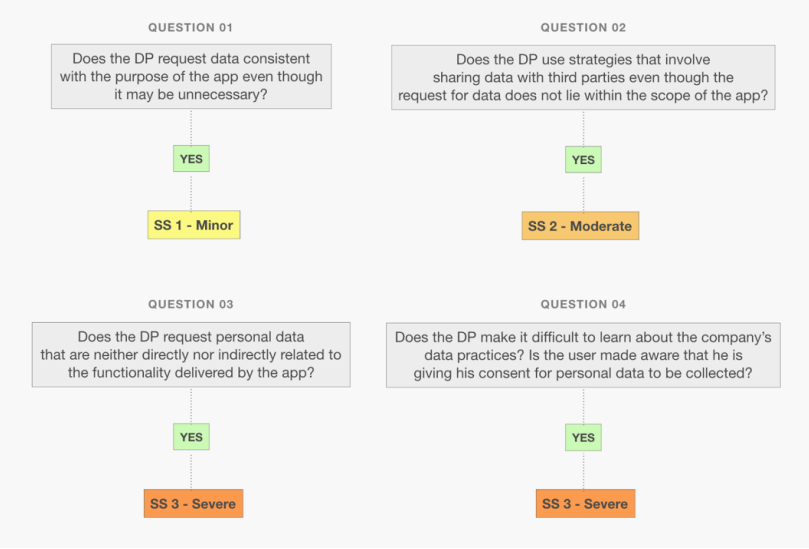


Fig. 3: Severity Scale (SS) classification scheme: Source: LEMOS; MARQUES, 2019.

4 Distribution of MIs by app

The following example illustrates how we performed the analysis for all the apps. As shown in Figure 4, in Bike Itaú,[11] the user is forced to register to gain access to the service (MI – Forced Registration, SS1). We highlight that the call to action to register/login does not appear immediately. At the first time accessing the app, the user only sees the map with stations and bicycles available. This strategy encourages the user to interact freely with the app without the initial inconvenience of filling out a form. The users have to register only when they ask to release and use the bike.

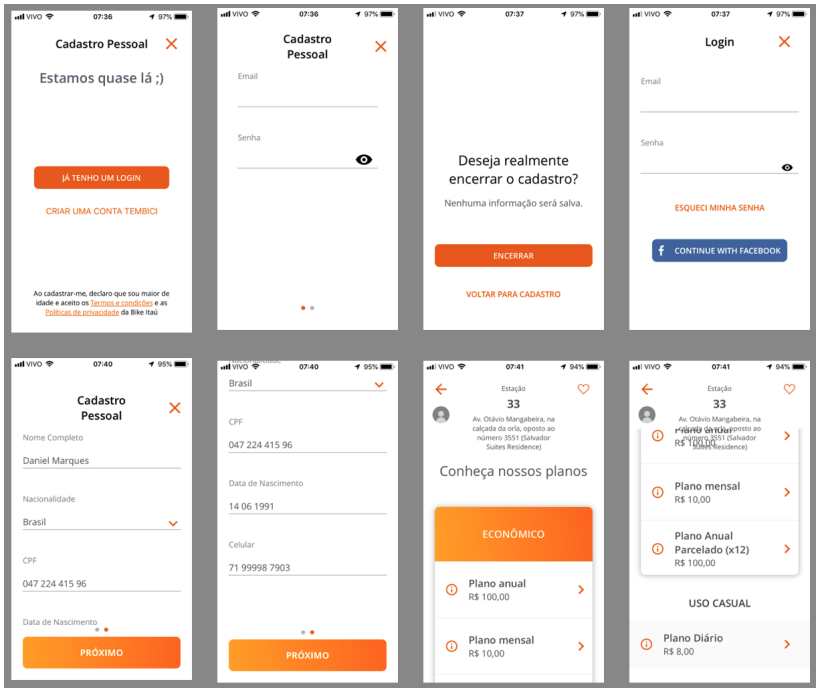
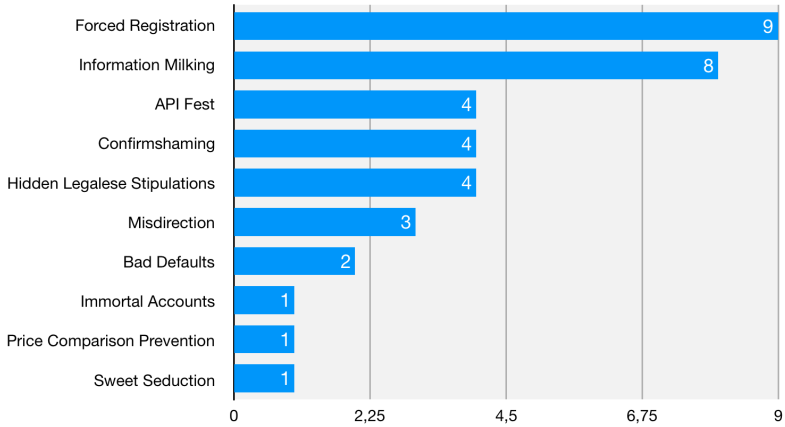


Fig. 4: Forced Registration in Bike Itaú. Source: Lemos, Marques, 2019.

On the fourth screen, the user is encouraged to log in using a Facebook registration API (MI – Forced Registration and API Fest). We evaluate this as moderate (2) SS since there are signs that the app shares data with third parties (Facebook). On the first screen, as shown above, we have an example of SS3 (MI – Hidden Legalese Stipulations), since the user's consent is requested before registration and information about the Itaú's data practices, alienating the user from its content. Thus, this app exhibits three levels of threat to users' privacy.

After analysis, we found 9 of the 21 types of MI already catalogued in websites and the specialized literature[12] as well as a different kind of MI not previously listed, API Fest, giving a total of 10 MIs. Graph 1 shows the number of occurrences of each MI in the apps analyzed as a whole. The most common MIs are "Forced Registration" (nine occurrences) and "Information Milking" (eight occurrences). Forced Registration means that the user is obliged to register. Information Milking regards asking for information that is not strictly necessary for the task in question. Both MIs are directly associated with a process of maximizing data collection by constantly inputting data into the system and can, depending on the application, characterize the three levels of threat (as we shall see later on, in Graph 5).



Graph 1: The number of occurrences of the MIs in the apps analyzed as a whole (n = 10 apps analyzed). Source: Lemos, Marques, 2019.

We observed API Fest, Confirmshaming and Hidden Legalese Stipulations for four times, so these MIs are also worthy of notification. These MIs directly or indirectly involve expanding the collection of personal data and modulation of behavior. In the first case (API Fest), the interface uses systems from other partners' platforms (Google and Facebook, for example) to perform the task. When these APIs are adopted, however, trackers adding new data sources to the platforms' databases are also implemented. Confirmshaming is a discursive strategy used to embarrass the user into giving information or performing a task. It involves manipulating the user to make him feel guilty if he does not do what the app asks him to. This MI subverts the logic of informed

consent as it uses persuasive language to convince users to allow their personal information to be collected and processed (see severity in Graph 5). The Figure 5 shows some examples of Confirmshaming.

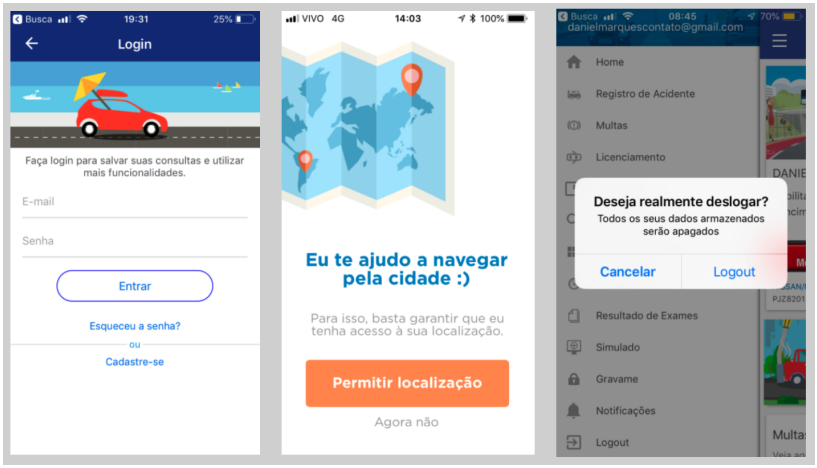
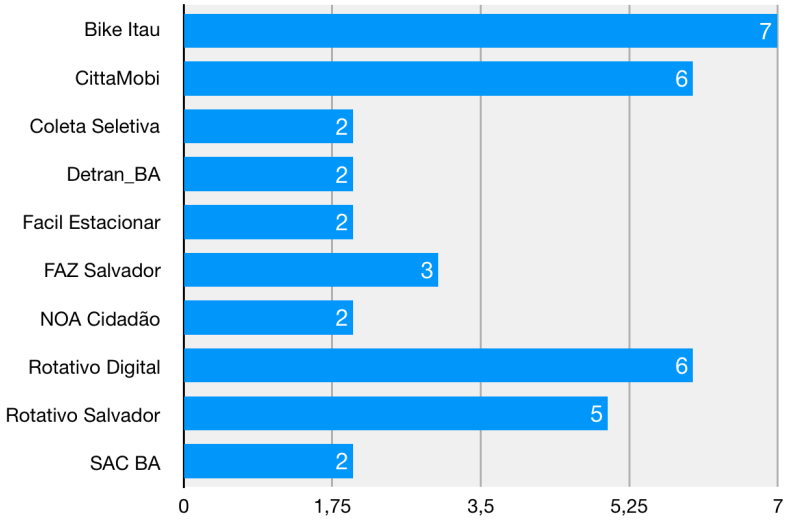


Fig. 5: Confirmshaming in Detran.BA (1,3) and Cittamobi (2). Source: Lemos, Marques, 2019.

The Hidden Legalese Stipulations MI involves hiding access to essential legal information about the performed task. In the present case, we consider documents such as Privacy Policy and Terms of Use as legal information. As seen in the Mi Fit example, this MI potentially may result in alienating the user from these documents. The alienation means the user is unaware of the data practices used in the platform, turning him into a tame user willing to follow the steps suggested by the app.

Looking at the number of MIs per app, we can see that Bike Itaú (7), CittaMobi (6), Rotativo Digital (6) and Rotativo Salvador (5) have the most MIs. Private companies developed and operate all these apps. Although they perform different functions, they all involve urban mobility and deal mainly with geolocation data. Graph 2 shows the results.



Graph 2: Number of MIs per app (n = 10 MIs investigated). Source: Lemos; Marques, 2019.

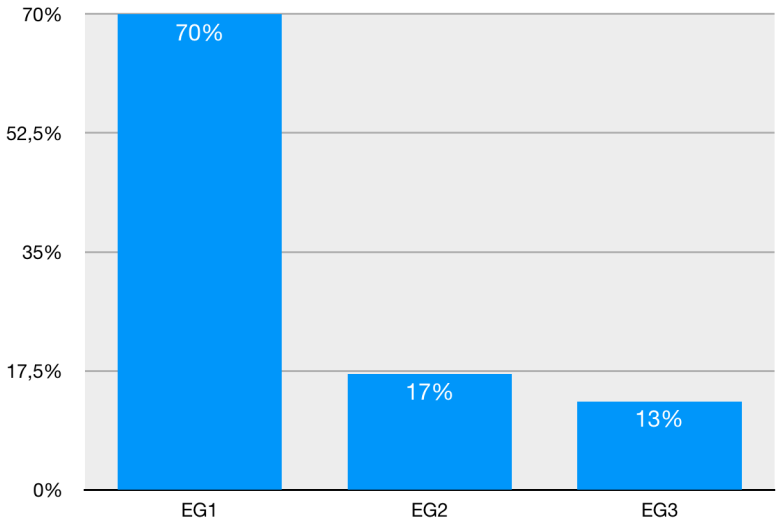
It seems to be expected that there will be a more significant commitment by private companies to explore the capture of personal data. Accordingly, the apps more closely related to public administration (Coletiva Seletiva, Detran BA, NOA Cidadão and SAC BA) have fewer MIs. Although this is an interesting finding, further discussion of this result would require a better understanding of the context in which the apps were produced and how they are currently managed in the public and private sector.

Apps in the same category can have different MIs, as Fácil Estacionar, FAZ Salvador, Rotativo Digital and Rotativo Salvador. All are registered with Transalvador to sell credits for the Zona Azul Digital. The use of a particular interaction strategy cannot, therefore, be linked to the provision of specific functionality.

5 Severity scale

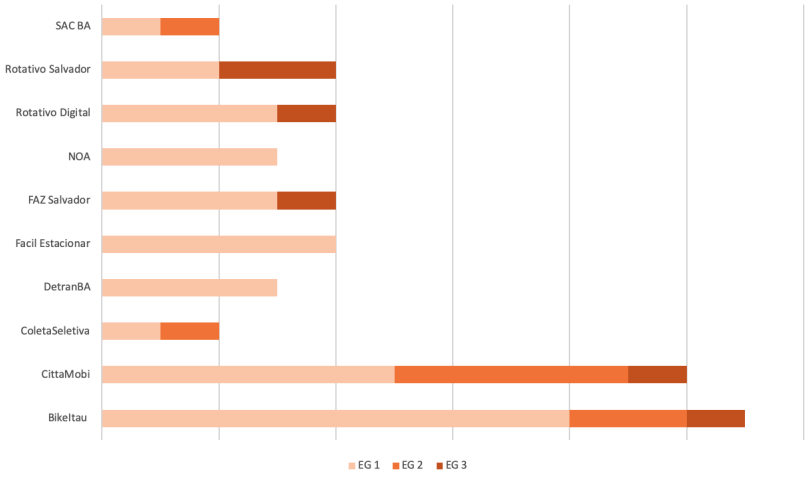
All analyzed apps contain MIs, as shown in Graph 3, and this fact corroborates the hypothesis that MIs are a characteristic of PDAP. Just over two-thirds of the apps (70%) were classified as level 1 (minor), while 17%

and 13%, respectively, were classified as levels 2 and 3. These results suggest that MIs are becoming increasingly common and pervasive[13], potentially impacting our attitude to negotiating access to personal data with platforms as the more common abusive interface practices become, the more willing consumers are to relinquish their privacy.



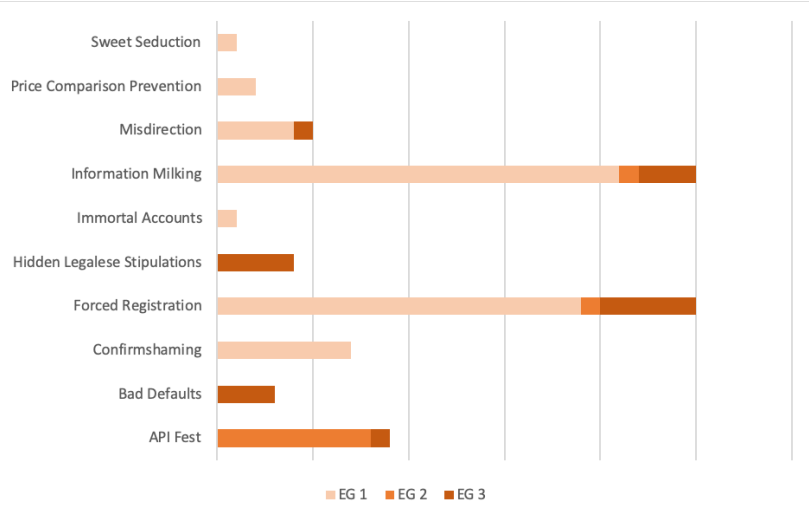
Graph 3: Distribution of MIs by SS. Source: the authors 2019.

Turning to the distribution of SSs, MIs classified as SS2 and SS3 were more common in apps produced and administered by companies in the private sector. The most severe cases were CittaMobi and Bike Itaú, in which we found all three SS levels. In both cases there is a public-private partnership, in which the companies involved provide and manage a particular service of interest to the public. The other more serious cases were Rotativo, Salvador Digital and Faz Salvador, which had MIs corresponding to levels SS1 and SS3. Graph 4 shows detailed results.



Graph 4: Distribution of SSs by app. Source: the authors 2019.

Graph 5 shows the relationship between MIs and SS. In ten categories of MI found in the corpus, four correspond only to SS1 (minor) (Sweet Seduction, Price Comparison Prevention[14], Immortal Accounts[15] and Confirmshaming), three to SS2 (moderate) (Information Milking, Forced Registration and API Fest) and six to SS3 (severe) (Misdirection[16], Information Milking, Hidden Legalese Stipulations, Forced Registration, Bad Defaults and API Fest). Although the MIs corresponding to SS2 tend to vary less, they were present in higher numbers (Graph 3).



Graph 5: SS levels by MI. Source: the authors 2019.

Many of the MIs classified as SS1 lend credence to the argument that this type of interface is increasingly forming the basis of data capitalism, leading to the development of a series of datafied products and services. Sites and apps that require the user to register (Forced Registration) and that make use of a variety of strategies to encourage users to give up their personal data (Information Milking and Confirmshaming) are becoming more and more common. At level SS2, there are signs that data are being shared with third parties, leading to profiling, and the threat to privacy tends to increase (Ponciano et al., 2017, Silveira, 2018). Particularly in relation to SS2, we highlight the presence of the API Fest MI and the use of third-party APIs without the user having a clear understanding of the company's data practices. A more "conservative" implementation of this MI can be seen in the forms requesting personal data when the user registers, as seen previously in Figure 4. Figure 6 shows other instances of API Fest.

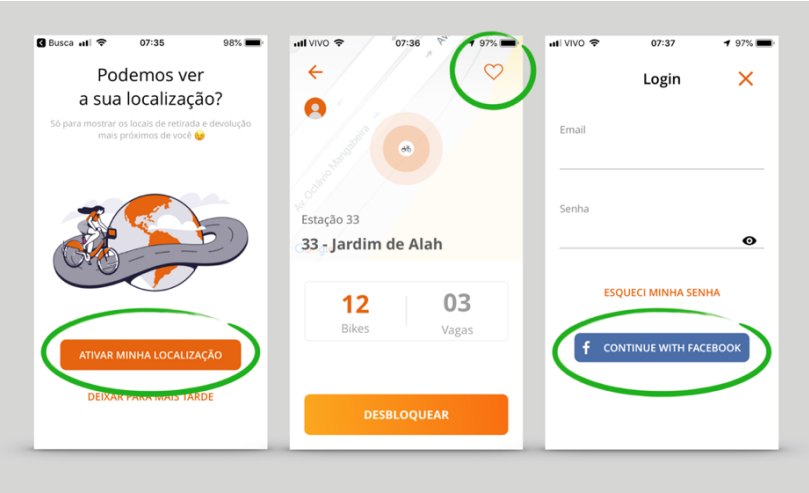


Fig. 6: Information Milking in Bike Itaú. Source: Lemos, Marques, 2019.

The first screen requests access to the user's geolocation so that the service can be optimized and the nearest stations displayed. On the second screen, in a subtler approach, we can choose to make a particular station a favorite (see detail in green). This step, in addition to the integration with the Facebook API, allows more detailed data to be collected, enriching the user's profile and enhancing the value of the data. In each case, a request is made to collect data that are not strictly necessary for the provided service, and there are signs of shared data with third parties.

6 Conclusion

In this article we have analyzed ten apps intended for the general public in use in the city of Salvador. We highlight the ongoing discussion on privacy at a time when PDAP and the use of dark patterns are expanding. As we showed in the analysis of the corpus, all the apps contain MIs, albeit with different levels of severity, suggesting a tendency for these patterns to become more and more common as part of the increasing platformization and datafication of society and the performative agency of algorithms. The growth and spread of these processes, as confirmed in the analysis of the MIs, indicates that there is a need to raise awareness of these new forms of mediation of urban social life. Many of the apps analyzed seek in some way to act in the relationship between citizen and city, mediating and affecting our experience in the city. This new urban

sociability has, therefore, become a target of new strategies for collecting and producing personal data given its value in a digital culture marked by PDAP. These strategies attempt to construct information as a new urban experience while at the same time domesticating users so that they become accustomed to producing this information daily, thereby feeding surveillance capitalism.

The study adopted a pragmatic, neomaterialist approach in which the actions generated through the materiality of the interfaces were analyzed and correlated with the capture of data without the user being aware of this. To create a mechanism for classifying and comparing the severity of the threat to privacy, we proposed a three-level severity scale (SS) (1-minor, 2-moderate, 3-severe). After analyzing the coding of the MIs in ATLAS.ti, we concluded that 70% of the apps correspond to SS1. The most severe cases are the Cittamobi and Bike Itaú apps, which contain MIs corresponding to all three severity levels, and the Rotativo Salvador, Rotativo Digital and Faz Salvador, which correspond to SS1 and SS3.

The results of the study indicate that further research is required to develop a more comprehensive picture of the use of MIs. Additional analysis of documents (the invitations to tender for the services and the technical manuals for the apps), interviews with developers, user surveys and analysis of a larger empirical corpus, among other things, are essential elements of any future studies to investigate the problem in greater detail.

It is essential to understand the position of the various actors concerning the issue of privacy, and so establish concrete ways of constructing and discussing privacy in contemporary digital society. Several questions that emerged from the study suggest that there is a need to discuss political and legal aspects of the problem. In the particular cases studied here, how did City Hall put these apps out to tender? What is City Hall's view of privacy? How were users asked to participate (if indeed they were)? Will these platforms comply with the LGPDP (General Personal Data Protection Law)? What type of pressure will be exerted by users as they are obliged to use the platforms in their daily activities as citizens?

References

Alexander, C.; Ishikawa, S.; Silverstein, M., 1977. *A Pattern Language: Towns, Buildings, Construction.* Nova Iorque: Oxford University Press.

Ash, J.; Anderson, B.; Gordon, R.; Langley, P., 2018b. Digital interface design and power: Friction, threshold, transition. *Environment and Planning D: Society and Space*, v. 36, n. 6, pp. 1136-1153. Available at: <http://journals.sagepub.com/doi/10.1177/0263775818767426>. Acessed in: 28 jan. 2019.

Ash, J.; Anderson, B.; Gordon, R.; Langley, P. 2018a. Unit, vibration, tone: a post-phenomenological method for researching digital interfaces. *Cultural geographies,* v. 25, n. 1, pp. 165–181, Available at: <http://journals.sagepub.com/doi/10.1177/1474474017726556>. Acessed in: 28 jan. 2019.

Brignull, H. 2010. *Dark Patterns: dirty tricks designers use to make people do stuff. 90 Percent of Everything.* [Blog] Available at: <https://www.90percentofeverything.com/2010/07/08/dark-patterns-dirty-tricks-designers-use-to-make-people-do-stuff/>. Accessed in: 28 jan. 2019.

Bösch, C.; Erb, B.; Kargl; Kopp, H.; Pfattheicher, S., 2016. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Privacy Enhancing Technologies*, n. 4, pp. 237-254, Available at: <https://www.degruyter.com/view/j/popets.2016.2016.issue-4/popets-2016-0038/popets-2016-0038.xml>. Accessed in: 28 jan. 2019.

Bucher, T., 2017. The algorithmic imaginary: exploring the ordinary affects of Facebook algorithms. *Information Communication and Society*, v. 20, n. 1, pp. 30–44. Available at: <https://www.tandfonline.com/doi/full/10.1080/1369118X.2016.1154086>. Access in: 28 jan. 2019.

Chung, E. S.; Hong, J. I.; Lin, J.; Prabaker, M. K.; Landay, J. A.; Liu, A. L. 2004. Development and evaluation of emerging design patterns for ubiquitous computing. In: *Conference On Designing Interactive Systems Processes, Practices, Methods, And Techniques,* 5., Cambridge. Proceedings ... Nova Iorque: ACM, 2004. pp. 233-242. Available at: <http://portal.acm.org/citation.cfm?doid=1013115.1013148>. Accessed in: 12 jul. 2018.

Colesky, M.; Hoepman, J. H.; Hillen, C., 2016. A Critical Analysis of Privacy Design Strategies. *In: Ieee Symposium On Security And Privacy Workshops,* San Jose. Proceedings... Available at: <https://ieeexplore.ieee.org/document/7527750>. Accessed in: 12 jul. 2018.

Danaher, J., 2016. The Threat of Algocracy: Reality, Resistance and Accommodation. *Philosophy and Technology*, v. 29, n. 3, pp. 245-268.

Diamantopoulou, V.; Kalloniatis, C.; Gritzali, S.; Mouratidis, H. 2017. Supporting privacy by design using privacy process patterns. In*:* Ifip International Conference On Ict Systems Security And Privacy Protection, Rome. Proceedings… Available at: <https://link.springer.com/chapter/10.1007/978-3-319-58469-0_33>. Accessed in: 12 jul. 2018.

Doty, N.; Gupta, M. 2013. Privacy Design Patterns and Anti-Patterns: Patterns Misapplied and Unintended Consequences. *In: Symposium On Usable Privacy And Security*, 9., Newcastle. Proceedings... Available at: <https://dl.acm.org/citation.cfm?id=2501604>. Accessed in: 12 jul. 2018.

Fox, N. J.; Alldred, P., 2017. *Sociology and the New Materialism: Theory, Research, Action.* Londres: SAGE Publications.

Fritsch, L., 2013. Privacy dark patterns in identity management. In: Fritsch, L.; Roßnagel, H.; Hühnlein, D. (Eds.). *Open Identity Summit 2017.* Bonn: Gesellschaft für Informatik.. pp. 93-104. Available at: <https://dl.gi.de/handle/20.500.12116/3583>. Accessed in: 12 jul. 2018.

Graf, C.; Wolkerstorfer, P.; Geven, A.; Tscheligi, M., 2010. A Pattern Collection for Privacy Enhancing Technology. *In: International Conferences Of Pervasive Patterns And Applications*, 2., Lisboa. Proceedings… Available at: <http://www.thinkmind.org/index.php?view=instance&instance=PATTERNS+2010>. Accessed in: 12 jul. 2018.

Gray, C. M.; Kou, Y.; Battles, B.; Hoggatt, J.; Toombs, A. L., 2018. The Dark (Patterns) Side of UX Design. *In: Conference On Human Factors In Computing Systems* - Chi '18, Montreal. Proceedings... Montreal: ACM Press, 2018. Available at:: <http://dl.acm.org/citation.cfm?doid=3173574.3174108>. Accessed in: 30 abr. 2019.

Greenberg, S.; Boring, S.; Vermeulen, J.; Dostal, J. 2014. Dark patterns in proxemic interactions. *In: Conference On Designing Interactive Systems* - DIS '14, Vancouver. Proceedings… Available at: <http://dl.acm.org/citation.cfm?doid=2598510.2598541>. Accessed in: 30 abr. 2019.

Hoepman, J.H., 2014. Privacy Design Strategies. In: Cuppens-boulahia, N.; Cuppens, F.; Jajodia, S.; Abou El Kalam, A.; Sans, T. (Eds.). *ICT Systems Security and Privacy Protection:* SEC. Berlim: Springer,. pp. 446-459. Available at: <https://link.springer.com/chapter/10.1007/978-3-642-55415-5_38>. Accessed in: 30 abr. 2019.

Lacey, C.; Caudwell, C., 2019. Cuteness as a "Dark Pattern" in Home Robots. In: *Acm/Ieee International Conference On Human-robot Interaction,* Daegu-South Korea. Proceedings... Daegu-South Korea: IEEE. pp. 374-381. Available at: <https://ieeexplore.ieee.org/document/8673274/>. Accessed in: 30 abr. 2019.

Lemos, A. 2019a (in press). *Epistemologia da Comunicação, Neomaterialismo e Cultura Digital*.

Lemos, A., 2019b (in press). *Plataformas, dataficação e performatividade algorítmica (PDPA)*: Desafios atuais da cibercultura.

Lewis, C., 2014. *Irresistible Apps*. Berkeley: Apress.

Mathur, A.; Acar, G.; Friedman, M. J.; Lucherini, E.; Mayer, J.; Chetty, M.; Narayanan, A., 2019. Dark Patterns at Scale: *Findings from a Crawl of 11K Shopping Websites.* Proceedings ACM Human-Computer Interaction, v. 1. Available at: <https://arxiv.org/abs/1907.07032>. Accessed in: 18 Ago. 2019.

Mayer-Schonberger, V.; Cukier, K. 2013. *Big Data: A Revolution That Will Transform How We Live, Work, And Think*. Boston: Eamon Dolan/Houghton Mifflin Harcourt.

Nodder, C. 2013. *Evil by Design: Interaction Design to Lead Us into Temptation*. Indianapolis: John Wiley & Sons.

Patrick, A. S.; Kenny, S., 2003. From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interactions. In: Dingledine R. (Ed.). 2003. *Privacy Enhancing Technologies – Lecture Notes in Computer Science*. Heidelberg: Springer. pp. 107–124. Available at: <https://link.springer.com/chapter/10.1007/978-3-540-40956-4_8>. Accessed in: 30 abr. 2019.

Pearson, S.; Shen, Y., 2010. Context-aware Privacy Design Pattern Selection. *In: International Conference On Trust, Privacy And Security In Digital Business,* 7., 2010, Bilbao-Spain. Proceedings... Berlim/Heidelberg: Springer-Verlag. pp. 69-80. Available at: <http://dl.acm.org/citation.cfm?id=1894888.1894898>. Accessed in: 12 jul. 2018.

Ponciano, L.; Barbosa, P.; Brasileiro, F.; Brito, A.; Andrade, N., 2017. Designing For Pragmatists And Fundamentalists: Privacy Concerns And Attitudes On The Internet Of Things. *In: Brazilian Symposium On Human Factors In Computing Systems (IHC'17),* 16, Joinville. Proceedings... Available at: <http://arxiv.org/abs/1708.05905>. Accessed in: 12 jul. 2018.

Sadowski, J., 2019When data is capital: Datafication, accumulation, and extraction. Big Data & Society, v. 6, n. 1, p. 1-12, 2019.

Silveira, S. A., 2018. *Tudo sobre Tod@s: Redes digitais, privacidade e venda de dados pessoais.* São Paulo: Edições Sesc SP..

Srnicek, N., 2017. *Platform capitalism.* Cambridge: Polity Press.

Trice, M.; Potts, L., 2018. Building Dark Patterns into Platforms: How GamerGate Perturbed Twitter's User Experience In: *Present Tense. Present Tense: A Journal of Rhetoric in Society,* v. 6, n. 3, p. 1. Available at: <https://www.presenttensejournal.org/volume-6/building-dark-patterns-into-platforms-how-gamergate-perturbed-twitters-user-experience/>. Accessed in: 12 jul. 2018.

Van Dijck, J.; Poell, T.; De Waal, M., 2018. *The Platform Society.* Nova iorque: Oxford University Press.

Williams, M.; Nurse, J. R. C.; Creese, S., 2016. The perfect storm: The privacy paradox and the Internet-of-things. In: *International Conference On Availability, Reliability And Security,* 11, 2016, Salzburg-Áustria. Proceedings... Available at: <https://ieeexplore.ieee.org/document/7784629>. Accessed in: 12 jul. 2018.

Zagal, J. P.; Björk, S.; Lewis, C., 2013. Dark Patterns in the Design of Games. In: FDG 2013 - International Conference On The Foundations Of Digital Games, 8, Chania-Grécia. Proceedings… Available at: <http://www.fdg2013.org/program/papers.html>. Acessed in: 12 jul. 2018.

ZUuboff, S., 2015. Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, v. 30, n. 1, pp. 75-89.

---

1 Available at youtube.com/watch?v=zaubGV2OG5U

2 The use of design patterns to create a universal language for architecture was postulated by the architect Christopher Alexander (1977). As his work became more widely known, it inspired similar efforts in other fields, such as software engineering and interaction design.

3 Disponível em: ft.com/content/e24dea0a-6b57-11e9-80c7-60ee53e6681d.

4 Available at gizmodo.com/senators-introduce-bill-to-stop-dark-patterns-huge-plat-1833929276.

5 Available at nytimes.com/2016/05/15/technology/personaltech/when-websites-wont-take-no-for-an-answer.html.

6 Available at theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you.

7 Available at https://www.darkpatterns.org/types-of-dark-pattern.

8 Acronym for the Big Five: Google, Amazon, Facebook, Apple and Microsoft.

9 Available at https://bikeitau.com.br/bikesalvador/politica-de-privacidade/.

10 The screenshots were manually captured and imported into the software. There is no isonomy in the number of screenshots of each app. Subsequently, focused coding was conducted to identify the MIs. Not all MIs described in literature concern privacy issues; therefore, not all of them appear in the corpus.

11 A partnership between Salvador City Hall and Itaú bank. Users can take advantage of 400 bicycles at 50 stations. The Bike Itaú app is a mediator that allows people to pay for the service (with daily, monthly or annual plans), locate the nearest station and borrow a bicycle.

12 Examples can be found in various sources, such as Brignull's official site (darkpatterns.org/hall-of-shame), the Dark Pattern project Twitter feed (twitter.com/darkpatterns), a community set up by researchers (dark.privacypatterns.eu), and Reddit communities dedicated to the subject (reddit.com/r/darkpatterns/) (reddit.com/r/assholedesign/). Several other articles have helped to expand the catalog of MIs, such as Bosch et al. (2016) and Gray et al. (2018).

13 This is confirmed by recent studies. Arunesh Mathur et al. (2019) showed that MIs were present in 11.1% of approximately 11,000 online shopping sites they analyzed. Their analysis revealed the existence of online services for implementing MIs in shopping sites in the form of plugins and add-ons. These services are advertised openly as a way of boosting sales.

14 Interaction strategies that make it difficult for consumers to compare prices. Although they are more common in e-commerce, we found Price Comparison Prevention patterns in the apps in the corpus in this study which sell service packages.

15The user is prevented from cancelling the service he has signed up for or cancelling his account in a particular app or website. Companies tend to put obstacles in the user's way so that he keeps his data linked to the platform.

16 The aim of this MI is to divert the user's attention from aspects of the interface that the company does not want him to see or to direct his gaze or efforts toward a particular task in the sequence of actions he is required to perform.