Article

SM+S
social media + society

Social Media + Society
July-September 2018: 1–16

DOI: 10.1177/2056305118795876
journals.sagepub.com/home/sms
SAGE

Affordance is Power: Contradictions Between Communicational and Technical Dimensions of WhatsApp's End-to-End Encryption

Marcelo Santos and Antoine Faure

Abstract

WhatsApp's implementation of end-to-end encryption has been celebrated by many. Intriguingly, though, the invisible affordance was made visible with an individual message to each conversation. In this research, we "properly scrutinize" the roll-out of the affordance in historical perspective inspired by the "platform biography" approach, critically comparing corporate and media documentation with an analysis of the attributes and affordances that refer to the realm of privacy and security with focus on the end-to-end encryption. After pointing the contradictions with evidences found, we conclude that the implementation should be interpreted neither as a plain idealistic saga for user privacy and security by the App's founders nor as simply a market-oriented approach—though both are clearly components of the company's motives—but as a strategic move inserted in a: (1) Public Relations guerrilla strategy from WhatsApp Inc. facing national States and respective intelligence agencies or law enforcement institutions, in which context the development and implementation of affordances reveals a (2) power move by corporate digital media to avoid political conflict against vigilante state power and therefore the App's subsistent vulnerabilities in terms of privacy and security should be read as (3) a tradeoff between commercial massiveness at the expense of technological utopia.

Keywords

social media, encryption, WhatsApp, privacy, affordances, platform biography.

Context

December 17, 2015, at 0:00, Brazilians were blocked out of WhatsApp. Motivated by the non-compliance of the company with a request to share messages from and to a criminal offender under investigation, a judge ordered all the national Internet Service Provider (ISPs) to interrupt the interchange of information with WhatsApp for 48 hr.[1] The result was a national blackout[2] that lasted about 12–13 hr during which approximately 1 million users of the App (10% of the App's users at the time) had no access to it, until the company's lawyers were able to overrun the prior decision. The center of the dispute was Brazilian's government persistence in soliciting the content of conversations between suspects involved in some high profile judicial case under investigation. The company held and still holds a technical position ensuring that it was impossible to deliver information, as Jan Koum (one of the cofounders) said himself during an interview prior to this episode: "There really is no key to give [to the NSA] [. . .] We don't save any messages on our servers, we don't store your chat history. They're all on your phone" (Rowan, 2014, par 15).

One way or another, the debate is ongoing in Brazil (Supremo Tribunal Federal do Brasil (STF), 2017) and several other attempts have been made to block once again the service. In total, three blockages were successful, enduring for different durations, the longest being 24 hr in 2016 (Abreu, 2017).[3] A few months after the first successful block in December 2015, and its respective controversy, WhatsApp finished the roll out of a new affordance that definitively operationalizes the technical impossibility to disclose information of users' conversations: end-to-end encryption (for all messages and all media). But one thing about this implementation

Universidad Finis Terrae, Chile

Corresponding Author:
Marcelo Santos, Universidad Finis Terrae, Pedro de Valdivia, 1646 Providencia, Santiago, RM, Chile.
Email: msantos@uft.cl

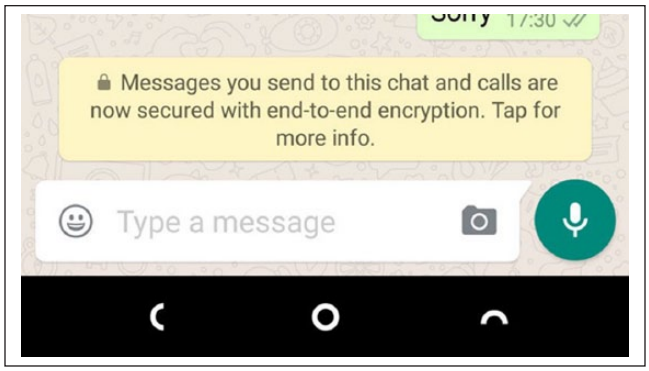


Figure 1. Message communicating implementation of end-to-end encryption on WhatsApp (Techadvisor.co.uk).

seemed outstanding: WhatsApp sent a message to both users engaged in a conversation, warning them that the conversation was encrypted (see Figure 1), though obviously the majority of the users do not understand well that meaning. So a few questions emerge: what exactly are the intentions behind such system message? Why make visible an invisible affordance such as encryption? Why should it matter to the mass of the App's users such information, besides the more tech-savvy users that are actually worried about the issue? Why focus so much on this decision when the defensive tactic of WhatsApp argued the nonexistence of stored data in first place? Following Dencik and Leistert (2015) we set out to "properly scrutinize" this story, looking precisely at what the affordances related to security and privacy enable and/or constrain, how have been the communication around this implementation and how both relate to each other.

This research is, therefore, placed within the critical Internet studies perspective, which "always situate such [empirical] analyses in theorizing and analyzing larger contexts, such as power structures, the state, capitalism, gender relations, social struggles, and ideologies, which shape and are shaped by the digital media landscape in dialectical processes" (Trottier & Fuchs, 2015, p. 3). In that sense, we will demonstrate how contradictions emerge over time as to how WhatsApp is self-represented regarding the issues of privacy and security and how other sources of evidence recollected by this research contradict public statements by WhatsApp Inc. or its spokespersons, leading us to conclude for the prevalence of commercial interest over idealist drivers. Furthermore, we will show how the development of affordances may be interpreted as a power move by WhatsApp to avoid conflict with national states as they translate strategic decisions of the former into code, putting the App in a situation of impossibility to collaborate, at the same time that a communicative dimension of the affordance serves as a tool to raise awareness on the users, as a means of co-opting them as constituents in case of political conflicts.

To do so, we will first contextualize how those issues emerge, and then explore the concept of affordances and how they relate to power struggles. After that, we explain the method used, how we gathered evidence to support a plausible explanation. Then we analyze the evidence around the issues of privacy and security under two dimensions: communicational (self-presentations of the company, tech media reviews and interviews that refer to the issue or the absence of references) and affordances (evidences based on expert reviews of the encryption affordance and App navigation by the authors). In the final section, we synthesize the conclusions.

Privacy and Security on Information and Communications Technology

One of the main contemporary issues in the realm of digital life, in particular in the aftermath of the Cambridge Analytica Facebook data breach scandal (Cadwalladr & Graham-Harrison, 2018), regards privacy and security. Those two intertwined issues refer to the way vigilance possibilities have irradiated through digital life via complementary fragments of distributed hard drives and the individualization of the Apps. It seems that digital life fits with control society as pictured by the French Philosopher Gilles Deleuze, "giving the position of any element within an open environment at any given instant [. . .] and tracks each person's position—licit or illicit—and effects a universal modulation" (Deleuze, 1992, p. 7). In other words, digital life operates control as a modulation, "like a self-deforming cast that will continuously change from one moment to the other" (Deleuze, 1992, p. 4). And to activate this control, it works through codes and passwords that encrypt or decrypt information.

Walking hand-to-hand with economic liberalism, the ideals of data privacy have been opportunistically framed within individualistic values, and frequently get mixed-up with free speech and other rights arguably identified with democratic values, such as market freedom or private property. On one side, the separation between public and private spheres is reaffirmed as an ideal from which corporations must protect individual rights of privacy and security, as a modulation of liberty enforced by digital media corporations, as a sort of outsourcing by the State (Hintz, 2015). On the other side, as privacy and security within the digital realm become issues of public interest, they concomitantly become an attractive marketing idea, hindering its usefulness as a source of profit in the form of data banks. Digital technology giants have incorporated a storytelling about the guarantee they offer to each consumer that their data are protected. And they use this argument to sell their product in a context of generalized competition (technologies, applications, platforms, etc.).

Nonetheless, the privacy and security issue has gathered lots of nuances, though, especially after Edward Snowden's revelations during 2013, leaking espionage (mal)practices by government agencies with the collaboration of corporations such as Microsoft, Apple, Google, Verizon, and others

(Greenwald, 2013; Greenwald & MacAskill, 2013; Scriberia, Kiss, Boyd, & Ball, 2013). In the aftermath of those revelations, Snowden made a clear recommendation presenting Signal as the paradigmatic secure chat application (Cimpanu, 2015).

Since then, mistrust is a must when it comes to analyzing marketing discursive strategies that sell the idea of any private-owned, for-profit, self-designated custodian of privacy in the digital media realm. As a similar example to WhatsApp's case of study, Hintz criticizes the growing autonomy with which private social media companies have been regulating its content (such as censorship of nudity on Facebook or copyrighted content on YouTube) and users (such as Amazon's active banning of Wikileaks from their services), which are not at all a-political decisions: "the state outsources interventions into citizens' communication to these platforms" (Hintz, 2015, p. 110). Such decisions help shape culture and constrain civil political action, possibly leading to power struggles behind WhatsApp's end-to-end encryption implementation on its messaging service, as we will see.

Affordances and Power

Affordances

To analyze the implementation of WhatsApp's end-to-end encryption, we will use affordances theory to elucidate options that otherwise could seem unmotivated, as is the case with making visible the implementation of the encryption. Furthermore, we can evaluate the possibilities and constraints that the end-to-end encryption offers to both company and App's users, as well as considering the gap between the technology communicational framing when confronted with the heuristic analysis (expert navigation) and specialized expert opinion over this improvement. In what follows, we will first discuss the way we will use this concept and then unveil its political dimension, which is the key to our gaze on WhatsApp implementation of end-to-end encryption.

Affordances are a particularly interesting approach to enquire technologies' possibilities in a digital environment. As Tenenboim-Weinblatt and Neiger (2018) have shown, the concept offers various advantages, between macro and micro level, to understand new forms of media, space-oriented networks and its ecological conditions. It serves to reduce complexity, and that is precisely what we pursue in this paper: how one particular affordance, the end-to-end encryption, enables WhatsApp to cope with the complexity of a privacy and security issue, not only limited to its users' experience, but also to its broader, political dimension? Furthermore, what is the meaning of the way it was implemented?

Following Langlois (2014), "both the practices of meaning making and the substance of meaning are material and technological first and foremost, and the technological and material context determines what constitute meaningfulness and meaninglessness" (p. 9). Affordances, in this sense, produce meaning and meaningfulness in two ways: first by "setting up the conditions within which meaningfulness and meaninglessness appear" (Langlois, 2014, p. 11) but also, even more subtly than the affordance as the constraints and potentials for communication and meaning-making within the software realm, through the process of implementation of a new affordance, which may even entail, as we will see, political implications, beyond its functionalities per se.

According to J. J. Gibson (1977, cited by Norman, 1999), to whom the term has been attributed, affordances are relationships that come as result of "actionable properties between the world and an actor (a person or an animal)" (p. 39). In other words, the properties of an environment open possibilities that are relative to each organism:

> The affordance of something does not change as the need of the observer changes. The observer may or may not perceive or attend to the affordance, according to his needs, but the affordance, being invariant, is always there to be perceived. (Gibson, 1986, p. 139)

Norman (1999) applied the concept to mechanical and electronic interfaces, thus dividing the concept into three different stages: (1) perceived affordances, (2) system feedback, and (3) affordances themselves. The first refers to visual cues (or sensorial cues to be more precise) that indicate that an affordance lies behind a button, an image, a gesture, a voice command. Such cues are a fundamental part of information and communications technology's (ICT's) design for they rely mostly on basic standard mechanic affordances (such as the single button of the iPhone, the keyboard-mouse-pointer navigation system on a desktop computer, and so on). So, to identify an affordance in the designed system, the user must have clues that lead him to push the button, swipe the finger, and so on. The absence of cues could lead to the user not realizing the affordance is there in the first place, even if the affordance, as Gibson (1986) states, is "invariant," is "always there to be perceived." The second element, feedback, refers to the signs that denounce the operation of the affordance, such as moving icons that indicate the system is searching or loading. Finally, the affordances are the functions themselves, that may or may not be accompanied by one or both the other elements. In fact: "the affordances, the feedback, and the perceived affordances can all be manipulated independently of one another" (Norman, 1999, p. 40).

Hutchby (2001) developed an affordances framework to analyze technologies between two traditions: determinism and constructivism. According to the author, affordances address the possibilities and constraints that materiality of every object offers with his own characteristics. Therefore, as medium theory (Meyrowitz, 1994) and materialities approach (Lévrier & Wrona, 2013) underscore, the affordances condition the uses

of social forces. In consequence, the political dimension of affordances refers to a sort of *framing* (Lakoff, 2008), that is, an action that constrains and enables, beyond its uses, also its interpretations. That is one of the crossroads of affordances theory with the communication field: framing may be interpreted as a mechanism of indirect persuasion corresponding to the way a message (or, in the present case, an affordance) is displayed and/or introduced.

Power

How do affordances, politics and power relate? We suggest that this power problematics expands beyond the discourse, incorporating precisely its technological components and their transformation, as affordances theory establishes. As Gillespie (2010) stated in his analysis of the role of digital technologies in contemporary life, neutrality discourse underlying platforms and apps elide "the tensions inherent in their service" (p. 348). In other words, part of the power struggles is played through the representation strategies of the technologies themselves, what appeals to platforms' projected images. Nevertheless, technology is not only the support of a discourse; it is also the discourse of the support (Lévrier & Wrona, 2013, p. 7).

As a matter of fact, literature has shown how every algorithm or interface characteristics is necessarily discursive and potentially political, as wrote Da Silveira (2014): "current technological disputes are becoming each day more of political disputes" (p. 28, our translation). If, since Ellul (1964), technological neutrality is no longer acceptable, and the understanding of power is what is in dispute, we can find complex definitions of technologies' politics, in this case platforms or apps.

Within the realm of platforms, users and power, agency is one of the complex questions. As ordinary users create the content that travels through most of those platforms, they become perhaps the most visible agents of what seems, on the surface, to be a neutral ground called "platform" (Gillespie, 2010). But they are not the only agents and most definitely not the most powerful: "Platform owners and app developers are producing agents and social forces; they can exercise economic and political power to change or sustain existing hierarchies and deploy their technologies to do so" (Van Dijck, 2013, p. 18). Actor-Network Theory helps situating non-human actors within platform's agency, as Langlois' (2014) definition of software, which implies its communicative role:

> a new kind of communicational actor, as an entity that produces meanings and meaningfulness, an entity that interacts with us. Embedded in these interactions [. . .] is often the specific interest of social media platforms, in particular for-profit ones. (p. 52)

In this view, power is not seen as an abstract thing that overhang digital life, but a socio-technological hegemony that affects political, economical and cultural authority's distribution in societies, with struggles that permeate from the offline to the online borders and vice-versa. In this article, we put economic power aside, despite its relevance, and focus on the political power of affordances using WhatsApp encryption as a case study.

We agree with Van Dijck (2009), that in face of such complexity, "a multidisciplinary approach to user agency should yield a model that accounts for users' multiple roles, while '*concurrently accounting for technologies and site operators-owners as actors who steer user agency*" (p. 55, our emphasis). Therefore, we propose to study platforms and apps not only from a top-bottom approach, but to consider its inner essence, as revealed by a due analysis of its affordances' evolution. On this basis, every affordance of a platform or an application must be situated in the moment of its political analysis for its study, so as to open the conclusion to esthetic, material, practical and discursive aspects that frame the perception of the apps' users, its imaginary and appropriation of these information technologies:

> The private platform might have antagonistic relationship with any single state, especially if it operates in a separate jurisdiction. Yet the more likely pattern is based on cooperation between private social media and the state [. . .] The best example of this phenomenon is that social media companies benefit from commodifying personal data by selling targeting advertisements, and that the NSA and GSCHQ-operated global PRISM Internet surveillance system enables the state to access the very same data collected and processed by companies such as Facebook, Google, Apple, AOL, Microsoft, Yahoo, Skype or Paltalk for the purpose of control. (Trottier & Fuchs, 2015, p. 23)

Consequently, social media refer to what the same researchers call "a corporate-state-power phenomenon, a force field in itself" (Trottier & Fuchs, 2015, p. 34). This perspective remains instrumental to see through the present analysis, as it considers this field as a surveillance-industrial complex in which users themselves collaborate to the practices of vigilance and the discourse of privacy and security.

Method

The method for this study is rooted on Burgess and Baym's (2016) Platform Biography, a systematic but also serendipitous approach to the analysis of digital platforms that uses a variety of secondary sources to circumscribe a platform's evolution as a means to "make sense of their complexity and the way they change over time" (Burgess & Baym, 2017). As the authors further explain,

> the term "biography" is chosen deliberately to invoke both the historical and the social aspects of how things are created, how they are used, and what they mean, while recognizing that, as with all biographies, the account is inevitably partial. (Burgess & Baym, 2016, p. 10)

This method vows that "the distinctive cultures of social media platforms owe much to the particularity of their key sociotechnical objects" (Burgess & Baym, 2016, p. 9). Examples would be "like" buttons on Facebook, Instagram filters or hashtag, retweet and reply buttons on Twitter -this latter the objects selected by the authors to perform a *Twitter Biography*. Through the lens of one or multiple key affordances, the authors defend the need for

> multiple data sources that allow researchers to get at many intertwined levels that together comprise their meaning and show how innovation happens over time. These levels include the material affordances of the site and its third-party clients, the media ecosystem within which the site operates, the company's changing and sometimes competing business models, and the experiences of users embedded in social practices of which the platform is only a part. (Burgess & Baym, 2016, p. 9)

The present research, though, does not intend to analyze the entirety of WhatsApp as a platform, but explore a plausible explanation for the visibilization of end-to-end encryption roll out in April, 2016. It is a fundamental affordance in the sense that it is decisively embedded in contemporary debates over the political dimension of privacy and security such as the recent clashes between encrypted chat Apps and governments that demand access to information, as has happened with WhatsApp in Brazil (2015, 2016), Iran (2014) and has been happening currently with its simile Telegram (Iran and Russia at the moment of the writing). Its scrutinization allows for the emergence of a series of contradictions that will be explored in the course of the next chapter.

To understand such implementation and the process around it, we have searched for the historical and social aspects of its creation and meanings. Our strategy was to compare self-representations and media presentations of the App with its affordances regarding questions of privacy and security to pursue explanations as to why encryption was made visible. Our sources, thus, are not strictly systematic as we mobilize "multiple data sources" (Burgess & Baym, 2016, p. 9) to distinguish the political dimension of a technological affordance and relate it to its media ecosystem and the strategies of the company.[4]

This method allows, then, to confront and contrast communicational discourse around the technology against technical analysis, either by the authors (Apps' exploration) or via secondary sources (experts on privacy and security), explained as follows.

Communication Perspective

The objectives of the communication perspective are as follows: (1) to compare the prevailing company values, as documented by the company and/or the other sources *prior to* and *after* the implementation of the encryption affordance and (2) to establish a point of comparison with Signal, the most emblematic chat App regarding security and privacy, as a strategy to make the discursive gaps visible. Have the company consistently been building its image upon the values of security and privacy? Taking Signal as the epitome of a secure, private chat App, how do WhatsApp's discourses relate to Signal's?

To achieve that, different sources of evidence were used. All of them were analyzed searching for communicational elements that build (1) self-representation and (2) media representation through elements that refer to issues of privacy and security. Within those criteria, the sources were the following:[5]

- Internet Archive: We systematically mapped the historical changes in WhatsApp's and Signal's websites, especially the home-page for the Apps and other pages with self-representation texts or images, such as "About us" and its variations, searching for values related to privacy and security;
- WhatsApp's Blog;
- Media interviews with founders and other representatives;
- Social Media comments from key WhatsApp managers (such as Zuckerberg's Facebook profile);
- Specialized media pieces on WhatsApp and/or its founders.

Affordances Perspective

The objectives of the affordances perspective are as follows: (a) to explore comparatively the App's affordances that relate to privacy and security with affordances from other similar Apps Signal, Telegram and Facebook Messenger and (b) to evaluate the validity of the encryption implementation as it has been scrutinized by privacy and security experts.

From the affordances perspective we set out to gather evidences of what is behind the words circulating around the image of WhatsApp's privacy and security values, and specifically its end-to-end encryption, that is, how the discourse materializes into affordances -or does not. To do so, the following sources were used, as done by the media materialities analysis:[6]

- App Navigation, centered on the specific affordances related to aspects of privacy and security, in WhatsApp. This includes affordances such as, but not limited to: encrypting services, secret messaging, screenshots, backup practices, web browser version;
- App Navigation, also centered on the specific affordances related to aspects of privacy and security in similar Chat Apps Facebook Messenger, Telegram and Signal, as a means to build a comparative perspective;
- Expert opinions via specialized media articles, personal blogs or organizational websites, with a remarkable role for Electronic Frontier Foundation (EFF),

> recognized world leading experts in privacy and security.

The results will also be presented as *Communicational* and *Technological* perspectives in the next section. But to start with the biographical approach of the App, it seems indispensable to build a quick history of WhatsApp.

Biographical Approach of WhatsApp End-to-End Encryption

In this section, we will first present some background on WhatsApp's history, then confront communicational and technological perspectives to understand the power struggles behind WhatsApp's end-to-end encryption implementation on its messaging service.

WhatsApp

WhatsApp is a messaging service founded in 2009 by two former Yahoo employees: the original idea came from Ukrainian Jan Koum, who left his country in his late adolescence. His ex-colleague from Yahoo Brian Acton joined the enterprise a few months after the first steps. Its initial success seems to be related to Jan Koum's envisioning of how new iPhone's affordances could play in favor of the App: the possibility of Apps to operate OTT (Over The Top), first available on the iPhone.[7] So what was originally a "status update" App, started to take the current form of text-messaging and Voice/Video over IP software functioning on top of the Internet and ISPs infrastructure.

In December 2009, the App launched one of its main functionalities: photo sending. As a direct consequence, WhatsApp website started to present the App as a MMS-like, focusing also on its freeness, unrestricted data traffic (as long as connected to a Wi-Fi service) and interoperability, which would be extended to Blackberry in June 2010 and incorporated gradually to Android and Nokia Symbian. The self-presentation discourse is more technical, but couldn't be farther from presenting the App as a guarantee of the users' privacy. On April 4, 2010, the webpage included this definition:

> WhatsApp Messenger is a smartphone messaging app which allows you to exchange messages with your friends and contacts without having to pay for SMS. WhatsApp Messenger is cross platform [. . .] To send and receive messages, WhatsApp utilizes your existing smartphone internet data plan.[8] (WhatsApp webpage as per Web Archive)

As we will show in what follows, despite a recent effort of the company owners to explicitly define the company as a guardian of free speech, a "connector of the world" (Zuckerberg, 2015) and despite also the history of concern with issues of privacy by one of its founders (Koum & Acton, 2016; Rowan, 2014), in the context of the launch of end-to-end encryption affordance, we found that, though security is one concern and perhaps even a core value, it competes with other issues when it comes to making business and strategic decisions, generating contradictory signs.

The first notorious attempt to block the App by a State was an Iranian reaction 2 months after the acquisition by Facebook (February 19, 2014). Authorities accused Zuckerberg of being an "American Zionist" (Daftari, 2014). In face of internal tensions and conflicts, the government of Iran itself retracted from the blockage so the company did not need to react directly. Nevertheless, with around 1 billion active users by the end of 2015, Brazil's blockage of WhatsApp, previously discussed, seems to have been more decisive to understand its technical and marketing discourse, as users become more interested in alternative Apps, such as Telegram. Graph 1 below displays the synchronicity between peaks on searches for WhatsApp Blockage ("Bloqueio WhatsApp" in Portuguese) and Telegram.

Communicational Perspective

Self-Representations. By comparing communicational strategies of WhatsApp and Signal—the paradigmatic secure App recommended by Edward Snowden—we expect to make explicit the contradictions on WhatsApp's recent discourse of security and privacy.

Signal was the result of the merger of two previously existing communication applications, called RedPhone and TextSecure, all developed by Open Whisper Systems. While the names already say a lot, the logo of the App is clearly centered on the idea of secrecy, or, better yet, protected conversation (see Figure 2).

The current websites[9] of both Signal and WhatsApp look surprisingly similar (Figures 5 and 6). If we consider that WhatsApp hired Open Whisper Systems to implement the

Figure 2. Signal App's logo emphasizing privacy/security issues in the center of its design (Source: Softpedia.com).

same end-to-end encryption model as Signal's, it could mean WhatsApp is trying to adhere to the values incorporated by Signal through visually and functionally mimicking its prior competitor. That's branding, perhaps. But Signal's welcoming page of the App is straightforward: "Privacy is possible. Signal makes it easy" (Figure 2). Through a biographical approach, if we take a historical and critical look at the discursive strategy behind the App Signal, it becomes evident how they demonstrated that preoccupation with privacy and security in the software's genesis—something that is not visible in WhatsApp's history. Website, marketing tagline, logo, names, all reinforce Signal's idea of working to

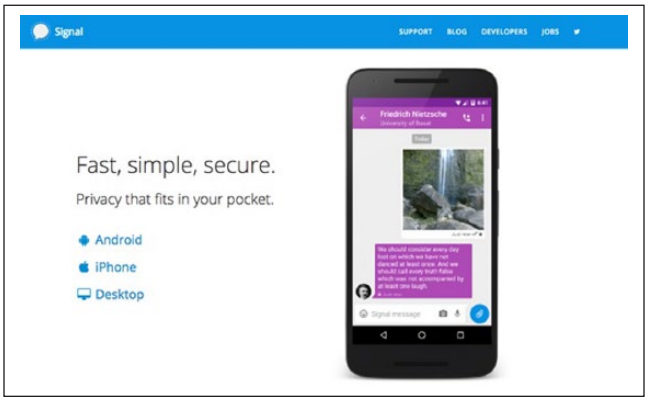


Figure 5. Screenshot from Signal's webpage November 16, 2017.

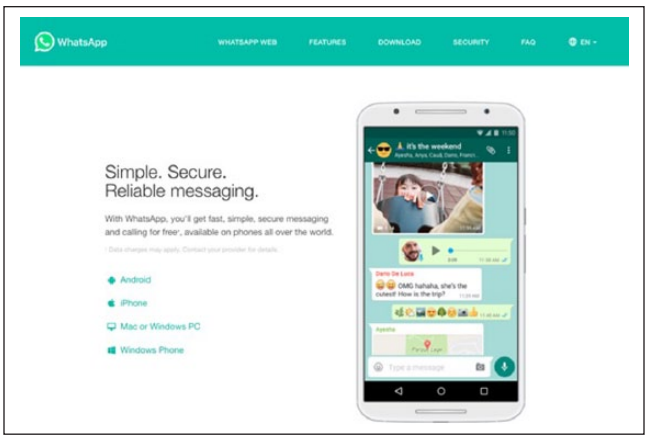
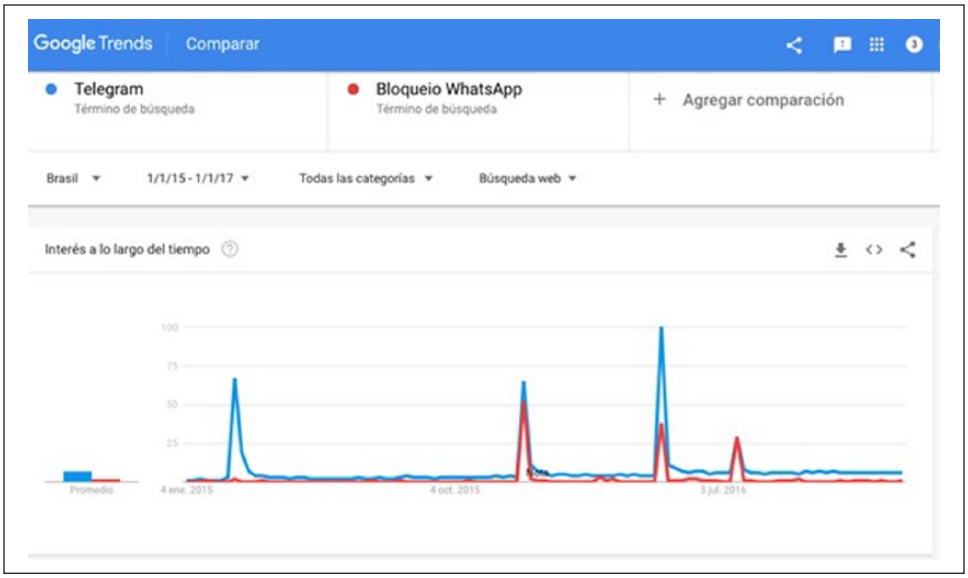


Figure 6. WhatsApp and Signal's webpages look surprisingly like each other at the time of the research (www.whatsapp.com, retrieved on November 16, 2017).



Graph 1. An analysis of search trends on Google depicts how interest on Telegram (upper blue line) goes hand in hand with the dates of the three WhatsApp blockages in Brazil (lower red line).

Table 1. WhatsApp's self-presentation over time as per its website (adapted from screenshots obtained at Archive.org).

Date	Self-Presentation	Interpretation
2009	"WhatsApp is a smarter Address Book for your Smartphone"	Idea of status update
2010	"WhatsApp is a smartphone to smartphone messenger/chat application"	Interoperability and chat service
Early 2011	"Fast. Personal. Awesome"	Technological efficiency, cultural and epochal values.
Late 2011	"Awesome. Cross-platform. Now with group chat"	Improvement of the technical affordances.
2012	Simple. Personal. Real-Time Messaging"	Accessibility, individuality and velocity.

maintain the privacy of the message interchanged in the provided service. In 2015, the website's tagline pointed to the core field of action of the organization Open Whisper Systems: "Security, Simplified. Open source security for mobile devices." In 2016, the corporate page was still up and the tagline was updated to "Privacy that fits in your pocket," a double meaning that holds together mobile with privacy, besides the pun regarding price (Figure 5).

WhatsApp's website, on the other hand, does not present a history of concern with security or privacy. As it can be assessed with the biographical evidence from the apps homepage, the company's *cuore* seems to rest on other values—at least in terms of self-presentation (see Table 1).

Finally, between 2013 and 2015, changes were very subtle, and focused on the visual aspects rather than text, which shows us how the company frames privacy and security as secondary values. The end result is that over the years, both the visual aspect and the taglines that define the product are reasonably stable and build WhatsApp's institutional communication, regardless of some permutation between terms used as the main attractions of the application: Simple, personal, Real-time, reliable, cross-platform, free, fast, awesome. Except for "Personal," neither of those terms is directly or indirectly related to security or privacy concerns. Nevertheless, "Personal" hinders an ambiguity as to whether the attribute relates to the fact that the App is embedded on a personal device or to the protection of data due to intimacy issues. We're inclined to vow for the former, supported also by the motivations behind the enterprise, declared on WhatsApp website, as Figure 3 below displays. It references a much more techno-optimistic view than an ethical pursuit for privacy and security. Our question's relevance grows: what has pushed WhatsApp to not only implement end-to-end encryption but to communicate it? (Figure 4 to 6).

Media Representation. Specialized press seems to understand that privacy is indeed an important issue to WhatsApp, at least, prior to the acquisition by Facebook in 2014. The founders have been called "devout privacy advocates" (Statt, 2018, par 5) and "big believers in privacy" (Dwoskin, 2018). The sharing of data with Facebook represents, for TechAdvisor's Henry Burrell (2017) "a small but significant sign that the Facebook-owned WhatsApp is having to concede some of its privacy values" (par 42). The same author defends that the company has installed end-to-end encryption "because as a company they believe in your right to have private conversations when you use their service" (Burrell, 2017, par 33). That story points to a previous preoccupation with privacy and security and is also backed by the typical American dream story of the land of freedom and opportunities that welcomes young oppressed Ukrainian Jan Koum, another self-made man in the democratic paradise. Curiously, on the same week that Facebook announced the acquisition (February 14, 2014), Wired magazine published a piece with important statements from Jan Koum, such as that "People need to differentiate us from companies like Yahoo! and Facebook that collect your data and have it sitting on their servers" (cited by Rowan, 2014, par 15). On the same piece there's

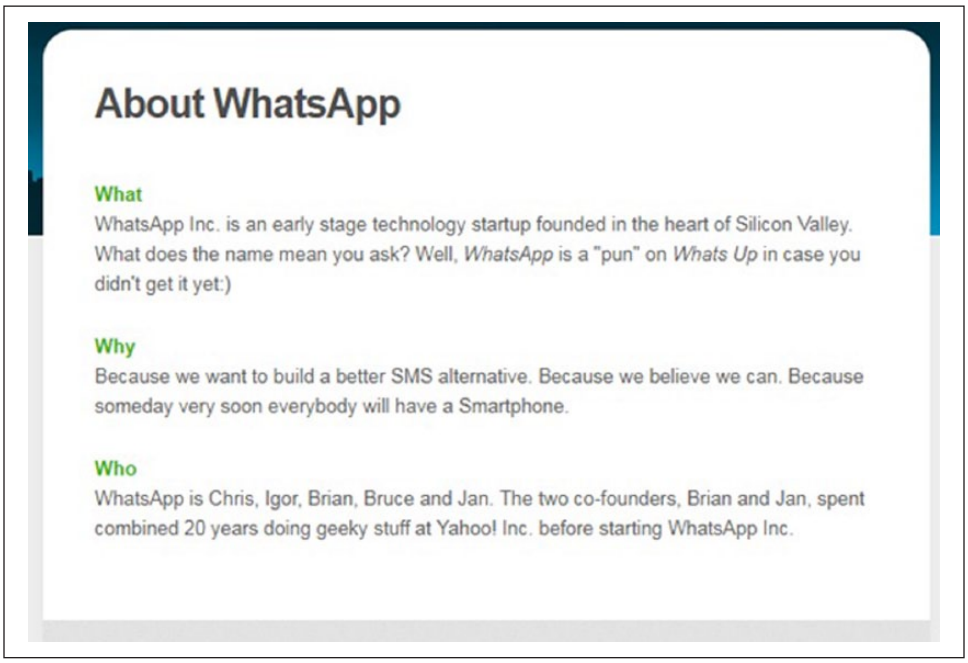


Figure 3. 2009 WhatsApp Screenshot displays the first "About Us" page. On section "Why" we see that motivations don't include security and privacy issues, but rather the idea of massiveness, popularity (Source: Archive.org).

Figure 4. Brian Acton's message on the aftermath of the Cambridge Analytica exposé (Source: Twitter).

another statement that could very well reflect the inspiration for the encryption initiative:

> [Koum] had just three rules as he experimented with the early iterations: his service would defiantly not carry advertising [. . .]; *it would not store messages and thus imperil individual citizens' privacy*; and it would maintain a relentless focus on delivering a gimmickless, reliable, friction-free user experience. (Rowan, 2014, par 3, our emphasis)

Whether Facebook should take all the blame for deviations in WhatsApp's user privacy realm it is a story to be informed further on, but Koum's recent departure from Facebook (Statt, 2018) apparently motivated by disagreements related to privacy issues (Dwoskin, 2018) and Acton's notorious remark after Cambridge Analytica scandal are symptomatic (Figure 4).

On the launch of the encryption affordance, the founders stated "WhatsApp has always prioritized making your data and communication as secure as possible" (Koum & Acton, 2016, par 1), referring retrospectively to the kind of principle or statement as those aforementioned by Koum. We can say, though, that behind such pretense appearance –or a real former intent- of privacy super-heroes, there are sufficient signs nowadays that suggest the prominence of other priorities that should follow a more pragmatic commercial approach. One evidence is that just a few months after the encryption roll-out, WhatsApp announced, behind what seemed as an innocent Terms of Service and Privacy Policy update (WhatsApp Inc., 2016), the sharing of information of WhatsApp with Facebook (Budington & Gebhart, 2016). The "small but significant" concession was put to work when the company privileged "gimmickless, reliable, friction-free user experience" at the cost of citizens' privacy and not the other way around.

Summing it up, though the free-America-against-repressive-communists' tale seem to corroborate the privacy-security prioritization, and specialized media vow for the founders' real commitment with privacy and security linked to liberty, the company's historical self-representations seem to show otherwise; or to the least, other higher priorities on the list. So, from a communicational perspective, as demonstrated in the history of the App's website, there are no signs whatsoever of a top priority regarding security or privacy prior to the launch of the end-to-end encryption -which happened a couple of years after Facebook's acquisition.

Affordance Perspective

While previous section examined the communicational contradictions as materialized on self-representations and media representations, the present section will demonstrate the contradictions evidenced by WhatsApp's affordances or affordance-related aspects (such as default configurations, accessory software and so on) on the privacy and security realm.

Public Relations Guerrilla. On April 5, 2016 WhatsApp's founders announced in the company's official blog: "Today more than a billion people are using WhatsApp to stay in touch with their friends and family all over the world. And now, every single one of those people can talk freely and securely on WhatsApp" (Koum & Acton, 2016, par 8). That was the end of a long roll-out process with probably no matching encryption project with such a scale: more than one billion people[10] were benefited with the new affordance. Such affordance is supposed to be technically "invisible," for it does not change perceptively the user experience: following Norman (1999) it has no *perceived affordance* neither *feedback*, unless the user finds himself under a security or privacy threat—such as governmental agencies pressure, criminal prosecution, or a lost or stolen mobile device. So, why would WhatsApp Inc. put an effort to make it visible *in the App* when it rolled out (see Figure 1)? This question resonates even more if we consider that the parent company's equivalent Facebook Messenger also installed the same protocol on October the same year (Greenberg, 2016), but (1) it is not set by default and (2) was hardly marketed, at least not even close to how WhatsApp encryption was. More importantly, on Facebook Messenger, the invisible affordance was not accompanied by cues that turned it visible.

Affordances are hard evidence that reflect what's underneath corporate speech: it is very unlikely that such a move to develop a very costly, complex, sophisticated affordance would be just about marketing. WhatsApp was acquired not long after Snowden's leaks and the encrypting project started right after the acquisition (Brandom, 2014) in what seems to have been impelled by the App founders (Dwoskin, 2018). Besides, Facebook has had its share of privacy violation accusations and have learned from the pain it causes to the company's reputation sharing information with governments or other third parties, such as the emblematic Cambridge Analytica scandal (Cadwalladr & Graham-Harrison, 2018). Other less mediatic law troubles were a € 110 million fine by European Commission in 2017 due to misleading information about WhatsApp takeover (European Commission, 2017), a similar case as Italy's antitrust agency € 3 million fine directed at WhatsApp for supposedly obliging users to share their information with Facebook (Reuters, 2017) and a

Figure 7. Zuckerberg's post after WhatsApp blockage in Brazil (Facebook personal page, December, 17, 2015).

class action lawsuit filed by a 26-year-old activist law student that Facebook lost (Garside, 2014). Users' dissatisfaction after acknowledging the leaks is no secret, so it seems encryption could be a strategic move into avoiding such conflicts in a creative legal-technical way.

Therefore, the media and blog announcements and the effort to make encryption affordance visible could be interpreted as an intent to project an image of privacy and security to the regular users who might be considering changing to competition Apps—such as Signal or Telegram (see Graph 1)—because of such affordances. And there's a clear framing in the freedom vs. control debate, as the founders' declaration on their blog articulate. Nevertheless, such decision encapsulates also a political move, evidenced by the conflicts with Brazilian courts: it is a way to inform regular non-tech-savvy users that it would be impossible to disclose information to any government, even if they would be obliged or if the company wanted to cooperate. By publicizing the message to all its users, WhatsApp is turning a very technical affordance into common knowledge as a strategy to co-opt public opinion by their side on a next conflict with any court in the world.

Such strategy is reinforced when the company sends co-founder Brian Acton to Brazil to explain end-to-end encryption on a public hearing (STF, 2017). WhatsApp seems to be engaging in a Public Relations symbolic war against Brazilian government—and all the other States that have been pushing for higher levels of "collaboration". By enlightening the public, the company engages in a sort of bottom-up guerrilla. This public and dramatic call for the sympathy of WhatsApp's users—as a collateral effect of awareness—is also explicit in Zuckerberg remarks after the first WhatsApp blockage: "It's a sad day for Brazil [. . .] If you're Brazilian, *please make your voice heard*. #ConnectBrazil #ConnectTheWorld" (Zuckerberg, 2015, our emphasis, see Figure 7). Zuckerberg calls for resistance against governments that don't understand they are asking for something technically impossible -perhaps implicitly qualifying as ignorant, unaware or even autocratic? Also, it hinders a discourse as if the end-to-end encryption had been bootstrapped by the App without any deliberation by its executives, subtly de-politicizing the decision.

This political chess move by WhatsApp is very well synthesized by Guardian's John Naughton's (2016) comment on WhatsApp encryption deployment:

> So when the cops come armed with a warrant, corporate executives are, regretfully, "unable to help." *This represents both shrewd corporate strategy and political astuteness*: it means that they can give the same reply to the Chinese or Russian governments as they do to the American or British authorities [. . .] the thing that really infuriates state authorities about the encryption systems that firms such as Apple and WhatsApp (now owned by Facebook) have created is that they do not involve the companies holding any decryption keys. (par 9, our emphasis)

Though much subtler, the whole process was mirrored on a most recent case: Pavel Durov's active resistance to Russian government's attempt to block Telegram in the country. The creator of the alternative messaging system not only openly incited people to take matters in their own hands—by protesting either on the streets (Durov, 2018a), throwing paper planes[11] (Reuters, 2018) or both—but he has declaredly fought either through the development of new affordances or

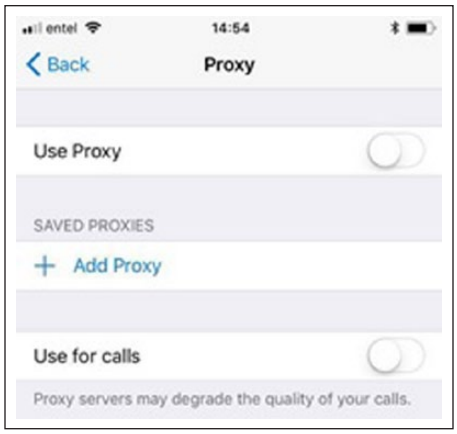


Figure 8. Telegram's affordance that allows bypassing an Internet Service Provider blockage by using a proxy (Source: Telegram interface, screenshot by authors).

urging users to adopt existing ones, such as the option to use a proxy (Figure 8) to bypass the ISP's blockage. Or as his final words on a statement in the beginning of the clash with Russian authorities state: "The history of our ancestors has taught us to fight until the end" (Durov, 2018b).

This staging of an asymmetric PR guerilla aims at assimilating WhatsApp users as its constituents, implying they belong to the "weak" (users and private corporation) against the strong (the State), even though WhatsApp and Facebook look much more like a "corporate-state-power phenomenon" (as we stated with Trottier & Fuchs, 2015, p. 34). So, to embody the weak, supposedly harassed by State power, the corporation strategy consists in two actions: first, to develop affordances that offer to those same users the possibilities to escape Intelligence's eye and records and second, to publicly motivate its own users to resist State's interference as a result of the awareness caused by making the encryption affordance perceivable.

Encryption Solves Everything. . . or Not? It is undeniable: end-to-end encryption is a giant step and even a herculean effort to advance in privacy and security for personal messaging, applauded by security and privacy experts. According to 2017's "Who has your back" report by Electronic Frontier Foundation (EFF) (Cardozo, Crocker, Lynch, Opsahl, & Reitman, 2017), WhatsApp has done a good job with end-to-end encryption using the *Signal Protocol*. But other issues don't confirm the same diligence, turning the same experts to not recommend the use of WhatsApp:

> We take no issue with the way this encryption is performed. In fact, we hope that the protocol WhatsApp uses becomes more widespread in the future. Instead, we are concerned about WhatsApp's security despite the best efforts of the Signal Protocol. (Budington & Gebhart, 2016, par 4 our emphasis)

In other words, the voiced concern for privacy and security WhatsApp has developed recently does not resonate with a few of the company's decisions turned into affordances, attributes or configurations. To explain it, we rely on the following diagnosis from EFF (Budington & Gebhart, 2016) that helped us to point out the technical contradictions that emerge between affordances possibilities, limitations, and the visibility the corporation gave to end-to-end encryption:

1. Unencrypted Backup: the app comes with options to backup information without any encryption in order to allow users to restore information after losing the cellphone or some other reason, which turns insufficient the protection generated with the communicational encryption.
2. Keychange notifications and Man in the Middle: There is some irony to the fact that the very nature of the App as a personal communication tool with a spin-off as a data management product, and the growing importance of the latter as WhatsApp use grows in importance in users' lives, means that whenever a person changes phone number or his device, WhatsApp allows pushes for a new key for the user, since the former was associated with a different device. This fact is only signaled to the user on the other end when the message (or messages) has already been delivered, opening a breach called Man in the Middle, "in which a third party pretends to be a contact you know."
3. Web App: Client downloadable software, though probably be a less commercial option, is highly recommendable from the security perspective, since it protects the source of the download. It is again a tradeoff that reflects priority on uncomplicated solutions for users' needs, probably aiming to reach for larger audiences.
4. Facebook data sharing: This is undeniably the most noticeable point, and obviously the less technical one. Sharing the users' information with a company that has no good reputation with privacy issues is clearly not motivated by the desire to provide a more secure or private service, but reveals the pursue of financial return over concerns of privacy or security. As stated by EFF, "This gives Facebook an alarmingly enhanced view of users' online communications activities, affiliations, and habits." And probably dragged away the App's founding fathers.

Besides those points made by EFF, one of the easiest ways to leak information from a private conversation are *screenshots*, even if you set a duration to the message (that works as a *self-destruction timer*). Telegram, for instance, has a functionality that notifies the other user of a screenshot

captured in secret conversations (see Figure 9). In consequence, it seems to be clear that end-to-end encryption is an affordance that presents a lot of possibilities and empowers users if correctly appropriated. But its limitations are also noteworthy and could be understood as cues, after a critical review, that suggest political and/or commercial raisons d'être.

Tradeoff: Commercial Massiveness X Technological Utopia. One of the security issues discussed above was prompted by the security key change (the Man in the middle issue), have generated some debate among specialized media and professionals, as it has been overstated as "backdoor" by The Guardian (Ganguly, 2017), and later tampered down by one of its senior editors who then defined as a "flaw" (Chadwick, 2017). It has since been called a "tradeoff" by some security (Chadwick, 2017; Portnoy & Bonneau, 2017) and cyberculture (Tufekci, 2017) specialists.

WhatsApp Inc. has made options that lead to commercial massiveness, as a tradeoff to other possible ways that could, for instance, be more secure or enhance privacy, presented in Table 2. In that sense, it stands as a remarkable example of the tensions described by Jose van Dijck (2013), on his critical history of Social Media: "Platforms had to navigate between Silicon Valley's venture capitalist culture, which pushed for quick turnovers and speedy IPOs, and the original participatory spirit, which had caused the platforms to grow in the first place" (p. 15). EFF synthesizes the tradeoff idea comparing WhatsApp to Signal, which helps make WhatsApp faults more visible, complementing what we did previously in this section:

> WhatsApp [. . .] was a massively popular tool before end-to-end encryption was added. The goal was to add encryption in a way that WhatsApp users wouldn't even know it was there [. . .] WhatsApp is not competing with Signal in the marketplace, but it does compete with many apps that are not end-to-end encrypted by default and don't have to make these security trade-offs. (Portnoy & Bonneau, 2017, par 12)

Figure 9. Telegram's secret messages screenshot notification (Softpedia).

Conclusion

Beyond the discourses of users' security and privacy protection, either from a commercial or an idealistic perspective, widely circulated after the implementation of end-to-end encryption on WhatsApp and behind the decision to make it visible for users, three stories emerge: (1) a Public Relations strategic bottom-up communicational guerrilla war carried out by WhatsApp Inc. who, through public opinion management in a very subtle ways, such as making visible the invisible affordance of the end-to-end encryption, mobilizes its billions of users as its constituents to help face (2) a power struggle between corporate and state power, into which the variable of technological development of affordances—such as encryption—is revealed as a techno-political statement or, to follow the belligerent metaphor, as a paralegal weapon; and its vulnerabilities and/or imperfections are read as (3) a tradeoff between commercial massiveness versus technological utopia, where at some point Koum's American dream tale is overcome by the pressures of Silicon Valley and the utopian startup-like speech concedes for a much less

Table 2. Tradeoffs make evident the privilege of commercial massiveness over privacy and security (Authors).

Tradeoffs	
Insecure Affordance	*Massiveness/Commercial benefit*
Unencrypted backup by default	User experience benefit: easier to keep memories of conversations backed up.
Key change with apparatus change	Easy to user to update device seamlessly, facilitating market tendency of programmed obsolescence.
Insecure Web App, relying on browser privacy and security affordances	More convenience to users, that don't need to download and update client-software.
Sharing data with Facebook	Probably a tradeoff to keep Koum's promise that the App will be forever advertisement-free. Or perhaps simply a condition to the billionaire acquisition by Facebook.
Screenshot allowed, no notifications (such as Telegram secret messages)	Useful affordance in daily routine, but opens to diverse possibilities of leaking private or intimate information.

inspiring and more pragmatic "Platform Capitalism" (Srnicek, 2017) logics in pursuit of revenue and profitable business models. In more detail:

1. Users' awareness is instrumentalized as a political guerrilla strategy. Since the legal department seems to be having problems with governments' demands—such as, notoriously, in the Brazilian case(s) for WhatsApp or Russia and Iran in the case of Telegram—then: let's communicate. Through making visible the implementation of end-to-end encryption WhatsApp Inc. sets the agenda, creates conversation (as this article is a constitutive part of) and therefore discretely starts an awareness PR guerrilla by engaging its "constituents" with the issue of privacy and security against States that don't accept the lack of control over the content that travels through the ICT networks;
2. Changing the software is a form of power, carried out by its developers. It implies options. WhatsApp's encryption implementation has not been propelled by digital culture idealism—at least, not exclusively or not in such a heroic way as it has been publicized. Rather, as demonstrated, there are plenty of evidences that such a technical move responds to a political need to enhance the position of the company in a strategic way when facing legal dilemmas regarding privacy and security issues when and where national states, enforcement agencies or other actors try to coerce it to "collaborate". The affordances themselves are the concrete manifestation of the company's power. As the other side of the previous point, strategic options of development have such a relevance that they eventually generate strong reactions from governments such as it happened with end-to-end encryption: United Kingdom (Burrell, 2017; Hintz, 2015), Brazil (Abreu, 2017), and United States (McCarthy, 2015), if not others, have manifested their opposition to the affordance. Thus, the implementation of a strategic software affordance in an App with such a social, economic, and even political relevance such as WhatsApp has the potential to stand as an important political statement. Such statement is revealed on Acton's answer during an interview while he was in Brazil to defend WhatsApp against the recurring blocks determined by justice: "Nobody can read. Neither WhatsApp nor [the governments of] USA or Brazil. Neither the countries nor the companies. That creates a system that protects security and privacy from its users" (Simões Gomes & Rodrigues, 2017);
3. Massiveness wins over privacy, security, and other possible functional commitments that the company or its original founders might sympathize or defend. Privacy and security, in this reading, would be much more of attractive branding and market positioning strategies[12] than a company value, an ethical-legal dilemma or a personal techno-political ideal. If otherwise, how could we explain the contradictions behind the tradeoffs? Massive personal data is a source of real profit for social media nowadays: "the golden egg their geese produced" (Van Dijck, 2013, p. 16). In addition, as Facebook gradually broke WhatsApp's promises and the contradictions grew, even the chat App's founders left the stage.

Affordances such as end-to-end encryption are a sophisticated technological response from WhatsApp Inc. to States' pressure to "collaborate," exempting them from actually being even able to cooperate even if they would "want" to, putting WhatsApp in a comfortable position regarding such an uncertain territory. Apple moved in the same direction when encrypted iPhone 6 and others might move the same way. On the other hand, the growing users' awareness around privacy and security issues regarding WhatsApp (and perhaps other social media) has a positive collateral effect to avoid misinterpretation of its affordances, as recently exposed by late scandal of evidence manipulation by Chilean Police during Huracán Operation during 2017, who falsely claimed being able to "wire" Mapuche[13] dissidents on WhatsApp.[14]

The politics of social media seem, consequently, to move between its vigilance capacity and privacy patches. In the "surveillance-industrial complex" (Trottier & Fuchs, 2015, p. 34), it seems that corporate-state-power shows the direct struggle of WhatsApp not only with several single States, but also with ethical discourse of privacy, and security norms of governing people. The cooperation seems to operate as a permanent negotiation, about what kind of regulation would the company comply with in a way that aforesaid State also wins. In synthesis, legal and political get mingled as tech companies protect themselves from both through putting themselves in a position of impossibility to cooperate: *ad impossibilita nemo tenetur.*[15]

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Notes

1. *Justiça manda bloquear WhatsApp por 48 horas a partir desta quinta-feira* (EBC Website), available at http://agenciabrasil.ebc.com.br/geral/noticia/2015-12/justica-manda-bloquear-whatsapp-por-48-horas-partir-desta-quinta-feira, retrieved December 26, 2017.
2. It was not exactly a total blackout, since some people installed VPNs to elude the ISPs.

3. Detailed information may be found on website www.bloqueios.info. Retrieved June 15, 2018.
4. We take advantage of this statement to clarify that we do not consider the user perspective (appropriation, user experience etc.) for this article for it is not central to the analysis of an automatic affordance, that is, one that does not demand user interaction.
5. We tried to contact WhatsApp but had no response from the company at the time of the writing.
6. Materialities are as follows: "the arrangement of elements that come into play to enable the physical existence of the journalistic text" ("l'ensemble des éléments qui entrent en jeu pour faire exister physiquement le texte périodique") (Lévrier, & Wrona, 2013, p. 8).
7. Wikipedia, retrieved from https://en.wikipedia.org/wiki/WhatsApp.
8. Extracted from archived webpage from archive.org's wayback machine.
9. The accepted manuscript was written in June, 2018.
10. In January 2018 the App had surpassed 1.5 billion users, according to a Zuckerberg's post on Facebook on June 14, 2018, retrieved from https://www.facebook.com/zuck/posts/10,104,501,954,164,561.
11. Telegram's logo is a paper plane.
12. This could be partly triggered by Snowden's revelations and his endorsement of Open Whisper Systems products (Cimpanu, 2015).
13. Native population engaged in historical struggle for ancestral land recovery.
14. Caso Huracán: ¿es factible técnica y legalmente "hackear" WhatsApp? Available at http://ciperchile.cl/2018/02/07/caso-huracan-es-factible-tecnica-y-legalmente-hackear-whatsapp/ retrieved June 15, 2018.
15. Latin expression of legal maxim that translates as "Nobody is held to the impossible." Accessed December 26, 2017. http://www.oxfordreference.com/view/10.1093/acref/9780195369380.001.0001/acref-9780195369380-e-113.

ORCID iD

Marcelo Santos https://orcid.org/0000-0002-2658-3764

References

Abreu, J. S. (2017, July 26). Public hearing on encryption and WhatsApp blockages: The arguments before the STF. *Bloqueios.info, Internetlab* (A. L. Araujo Trans.). Retrieved from http://bloqueios.info/en/public-hearing-on-encryption-and-whatsapp-blockages-the-arguments-before-the-stf/

Brandom, R. (2014, November 18). WhatsApp rolls out end-to-end encryption using TextSecure code. *The Verge*. Retrieved from https://www.theverge.com/2014/11/18/7239221/whatsapp-rolls-out-end-to-end-encryption-with-textsecure

Budington, B., & Gebhart, G. (2016). Where WhatsApp went wrong: EFF's four biggest security concerns. *EFF*. Retrieved from https://www.eff.org/deeplinks/2016/10/where-whatsapp-went-wrong-effs-four-biggest-security-concerns

Burgess, J., & Baym, N. (2016, October 5-8). @RT#: Towards a platform biography of Twitter. In J. Burgess, N. Baym, T. Bucher, A. Helmond, N. John, A. Nissenbaum, . . . Craig, D. (Eds.), *Platform Studies: The Rules of Engagement*. *Panel Presented at AoIR 2016: The 17th Annual Conference of the Association of Internet Researchers*. Berlin, Germany. Retrieved from http://spir.aoir.org

Burgess, J., & Baym, N. (2017). *Platform biography* [Powerpoint Slides]. Brisbane, Queensland, Australia DMRC Summer School.

Burrell, H. (2017, March 27). How secure is WhatsApp? WhatsApp security and encryption explained. *Tech Advisor* Retrieved from https://www.techadvisor.co.uk/feature/internet/how-secure-is-whatsapp-whatsapp-security-encryption-explained-3637780/

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. Retrieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Cardozo, N., Crocker, A., Lynch, J., Opsahl, K., & Reitman, R. (2017, July 10). Who has your back 2017. *EFF*. Retrieved from https://www.eff.org/who-has-your-back-2017#whatsapp-report

Chadwick, P. (2017, June 28). Flawed reporting about WhatsApp. *The Guardian*. June, 28. Retrieved from https://www.theguardian.com/technology/commentisfree/2017/jun/28/flawed-reporting-about-whatsapp

Cimpanu, C. (2015, December 3). Signal encrypted messaging app comes to desktops. *Softpedia News*. Retrieved from http://news.softpedia.com/news/signal-encrypted-messaging-app-comes-to-desktops-497084.shtml

Daftari, L. (2014, May 4). Iran bans WhatsApp because of link to "American Zionist" Mark Zuckerberg. *Fox News World*. Retrieved from http://www.foxnews.com/world/2014/05/04/iran-bans-whatsapp-because-link-to-american-zionist-mark-zuckerberg.html

Da Silveira, S. A. (2014). Para Analisar o Poder Tecnológico como Poder Político. In S. A. Da Silveira, S. Braga, & C. Penteado (orgs.), *Cultura, política e ativismo nas redes digitais*. São Paulo, Brazil: Fundação Perseu Abramo.

Deleuze, G. (1992). Postscript on the societies of control. *October*, *59*, 3–7. Retrieved from https://www.jstor.org/stable/778828

Dencik, L., & Leistert, O. (2015). *Critical perspectives on social media and protest: Between control and emancipation* (Kindle ed.). London, England: Rowman & Littlefield.

Durov, P. (2018a, 29 April). *VK wall post*. Retrieved from https://vk.com/wall1_2401089

Durov, P. (2018b, may 8). *VK wall post*. Retrieved from https://vk.com/tnews?w=wall1_2442097

Dwoskin, E. (2018, April, 30). WhatsApp founder plans to leave after broad clashes with parent Facebook. *The Washington Post*. Retrieved from https://www.washingtonpost.com/business/economy/whatsapp-founder-plans-to-leave-after-broad-clashes-with-parent-facebook/2018/04/30/49448dd2-4ca9-11e8-84a0-458a1aa9ac0a_story.html?noredirect=on&utm_term=.dd7d539d05e5

Ellul, J. (1964). *The technological society*. New York, NY: Vintage Books.

European Commission. (2017, May 18). Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover. *European Commission Press Release Database*. Retrieved from http://europa.eu/rapid/press-release_IP-17-1369_en.htm

Ganguly, M. (2017, January 13). WhatsApp design feature means some encrypted messages could be read by third party. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2017/jan/13/whatsapp-design-feature-encrypted-messages

Garside, J. (2014, August 5). More than 17,000 sign up to Austrian student's Facebook privacy class action. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2014/aug/05/sign-up-austrian-student-facebook-class-action-data-violations

Gibson, J. J. (1977). The theory of affordances. In R. E. Shaw & J. Brandford (Eds.), *Perceiving, acting, and knowing: Toward an ecological psychology* (pp. 67-82). Hillsade, NJ: Lawrence Erlbaum.

Gibson, J. J. (1986). *The ecological approach to visual perception*. Hillsade, NJ: Lawrence Erlbaum.

Gillespie, T. (2010). The politics of "platforms." *New Media & Society*, *12*, 347–364.

Greenberg, A. (2016, October 4). You can all finally encrypt Facebook Messenger, So do it. *Wired Magazine*. Retrieved from https://www.wired.com/2016/10/facebook-completely-encrypted-messenger-update-now/

Greenwald, G. (2013, June 6). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Greenwald, G., & MacAskill, E. (2013, June 7). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Hintz, A. (2015). Social media censorship, privatized regulation and new restrictions to protest and dissent. In L. Dencik & O. Leistert (Eds.), *Critical perspectives on social media and protest: Between control and emancipation* (Kindle ed.). (pp. 109-126). London, England: Rowman & Littlefield.

Hutchby, I. (2001). Technologies, texts and affordances. *Sociology*, *35*, 441–456.

Koum, J., & Acton, B. (2016, April 5). End-to-end encryption. *What App Official Blog*. Retrieved from https://blog.whatsapp.com/10000618/end-to-end-encryption?l=en

Lakoff, G. (2008). *Puntos de Reflexión* (Manual del Progresista). Barcelona, Spain: Península.

Langlois, G. (2014). *Meaning in the age of social media*. New York, NY: Palgrave MacMillan.

Lévrier, A., & Wrona, A (Eds.). (2013) *Matière et esprit du journal. Du Mercure Galant Mercure à Twitter*. Paris, France: PUPS [Histoire de l'imprimé].

McCarthy, T. (2015, February 23). NSA director defends plan to maintain "backdoors" into technology companies. *The Guardian*. Retrieved from https://www.theguardian.com/us-news/2015/feb/23/nsa-director-defends-backdoors-into-technology-companies

Meyrowitz, J. (1994). Medium theory. In D. Crozley & D. Mitchell (Eds.), *Communication theory today* (pp. 50–77). Standford, CA. Standford University.

Naughton, J. (2016, April 10). Your WhatsApp secrets are safe now. But Big Brother is still watching you…. *The Guardian*. Retrieved from https://www.theguardian.com/commentisfree/2016/apr/10/whatsapp-encryption-billion-users-data-security

Norman, D. (1999). Affordance, conventions and design. *Interactions*, *6*, 38-43. Retrieved from http://www-ihm.lri.fr/~mbl/ENS/DEA-IHM/papers/Norman-Affordances.pdf

Portnoy, E., & Bonneau, J. (2017, January 14). Google launches key transparency while a trade-off in WhatsApp is called a backdoor. *EFF*. Retrieved from https://www.eff.org/deeplinks/2017/01/google-launches-key-transparency-while-tradeoff-whatsapp-called-backdoor

Reuters. (2017, May 12). WhatsApp é multado por obrigar usuário a aceitar dividir dados com Facebook. *Folha De São Paulo*. Retrieved from http://www1.folha.uol.com.br/tec/2017/05/1883472-whatsapp-e-multado-por-obrigar-usuario-a-aceitar-dividir-dados-com-facebook.shtml

Reuters. (2018, April 30). Paper plane protesters urge Russia to unblock Telegram app. *Reuters*. Retrieved from https://www.reuters.com/article/us-russia-telegram-protests/paper-plane-protesters-urge-russia-to-unblock-telegram-app-idUSKBN1I11O5

Rowan, D. (2014, February 19). WhatsApp: The inside story. *Wired Magazine*. Retrieved from http://www.wired.co.uk/article/whatsapp-exclusive

Scriberia, C. S., Kiss, J., Boyd, P., & Ball, J. (2013, November 26). The NSA and surveillance . . . made simple. *The Guardian*. Retrieved from https://www.theguardian.com/world/video/2013/nov/26/nsa-gchq-surveillance-made-simple-video-animation

Simões Gomes, H., & Rodrigues, M. (2017, June 2). WhatsApp no STF: caso é único no mundo, dizem executivos do app. *G1*. Retrieved from https://g1.globo.com/tecnologia/noticia/whatsapp-no-stf-caso-e-unico-no-mundo-dizem-executivos-do-app.ghtml

Srnicek, N. (2017). *Platform capitalism*. Hoboken, NJ: John Wiley & Sons.

Statt, N. (2018, April 30). WhatsApp co-founder Jan Koum is leaving Facebook after clashing over data privacy. *The Verge*. Retrieved from https://www.theverge.com/2018/4/30/17304792/whatsapp-jan-koum-facebook-data-privacy-encryption

Supremo Tribunal Federal do Brasil (STF). (2017, June 5). Audiência pública—Bloqueio judicial do WhatsApp e Marco Civil da Internet (1/4) [Direct link to Brian Acton deposition]. *STF Youtube Channel*. Retrieved from https://www.youtube.com/watch?v=3TNsQCNIOO0&feature=youtu.be&t=43m30s

Tenenboim-Weinblatt, K., & Neiger, M. (2018). Temporal affordances in the news. *Journalism*, *19*, 37–55.

Trottier, D., & Fuchs, C. (2015). Theorising social media, politics and the state. In D. Trottier & C. Fuchs (Eds.), *Social media, politics and the state: Protest, revolutions, riots, crime and policing in the age of Facebook, Twitter and YouTube* (pp. 3–38). New York, NY: Routledge.

Tufekci, Z. (2017). *In response to guardian's irresponsible reporting on WhatsApp: A plea for responsible and contextualized reporting on user security*. Retrieved from. http://technosociology.org/?page_id=1687

Van Dijck, J. (2009). Users like you? Theorizing agency in user-generated content. *Media, Culture & Society*, *31*, 41–58.

Van Dijck, J. (2013). *The culture of connectivity: A critical history of social Media* (Kindle Version). Oxford, UK: Oxford University Press.

WhatsApp Inc. (2016, August 29). Un vistazo al futuro de WhatsApp. *WhatsApp Official Blog*. Retrieved from https://blog.whatsapp.com/10000627/Un-vistazo-al-futuro-de-WhatsApp

Zuckerberg, M. (2015, December 17). *Facebook post*. Retrieved from https://www.facebook.com/zuck/posts/10102530374780451?pnref=story

Author Biographies

Marcelo Santos (PhD Communications Science, PUC, Chile) is a researcher of Centro de Investigación y Documentación (CIDOC) and Assistant Professor of Humanities and Communications Faculty at Universidad Finis Terrae (Santiago de Chile). His research interests are on the crossroads of communication technologies and democracy, focusing recently on the ICT social appropriation by ordinary people during acute events, such as street demonstrations and disasters, to create and circulate content through Social Media.

Antoine Faure (PhD Political Science, IEP Grenoble, France) is a researcher of Centro de Investigación y Documentación (CIDOC) and Associate Professor of Humanities and Communications Faculty at Universidad Finis Terrae (Santiago de Chile). His research is focused on the political dimension of the practices of journalism. Some of his work deals with ICTs politics and other with TV series. His current research project is entitled "Chilean History of Journalistic Temporalities (1973–2013): Another Gaze Regarding Professional Journalism's Political Dimension," which was funded by CONICYT (FONDECYT N°11170348).