The Nothing to Hide as a libertarian trap: Critical Reflections on the spread of John Soloves thesis

Lucas Domínguez Rubio
CeDInCI/UNSAM - CONICET
Argentina
lucaslmdr@autistici.org

ABSTRACT: *The phrase "Nothing to Hide" is usually the initial way in which nowadays the mass media deal with problems around privacy. For several years now, when journalists, academics and activists discuss why privacy matters, they usually attack this argument. In fact, now there is a Nothing to hide genre established through blogs, conferences and books. The analysis of the various counter-arguments proposed in journalistic interventions allows us to evaluate assumptions, limits and similarities. In general, the set of counter-arguments seeks to generate some fear of potential personal inconvenience to show the importance of updating privacy as a social value. If the Nothing to hide aims that big data bases do not involve any personal, social or political problem, the different counter-arguments against it only point out that it could involve potential personal problems. In this way the Nothing to hide usually is the first obstacle to open political discussions around internet, since it could be a way to close the discussion about how we use the internet or it could be a way to spread this topic.*

Keywords: Privacy, Nothing to Hide, Cryptography, Software and Internet Politics

Received: 10.6025/jdp/2018/8/3/95-99

1. Introduction

For almost fifteen years, the phrase "Nothing to Hide" has become a common place in any discussion regarding privacy. Of course, this is because the question about the use of strongly centralized digital services usually has a repeated answer: its not a problem, I have nothing to hide. Thereby, this phrase has established a well-known challenge. According to it, only those who develop illegal activities could have an objection against the different digital recollection programs. But, in fact, this phrase works rejecting beforehand the existence of social or political problems around big data bases. Nowadays, all those who analyse privacy have something to say about the Nothing to hide problem. And when journalists, academics and activists discuss why privacy matters, they usually attack this argument. Thus, there is a Nothing to hide genre established through blogs, conferences and books by, for example, Julian Assange, Marta Peirano, Natalia Zuazo, Jakob Appelbaum, Jrmmie Zimmerman, Glenn Greenwald and Daniel Solove, among others. As a common strategy, all of them have proposed a revaluation of the importance of privacy in different ways: they have either tried to awake a "libertarian" intuitive feeling or have considered privacy as a basic right in a confusing but fundamental way. This is because the answers have been proposed in the same terms as the challenge. And, in

fact, this is the tactic of one of the first and most well-known academics on this topic, Daniel Solove. In this way, his analysis results extremely representative of the general terms in which the problem continues to be thought.

2. Nothing To Hide / Nada Que Ocultar / Rien Cacher

As an example, the texts of Timothy May (1992, 1994) show the ideology in the first type of political stance against the technological surveillance identified only with the State. Basically the cryptonarchism present in his texts is nothing more than the enthusiasm for the use of cryptography to achieve individual freedom and privacy. Undoubtedly, a new chapter in favor of privacy is given in the moment of the creation of gigantic databases by the main web content companies. As the current hypothesis proposes, this is the new way of capital accumulation of the twenty-first century.

Nowadays, a big amount of internet traffic goes through the servers of the main United States web content enterprises. These companies generate data analysis to develop targeted advertising. This new kind of capital has its origin at the same time as the working and recreational activities of all internet users. Each user works spontaneously as a data-entry for the free digital services that they receive. It would be idle to describe the big number of digital traces that we permanently leave Apparently, it is a win-win situation. On the one hand, we interchange high quality digital services for our user profiles and we win more suitable advertisement for us. On the other hand, this data bases could allow better tools to fight terrorism, illegal-pornography and drug trafficking. In theory, by default big data bases do not treat information in a personal way.

Therefore, the Nothing to hide is stronger than it seems. If we think it in relation to NSAs programs like PRISM, it has the shape of a dilemma. If these programs discover illegal activities, they meet their goal. Of course, people involved in these activities do not deserve any privacy right, while those who do not develop any illegal activity do not have to worry about any impersonal filtering of their information. According to this situation, why is it important to considerer the argument known as Nothing to hide? Preliminary, we could determine at least two reasons.

Firstly, the Nothing to hide works in a tacit way in the entire internet users behaviour. Indeed, we can think that the nothing to hide is not an argument, but rather an implicit way of using the internet. Wondering about it, we put in discussion our every day habits. Some years ago, this problem was raised in terms of privacy vs. national security (Solove, 2007). Nowadays, it works as a problem of privacy vs. comfort. Our passwords preserve information that nobody cares and the hegemonic servers are, by far, much easier to use.

Secondly, at the same time, a good answer against the Nothing to hide involves arguments to use software libre, cryptography and some internet services and not others. According to this, to have better counter-arguments on this discussion allow us to think the importance of the political agenda promoted by the activists on these topics.

In summary, in order to open a political question about the use of the internet, the Nothing to hide appears like a first common obstacle.

3. A Libertarian Sensitivity: Counter-arguments Objectives and Scope

The different counter-arguments tend to repeat themselves, and we can see the existence of a sort of canon. It is necessary to say that these interventions have arisen from lectures, TEDx talks and videos available on the internet. We are talking about material whose authors have develop in order to spread information about this problems. This is the reason why most of these counter-arguments attack a ridiculously exaggerated version of the Nothing to hide.

(a) For example, the most common answers state things like if you have nothing to hide, why do you use curtains? (see for example: Zimmerman, Rien cacher). Or: Well, so give me all your passwords of your social networks and email (Greenwald, Why privacy matters?). Or also: If you have nothing to hide, why do you not let us put cameras in your house, in your room and in your bathroom? (Zimmerman, Rien cacher). Or another one: It is false. Everyone has something to hide, from our partners, from our boss, etc. (Stallman, interview). In general, all of them, in order to increase their persuasive power, try to wake a sort of paranoid sensitivity. They try to install the possibility of a very personal intromission. However, the solution is not that obvious and these exaggerated responses do not change anybodys digital behaviour.

(b) Another common set of arguments takes the form of a mental experiment: what happens if all your digital profile suddenly

falls under an adverse political condition? To address this point, this counter-arguments propose concrete examples of political militant experiences in Middle West countries (Appelbaum, The Tor Project, protecting online anonymity), or, without going too far, dangerous situations in which you can be accidentally involved. As Marta Peirano says: there are a thousand ways to be in the wrong place (Peirano, Por qu me vigilan, si no soy nadie?). As usual, this type of counterargument fails because it cannot convince a public that believes to be in a stable political situation.

(c) Another strategy is to determine a specific target for the argument. In this way, nowadays we have courses or manuals about digital privacy practices specific for journalists or activists (e.g. Peirano, 2015). That is to say, only for those who might have something to be worried about. Here we lose the question about why a user with harmless practices does not have to think about it. On the contrary, this sort of argument accepts the Nothing to hide statement: it is ok for some people to have something to hide.

(d) Other arguments are in favour of the importance of privacy as an essential element of freedom of expression and democracy (e.g. Zuazo, Escritora Natalia Zuazo habla sobre su libro Guerras de Internet; Snowden, Why Privacy is the Most Important Human Right). Although we could think privacy as a right that must be respected, in every case, there is still the unsolved task of defining privacy in legal terms (Solove, 2011). In addition, although we could think privacy as a condition for democracy and republicanism, in fact, the current situation does not seem to have fundamental changes in the politicaleconomic system (Preibusch, 2015).

(e) Finally, other texts start from an environment of tacit danger and they want to function as a fire warning. From this perspective, they do not largely justify why everyday encryption should be used. So they seem to target a community of activists already convinced. In this direction, for example, Cypherpunks (2012), the book by Julian Assange, uses a warlike language and impels the idea of a guerrilla war of cryptographic weapons (Assange, et.al. 2012). Somehow, taking into account that one of the first ways to limit the circulation of cryptography has been to treat it as ”war munitions”, these texts may seem counterproductive. This warlike language would continue stigmatizing what, in short, is today just a small add-on in our email manager with software capable of handling a complex mathematical algorithm. While the activist community carries out campaigns to spread the use of cryptography, this ”war” will never begin unless there are clear arguments about why to use cryptography.

Summarizing, the tactic of all counter-arguments against the Nothing to hide lies in revaluating the notion of privacy in different ways, probably because, in order to promote interest in the subject, the easiest way is to arouse fear of a possible personal danger. But these arguments fail either by simplicity or by the certainty of being immersed in a democratic system with certain enduring guarantees, mainly because no one believes that our privacy is violated by the daily use we make of digital services.

4. Systematizing Privacy

Even before Snowden’s revelations in 2013, the Nothing to hide was already a genre of counter-arguments disorderly expanded on different web pages. The first one to notice its relevance from the academic arena was Daniel Solove (2007, 2011). Solove has performed a meticulous work in which he traces the presence of the Nothing to hide through the American and British public media. He has made a similar analysis of these counter-arguments, and his own project is to develop a theory about privacy for its legal protection. In this way, Solove is one of those who has most decisively insisted on the importance of the notion of privacy. Accordingly, it is remarkable that, in addition to his role as an academic, he founded a digital security company, which mainly provides courses on how to protect personal and corporate information.

His case, as a reference on the subject, becomes especially clear in the literary metaphor that he chooses to think the problems around the Nothing to hide (Domnguez Rubio, 2018). The Big Brother metaphor does not work any longer, says Solove: oppression is not so explicitly bloody. Instead, he proposes to take as a reference the type of domination presented in The Process (1925) by Franz Kafka. There, the protagonist moves under the force of an abstract and unintelligible power in front of which he is disoriented. The remarkable thing is that his libertarian militancy makes him leave aside the need of a better understanding of the actors responsible for the infrastructure and content behind the internet. It is not by chance that Solove has chosen a non-political literary metaphor where a character in solitude is on his own. In short, it is the libertarian attitude that alerts about the danger of State surveillance and, at the same time, underestimates the importance of the accumulation of data by companies with its implications.

The media outburst of Snowden’s revelations has not brought about further consequences. Within the United States, the

dispute resulted in a debate about whether Snowden should be considered a hero or a traitor. Jealous of individual liberties vis-a-vis the State, the so-called libertarians were the ones who most raised their voices. Outside, one of the reasons why the German University in Rostock academically recognized Snowden was because it ”he helped us to think democracy again”. Snowden has allowed us to think again about the great set of changes that involve the reformulations of liberalism as neoliberalism and the relations between society, State, individuals and corporations, at the same time when legal internet frameworks are beginning to be discussed.

Against this, a political view of this topic keeps the question about the bonds of companies of the same flag and their government. This could make it clear that transnational corporations handle more capital than the gross domestic product of many countries. Although this task seems difficult, against Solove, it is about identifying the actors responsible for the infrastructure and content behind the internet.

5. Conscious Practices Around A New Political Agenda

The Nothing to hide could be a way to close the discussion about how we use the internet or it could be a way to spread this topic. If the Nothing to hide aims that big data bases does not involve any personal, social or political problem, the different counter-arguments against it only point that it could involve potential personal problems.

From the beginning, the Nothing to hide poses the problem as a trap. In order to deactivate it on its own terms, the set of counter-arguments seeks to generate some fear of potential personal inconvenience to show the current importance of privacy as a social value.

On the contrary, another method of analysis that has not yet been sufficiently explored requires an interpretation of the political conjuncture, which can only consist in a diagnosis of the actors responsible for providing digital services. The question ”who built Thebes?” is not only necessary for historical studies, it shows how strongly necessary is to understand the present. As we pointed out, nowadays, identifying actors and interests presents great difficulty, as we use platforms and consume products that by the complexity of their production chains and marketing strategies appear to be neutral. In this context, identifying actors and interests becomes a political action in itself. The diffusion of such analyses could break several levels of naivety, or at least leave behind the initial attitudes to ask ourselves about the political nature of hegemonic computer tools.

In fact, this perspective against the Nothing to hide helps us to better pose the problem. It’s not about thinking about something that we have to hide. The challenge is to think about how to politicize these counter-arguments to look for elements that take the attention, perhaps not to any user, but at least to those who have certain political-social convictions. For example, it is possible to outline counter-arguments that appeal to responsible consumption. Or with a correct diagnosis, expand the counter-arguments according to their antimonopoly implications. Or suggest the advantages of using cooperative or autonomist services also in the digital world.

If big data bases bring political problems that are still inscrutable, activist groups opened two fronts: one regarding their legal regulations and other promoting tools such as cryptography, free software and decentralized networks. In any case disseminating these discussions not only makes our digital practices more conscious, but, at the same time, the discussion allow us to discover a new political agenda until now largely invisible. And, for example, give rise to consider some of the on-going discussions promoted by the activists: on the political scope of new licenses and free software, on ways of inhabiting the internet, and on the so-called internet governance and digital sovereignty.

References

[1] Appelbaum, Jakob. The Tor Project, protecting online anonymity, Filmed November 2012 at TEDxFlanders, https://archive.org/details/JacobAppelbaumAtTEDxFlanders

[2] Assange, Julian., Appelbaum, Jacob., Mller-Maguhn, Andy., Zimmermann, Jrmie. (2012). Cypherpunks. New York: OR Books.

[3] Rubio, Domnguez., Lucas. (2017). La trampa nada que ocultar, Nueva sociedad, 269:137-147.

[4] Rubio, Domnguez., Lucas. (2018). Literature and Control: from Stalinism to Cyberpunk, Pervasive Labor Union, 12.

[5] Greenwald, Glenn. Why privacy matters? Filmed October 2014 at TEDGlobal, https://archive.org/details/GlennGreenwaldWhyPrivacyMatters

[6] May, Timothy. (1992). The Crypto Anarchist Manifesto. Nakamoto Institute. Accessed June 28, 2017. http://nakamotoinstitute.org/literature/crypto-anarchist-manifesto/

[7] May, Timothy. (1992). Libertaria in Cyberspace, Nakamoto Institute. Accessed June 28, 2017. http://nakamotoinstitute.org/literature/libertaria-incyberspace/¿.

[8] May, Timothy., Hughes, E. (1992). Crypto Glossary. Nakamoto Institute. Accessed June 28.

[9] May, Timothy. (1992). Libertaria in Cyberspace, Nakamoto Institute. Accessed June 28, 2017. http://nakamotoinstitute.org/literature/libertaria-incyberspace/¿.

[10] Peirano, Marta. Por qu me vigilan, si no soy nadie?. Filmed September 2015 at TEDxMadrid, https://archive.org/details/PorQuuMeVigilanSiNoSoyNadieiPorMartaPeiranoTEDxMadrid.

[11] Peirano, Marta. (2015). El pequeo libro rojo del activista en la red. Barcelona: Roca.

[12] Preibusch, Sren. (2015). Privacy Behaviors After Snowden. ACM communications 58 (5) 48-55., https://doi.org/10.1145/2733108

[13] Solove, Daniel. (2007). Ive Got Nothing to Hide and Other Misunderstandings of Privacy. *San Diego Law Review*, 44. 745-772.

[14] Solove, Daniel. (2011). Nothing To Hide: The False Tradeoff Between Privacy and Security. New Haven and London: Yale University Press.

[15] Snowden, Edward. (2016). Why Privacy is the Most Important Human Right. Interviewed by The Guardian, (July). https://archive.org/details/WhyPrivacyIsTheMostImportantHumanRight

[16] Stallman, Richard., Snowden. (2013). Assange besieged by empire but not defeated. Interviewed by Sophie Shevardnadze. Sophie and Co, RT (Russia Today), July 15, 2013. https://archive.org/details/RichardStallmanSnowdenAssangeBesiegedByEmpireButNotDefeated

[17] Zimmerman, Jrmie. Rien chacher, Filmed 2014, https://archive.org/details/RienNCacherJrrJmieZimmermannEtLaParisienneLiberLeenglishSpanishHungarianSubtitles

[18] Zuazo, Natalia. (2015). Escritora Natalia Zuazo habla sobre su libro Guerras de Internet. Interviewed by La Capital, Mar del Plata. https://archive.org/details/EscritoraNataliaZuazoHablaSobreSuLibroGuerrasDeInternet