Hiding from Whom? Threat-models and in-the-making encryption technologies

Ksenia Ermoshina, Francesca Musiani

To cite this version:

Ksenia Ermoshina, Francesca Musiani. Hiding from Whom? Threat-models and in-the-making encryption technologies. Intermédialités : Histoire et théorie des arts, des lettres et des techniques / History and Theory of the Arts, Literature and Technologies, 2018, Cacher/Concealing, 32, 10.7202/1058473ar . halshs-02320706

HAL Id: halshs-02320706

https://shs.hal.science/halshs-02320706

Submitted on 19 Oct 2019

Hiding from whom?
Threat-models and in-the-making encryption technologies

Ksenia Ermoshina and Francesca Musiani[1]

Intermédialités: Histoire et théorie des arts, des lettres et des techniques, n°32, special issue Cacher/Concealing *edited by Nathalie Casemajor and Sophie Toupin.*

Abstract. Following the Snowden revelations, end-to-end encryption is becoming increasingly widespread in messaging tools – solutions that propose a large variety of ways to conceal, obfuscate, disguise private communications and online activities. Designing privacy-enhancing tools requires the identification of a threat-model that serves to agree upon an appropriate threshold of anonymity and confidentiality for a particular context of usage. We discuss different use-cases, from "nothing-to-hide" low-risk situations, to high-risk scenarios in war zones or in authoritarian contexts, to question how users, trainers and developers co-construct threat-models, decide on which data to conceal and how to do it. We demonstrate that classic oppositions such as high-risk versus low-risk, privacy versus security, should be redefined within a more relational, processual and contextual approach.

Résumé. Suite aux révélations d'Edward Snowden, le chiffrement de bout-en-bout devient de plus en plus diffus dans les outils de messagerie – solutions qui proposent de cacher ou déguiser les communications privées et les activités en ligne. La conception d'outils renforçant le droit à la vie privée préconise l'identification d'un « modèle de menace », qui sert à obtenir un consensus sur le seuil d'anonymat et de confidentialité approprié à un contexte d'usage particulier. On discute différents cas d'usage, de situations à bas risque où il n'y a « rien à cacher » à des scénarios à haut risque, de guerre ou d'autorité étatique, pour nous demander comment les utilisateurs, les consultants en sécurité et les développeurs co-construisent des modèles de menace, décident quelles données dissimuler, et comment. On démontre que les oppositions classiques, comme « haut risque » versus « bas risque », vie privée versus sécurité, doivent être redéfinies dans une approche relationnelle, processuelle et contextuelle.

Introduction

With the introduction of end-to-end encryption[2] in WhatsApp, the most popular instant messenger, billions of users started protecting their communications by default and on an everyday basis, often

[1] This work is supported by the European Union's Horizon 2020 Framework Programme for Research and Innovation (H2020-ICT-2015, ICT-10-2015) under grant agreement nº 688722 – NEXTLEAP.

[2] "End-to-end encryption refers to systems which encrypt a message in-transit so that only the devices at either end of the exchange have access to the keys required to decrypt the data" (see Lex Gill, Tamir Israel, Christopher Parsons, "Shining a Light on the Encryption Debate: A Canadian Field Guide", report by Citizen Lab and the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, 2018, p. 5, https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf)

without realizing it. While the mantra "I have nothing to hide" is still widespread among Internet users, mass adoption of encryption has important socio-technical consequences for those whose lives depend on strong cryptographic protocols, because of their risk-related profession or political context. In response to these different use-cases, a dynamic and vibrant field -- that of the so-called privacy-enhancing tools -- offers a large variety of solutions to conceal, obfuscate, disguise private communications and other online activities. From the more popular centralized solutions such as Wire, Telegram, Signal and WhatsApp to decentralized Ricochet, Briar, OTRand email clients supporting PGP encryption, these solutions are tailored to protect against specific "adversaries". Security and privacy features worked into different protocols offer various degrees of protection and let users "hide" different parts of their online identities.

Research Question and Theoretical Framework

Our online traces are multi-layered and embedded in the material infrastructure of the Internet. Our identity can be disclosed not only by the content of our messages, but also by the unique identifiers of our hardware devices (such as MAC addresses), our IP addresses, and other related metadata[3], thus contributing to the "turn to infrastructure" in privacy and its governance[4]. Which of our multiple online identifiers can be considered as personal? Which data should we hide, and from whom? Referring to the "mosaic theory"[5], when does a combination of several items of a priori un-identifying information construct a degree of personalization sufficient to de-anonymize a user?

Drawing upon previous work such as the anthropology of spam filters[6], we understand cryptographic systems as sieves that separate items of information that have to be hidden from items that can be shown. Encryption algorithms appear as inverses or shadows of the information they sort. In fact, designing privacy-enhancing tools requires imagining the "worst of the possible worlds", constructed through various scenarios implying risk, uncertainty and security flaws. Identification of a threat-model serves to agree upon an appropriate threshold of anonymity and confidentiality for a particular context of usage. Thus, an interesting question arises, which will be the main research question this article seeks to address: how do different users define who their adversary is? How do they agree, if they agree, on which types of data should be concealed? And how do they choose the tools able to give them the level of protection they need?

This article discusses different use-cases, from "nothing-to-hide" low-risk situations, to high-risk scenarios in war zones o in authoritarian contexts. We will question how users, trainers and developers co-construct threat-models and decide on which data to conceal and on the ways in which to do it. We

[3] Metadata is usually defined as « information about information ».

[4] Francesca Musiani, Derrick L. Cogburn, Laura DeNardis & Nanette S. Levinson (eds.). *The Turn to Infrastructure in Internet Governance*, New York, Palgrave/Macmillan, 2016.

[5] David E. Pozen (2005). "The mosaic theory, national security, and the freedom of information act", *The Yale Law Journal*, vol. 115, n° 3, 2005, pp. 628-679.

[6] Paul Kockelman, "The anthropology of an equation. Sieves, spam filters, agentive algorithms, and ontologies of transformation", *HAU: Journal of Ethnographic Theory*, vol. 3, n° 3, 2013, pp. 33-61.

will also explore the variety of *arts de faire* deployed by users to “hijack” [*détourner*][7] existing encryption tools and develop their own ways to conceal themselves.

This article seeks to contribute to, and draws from, several sets of literature. In addition to the already-mentioned infrastructure studies, a subfield of science and technology studies (STS), our findings speak to a number of fields and sub-fields investigating the relationship between privacy, surveillance, security and digital tools. First of all, our approach in this paper owes greatly to the interdisciplinary work that, in the last fifteen years, has explored the “collective” dimension of privacy and the extent to which protecting it requires the interdependency of multiple factors and actors. For instance, Daniel Solove has described the ways in which the contours of social representation online are gradually identified as a result of the informational traces left behind by different interactions, dispersed in a variety of databases and networks[8].

These traces are at the core of both states and corporations’ attempts to track and profile citizens and users, and activists’ strategies to expose corporate and state malfeasance; thus, successfully preserving one’s privacy in the connected world is about managing visibilities[9]. Along the same lines, placing emphasis on the ways in which users can be active actors of their own privacy, Antonio Casilli has shown how the right to privacy has turned into a “collective negotiation” whose main objective is to master one’s projection of self in social interactions with others[10]. Dourish and Anderson sum up well the core message put forward by this approach to privacy and security when they suggest that these are “difficult concepts to manage from a technical perspective precisely because they are caught up in larger collective rhetorics and practices of risk, danger, secrecy, trust, morality, identity, and more”, and argue that we should move “toward a holistic view of situated and collective information practice”[11].

Surveillance studies have also paid specific attention to the collective and relational dimensions of surveillance, privacy and security. Authors interested in exploring the concept of resistance have underlined the algorithmic and “rhizomatic” nature of new surveillance practices and the responses needed to counter them[12]; others show how a traditional conceptualization of surveillance, that of an exclusive relationship between the surveillant and his object, do not take properly into account the “surveillant assemblages” (and those that seek to respond to surveillance) that are currently on display

[7] Michel Callon, “The Sociology of an Actor-Network: The Case of the Electric Vehicle”, in Michel Callon, John Law and Arie Rip (eds.), *Mapping the Dynamics of Science and Technology: Sociology of Science in the Real World*, London, Macmillan Press, 1986, pp. 19-34.

[8] Daniel J. Solove, “A Taxonomy of Privacy”, *University of Pennsylvania Law Review*, vol. 154, n°3, 2006, pp. 477-560.

[9] Mikkel Flyverbom, Paul M. Leonardi, Cynthia Stohl, Michael Stohl, “The Management of Visibilities in the Digital Age”, *International Journal of Communication*, n°10, 2016, pp. 98-109.

[10] Antonio Casilli, « Quatre thèses sur la surveillance numérique de masse et la négociation de la vie privée », in *Rapport du Conseil d’Etat*, 2015, pp. 423-434.

[11] Paul Dourish and Ken Anderson, “Collective information practice: exploring privacy and security as social and cultural phenomena”, *Human-computer interaction*, vol. 21, n°3, 2006, pp. 319-342.

[12] Aaron Martin, Rosamunde van Brakel and Daniel Bernhard, “Understanding Resistance to Digital Surveillance: Towards a Multi-Disciplinary, Multi-Actor Framework”, *Surveillance & Society*, vol. 6, n°3, 2009, pp. 213-232.

in networked media, and are transforming the targets and the hierarchies of surveillance activities at the same time as they reconfigure the notion of privacy[13].

Methodology

This article builds upon an eighteen-months-long and ongoing fieldwork conducted as part of the NEXTLEAP (Next-Generation Techno-social and Legal Encryption, Access and Privacy, nextleap.eu) H2020 research project on privacy-enhancing technologies. We have conducted 52 in-depth self-structured interviews with high-risk and low-risk users from Western Europe, Russia, Ukraine and Middle Eastern countries, as well as with trainers and authors of encryption tools[14]. We also observed informational security trainings, where users, trainers, developers and privacy activists conduct risk assessment and construct what is called a "threat-model".

When we started our fieldwork in September 2016, we aimed at developing three case studies of end-to-end encrypted messaging and email in depth (namely, Signal, LEAP/Pixelated and Briar). However, we quickly understood that these projects could hardly be singled out with respect to their connections with other initiatives in the field of encrypted messaging and email. In fact, the underlying protocols used by these three projects (such as Signal protocol, for example) gave birth to a number of implementations, forked or actively interacted with various applications in the field. We thus decided to follow the three projects as they grow and transform, and use them as our threads of Ariadne, respecting the loops and knots that these threads were naturally forming on their way. In the end, the study of encrypted communication of which we present a sample here more closely resembles a "portrait of an ecosystem" than a series of case studies, telling a complex story of media "intermediated" by their developers, their users, their wannabe regulators, and their technologies.

We draw from STS to analyze the interfaces of messaging apps as "meeting points" between the intentional goals of developers and the needs of users[15]. We aim at problematizing[16] encryption as an emerging system and community of practice, doing fieldwork-driven "analytical thick descriptions" of events and organizations to try and understand the life of a technical artifact, from its creation to its appropriation and reconfigurations by users, to its becoming a subject of public debate, of governance, of lobbying.

[13] Kevin D. Haggerty and Richard D. Ericson, "The Surveillant Assemblage", *British Journal of Sociology*, vol. 51, n°4, 2000, pp. 605-622.

[14] More precisely, we interviewed (17) developers, experts from NGOs focused on privacy and security, such as EFF, Tactical Tech and Privacy International (3) and everyday users (32). Developers from LEAP and Pixelated (PGP), ChatSecure (OTR), Signal protocol and its implementations and forks (including Wire, Matrix-OLM and Conversations-OMEMO) were interviewed, as well as developers from Tor, Briar and Ricochet that use their own custom protocols. Within user groups we distinguish between high-risk users (14) and users (including researchers and students) from low-risk countries (18). Details about the ethics protocol and approval related to the study may be found in the NEXTLEAP deliverable 3.5, available here https://nextleap.eu/deliverables/D3.3DraftDecentralizedCaseStudies.pdf

[15] Nelly Oudshoorn and Trevor Pinch, *How users matter: The co-construction of users and technology*, Cambridge, United States, The MIT Press, 2005.

[16] Michel Foucault (J. Pearson, ed.), *Fearless Speech*, Semiotexte, distributed by MIT Press, Cambridge, MA, 2001.

Just as we seek to have a nuanced understanding of developers' motivations and the representations they have of users and their needs, in the tradition of "user studies" developed within STS, we understand users not as a homogeneous and passive group, but as active contributors participating in innovation and co-shaping technologies. In this article, we distinguish users as high-risk or low-risk, depending on their own analysis and description of their situation. Our interviews include both tech-savvy users (who become trainers and teach other users) and low-knowledge users who are nonetheless possibly in a very high-risk situation (i.e. a situation where the misuse of secure messaging would likely lead to death or high prison sentences). At first we focused on interviewing users from Western Europe, unlikely to be in high-risk situations, and moved on to "high-risk" activists and journalists from Eastern Europe and the Middle East. Our initial hypothesis was that geopolitical context would strongly influence the choice of privacy enhancing technologies, as well as the definition of threat models, resulting in a different pattern of tool adoption for high-risk users as compared to low-risk users.

Interviewed users were selected via their attendance at training events in their local environments, both high-risk and low-risk, or at conferences likely to attract high-risk users who could not have been interviewed in their native environment due to repression. This was the case for users from Egypt, Turkey, Kenya, Iran, for whom the interviews took place in March 2017 at the Internet Freedom Festival and at RightsCon. All interviews were conducted between Fall 2016 and Spring 2017, transcribed and coded around Summer 2017 – beginning of Fall 2017.

This article focuses mostly on users and digital security trainers, as they are engaged in a collective and iterative activity of "risk assessment" and "threat modelling". However, we aim to further link these efforts to our study of technical communities, in order to see how encryption protocols and tools incorporate specific profiles of "user", and specific ideas of "what is to be hidden".

"Know your enemy": threat-modelling as a tool for trainers

In design studies and software engineering, threat-modelling is considered as an inherent part of the normal design cycle where 'security needs' are understood as yet another facet of the complex design process: "We must consider security needs throughout the design process, just as we do with performance, usability, localizability, serviceability, or any other facet"[17]. When applied to the software development process, threat-modelling is defined as a "formal process of identifying, documenting and mitigating security threats to a software system"[18]. Threat-modelling enables development teams to examine the application 'through the eyes of a potential adversary' in order to identify major security risks. However, threat-modelling process and techniques are also applied to human agents, in order to find security flaws in user behavior patterns (both online and offline), identify sensitive information 'to be protected', determine potential adversaries, evaluate their capacities and propose solutions for risk mitigation and protection.

[17] Peter Torr, « Demystifying the threat modeling process, » *IEEE Security & Privacy*, vol. 3, n° 5, 2005, pp. 66-70.

[18] Ebenezer A. Oladimeji, Sam Supakkul, and Lawrence Chung, « Security threat modeling and analysis: A goal-oriented approach, » *Proceedings of the 10th IASTED International Conference on Software Engineering and Applications (SEA 2006)*, 2006, pp. 13-15.

The idea of a threat modelling applied to users instead of informational systems is related to the difficulty -- rather, the impossibility -- to "hide from everyone". As the Electronic Frontier Foundation, a leading NGO in the digital security sphere, puts it: "It's impossible to protect against every kind of trick or attacker, so you should concentrate on which people might want your data, what they might want from it, and how they might get it. Coming up with a set of possible attacks you plan to protect against is called threat modeling"[19].

Threat-modelling is linked to another instrument called risk assessment. While threat-modelling means identifying from whom a user needs to hide, risk assessment is a tool that trainers and digital security organisations use in order to analyse the possibility or chance of a threat to happen. It becomes important not only to know who to hide from, but also evaluate the chances one has to actually "meet" this adversary. While risk has been described as a cultural "translation" of danger[20], risk assessment is a "quantification of uncertainty"[21], that produces risk as something that can be "known, mitigated, increased and decreased, calculated"[22].

Our study has shown that, for digital security trainers, threat-modelling and risk assessment have become powerful instruments to narrow down and structure their trainings. Several trainings that we have observed in Ukraine and Russia used different techniques for threat-modelling. For example, the training "Digital security for activists" that took place in Saint-Petersburg, Russia, on April 10, 2016, started with the following introduction by P., the trainer:

> *"Before we start, we need to decide: from whom are we protecting? First of all, from the state. Only during last year 200 court cases were opened because of online publications, comments and so on. Second moment, we should be protecting ourselves from corporations. It may be naive to say so, but it is clear that different corporations are accumulating information, and a lot of useful services that are given to us for free but in exchange these companies are appropriating information about us. Third moment - there are other malicious agents who would like to get access to our online wallets or to hack us just for fun".*

This division between three kinds of adversaries was not only a rhetorical figure used to introduce the training: it was subsequently used all along the three-hour workshop, in order to group various privacy-enhancing tools that people might need, around the three big categories of adversaries. Structuring a training around a specific adversary means identifying the technical resources an adversary actually has, but also the extra-technical parameters, such as the legal context.

Another way of structuring a training was experimented by Ukrainian trainers V. and M., both specialized on high-risk users likely to face powerful, state-level adversaries, or may face a physical

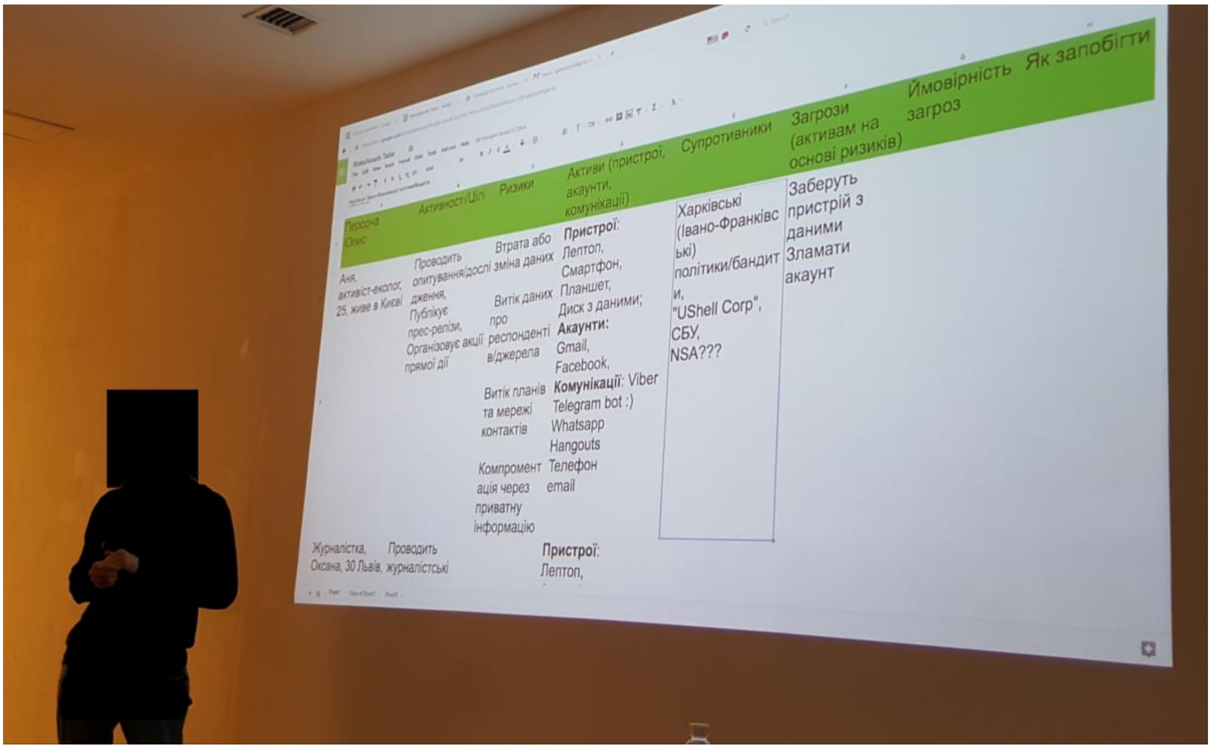
[19] https://ssd.eff.org/en/glossary/threat-model

[20] Mary Douglas and Aaron Wildavsky, *Risk and Culture*, Berkeley, University of California Press, 1982; Paulo Vaz and Fernanda Bruno, « Types of Self-Surveillance: from abnormality to individuals 'at risk' », *Surveillance and Society*, vol. 1, n° 3, 2003, pp. 272-291.

[21] Sun-ha Hong, « Criticising Surveillance and Surveillance Critique: Why privacy and humanism are necessary but insufficient », *Surveillance & Society*, vol. 15, n° 2, 2017, pp. 187-203.

[22] Theodore M. Porter, *Trust in Numbers: The Pursuit of Objectivity in Science and Public Life.* Princeton, NJ, Princeton University Press, 1995.

threat. The training, held on January 15, 2017 in Kyiv, involved the usage of a spreadsheet for participants to complete together with trainers (Figure 1).



[redacted]

Персона Опис	Активності/Цілі	Ризики	Активи (пристрої, акаунти, комунікації)	Супротивники	Загрози (активам на основі ризиків)	Ймовірність загроз	Як запобігти
Аня, активіст-еколог, 25, живе в Києві	Проводить опитування/дослідження, Публікує прес-релізи, Організовує акції прямої дії	Втрата або зміна даних Витік даних про респондентів/джерела Витік планів та мережі контактів Компрометація через приватну інформацію	**Пристрої**: Лептоп, Смартфон, Планшет, Диск з даними; **Акаунти:** Gmail, Facebook, **Комунікації**: Viber Telegram bot :) Whatsapp Hangouts Телефон email	Харківські (Івано-Франківські) політики/бандити, "UShell Corp", СБУ, NSA???	Заберуть пристрій з даними Зламати акаунт		
Журналістка, Оксана, 30 Львів,	Проводить журналістські		**Пристрої**: Лептоп,				

Figure 1. Digital security training observed in Kyiv, January 2017. The table includes the following columns (from left to right): Description of a person, its functions and activities, risks, "assets" (devices, accounts, types of communications used), adversaries, threats (applied to the assets based on risks), possibility of a threat to happen, how to avoid risks.

The training was organised as a collaborative construction of several fictional profiles (Anya, 25 years old, ecological activist; Oksana, 30 years old, journalist etc.) and identification of corresponding assets, adversaries and threats. In this way, trainers were focused not on enumerating existing privacy-enhancing tools, but on explaining a precise methodology of personalized threat-modelling. For trainers, users' ability to analyze a very concrete situation and context becomes more important than a high-level knowledge about multiple tools. Though some of the observed trainings were still centered around 'tool demonstration', the majority of trainers are largely criticizing tool-centered approach and insist on a tailored, threat-model based training:

> *'Very often trainings turn into tool-trainings. But in our work tools are not our primary and even not secondary concerns. What's primary is the evaluation of what participants need, what they already use. And only after we think of what we can suggest them to use, and again, without any hard recommendations ' you need only this tool and that's all ' . [M., informational security trainer, Ukraine].*

The digital security community is highly reflective upon its own training practices and criteria of evaluation of secure messaging applications and mail clients[23]. In recent years, a paradigm shift has occurred, bringing trainers and experts from a tool-centered approach to user-centered one, where the

[23] Francesca Musiani and Ksenia Ermoshina, « What is a Good Secure Messaging Tool? The EFF Secure Messaging Scorecard and the Shaping of Digital (Usable) Security », *Westminster Papers in Communication and Culture*, vol. 12, n°3, 2017, pp. 51-71.

user's capacities to evaluate their own threat model become crucial. As the famous EFF's guide "Surveillance Self-Defense" puts it, "trying to protect all your data from everyone all the time is impractical and exhausting. But, do not fear! Security is a process, and through thoughtful planning, you can assess what's right for you. Security isn't about the tools you use or the software you download. It begins with understanding the unique threats you face and how you can counter those threats"[24].

This shift also results in a change of methodology used to rank, evaluate and recommend secure communication tools. One of the examples of this is the revision of the famous EFF's Secure Messaging Scorecard, that have been used as a quasi standard-setting instrument by a large community of trainers, users and technologists[25]. Bringing users and their self risk-assessment in the center had an impact on digital literacy practices and the development of a new sort of guide, such as Security Self-Defense. In this kind of guide, a tool is never good 'in itself', from a purely cryptographic point of view, but should always be considered in the specific context of use:

> *The key to the guide that we've created is that we want people to start with understanding their own personal situation, so their threat-model, rather than saying them just use these tools, I don't think that's a productive guide. [...] WhatsApp for example, it has end to end encryption. It may be good for an average person to just keep using that if they are already using it and learn how to use it well and correctly. But I think other people have much more extreme threat-models and have to use more secure tools'. [EFF]*

This 'tailored approach' to security trainings is also relevant because of a number of unsolved cryptographic problems currently discussed by the security community, such as metadata storage, vulnerabilities of centralized infrastructures, usage of telephone numbers as identifiers and so on. In the absence of a 'perfect tool', trainers recommend patchworks of different tools and operational security practices ("physical security") that aim at minimizing the drawbacks of existing tools and offer different features, from encryption «in transit» to encryption «at rest», metadata obfuscation and so on. Threat-modelling is a practice that helps to fix some of the unsolved technical problems:

> *Not everyone has to put a tin foil hat and create an emergency bunker. Lots of people do, but not everybody. Tailoring it to the right people. I think that would be great to have an app that we would recommend to everyone because it's usable and easy, popular and secure and everything else but since it's not there I think it's useful to tailor things, tailor the threat model. [EFF]*

For a specific threat-model, extra-cryptographic factors, such as low learning curve, peer pressure or network effect may be more important than technical efficiency of a cryptographic protocol. Thus, trainers in Ukraine would often advice their high-risk users to use WhatsApp and Gmail instead of Signal and a PGP-encrypted email, as "everyone already uses it and knows how it works", so the adoption of these tools will happen quicker and with less mistakes. Thus, time and learning curve become additional factors to recommend a specific tool. The shift to a user-centered threat-modelling in the digital security training community has an important impact on the evaluation, ranking and recommendation of privacy-enhancing tools; the latter giving importance to the non-cryptographic

[24] https://ssd.eff.org/en/playlist/academic-researcher#assessing-your-risks

[25] Musiani & Ermoshina, 2017, *cit.*

features of a tool, and suggesting combinations of tools and operational security techniques as "compensation" for unsolved academic cryptography problems.

From "nothing to hide" to "tinfoil hat freaks": continuum of risk levels

Aside from trainers and digital security experts, users develop their own methods to evaluate their risks, and invent specific *ad hoc* practices of digital self-defense. However, even after the Snowden revelations, a very important percentage of European citizens share the idea that they have "nothing to hide", thus considering the mere fact of concealing online traces as an indicator of criminal activity. A recent study focused on the "general public" has revealed a certain state of apathy: "though online users are concerned and feel unease about the mass collection of their personal data, the lack of understanding as to how such data is collected as well as a sense of powerlessness leads to the public's resignation and apathy"[26].

The "nothing to hide" argument has been widely criticized by the security community, resulting in the production of a variety of cultural content and online tutorials in order to increase the awareness of the "general public" about digital security[27]. These contributions fuel the ongoing debate about the thin line separating targeted surveillance and mass surveillance, as well as high-risk and low-risk users. Hiding from governments would also imply hiding from corporations, and vice versa: the image of the "adversary" becomes much more complex and hybrid while the traditional opposition between "privacy" and "security" is more and more questioned.

While the vast majority of user studies in usable security have been conducted with subjects from the "general population" (namely, university students), our research has given slightly different results regarding users awareness and concerns in privacy. Indeed, we have classified the interviewed population according to 2 axes, individuals' knowledge about technologies and their risk situation, thus obtaining four groups. Within the so-called 'high-knowledge, low risk' group the awareness of privacy and security related risks was very high, however, the adopted user behavior was not holistically secure: a large number of tech developers or trainers was using unencrypted email and text messaging applications.

For example, while recent research in usability showed that Telegram was suffering from a number of important usability and security problems[28], Pirate Party activists, themselves software developers, system administrators or hosting providers, are using Telegram on a daily basis (the group of Pirate Party Russia on Telegram counts 420 users as on October 24, 2017). Telegram group chats remain popular among high-risk and high-knowledge users despite the fact that encryption for group chat

[26] Arne Hintz and Lina Dencik, « The politics of surveillance policy: UK regulatory dynamics after Snowden, » *Internet Policy Review*, vol. 5, n° 3, 2017. DOI: 10.14763/2016.3.424

[27] Among recent attempts, the documentary "Nothing to Hide": http://www.allocine.fr/video/player_gen_cmedia=19571391&cfilm=253027.html

[28] Ruba Abu-Salma, Kat Krol, Simon Parkin, Victoria Koh, Kevin Kwan, Jazib Mahboob, Zahra Traboulsi, and M. Angela Sasse, « The Security Blanket of the Chat World: A Usability Evaluation and User Study of Telegram, » in Internet Society (ed.), *Proceedings of the 2nd European Workshop on Usable Security (EuroUSEC)*, Paris, France, 2017.

offered in Telegram is very basic. However, other tactics of self-defense are used, such as self-censorship (avoiding to talk about specific topics) and pseudonymisation (avoiding real profile photos and usernames).

Surprisingly, according to the interviews, there is no strict correlation between users' threat models, level of technical knowledge, security features of a tool[29] and adoption dynamics. Other extra-cryptographic and extra-security features may become arguments for adoption of a specific tool. In the case of Telegram, it is interesting to observe how the actual cryptographic protocol and security and privacy properties lose their importance for users, compared to the features of the interface and to the reputation of the app's creator. The trust in Telegram, according to our interviews, is not in the technology, but in the person and his political position:

> *"User1: Maybe you should not discuss that over Telegram?*
> *User2: Why not? Pashka Durov will never give away any of our data, he does not care about Russian police" [from online discussion in a group chat "Soprotivlenie" [Resistance], posted on June 11, 2017]*

Within high-risk and low-knowledge populations, however, the awareness of risks regarding privacy issues (such as the necessity to use privacy-preserving browser plugins) was not absolute while the behavior related to email and messaging was estimated as more important. Even if these users could not always clearly describe possible attack vectors, they had a very multi-faceted and complex image of who their adversary was. This was clearly expressed in the drawings collected during interviews and observed workshops (Figure 2).

[29] Such as key length and key generation algorithm.

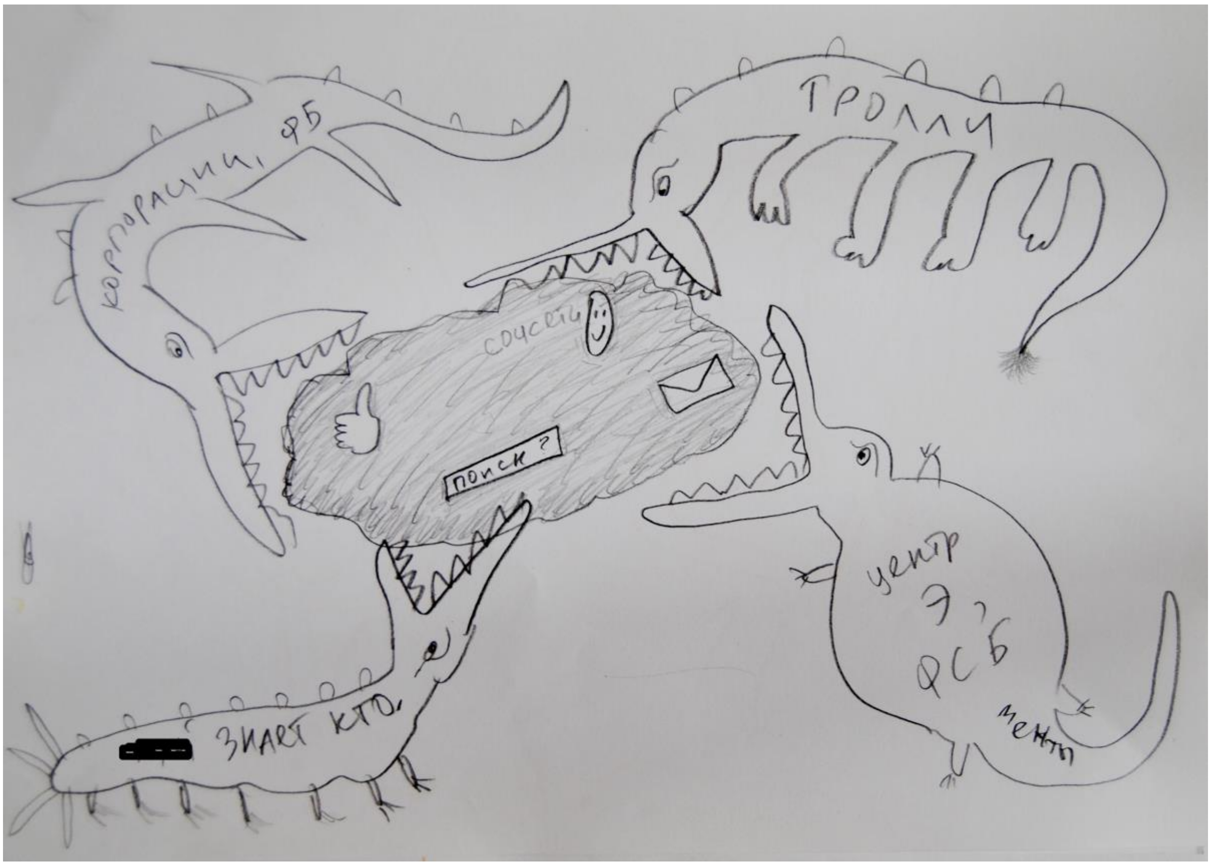


*Figure 2: user representation of "insecure communications". Drawing collected during a digital security workshop in Saint-Petersburg, April 2017. Female, activist of a feminist collective. On the "crocodiles" (from left top clockwise): "Corporations, Facebook; Trolls; Center against extremism, FSB, police; Who the f**k knows". On the cloud: "Search; Social networks").*

'Low-knowledge, high-risk' users have deployed specific, often unique and personal, methods to protect communications and information that present an assemblage of different tools and practices, both in offline (social engineering, operational security or "*opsec*") and online behavior (Figure 3).

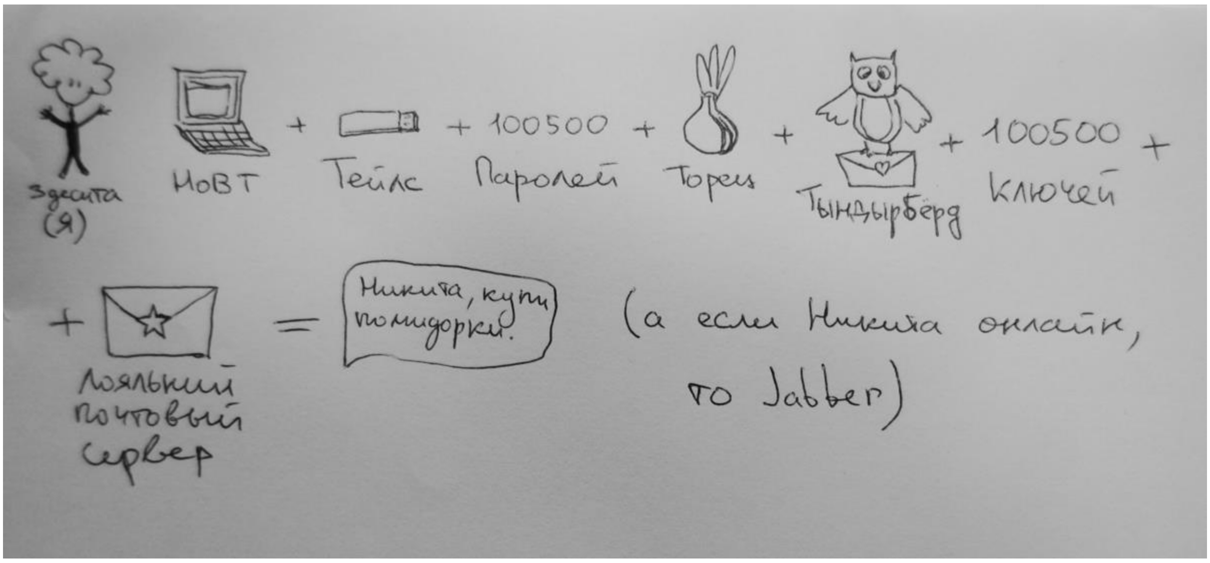


Figure 3. User representation of "secure communications". Drawing collected during a digital security workshop in Saint-Petersburg, April 2017. Female, antifascist activist. From the left: "Me: laptop + Tails + 100500 passwords + Tor +

Thunderbird + 100500 keys + trusted email provider = message "Nikita, could you buy some tomatoes please?" (And if Nikita is online, than Jabber)"

For instance, high-risk users in Russia and Ukraine, namely left-wing activists who have been facing police threats and targeted surveillance between 2012 and 2017, are widely using the so-called "one-time secrets", special web-based pastebins or pads that say to be zero-knowledge and destroy messages once read[30]. As these users describe, the main threat for them consists in their devices being seized. Thus, according to them, a self-destroying link is the most secure way to communicate, even though the links are often sent via unsecured channels, such as Facebook Messenger. These users prefer combining a mainstream messaging tool such as Facebook, and self-destroying links, instead of a more activist-targeted application such as Signal.

Secure messaging is a vibrant and rapidly developing field[31], and the multitude of messaging apps is echoing the variety of user behavior and risk assessment practices. In fact, users perceive themselves not as a single identity but as a set of "profiles" or "personas": daughter, journalist, lover, activist, colleague… Every role, according to users, may require a specific digital self-care or a specific set of tools. These different personas imply a specific online behavior pattern, thus creating what is called "*security by compartmentalization*".

Users use different messaging apps for different groups of contacts, according to the perceived level of risk. Even some of our high-risk interviewees report that they use WhatsApp or Facebook Messenger for work and family relations, while preferring PGP-encrypted email, Signal or Privnote for activist-related contacts. Some prefer to move all the communications to a single application, but say to have a hard time convincing relatives to change their online behavior ("digital migration problem") or face compatibility problems (for example older phones can not run Signal).

By consequence, when applied to digital security, risk is a relational and socially-defined concept, as it highly depends on user's social graphs and communication context. A high-risk user from Ukraine, involved in a collective for support of political prisoners, explains:

> *"My risk is always connected to the risk of other people. I do not want to use my mobile phone to connect to my activist account, as it will be possible to connect the two. And even if I think that I have not done anything, other people have reasons to hide themselves. And finally... I never know when someone comes after me. Predicting future is not wise. Khodorkovsky just before his arrest also said that no one was interested in him".*

In this sense, the difference between low-risk and high-risk users is very context-dependent, and always moving: a low-risk person in contact with high-risk ones has to heighten her level of security and may herself become high-risk. As a user from Austria, a festival organizer self-identifying as a low-risk person, puts it:

[30] The most popular services are "One Time Secret" (https://onetimesecret.com/) and Privnote (https://privnote.com/)

[31] Ksenia Ermoshina, Francesca Musiani and Harry Halpin, « End-to-end encrypted messaging protocols: An overview, » in Franco Bagnoli et al. (eds.), *Proceedings of the Internet Science Third International Conference*, INSCI 2016, Florence, Italy, 12–14 September, Berlin, Springer, 2016, pp. 244–254.. DOI: https://doi.org/10.1007/978-3-319-45982-0_22

> *"I work on a festival which is all about generating outreach. And I adapt to the people I invite or strategize projects with. So the risk of my communication is related to the risk the people take I am talking to. So for example with [X], [Y][32] or others I always encrypt everything of course and I also always check if a guest I am inviting has a public key on a keyserver so I start communication encrypted [...] Enemy? Lots of my guest speakers have serious enemies; so I again adapt to that".*

This "compartmentalization" approach to security also results in some hardware-based user bricolages or tinkering, from the more popular "dual-boot" (combining an "activist" and a "normal" OS on the same machine), to more sophisticated hidden containers or hidden operational systems. This user behavior and user-driven practices of "security by compartmentalization" have been recently incorporated *by design* in a project named Qubes, an operational system based on a multitude of virtual machines creating isolated working environments that let users coordinate and manage different "parts" of their online identities that may require different security levels and needs.

However, risks and threat-models are also evolving over time. Not only are they dependent on users' relational networks, but also on the supposed reactions and behavior of "the adversary". Thus, for this high-risk and high-knowledge user from Greece, it is important to constantly reinvent the everyday security practices:

> *"According to the act or what I do I have a specific OPSEC. I remember the main steps by heart, though I don't use the same practices every time as once used a specific methodology then it's burned. Depending on the place I try to masquerade to the common practices of this area rather than blindly improvise. The adversary is always learning from me and from trusted people or friends that are not careful enough".*

Not only the distinction between high-risk and low-risk should be questioned, but also the definition of sensitive and insensitive data. Religion, morality, gender become important parameters that influence the definition of what "sensitive information" is. For example, our interviews with Middle Eastern users show that one of the most important "adversaries" from whom Muslim women have to hide is their own partner or family member. As one of our interviewees, a twenty-seven-year-old Iranian woman, explains, photos of a non-religious wedding can become as sensitive as political critique, and can bring the person sharing them photos to a high-risk level. Thus, it is not the type of information itself that defines high-risk, but the user's broader context; threat-models and risk levels appear to be gender and culture-dependent.

"If you use that tool, you have something to hide": paradoxes of mass adoption of encryption

According to our fieldwork, open-source and licensing choices are less covered in high-risk trainings, as high-risk users do not always associate open-source with security. Open-source was perceived as a less important criterion in the context of an immediate physical threat, as when a proprietary but "efficient" and "easy to explain" solution exists, trainers will give priority to it. For example, in Ukraine, WhatsApp is the most recommended application, because it is considered easy to install. Trainers

[32] Mentioning two important and well-known tech and human rights activists.

consider WhatsApp's proprietary license and collaboration with Facebook in terms of metadata less important than users' perception of immediate security. The primary task in high-risk contexts with low-knowledge users is to help them to quickly abandon unencrypted tools, as well as tools that collaborate with their adversaries.

> *"Since WhatsApp adopted end-to-end encryption, we usually do not spend that much time on instant messaging encryption [during trainings], and recommend to stay with WhatsApp if people already use it. So they can still communicate with all of their friends, and also… it looks familiar, and it does not shock. And people say [during trainings] if they use WhatsApp it's less suspicious than if they use a special app for activists" [I., female informational security trainer, Ukraine]*

This quote mentions an important concern addressed by a number of interviewed users, and observed during cryptoparties and informational security trainings: *does the very fact of using an activist-targeted app constitute a threat in itself?* This refers to the famous "Cute Cat Theory of Digital Activism" by Ethan Zuckerman[33], according to which it is safer and easier for activists to use the same mainstream platforms as those used for sharing "lolcats" pictures, whereas using a tool marked as "activist" may put users under targeted (and thus, easier and cheaper) surveillance.

This concern reveals a shared (but often underexplored) users' anxiety over their "metadata" (even though this particular term is not always used explicitly). Often, in our interviews, we were confronted to an extensive critique of all the existing tools by both informational security trainers and non-technical users. This echoes the findings of another recent usability study of end-to-end encryption tools, stating that "most participants did not believe secure tools could offer protection against powerful or knowledgeable adversaries"[34]. An important number of users mentioned as a reason for not adopting encryption the fact that their social graphs and "activist" lifestyle were exposed to adversaries because of the usage of specific tools. A Russian user also mentioned the opposite effect (using an activist-targeted tool as means of "earning trust"), with a story on an undercover police officer using a @riseup.net email account as one of the means to penetrate a student movement mailing list during mass protests in 2011-2012.

The quintessence of this "tool-scepticism" may be illustrated with a drawing (Figure 4) authored by one of our respondents, a European high-risk journalist working on war conflicts in Middle Eastern countries.

[33] http://www.ethanzuckerman.com/blog/2008/03/08/the-cute-cat-theory-talk-at-etech/

[34] Abu-Salma et al., 2017, *cit.*, p. 2.

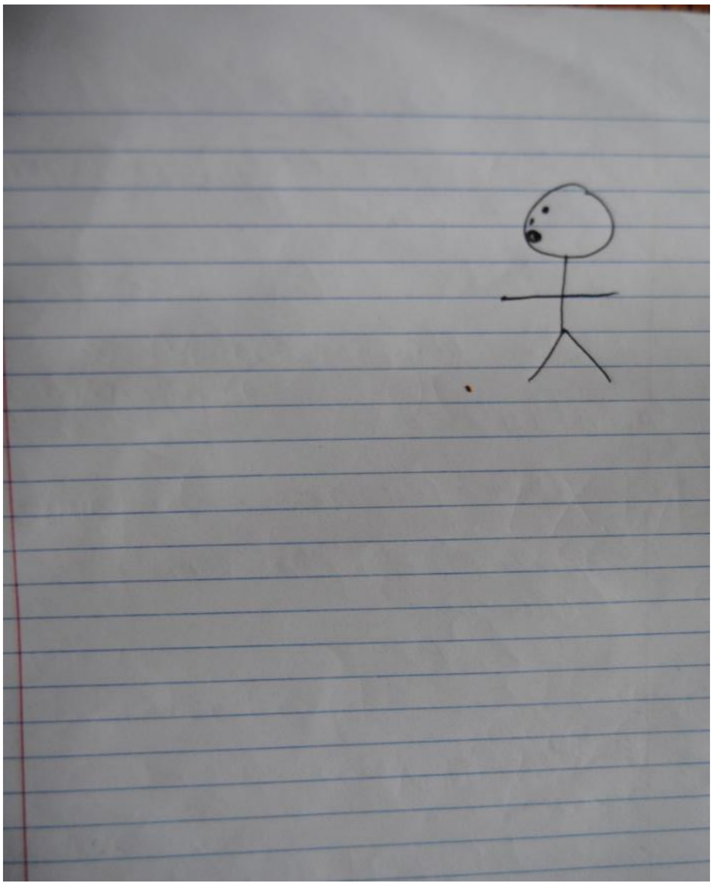


Figure 4. Drawing collected during the interview on February 16, 2017.

The user commented the drawing in this way:

> *"In case of a truly secure communication I say something but no one knows what I said and to whom [...] I could have just given you a blank sheet of paper, it would have meant that no traces of a communication act are visible. But as soon as you asked me to draw you something…" [C, male, journalist, high-risk]*

The adoption of encryption by "mainstream" messaging applications (as opposed to "activist-targeted" applications) leads to a specific effect that our respondents called "fish in the sea":

> *"Imagine if I have nothing to hide, but I still use an end-to-end encrypted app, then people who need to hide themselves... like whistleblowers for example... it will be easier for them, say, to disappear in this big flow of cat photos or love messages. So I feel like I am helping someone when I use encryption all the time for all of my communications". [female, low-risk user, tech-journalist, Austria]*

An interesting phenomena of "shared responsibility" arises from the mass adoption of encryption: according to the "fish in the sea" metaphor (used in the sense of "one among many similar entities" in a wide space, that can protect one another by mutual concealment), the more users opt for end-to-end encryption tools, the more secure it becomes for everyone to use these tools, but specifically for high-risk users, whose life and freedom depend on these tools. While mass adoption of distributed or peer-to-peer apps has a real technical correlation between number of users and privacy protection level (example: Pond or Tor), for centralized apps (like Signal and WhatsApp) or for email encryption the consequences of mass adoption are often described from a "social" or economic standpoint:

> *"The more people use encryption, the more expensive it will be for the governments to read everything. It's not about reaching 100% security… This simply does not exist! It's about making them waste their time and money to decrypt our stuff and in the end they are reading something like 'Let's go eat pizza tonight'…" [male, informational security trainer, Ukraine]*

Even though the collaboration of Moxie Marlinspike, head developer of Signal, with WhatsApp and Facebook was subject to controversies and critiques among a number of tech-savvy FLOSS (Free Libre Open Source Software) circles, mass adoption of end-to-end encryption had an important impact on Internet governance. A critical discourse bridging encryption and terrorism was also present in mass media and at important community gatherings as Internet Freedom Festival or RightsCon, where specific sessions on regulation of encryption were held in 2017, bringing together representatives of technical community and EU and international regulators.

After bringing strong cryptography in mainstream messaging applications such as WhatsApp, the thesis of "encryption as a human right" and a demand for "equal access to encryption" have become more widespread. The most recent initiative has been a letter signed by 65 privacy-focused NGOs (including Privacy Now, EFF and Article 19) and addressed to the UN on September 19, 2017, with a demand to decriminalize users of privacy-enhancing technologies and digital security trainers[35]. Privacy and the right to conceal are presented as part of the freedom of opinion and expression:

> *"Discussions of encryption and anonymity have all too often focused only on their potential use for criminal purposes in times of terrorism. But emergency situations do not relieve States of the obligation to ensure respect for international human rights law <...> General debate should highlight the protection that encryption and anonymity provide, especially to the groups most at risk of unlawful interferences"[36].*

Developers and information security trainers underlined the urgency to find a reliable solution to the metadata collection problem, and stated that no current solution in the field of end-to-end encrypted instant messaging apps actually offers good metadata protection. Developers and trainers associated the leaking of metadata with centralization:

> *"Metadata connects you weirdly with other people, and there's more sense in the metadata than in the data itself for technological reasons [...] No one from the messaging apps is trying to solve that. Instead they suggest to sync your address books so they know exactly who you're talking to even though you trust them to somehow make it into hashes or whatever. That's the issue we are not solving with the apps, we make it worse. We now have centralized servers that become honeypots, and it's not about the data, it's about the metadata" [Peter S., Heml.is].*

[35] https://www.ifex.org/turkey/2017/09/19/apc_ifex_hrc36_4_statement/

[36] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, published on May 22, 2015 and presented on June 17, 2015 https://www.eff.org/deeplinks/2015/06/strong-encryption-and-anonymity-are-guardians-free-expression

Towards a deconstruction of the privacy-security dichotomy

When we first attempted to interpret our fieldwork, our hypothesis was to distinguish high and low risk users, who would have very distinct threat-models. However, our fieldwork has shown the limits of this opposition, demonstrating the relativity of the traditional binary vision that opposes privacy and security: these two concerns, and related defensive practices, are in fact interpenetrating.

Indeed, citizens of low-risk countries were more concerned with privacy-related issues, while individuals at high-risk focused on urgent needs and life-and-death situations, sometimes adopting technical solutions that are easier to install and use, even if they do not, in fact, display strong levels of privacy protection (like WhatsApp). The critique of GAFAM[37], the Net's giants, is mostly spreading among high-knowledge Western users, while high-risk users shared the idea that Gmail, for example, offers a better security-usability ratio. In the context of urgency, the compromise is between user-friendliness and security, while technically experienced low-risk users develop genuinely complex and multilayered privacy and security preserving toolkits.

However, some of the anti-GAFAM debates that have originated within the FLOSS community have touched larger, non-technical populations in high-risk countries. An example is the famous controversy about Signal's Google Play and Google Services dependencies[38], which originated within free software circles with the launch and quick shutdown of the project LibreSignal[39]. The Google dependencies of Signal became a problem for a specific user community, both privacy-aware and tech-savvy, who opt for decentralized and anti-GAFAM communication tools. In this context, the choice of a "Google-free" messenger can also be perceived as a "lifestyle" choice. We have noticed that this choice often coexists with alternative hardware choice (Linux phone, Fair Phone, Copperhead OS or other privacy enhancing tools), or Google Play-free customized Android. As a tech-savvy user puts it:

> *"If I don't like mainstream in media, if I don't like mainstream in music – why would I like mainstream on my computer?" [Daniel, mail service provider, festival organizer]*

However, according to our interviews, the Google Play dependencies in Signal had an important impact not only on tech-savvy low-risk users, but also on high-risk low-knowledge users -- for example, in Syria, because of the country-wide blocking of Google Play. Technical decisions made by developers of privacy-enhancing technologies, such as dependencies on third-party libraries, licensing and protocol choices, are not only an issue of preference or life choice, but may impact users' security in life-and-death contexts.

High-risk users also mentioned the decentralization of networks, that was considered for a long time as a "high-tech, low-risk" concern, as an issue important for their threat-models. Our recent exchanges

[37] GAFAM – Google, Apple, Facebook, Amazon and Microsoft. Also known as « GAFA » (Microsoft put aside), or « Big Five » tech companies.

[38] https://github.com/WhisperSystems/Signal-Android/issues/127

[39] https://github.com/LibreSignal/LibreSignal

with Russian and Ukrainian left-wing activists have shown a growing concern by these populations to be able to run their own infrastructures (servers) for storage of their files and for a decentralized communication.

On their end, federated models find their adepts in the context of state-level censorship, where centralized servers can be easily blocked. For example, our analysis of the Russian context shows that messaging solutions based on the XMPP protocol[40] are now experiencing a rebirth in response to the growing control of online communications by the state. A recent law project (25 May 2017) proposes to ban usage of anonymous messaging by obliging instant messaging applications to guarantee user authentication via phone numbers. Several messaging services have since been blocked in Russia, such as WeChat, Zello (massively used by the Russian truck drivers movement), Line and Blackberry. In this context, we observed growing interest of Russian users to XMPP/OTR as alternative to centralized systems.

Conclusion

The “dangerous liaisons” between private actors and governments[41], unveiled in particular by the Snowden revelations but existing way before that, undermine the distinction between the privacy and security paradigms -- and may even make such distinction dangerous. In this sense, hiding from governments also supposes changing consumer habits and migrating from closed-source platforms with business models based on user data. In this context, the “adversary” resembles a constantly-evolving, fluid network connecting with both private and governmental infrastructures, rather than a single entity with well-defined capacities and a pre-determined set of surveillance and attack techniques and tools.

Trainers and digital security organisations are shifting towards a user-centered approach and user-tailored trainings. However, privacy-preserving tools do not guarantee absolute security. Unsolved cryptographic challenges, such as building usable metadata-preserving solutions, are somehow “compensated for” by a patchwork of operational security techniques and combination of tools that users invent and constantly modify. Thus, the identification of “who we must conceal from” -- the processes of threat-modelling and risk assessment -- is a constantly-changing process that depends upon a large set of often non-technical or non-cryptographic parameters, such as a user’s social graph, gender, religious or ethical norms, political regime, profession, geopolitical situation, or the reputation and charisma of app creators.

In this sense, encrypted messaging speaks to the concept of intermediality, as the set of processes that contribute to bring a medium into existence by “resorting to institutions that allow for its efficiency, and material supports that determine its effectiveness[42]”. Indeed, encrypted communication is the product, and sometimes the catalyst of change, of a vast network including institutions (or actors positioning themselves in opposition or resistance to them) and of course, myriad infrastructures and technical *dispositifs* in which concepts such as security and privacy are embedded.

[40] https://xmpp.org/

[41] Francesca Musiani, « Dangerous Liaisons? Governments, companies and Internet governance », Internet Policy Review, n° 2, vol. 1, 2013, DOI: 10.14763/2013.1.108

[42] Éric Méchoulan, « Intermédialités : le temps des illusions perdues », no. 1 « Naître », 2003, p. 10

The very distinction between high-risk and low-risk, while useful operationally for the researcher as a practical methodological tool in order to diversify respondents and build a diverse sample of users for interviews, shows its limits, mainly due to the ‘relational’ nature of risk we have explored in this article. Having at least one high-risk user in her social graph, a low-risk user may adopt a higher level of protection and even install a specific tool for communicating with this contact -- and inversely, in a specific socio-political context, low-risk data (or a priori non-sensitive data) may put its owner in a high-risk context. Indeed, if designing privacy-enhancing tools requires imagining the “worst of the possible worlds”, this world may well be that of the individual who, among our contacts, is in most need of concealing. The ongoing turn to “mass encryption” would do well to take this into account.