Intermédialités
Histoire et théorie des arts, des lettres et des techniques
Intermediality
History and Theory of the Arts, Literature and Technologies

Hiding from Whom?
Threat Models and In-The-Making Encryption Technologies

Ksenia Ermoshina and Francesca Musiani

Number 32, Fall 2018

cacher
concealing

URI: https://id.erudit.org/iderudit/1058473ar
DOI: https://doi.org/10.7202/1058473ar

See table of contents

Publisher(s)

Revue intermédialités

ISSN

1920-3136 (digital)

Explore this journal

Cite this article

Ermoshina, K. & Musiani, F. (2018). Hiding from Whom? Threat Models and In-The-Making Encryption Technologies. *Intermédialités / Intermediality*, (32). https://doi.org/10.7202/1058473ar

Article abstract

Following Edward Snowden's 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. In this article, 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 which data to conceal, and how to conceal 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.

Hiding from Whom? Threat Models and In-The-Making Encryption Technologies[1]

Ksenia Ermoshina
Francesca Musiani

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 without realizing it.[3] While the mantra "I have nothing to hide" is still widespread among Internet users, mass adoption of encryption has important sociotechnical consequences for those whose lives depend on strong cryptographic protocols, because of their risk-related profession or the political context in which they live. In response to these different use-cases, the dynamic and vibrant field 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, OTR, and 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 aspects of their online identities.

[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] According to Gill, Israel, and Parsons, "[e]nd-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" Lex Gill, Tamir Israel, and 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 (accessed 20 October 2018).

[3] Cade Metz, "Forget Apple Vs. The FBI: WhatsApp Just Switched On Encryption for a Billion People", Wired, 4 May 2016, https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/ (accessed 15 November 2018).

Research Questions and Theoretical Framework

¶2 Our online traces are multilayered and embedded in the material infrastructure of the Internet. Our identity can be disclosed not only through the content of our messages, but also through the unique identifiers of our hardware devices (such as MAC addresses), our IP addresses, and other related metadata,[4] thus contributing to the "turn to infrastructure" in privacy and its governance.[5] Which of our multiple online identifiers can be considered personal? Which data should we hide, and from whom? Referring to the "mosaic theory,"[6] when does a combination of several items of *a priori* un-identifying information construct a degree of personalization sufficient to de-anonymize a user?

¶3 Drawing upon previous work, such as the anthropology of spam filters,[7] we understand cryptographic systems as sieves separating 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. The identification of what is known as a "threat model" serves to agree upon an appropriate threshold of anonymity and confidentiality for a particular context of usage. Thus, interesting questions arise, which are the main research questions this article seeks to address: How do different users define who their adversary is? How do they agree—if they do 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?

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

[4] Metadata is usually defined as information about information.

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

[6] David E. Pozen, "The Mosaic Theory, National Security, and the Freedom of Information Act," *The Yale Law Journal*, 2005, no. 115, p. 628–679.

[7] Paul Kockelman, "The Anthropology of an Equation. Sieves, Spam Filters, Agentive Algorithms, and Ontologies of Transformation," *HAU: Journal of Ethnographic Theory*, 2013, vol. 3, no. 3, p. 33–61.

doing deployed by users to *détourner*[8] existing encryption tools and develop their own ways of concealing their identities.

¶5 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. 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 its protection requires the interdependency of multiple factors and actors. For instance, Daniel Solove has described the ways in which the contours of social representation online can be gradually identified as a result of the informational traces left behind by different interactions, dispersed in a variety of databases and networks.[9] These traces are at the core of attempts by states and corporations to track and profile citizens and users, as well as of activists' strategies to expose corporate and state malfeasance; thus, successfully preserving one's privacy in the connected world is about managing visibilities.[10] 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.[11] 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."[12]

---

[8] 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, p. 19–34.

[9] Daniel J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, vol. 154, no. 3, 2006, p. 477–560.

[10] Mikkel Flyverbom, Paul M. Leonardi, Cynthia Stohl, and Michael Stohl, "The Management of Visibilities in the Digital Age," *International Journal of Communication*, no. 10, 2016, p. 98–109.

[11] Antonio Casilli, "Quatre thèses sur la surveillance numérique de masse et la négociation de la vie privée," *Rapport du Conseil d'État*, 2015, p. 423–434.

[12] Paul Dourish and Ken Anderson, "Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena," *Human-Computer Interaction*, vol. 21, no. 3, 2006, p. 319–342.

¶6 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.[13] Others show how a traditional conceptualization of surveillance, that of an exclusive relationship between the surveillant and his or her object, do not take properly into account the "surveillant assemblages" (and those that seek to respond to surveillance) that are currently on display 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.[14]

Methodology

¶7 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[15]) H2020 research project on privacy-enhancing technologies. We have conducted fifty-two in-depth self-structured interviews with high-risk and low-risk users from Russia and Ukraine and from countries in Western Europe and the Middle East, as well as with trainers and authors of encryption tools.[16] We also observed informational security trainings where users, trainers, developers, and privacy activists conducted risk assessment and constructed threat models.

¶8 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

13 Aaron Martin, Rosamunde van Brakel, and Daniel Bernhard, "Understanding Resistance to Digital Surveillance: Towards a Multi-Disciplinary, Multi-Actor Framework," *Surveillance & Society*, vol. 6, no. 3, 2009, p. 213–232.

14 Kevin D. Haggerty and Richard D. Ericson, "The Surveillant Assemblage," *British Journal of Sociology*, vol. 51, no. 4, 2000, p. 605–622.

15 To learn more about the project, see nextleap.eu (accessed 20 October 2018).

16 "We interviewed 17 developers, 3 experts from NGOs focused on privacy and security, such as EFF, Tactical Tech and Privacy International, and 32 everyday users. 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 14 high-risk users and 18 users (including researchers and students) from low-risk countries" Ksenia Ermoshina and Francesca Musiani, *NEXTLEAP deliverable 3.3. Draft Decentralized Case Study*, p. 6.

protocols used by these three projects (such as the Signal protocol, for example) brought forth 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 Ariadne's thread, respecting the loops and knots that it was naturally forming on its 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, and tells a complex story of media that are "intermediated" by their developers, users, wannabe regulators, and technologies.

¶9 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.[17] We aim at problematizing[18] encryption as an emerging system and community of practice, doing fieldwork-driven "analytical thick descriptions"[19] of events and organizations in order to 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, governance, or lobbying.

¶10 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 who participate in innovation and in the co-shaping of 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 long 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.

---

[17] Nelly Oudshoorn and Trevor Pinch, *How Users Matter: The Co-Construction of Users and Technology*, Cambridge, Massachusetts, The MIT Press, 2005.

[18] Michel Foucault, *Fearless Speech*, in Joseph Pearson (ed.), *Semiotext(e)*, Cambridge, Massachusetts, The MIT Press, 2001.

[19] Clifford Geertz, "Thick description: Toward an interpretive theory of culture", in *The Cultural Geography Reader*, London, Routledge, 2008, p. 41–51 (reprint).

¶11 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, and were then transcribed and coded during the summer and early fall of 2017.

¶12 This article focuses primarily 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

¶13 In design studies and software engineering, threat modelling is considered 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."[20] 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."[21] Threat modelling enables development teams to examine the application "through the eyes of a potential adversary"[22] 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 behaviour 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.

[20] Peter Torr, "Demystifying the threat modeling process," *IEEE Security & Privacy*, vol. 5, no. 3, 2005, p. 66, https://www.computer.org/csdl/mags/sp/2005/05/j5066.pdf (accessed 20 October 2018).

[21] 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, p. 13, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.2997&rep=rep1&type=pdf (accessed October 20 2018).

[22] *Ibid.*

¶14 The idea of a threat modelling applied to users instead of informational systems is related to the difficulty—or rather, the impossibility—to "hide from everyone." As the Electronic Frontier Foundation (EFF), 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."[23]

¶15 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 organizations use in order to analyze the possibility that a threat might happen. It becomes important not only to know who to hide from, but also to evaluate the chances one has to actually "meet" this adversary. While risk has been described as "a cultural 'translation' of danger," risk assessment is a "quantification of uncertainty" that produces risk "as something that can be known, mitigated, increased and decreased, calculated."[24]

¶16 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 observed in Ukraine and Russia used different techniques for threat modelling. For example, the training Digital Security for Activists, which took place in Saint-Petersburg, Russia on 10 April 2016, started with the following introduction by the trainer P.:

> Before we start, we need to decide: from whom are we protecting? First of all, from the state. Only during last year two hundred 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

23 Electronic Frontier Foundation, *Surveillance Self-Defense: Threat Model*, https://ssd.eff.org/en/glossary/threat-model (accessed 20 October 2018).

24 Sun-ha Hong, "Criticising Surveillance and Surveillance Critique: Why privacy and humanism are necessary but insufficient," *Surveillance and Society,* vol. 2, no. 15, 2017, p. 194. See also Mary Douglas and Aaron Wildavsky, *Risk and Culture*, Berkeley, California, University of California Press, 1982; Paulo Vaz and Fernanda Bruno, "Types of Self-Surveillance: From Abnormality to Individuals 'At Risk'," *Surveillance and Society*, vol. 3, no. 1, 2003, p. 272–291; Theodore M. Porter, *Trust in Numbers: The Pursuit of Objectivity in Science and Public Life*, Princeton, New Jersey, Princeton University Press, 1995.

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 throughout the three-hour workshop in order to group various privacy-enhancing tools that people might need around these three categories of adversaries. Structuring a training around a specific adversary means identifying an adversary's actual technical resources as well as extra-technical parameters, such as the legal context.

¶17 Another way of structuring a training was demonstrated by Ukrainian trainers V. and M., both specializing in high-risk users who are likely to face powerful, state-level adversaries, or who may face a physical threat. The training, held on 15 January 2017 in Kiev, Ukraine, involved the usage of a spreadsheet for participants to complete together with the trainers (see Fig. 1).

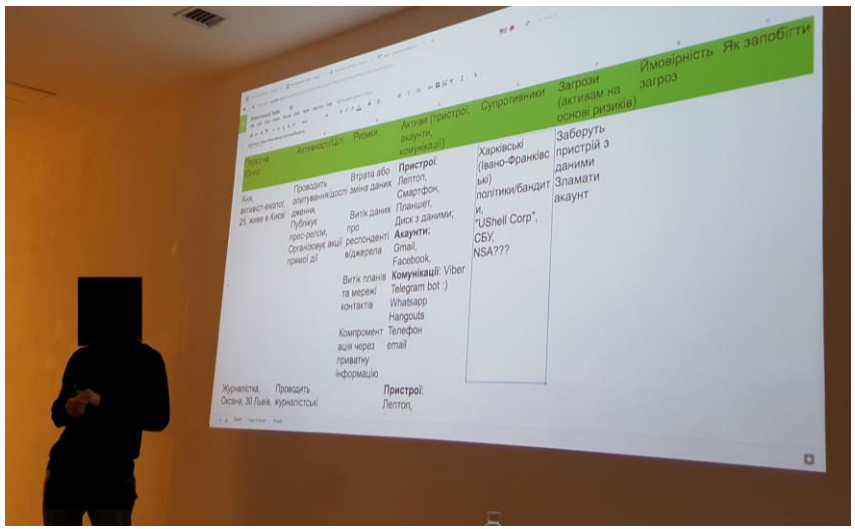

Fig. 1. Digital security training observed in Kiev, January 2017. The table includes the following columns (from left to right): Description of a person, his/her functions and activities, risks, "assets" (devices, accounts, types of communications used), adversaries, threats (applied to the assets based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

¶18 The training was organized around the collaborative construction of several fictional profiles (Anya, 25-years-old, ecological activist; Oksana, 30-years-old, journalist, etc.) and the identification of corresponding assets, adversaries, and threats. In this way, the trainers 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 concrete situation and context is more important than a high-level knowledge about multiple tools. Though some of the observed trainings were still centred around "tool demonstration," the majority of trainers were largely criticizing tool-centred approaches and insisted on a tailored training, based on threat modelling. As M., informational security trainer from Ukraine, explained:

> Very often trainings turn into tool-trainings. But in our work tools are not our primary, and not even secondary, concern. What's primary is the evaluation of what participants need, what they already use. Only afterwards we think of what we can suggest to them to use, and again, without any hard recommendations—you need only this tool and that's all.

The digital security community is highly reflective upon its own training practices and criteria of evaluation of secure messaging applications and e-mail clients.[25] In recent years, a paradigm shift has occurred, bringing trainers and experts from a tool-centred approach to user-centred one where the users' capacities to evaluate their own threat model become crucial. As the well-known EFF online 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."[26]

¶19 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 Secure Messaging Scorecard, which has been used as a quasi-standard-setting instrument by a large community of trainers, users, and technologists.[27] Bringing users and their self-risk-assessment to the centre has had an impact on digital literacy practices and the development of a new sort of guide, such

[25] 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. 3, no. 12, 2017, p. 51–71, https://doi.org/10.16997/wpcc.265 (accessed 20 October 2018).

[26] Electronic Frontier Foundation, *Surveillance Self-Defense: Assessing Your Risks*, https://ssd.eff.org/en/playlist/academic-researcher#assessing-your-risks (accessed 20 October 2018).

[27] Musiani and Ermoshina, 2017.

as the *Surveillance 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. In the words of an EFF Surveillance Self-Defense Guide trainer:

> 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.[28]

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; in the words of the EFF trainer,

> 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.

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 often advise 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 in the recommendation of a specific tool. The shift to a user-centred threat modelling in the digital security training community has an important

[28] *Ibid.*

impact on the evaluation, ranking, and recommendation of privacy-enhancing tools. In these instances, non-cryptographic features of a tool are now considered important, and a combination of tools and operational security techniques is proposed as "compensation" for unsolved academic cryptography problems.

From "Nothing to Hide" to "Tinfoil Hat Freaks": Continuum of Risk Levels

¶20 Aside from trainers and digital security experts, users develop their own methods of evaluating risk, and invent specific *ad hoc* practices of digital self-defense. However, even after Edward Snowden's revelations, an 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 focusing on the general public has revealed "a prominentconcern withthe collection of online data by a number of different actors, but also a lack of understanding or sense that it is possible to do muchabout it. In that sense [...] state surveillance isbeing carriedouton thebasis of public resignation rather than apathy or consent".[29] Researchers talk about a general public feelings of disempowerment and even about a certain form of "normalisation" of surveillance.[30]

¶21 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 an attempt to increase the general public's awareness about digital security.[31] 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 questioned more and more.

---

[29] Vian Bakir et al., "Public Feeling on Privacy, Security and Surveillance" report by DATA-PSST and DCSS, 2015, http://eprints.glos.ac.uk/5433/1/Public-Feeling-on-Privacy-Security-Surveillance-DATAPSST-DCSS-Nov2015.pdf (accessed 18 November 2018).

[30] Arne Hintz and Lina Dencik, "The Politics of Surveillance Policy: UK Regulatory Dynamics after Snowden," *Internet Policy Review*, vol. 5, no. 3, 2016, https://policyreview.info/articles/analysis/politics-surveillance-policy-uk-regulatory-dynamics-after-snowden (accessed 20 October 2018).

[31] Among more recent attempts is the documentary *Nothing to Hide* (Marc Meillassoux, 2017).

¶22 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 about privacy. Indeed, we have classified the interviewed population according to two axes: the individuals' knowledge about technologies and their risk situation—we have thus obtained 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 behaviour was not holistically secure: a large number of tech developers or trainers were using unencrypted email and text messaging applications.

¶23 For example, while recent research in usability showed that Telegram was suffering from a number of important usability and security problems,[32] Pirate Party activists, themselves software developers, system administrators, or hosting providers, are using Telegram on a daily basis (the Pirate Party Russia group on Telegram numbered 420 users as of 24 October 2017). Telegram group chats remain popular among high-risk and high-knowledge users despite the fact that the app's encryption for group chat is very basic. However, other tactics of self-defense are used, such as self-censorship (avoiding to talk about specific topics) and pseudonymization (avoiding real profile photos and usernames).

¶24 Surprisingly, according to the interviews, there is no strict correlation between users' threat models, level of technical knowledge, the security features of a tool,[33] and adoption dynamics. Other extra-cryptographic and extra-security features may become arguments for the 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 diminish in importance for users, compared to other aspects, such as the features of the interface and the reputation of the app's creator. The trust in Telegram, according to our interviews, is not with the technology, but with the main developer and his political position. Here is an excerpt from an online discussion in a group chat called *Soprotivlenie* [Resistance], posted on 11 June 2017:

[32] 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 *Proceedings of the 2nd European Workshop on Usable Security (EuroUSEC)*, Paris, France, 29 April 2017, https://usec.cispa.uni-saarland.de/eurousec17/ (accessed 20 October 2018).

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

User 1: Maybe you shouldn't discuss that over Telegram?
User 2: Why not? Pashka Durov will never give away any of our data, he doesn't care about the Russian police.

¶25 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 behaviour related to email and messaging was estimated to be more important. Even if these users could not always clearly describe possible attack vectors, they had a very multifaceted and complex image of who their adversary was. This was clearly expressed in the drawings collected during interviews and the observed workshops (see Fig. 2).

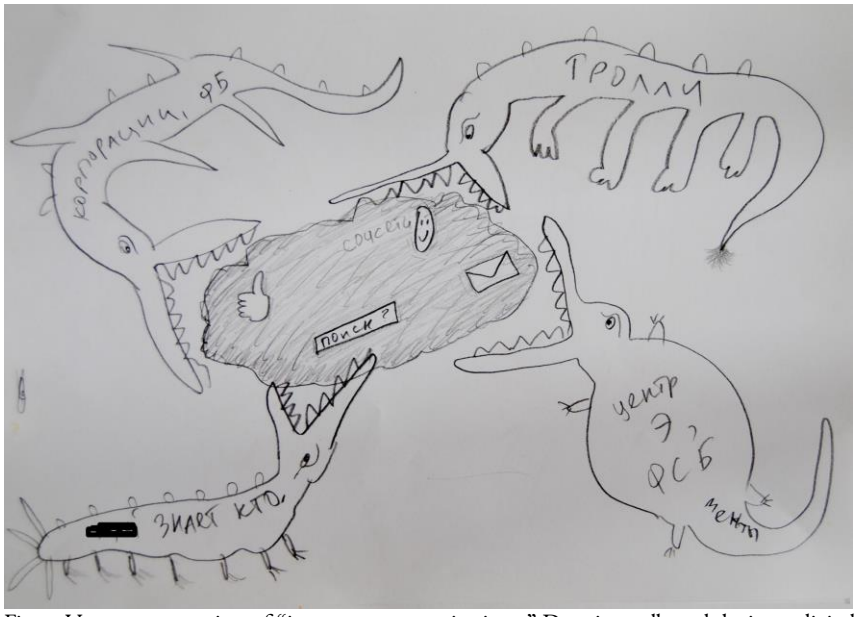

Fig. 2. User representation of "insecure communications." Drawing collected during a digital security workshop in Saint-Petersburg, April 2017. Female, activist of a feminist collective. The text written on the bodies of the "crocodiles" (clockwise, from top left) reads: "Corporations, Facebook; Trolls; Centre against extremism, FSB [Russia's principle security agency], police; Who the f**k knows." The text written on the cloud in the middle of the drawing reads: "Search; Social networks").

¶26 Low-knowledge, high-risk users have deployed specific, often unique and personal, methods of protecting communications and information, methods that present an assemblage of different tools and practices, both in offline (social engineering, operational security or "*opsec*") and online behaviour (see Fig. 3).

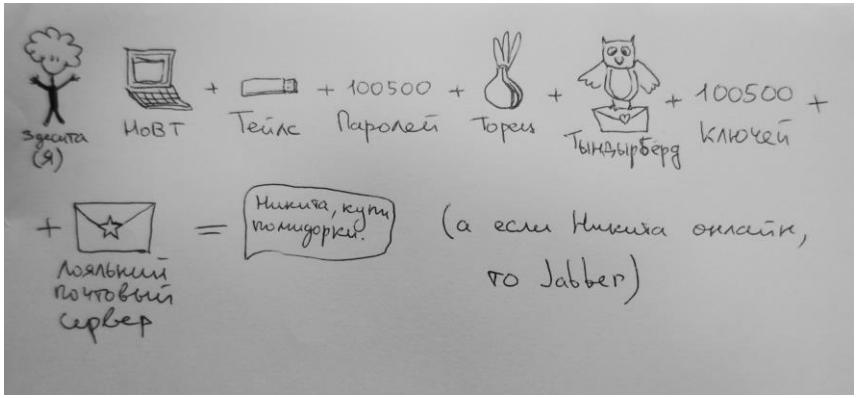

Fig 3: User representation of "secure communications." Drawing collected during a digital security workshop in Saint-Petersburg, April 2017. Female, antifascist activist. From the left: "Me: laptop + Tails + 100,500 passwords + Tor + Thunderbird + 100,500 keys + trusted email provider = message "Nikita, could you buy some tomatoes please?" (And if Nikita is online, then Jabber)."

¶27 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 affirm to be zero-knowledge and to destroy messages once read.[34] For these users, the main threat 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.

¶28 Secure messaging is a vibrant and rapidly developing field,[35] and the multitude of messaging apps is echoing the variety of user behaviour 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.

[34] The most popular services are One Time Secret, https://onetimesecret.com/, and Privnote https://privnote.com/ (accessed 20 October 2018).

[35] Ksenia Ermoshina, Francesca Musiani, and Harry Halpin, "End-to-End Encrypted Messaging Protocols: An Overview," F. Bagnoli, *et al.* (eds.), *Internet Science. Proceedings of the Third International Conference, INSCI 2016, Florence, Italy.* New-York, Springer, 2016, p. 244–254, DOI: https://doi.org/10.1007/978-3-319-45982-0_22 (accessed 20 October 2018).

These different personas imply a specific online behaviour pattern, thus creating what one of our interviewees has called "*security by compartmentalization.*"

¶29 Users use different messaging apps for different groups of contacts, according to the perceived level of risk. Even some of our high-risk interviewees reported 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 their communications to a single application, but say that they have a hard time convincing relatives to change their online behaviour (what we have called the "digital migration problem"[36]) or face compatibility problems (for example, older phones cannot run Signal).

¶30 Consequently, when applied to digital security, risk is a relational and socially defined concept, highly dependend on the user's social graphs and communication context. A high-risk user from Ukraine, involved in a collective for support of political prisoners, explained:

> 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 is coming after me. Predicting the 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 shifting: a low-risk person in contact with a high-risk one has to heighten his or her level of security and may him/herself become high-risk. As a user from Austria, a festival organizer self-identifying as a low-risk person, put it:

> 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][37] 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.

---

[36] *Ibid.*

[37] Here, the interviewee mentioned two important and well-known technology and human rights activists.

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 behaviour and user-driven practices of "security by compartmentalization" have recently been 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.

¶31 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 behaviour of "the adversary." Thus, for this high-risk and high-knowledge user from Greece, it is important to constantly reinvent 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, moral values, gender become important parameters that influence the definition of what "sensitive information" is. For example, our interviews with users from the Middle East show that one of the most important "adversaries" from whom Muslim women have to hide is their own partner or another family member. As one of our interviewees, a 27-year-old Iranian woman, explained, photos of a non-religious wedding can become as sensitive as political critique and can bring the person sharing them 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

¶32 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; if 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 consider WhatsApp's proprietary license and collaboration with Facebook in terms of metadata less important than the 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. I., a female informational security trainer from Ukraine, said:

> 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.

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 Ethan Zuckerman's famous "Cute Cat Theory of Digital Activism,"[38] 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.

¶33 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, both informational security trainers and non-technical users offered extensive critique of all existing tools. 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."[39] 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") and told

[38] Ethan Zuckerman, "The Cute Cat Theory Talk at ETech," *…My heart's in Accra* (blog), 8 March 2008, http://www.ethanzuckerman.com/blog/2008/03/08/the-cute-cat-theory-talk-at-etech/ (accessed 20 October 2018).

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

the story of an undercover police officer using a @riseup.net email account as one of the means to penetrate a student movement mailing list during the mass protests in 2011–2012.

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

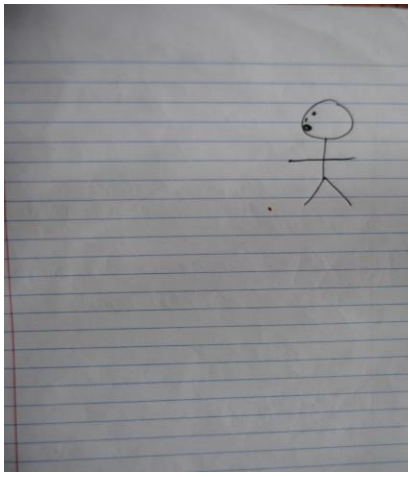

Fig 4. Drawing collected during one of our interviews on 16 February 2017.

¶35 He commented on 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...

¶36 The adoption of encryption by "mainstream" messaging applications (as opposed to "activist-targeted" applications) leads to an effect that our respondents called "fish in the sea." This is how a female, low-risk user and tech-journalist from Austria described it:

> 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.

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 (for 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, as in this interview with a male informational security trainer from Ukraine:

> 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…"

¶37 Even though the collaboration of Moxie Marlinspike, head developer of Signal, with WhatsApp and Facebook was subject to controversies and critiques in a number of tech-savvy FLOSS (Free Libre Open Source Software) circles, mass adoption of end-to-end encryption has 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 such as the Internet Freedom Festival or RightsCon where sessions on regulation of encryption were held in 2017, bringing together representatives of the technical community and EU and international regulators.

¶38 After the introduction of 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 sixty-five privacy-focused NGOs (including Privacy Now, EFF, and Article 19) and addressed to the UN on 19 September 2017, with a demand to decriminalize users of privacy-enhancing

technologies and digital security trainers.[40] 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.[41]

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, as does Peter S., developer of secure messaging project Heml.is:

> 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.

Towards a Deconstruction of the Privacy-Security Dichotomy

¶39 When we first attempted to interpret the results from 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

[40] IFEX, "HRC 36: Secure Digital Communications Are Essential for Human Rights," *IFEX.org*, 19 September 2017, https://www.ifex.org/turkey/2017/09/19/apc_ifex_hrc36_4_statement/ (accessed 20 October 2018).

[41] Human Rights Council, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye," 2015, article 58, p. 19, https://theintercept.com/2015/05/28/u-n-report-asserts-encryption-human-right-digital-age/ (accessed 20 October 2018).

security: these two concerns, and related defensive practices, are in fact interpenetrating.

¶40 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). Critiques of GAFAM,[42] the Net's giants, are 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.

¶41 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 dependencies on Google Play and Google Services,[43] which originated within free software circles with the launch and quick shutdown of the LibreSignal project.[44] Signal's Google dependencies became a problem for a specific user community, both privacy-aware and tech-savvy, who opts 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 selection (Linux phone, Fairphone, Copperhead OS, or other privacy-enhancing tools), or customized Android without the inclusion of Google Play. As Daniel, a tech-savvy user, e-mail service provider, and festival organizer put 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?

However, according to our interviews, Signal's dependencies on Google Play 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

[42] GAFAM stands for "Google, Apple, Facebook, Amazon, and Microsoft," also known as "GAFA" (without Microsoft), or the "Big Five" tech companies.

[43] GitHub.com, "Can NOT send encrypted MMS with attachments #12," (message thread), 28 December 2011, https://github.com/WhisperSystems/Signal-Android/issues/127 (accessed 20 October 2018).

[44] GitHub.com, "LibreSignal," https://github.com/LibreSignal/LibreSignal (accessed 20 October 2018).

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.

¶42 High-risk users also mentioned the decentralization of networks, considered for a long time a "high-tech, low-risk" concern, as an issue important for their threat models. Our recent exchanges with Russian and Ukrainian left-wing activists showed a growing concern among these populations about being able to run their own infrastructures (servers) for storage of their files and for decentralized communication.

¶43 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[45] are now experiencing a rebirth in response to the growing control of online communications by the state. On 27 October 2018 Russian Prime Minister Dmitriy Medvedev signed resolution #1279, that obliges instant messaging applications to guarantee user authentication via phone numbers. Russian government has been trying to reduce technical and legal means for anonymous messaging for more than a year. Since then, several messaging services have been blocked in Russia, such as WeChat, Zello (widely used by the Russian truck drivers movement), Line, Blackberry Messenger and, since 16 April 2018, Telegram, which is still technically accessible because of its embedded circumvention protocol. In this context, we observed a growing interest by Russian users in XMPP/OTR and Riot.im, as alternatives to centralized systems.

Conclusion

¶44 The "dangerous liaisons" between private actors and governments,[46] unveiled 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 away from closed-source platforms with business models based on user data. In this context, the "adversary" resembles a

[45] For more information, see the website at https://xmpp.org/ (accessed 20 October 2018).

[46] Francesca Musiani, "Dangerous Liaisons? Governments, Companies and Internet Governance," *Internet Policy Review*, vol. 1, no. 2, 2013, https://policyreview.info/articles/analysis/dangerous-liaisons-governments-companies-and-internet-governance (accessed 20 October 2018).

constantly evolving, fluid network connecting with both private and governmental infrastructures, rather than a single entity with well-defined capacities and a predetermined set of techniques and tools for surveillance and attack.

¶45 Trainers and digital security organizations are moving towards a user-centred 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, identifying "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, profession, the political regime and geopolitical situation of his or her country or region, or, furthermore, the reputation and charisma of app creators.

¶46 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."[47] 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 institutions) and myriad infrastructures and technical *dispositifs* in which concepts such as security and privacy are embedded.

¶47 The very distinction between high-risk and low-risk, while useful operationally for the researcher as a practical methodological tool in order to build a diverse sample of users for interviews, shows its limits, mainly due to the relational nature of risk that we have explored in this article. Having at least one high-risk user in his or 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 sociopolitical 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 concealment. The ongoing turn to "mass encryption" would do well to take this into account.

47 Éric Méchoulan, "Intermédialités : le temps des illusions perdues," *Intermedialités/Intermediality*, no. 1, "naître," Spring 2003, p. 10, https://www.erudit.org/fr/revues/im/2003-n1-im1814473/1005442ar.pdf (accessed 20 October 2018).

Hiding from Whom? Threat Models and In-The-Making Encryption Technologies

Ksenia Ermoshina, CNRS/CIS
Francesca Musiani, CNRS/CIS

ABSTRACT

Following Edward Snowden's 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. In this article, 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 which data to conceal, and how to conceal 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.

NOTE BIOGRAPHIQUE

Ksenia Ermoshina, holds a PhD in socio-economics of innovation from Mines ParisTech. She currently works as a postdoctoral researcher for the French National Centre for Scientific Research (CNRS), Center for Internet and Society (CIS), and is an Associate Researcher at the Citizen Lab, Munk School of Global Affairs, University of Toronto. Her research focuses on information operations within the

Russian-Ukrainian armed conflict, including digital threats to journalists and civil society organizations, Internet censorship, and surveillance. Her previous work as a Postdoctoral Fellow with the NEXTLEAP research project studied the usage and development of end-to-end encrypted messaging and email protocols and clients.

Francesca Musiani, (PhD, MINES ParisTech, 2012) is Associate Research Professor (*chargée de recherche*) at the French National Centre for Scientific Research (CNRS), Deputy Director of the Center for Internet and Society (CIS), Associate Researcher with the Centre for the Sociology of Innovation (i3/MINES ParisTech), and academic editor for the *Internet Policy Review*. Her research explores Internet governance. She was one of the Principal Investigators for the European H2020 NEXTLEAP (Next-Generation Techno-Social and Legal Encryption, Access, and Privacy) project (2016–2018).