CRYPTO PARTIES AND THE CREATION OF ANONYMITY AND PRIVACY

Linda Monsees

Introduction[1]

Increasing awareness of surveillance practices over the past decade led users to learn about tools to protect their privacy and security in the digital realm. There is a huge knowledge gap between experts and hackers who are able to use complex tools and many citizens who feel overwhelmed and lost.[2] In this contribution, I am taking a look at the practice of >Crypto Parties< which promises to reduce this knowledge gap and spread better anonymity and security practices.[3]

Crypto Parties (CPs) are an interesting phenomenon because they present a globally decentralized movement in which citizens come together and learn about internet safety and how to counter dataveillance. So far, not much research has engaged with this practice and little is known about this small but ongoing activist movement. This short paper introduces Crypto Parties as a relevant site in which knowledge about anonymity is created and spread. The following section gives an overview about the implementation of Crypto Parties. I am presenting the decentralized movement that emerged in 2012 and organizes events until today. In the second section, I am giving a brief introduction into my methods of participant observation of Crypto Parties in Germany. This study is based on participant observation of three Crypto Parties and corroborated by attendance of other meetings where I have held informal interviews with people involved in organizing Crypto Parties as well as follow-up emails and the analysis of documents that were publicly accessible. In the last two sections, I zoom in on two aspects of Crypto Parties. I argue that CPs actively try to counteract the ever-present hierarchies between experts and laypeople. I also argue for understanding CPs as a distinct political practice even though participants rarely talk about politics proper.

1 I thank Paula Helm for the invitation to the panel and the conference.

2 This assessment is based on my informal interviews in summer and fall 2019 (see below).

3 A more detailed description of my results has been published as *Linda Monsees:* Cryptoparties: Empowerment in Internet Security? In: Internet Policy Review 9 (2020), issue 4. URL: https://policyreview.info/articles/analysis/cryptoparties-empowerment-internet-security (Accessed: 7. 2. 2021).

Crypto Parties: A global, decentralized movement

Crypto Parties were developed in 2012 and became more popular in the aftermath of the revelations by Edward Snowden. Today, CPs are organized around the world with the most regular parties occurring in Europe.[4] CPs aim at educating people about possible privacy intrusions and insecurities caused by networked technology. Participants can improve their knowledge about the internet, safe surfing and tools such as encryption. CPs »aim to empower ordinary people by informing them about critical aspects of datafication processes as well as enabling them to sensitively engage with their digital media technologies, encrypt those and their online communication processes«.[5]

CPs do not rely on one centralized organization. Indeed, everybody can organize a Crypto Party. The main organizational tool is a ›wiki‹ where all dates and information are collected. However, sometimes CPs are also organized in the context of academic conferences, at universities or by political parties. Crypto Parties are thus open in scope, size and format and anybody can organize them. Attendance might range from zero to twenty, larger events seemed to only have occurred in the immediate aftermath of the Snowden revelations.[6] Participants and organizers are predominantly male except for CPs that are deliberately organized for women, transgender and non-binary persons.[7] CPs take place in cafés or other publicly accessible spaces and some organizers aim to host them regularly on a monthly or bi-weekly basis. The Code of Conduct is also published on the wiki and guides the CPs. All organizers of CPs, which I observed, referred at least implicitly to the Code of Conduct. Some of the tenets within this code are that every CP needs to be open to the public, that harassment is not tolerated and that no one is allowed to touch the keyboard of another person without explicit consent of that other person.

The CPs themselves differ in their particular ways of teaching technological tools. One CP might mainly provide one-on-one tutorials, whereas others split the whole group into smaller units for discussions, and yet others might focus on one particular theme and carry out a lecture-style presentation. However, certain ideas (e. g. 100% security is impossible) or tools (e. g. Mozilla Firefox as a safer option for browsing the

4 *Crypto Party:* Parties:upcoming [CryptoParty.] (12. 12. 2019). URL: https://www.cryptoparty.in/parties/upcoming (Accessed: 11. 3. 2020).

5 *Sigrid Kannengießer:* Reflecting and Acting on Datafication – CryptoParties as an Example of re-active Data Activism. In: Convergence: The International Journal of Research into New Media Technologies (2019) (Online First), pp. 1–14, here p. 12.

6 This assessment is based on my interviews.

7 This was the case in my fieldwork but was also commented on by most organizers who consider it a huge problem.

internet) are commonly taught. More complex tools such as >Tails<[8] are explained rather rarely while most CPs usually focus on more fundamental sessions about >how the internet works< (in-vivo reference of a participant in a German CP). In this context, participants learn for example about add-ons like >https-everywhere< or about the advantages of certain web-browsers as opposed to others when it comes to privacy. The organizers call this >digital self-defence< or the development of a »security culture«.[9] CPs are thus a very distinct practice in which knowledge about anonymity and privacy is created and circulated among different groups. CPs are a form of everyday engagement where specialists engage with non-specialists in the transfer of technological knowledge.

Data collection and analysis

Methodically, the analysis below relies on a combination of document analysis, participant observation and informal interviews.[10] The research followed a qualitative-interpretative research design[11] which means that I was generally interested in structures of meaning.[12] The focus lay on CPs in Germany, but I also attended one in Denmark. Germany is probably the most active country when it comes to Crypto Parties. I conducted interviews in three different cities. These cities were chosen for their accessibility and presence of CPs movement. In order to preserve the anonymity of the participants, I will not disclose the exact location and time of CPs. I participated in three Crypto Parties, attended two meetings of hacker spaces and one meeting in preparation for a Crypto Party. These events allowed me not only to see how CPs are conducted but also to do a set of informal interviews. The meetings lasted between one and four and a half hours and took place between July and November 2019. I could rely on my background knowledge on encryption acquired during a previous

8 >Tails< allow users to boot from a DVD or USB stick and all communication is automatically directed via TOR (The Onion Router). Tails is a strong tool to protect anonymity on the internet, but it requires some knowledge and time to set it up and to operate it.

9 Participants at CP 2 and 3.

10 *Andra Gillespie/Melissa R. Michelson:* Participant Observation and the Political Scientist: Possibilities, Priorities, and Practicalities. In: PS: Political Science & Politics 44 (2011), issue 2, pp. 261–265.

11 *Peregrine Schwartz-Shea/Dvora Yanow:* Interpretive Research Design: Concepts and Processes. New York 2012.

12 *Ulrich Franke/Ulrich Roos:* Einleitung: Zu den Begriffen >Weltpolitik< und >Rekonstruktion<. In: ead. (eds.): Rekonstruktive Methoden der Weltpolitikforschung: Anwendungsbeispiele und Entwicklungstendenzen. Baden-Baden 2013, pp. 7–29; *Patrick Thaddeus Jackson:* The Conduct of Inquiry in International Relations: Philosophy of Science and Its Implications for the Study of World Politics. London 2011.

research project. I also analysed core documents such as the >wiki< that were being used for organizing the respective events. Since I was interviewing privacy sensitive actors, I was not able to record any interviews or conversations at the CPs. Producing any records or pictures is formally forbidden by the Code of Conduct of CPs.

The (non-)creation of hierarchies in Crypto Parties

As already stated above, anybody can organize a CP. In that way CPs are open and non-hierarchical. In practice, the organizers are usually also the >experts< that will teach the specific tools. This means that the hosts of a Crypto Party will probably have more knowledge about anonymity and security of digital technologies than the participants. Even though Crypto Parties were initially based on the idea that all participants learn together in mutual support, in practice the organizers teach participants. People who teach anonymity and security tools are also sometimes called >angels<. Activists and hackers enact their role as being the >expert<, that is: a more knowledgeable person, who can assess technology and offer valuable services to >laypeople<. These different kinds of knowledge – and indeed different levels of knowledge – therefore de-facto undermine the idea of an egalitarian space. Kannengießer, in her study on CPs, observes that despite the idea of being non-hierarchical »there are strong hierarchies persisting between >teachers< and >students<«.[13] While I made similar observations, I could also detect a more reflexive attitude towards this problem. The organizers and hosts of CPs I spoke to are aware of this problem and try to undo implicit hierarchies. One informant told me that he deliberately wants Crypto Parties to »not look too professional«. While CPs certainly tend to fall back on the classic expert/non-expert divide the same way classical citizen engagement practices do,[14] I could, nevertheless, observe concrete efforts to counteract this in order to create a more open, egalitarian space. For example, when teaching the principle of the internet and encryption the instructors paid a lot of attention to resist lecturing. They had also prepared flashcards and props to make the rather dry subject more accessible. Based on my observation I would say that most >teachers< try not to lecture and actively encourage discussions. The ambiguity between the self-proclaimed claim to be non-hierarchical and the empirical reality of an expert-laymen-divide is a result of the need for experts that know how to counter surveillance and improve privacy on the one hand, while, on the other hand, the format as such promotes egalitarian structures.

13 *Crypto Party*, wie Anm. 3.

14 *Brice Laurent:* Political Experiments That Matter: Ordering Democracy from Experimental Sites. In: Social Studies of Science 46 (2016), issue 5, pp. 773–794.

Creating Anonymity as a Political Practice

My initial assumption, before going into the field, was that the >hacker turned activists< would conceive of their activities as primarily political – as an act of resistance. But other motivations such as fun and a sense of responsibility towards society were much more present. Most of my interview partners did not really refer to any kind of direct political motivation or perceived of their acts as acts of resistance. The politicality of CPs revealed itself in a more dispersed and diffuse way when people talked about their discontent with politicians and companies and their (lack of) privacy protection and security measures. CPs enact a decentered mode of resistance. The concept of diffusion and decentering ties back into debates within political science and security studies where politically relevant security practices cannot any longer be conceptualised as being part of one core institution such as the state.[15] Similarly, the politicality of CPs does not exist in so far as >anonymity< is perceived as a political value by the participants. The politicality of anonymity lies in the many diffuse practices and in the way these practices entangle multiple issues and controversies. During CPs, issues such as the Snowden revelations or state policies in general are not discussed up front. However, what comes to the fore is that politics plays a crucial role below the surface. References to the global surveillance infrastructure and the quasi-monopolistic role of the big five tech companies are frequent.[16] Also, possibilities and realities of police surveillance are debated. Even more so, the knowledge about security and privacy measures that is being taught on a technological level is also not primarily >political<. Most participants do not frame fighting dataveillance as an activity against state surveillance. The concern is a more dispersed mixture of privacy, anonymity and security concerns.[17] As a result, this also means that the practices concern everyday activities such as browsing the web, securing passwords and covering up built-in cameras. Political practices and discourse are not so much significant in regard to state institutions. Instead, the politicality of CPs comes to the fore in the way it produces techno-political knowledge through a teaching that aims at altering

15 *Linda Monsees:* Crypto-Politics: Encryption and Democratic Practices in the Digital Era. Abingdon/Oxon/New York 2020; *Marieke De Goede:* Afterword: Transversal Politics. In: Xavier Guillaume/Pinar Bilgin (eds.): Routledge Handbook of International Political Sociology. London 2017, pp. 353–365.

16 *Mikkel Flyverbom/Ronald Deibert/Dirk Matten:* The Governance of Digital Technology, Big Data, and the Internet: New Roles and Responsibilities for Business. In: Business & Society 58 (2017), issue 1, pp. 3–19.

17 *Rocco Bellanova:* Data Protection, with Love. In: International Political Sociology 8 (2014), issue 1, pp. 112–115; *Colin J. Bennett:* In Defense of Privacy: The Concept and the Regime. In: Surveillance & Society 8 (2011), issue 4, pp. 485–496.

everyday-life socio-technical practices.[18] CPs therefore need to be conceptualised as a political practice, but not because they impact policies or shift power relations within the state. The politicality lies in the creation and decentred circulation of knowledge about anonymity.

CPs as a dispersed practice of knowledge production

This empirical study on CPs is one of the few studies that engage with this phenomenon. This contribution gave a brief introduction to CPs as a cultural, but also political practice concerning anonymity, privacy and security. CPs try to create egalitarian spaces. Even though hierarchies between >experts< and >laypeople< exist, attempts are made to counter this solidification of hierarchies. CPs are politically significant practices in which knowledge about anonymity is being co-produced and circulated among different groups. The political significance of these practices does not lie in its direct impact on, for example, state policies. CPs create and spread knowledge and technology about anonymity and privacy and alter everyday behaviour. In that way its political character is much more >diffuse<. The empirical study of CPs was just a first step in increasing our understanding of CPs as cultural and political practices and the possible impact of these practices on the production and dissemination of knowledge about privacy and anonymity.

Dr. Linda Monsees
Institute of International Relations Prague
Nerudova 3
110 00 Praha 1
monsees@iir.cz

18 *Noortje Marres:* Material Participation: Technology, the Environment and Everyday Publics. Houndmills etc. 2012.