INTERNET POLICY REVIEW
Journal on internet regulation

Volume 9 | **Issue** 4

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Cryptoparties: empowerment in internet security?

Linda Monsees *École normale supérieure* linda.monsees@ens.psl.eu

DOI: https://doi.org/10.14763/2020.4.1508

Published: 15 October 2020
Received: 20 December 2019 **Accepted:** 28 March 2020

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Monsees, L. (2020). Cryptoparties: empowerment in internet security?. *Internet Policy Review*, *9*(4). DOI: 10.14763/2020.4.1508

Keywords: Cryptoparties, Hacker, Citizen engagement, Privacy, Crypto communities

Abstract: Cryptoparties (CPs) are a global movement of forums where citizens can come to learn how to improve their digital privacy and security. The present paper is one of the few empirical studies on CPs and is based on participant observation of three CPs. I demonstrate that the organisers of CPs strive for an egalitarian space for teaching and learning. Even though this goal is not always achieved, CPs might still serve as an example of citizen education in a technological society where every citizen needs to deal with complex technological issues. In addition, this paper contributes to the emerging debate on ‘doing internet governance’, broadening our focus to include user-based and decentred practices. I argue for the political relevance of CPs showing how they enact decentred threat-scenarios to a non-expert public.

ACKNOWLEDGEMENTS
I am deeply indebted to all the generous people who took the time to explain to me what Cryptoparties are about and corrected my many misconceptions. I hope this article does justice to their perpetuous work to make cyberspace a better place for all of us.

Introduction

This paper starts from the assumption that understanding the governance of networked technologies and related societal values such as privacy and security requires us to go beyond a focus on legal and institutional aspects. Indeed, a more comprehensive understanding of the politics of the internet 'requires unpacking the micro-practices of governance as mechanisms of distributed, semi-formal or reflexive coordination, private ordering, and use of internet resources' (Epstein, Katzenbach, & Musiani, 2016, p. 4). The success of privacy and security is not only determined by legislation but is heavily dependent upon the use of individual practices to counter surveillance and retain privacy (Bauman et al., 2014; Marx, 2015; Bellanova, 2017). However, these practices are often perceived as highly complex, and end users are often hesitant about using seemingly complicated tools. The focus of this article lies on one practice - cryptoparties – which attempt to combat these anxieties and teach privacy and security tools to the layperson. In doing so, this paper offers a valuable empirical study into a largely unknown phenomenon (but see Kannengießer, 2019) and corroborates previous pleas in this journal (Epstein, Katzenbach & Musiani, 2016) that more attention must be paid to micro-practices.

Cryptoparties (CPs) are not actually 'parties' but rather open meetings where individuals can get the help they need to improve their digital privacy and security. These meetings happen all around the world, mostly in public spaces such as cafes or universities. CPs originated in 2011 in Australia, but today most of them occur in Europe (CryptoParty, 2013, p. 13). Sigrid Kannengießer summarises the rationale of these activities as practices that 'aim to empower ordinary people by on the one hand informing them about critical aspects of datafication processes and on the other hand enabling them to engage with their digital media technologies, encrypt those and online communication processes' (Kannengießer, 2019, p. 12; see Loder, 2014, p. 814). CPs create an entry point for studying everyday practices and how they fit into wider political debates. In the case of CPs, we can observe how mundane practices such as choosing a secure browser or implementing better passwords are key to enacting privacy. Being a 'mechanism of civic engagement', CPs qualify as a practice of internet governance under the definition of Epstein and colleagues (Epstein, Katzenbach, & Musiani, 2016, p. 7).

This article brings the political significance of CPs into the spotlight and explains the role of CPs in the broader development of privacy and security controversies. Political science has been rather silent on the topic of CPs, most studies instead focusing more broadly on encryption and internet governance (Herrera, 2002; Monsees, 2020; Schulze, 2017; Myers West, 2018). Shifting the focus to the *practices* of CPs also allows the conceptual focus to shift away from institutions and towards more mundane and decentered practices.

I demonstrate throughout the article how CPs enact a diffuse kind of security politics where neither threat nor countermeasures work through one central institution but through mundane, decentred practices (Huysmans, 2016). In the following section, I draw on more recent contributions in the field of internet governance and international relations in order to argue that a sensitivity towards mundane practices is crucial for understanding the creation of internet security and privacy. The empirical study is mainly based on participant observation, the methodology of which I lay out in the second section. The main part of the paper presents the results of this empirical study. I argue that the specific format of cryptoparties allows them to teach relevant privacy tools and adapt to both the abilities of end users and a changing socio-technical environment. I demonstrate how CPs themselves are decentred and can adapt over time: CPs enact a decentred threat scenario that focuses less on institutions and more on individuals and their needs. The paper therefore provides novel empirical insights while at the same time showing how a shift in perspective to mundane security practices can enrich the study of internet governance.

Internet governance: on the political significance of decentred practices

Internet governance (IG) is usually analysed as a form of ‘multistakeholderism’, which is defined as:

> two or more classes of actors engaged in a common governance enterprise concerning issues they regard as public in nature, and characterized by polyarchic authority relations constituted by procedural rules(Raymond & DeNardis, 2015, p. 573, see also Hofmann, 2016).

Private entities, NGOs and hybrid organisations such as ICANN, in addition to national governments, are all involved in the governance of the global infrastructure that constitutes the internet (DeNardis, 2010; Mueller, 2010). However, in line with more recent contributions that try to broaden the empirical and analytical focus of IG, I demonstrate in this paper the value of looking at less institutionalised practices. [1] For example, a special issue of this journal has shown the need to focus on 'doing internet governance' (Epstein, Katzenbach, & Musiani, 2016). Much IG research remains on the institutional level which 'largely overlooks the mundane practices that make those institutions tick, thus leaving important blind spots in both conceptual and substantive understanding of the practices and power arrangements of IG' (Epstein, Katzenbach & Musiani, 2016, p. 4). Taking it even further, van Eeten and Mueller argue that the constitution of the field of IG creates systemic blind spots: the specific boundaries between IG and other fields limit the scope and prevent deeper engagement with other fields. There is 'a tendency to think of governance as being produced by, or taking place in, formal organizations with explicitly institutionalized rules and procedures' (van Eeten & Mueller, 2012, p. 727). IG is, then, always linked to institutional settings in which IG is 'explicitly the topic of discussion' (ibid.). Limiting the analytical focus leads to a biased understanding of these formal structures and underestimates the political significance of informal practices (van Eeten & Mueller 2012, p. 730). Consequently, taking an analytical view to seemingly insignificant practices gives us a more thorough understanding of how 'privacy' or 'security' are enacted (Christensen & Liebetrau 2019). As I will argue throughout the article, we can then see how decentred practices are, in fact, politically significant.

Cryptoparties are not anchored in one central organisation but are rather a decentralised, global form of technological activism and education. My article provides both a much-needed empirical study of CPs and an illustration of the value in expanding the scope of IG. I investigate how activists and citizens come together and how knowledge about privacy and security, core aspects of IG, circulates and is put into practice. Such a 'bottom-up perspective focuses on the mutual adjustments we make in our daily social life' (Hofmann, Katzenbach, & Gollatz, 2016, p. 1414), thereby illustrating the ordering effects of 'day-to-day practices that organize our social lives' (idem). Such a shift in perspective illuminates how, for example, 'security' results from a multiplicity of practices, actors and technologies, and not solely from governmental institutions and legal regulations (Hofmann, Katzenbach, & Gollatz, 2016).

[1] For a more comprehensive discussion on the different conceptualisations of practices, see the contributions in: Cetina, Schatzki, & Von Savigny (2005).

Mikkel Flyverbom expanded on these insights by drawing on the field of science and technology studies. For him, a crucial issue that has been neglected by IG concerns ‘the entanglement of technology and social practices and the ordering effects of processes of digitalisation and datafication’ (Flyverbom, 2016, p. 2). Flyverbom argues that an understanding of regulation as ‘institutionalised, deliberate and goal-oriented interventions by public or private actors’ is too narrow. Indeed, the *de facto* enactment of ‘bigger’ issues such as privacy and security is not only a result of governance efforts but also largely relies on individual actions. The political significance of privacy and security lies not only in a particular institutional set-up but in the micro-practices of individuals (Solomon & Steele, 2016; Isin & Ruppert, 2015). These practices are important for maintaining security but also shape the insecurities people experience (Guillaume & Huysmans, 2013; Selimovic, 2019). Mundane practices such as firewalls or spam-filters are equally important to legal regulations when it comes to securing networked technology. These insights motivate the scope of this article in analysing informal, decentralised practices that shape privacy and security. The objective of this article is not to weigh the relative importance of institutionalised vs non-institutionalised practices. The aim is to provide a more thorough understanding of how the actions of users are shaped by more than formal rules and legislation.

Methodology and description of the field

From my theoretical discussion on the importance of a bottom-up perspective on decentred practices, it follows that I needed a methodological toolkit that allowed me to capture these practices. I combined document analysis, participant observation and informal interviews (Gillespie & Michelson, 2011). The research followed a qualitative-interpretive research design (Schwartz-Shea & Yanow, 2012, Jackson 2011, ch. 6). In this project, I first wanted to get a better understanding of the practice of CPs. Hence, I was interested in what kind of meaning the participants themselves ascribe to CPs and how they evaluate the experience. This idea of meaning-making is core to a qualitative-interpretive research design (see Franke & Roos, 2013). With this in mind, the particular methods of participant observation and data analysis allowed me to get a clear understanding of the participant perspective.

According to Gillespie and Michelson, participant observation is a valuable, if often overlooked, method for political science (Gillespie & Michelson, 2011, p. 261). Depending on the research objective, the researcher can be more of an ‘observer’ or more of a ‘participant’ (Gillespie & Michelson 2011, p. 262, see also: Schwartz-

Shea & Yanow, 2012, pp. 63-67). I remained more on the observing end of the spectrum but offered my opinions or knowledge within small groups on a few occasions. Observing allowed me to listen in on multiple small group discussions and approach participants for short, informal interviews. This open research logic was an ideal fit for my project as well as for the environment in which I conducted my research (for a broader discussion on how to adapt methods for a specific research context, see Leander, 2017). Being open to the views of participants and having the option of unstructured conversation are valuable aspects of participant observation. The choice of method allowed me to understand what the participants deemed important, without disturbing their activities. The combination of participant observation and interviews allowed me to understand CPs as they unfolded while at the same time gaining more knowledge about the background of CPs through my more detailed questions.

Since this research did not receive any financial support, I was limited in the sites I could access due to time and financial constraints. I contacted the organisers in different places in Germany (and one location in Denmark) who conducted CPs in summer and fall 2019. Once I received a positive reply, I attended the CP, making clear to everyone that I was a researcher and letting everybody know about my intentions. Because participants were concerned about privacy and because photography and filming are specifically forbidden during CPs, I made it clear from the beginning that I would not record anything and that all informants would remain anonymous. In general, the organisers welcomed me and were open about answering my questions. I was able to observe the CPs and ask questions. I also had the chance to ask more detailed questions before the CPs and at one meeting where they planned the next CP. This allowed me to get background information about the organisers and their views on CPs and how they developed.

I attended three CPs which took place in two different cities and one more meeting of a planning event for a CP. [2] The meetings lasted between one and four and a half hours and took place between July and November 2019. [3] I took only written notes while attending the meeting. Since my interviewees were sensitive to privacy, I was unable to record any interviews, but I took detailed notes which I expanded on immediately after the end of the CPs. These field notes form the base of the

[2] I also attended two hackerspaces in the hope of receiving access to people formerly involved in CPs. Even though these visits were helpful in gathering insights into the culture of the hacker scene (see Kubitschko, 2015; Coleman, 2010) they did not give me further access to people involved in CPs.

[3] In order to protect the privacy of the participants, I will refrain from mentioning the locations of the CPs.

results described below. I only use direct quotes for the statements that I was able to write down directly during the CP (see Emerson, Fretz, & Shaw, 2001). All this accounts for the scarcity of direct quotes in the presentation of the results below: I only use them when they come from written documents or when I was able to write the quote down completely. Further documents, mainly from the cryptoparty wiki page used for organising (see below for more on the role of that wiki), corroborated my results.

The number of participants at the CPs I attended ranged from zero [4] to fifteen, which seems to be within the normal range of up to 20 people. Participants and organisers are predominantly male except for CPs that are deliberately organised for women, transgender and non-binary persons. Participants also varied in age from their 20s to 50s. [5] Some participants were open about their left-leaning politics and declared that their motivation to participate in CPs was based in their activism.All of my interview partners stated that only very few people attend more than one CP and rarely more than two to three. Based on my observation, most new participants had only very basic knowledge about internet safety. Especially at the CP targeted towards the LGBTQ+ community, the participants were open about being rather overwhelmed by the complexity of internet security (for an exploration of gender stereotypes in the hacker scene see Tanczer, 2016). They also described a feeling of anxiety and the need to ‘start somewhere’ because they lacked an overview of possible threats. [6]

The conduct of cryptoparties

An Australian woman working under the pseudonym of Asher Wolf initiated the first CP out of an interest in digital privacy (Poulsen, 2014; Radio Free Europe, 2012). It is interesting to note that she was not a ‘hacker’ or an expert but started the movement out of an interest in learning about privacy and security practices. Today, CPs are organised around the world with the most regular parties occurring in Europe (CryptoParty, 2019d). CPs do not rely on one centralised organisation. Many are organised by people who were previously active in the hacker scene, and most organisers work in IT.

[4] One CP that I attended indeed had zero participants. Since people do not need to sign up beforehand, this can happen.

[5] I am aware that my selection is not representative in quantitative terms. However, based on my interviews and the existing literature I could confirm that the CPs I visited were typical in a ‘qualitative’ sense.

[6] Women also face challenges such as harsher and more violent forms of trolling (Herring et al., 2002)

One can generally distinguish between two kinds of CPs. Many CPs are organised by activists and advertised on a wiki which is at the central website with all information about how to organise a CP (CryptoParty, 2019b). Often, these CPs reoccur on a monthly or bi-weekly basis in the same space, often using public spaces such as cafes, cultural centres or hackerspaces. However, some are conducted by political parties, interest groups, academic conferences or other types of independent organisations. These CPs are not publicised to potential participants through the main website but through the specific network of that organisation.

The CPs themselves differ in their particular way of 'teaching' technological tools. One CP might mainly provide mostly one-on-one tutorials, whereas others split the whole group into smaller discussions, whereas others might focus on one specific theme taught through a lecture-style presentation. CPs often start with a round of introduction during which everybody states what he or she can teach or what one needs help with. While the organisers are usually in the position to provide expertise, the role of the 'teacher' is not fixed in advance. The round of introductions develops a sense of what issues are most important to the participants allowing small groups to form around their interests. Sometimes a participant lets an organiser know in advance if they need help with something specific. An organiser will then help with that issue. The small groups cover a range of issues from basic 'safe surfing tools' to a more abstract introduction into 'how the internet works' to detailed explanations of email encryption or how to use programmes such as Tor or Tails [7] to protect anonymity to a larger degree. Participants learn, for example, about add-ons like 'https-everywhere' or learn about the advantages of certain web browsers when it comes to privacy. The organisers call this 'digital self-defence' or the development of a 'security culture'. [8] A CP lasts a few hours, and the atmosphere is very informal and relaxed, allowing participants to ask their questions and raise specific concerns.

My fieldwork shows that certain ideas are commonly mentioned (e.g., 100% security is impossible) and that certain tools are frequently taught (e.g., selecting a safe browser for surfing the internet). These commonalities go back, at least in part, to a code of conduct which is published on the central wiki (CryptoParty, 2019a). All interview partners referred (at least implicitly) to the Code of Conduct. At two of

[7] Tor (The Onion Router) allows for anonymous surfing by bouncing a user's data and requests through a set of relay servers. References to the 'dark web' usually indicate browsing via Tor. Tails is a programme that allows one to boot from, for example, a USB stick and relies on Tor for even greater privacy. However, the programme as such is more time intensive. The installation process, done at one CP, took several hours.

[8] Organisers at cryptoparties 2 and 3.

the CPs that I attended, the Code of Conduct was explained in the beginning. [9] The Code specifies that harassment is not tolerated and that CPs should be open to the public. However, there are also more specific rules such as ‘Other People's Keyboards Are Lava - Don't touch anyone's keyboard, but your own’ (CryptoParty, 2019a). This rule is based on the pedagogical reasons that the participants learn more if they have to do everything on their own. For privacy reasons it is also considered a bad habit to use other people's devices.

The politics of cryptoparties

Diffused politics

The previous section outlined the conduct of CPs in detail. In this section, I will detail specific aspects of CPs to analyse how we can understand these activities as politically significant practices that are relevant to internet governance.

CPs first developed in response to a very specific controversy around Australian legislation but later spread in the context of global controversy about commercial and state-led mass-surveillance (Poulsen, 2014). They saw renewed interest in the aftermath of the Snowden revelations. Indeed, some of my informants told me that they held CPs with several hundred participants immediately after the Snowden revelations. Today, internet security and privacy are part of most people’s daily routines: entering passwords, shielding cameras, and deleting cookies are just a few of the most relevant practices. We can see that the context of CPs evolved from a very particular concern with a piece of legislation to a more diffuse understanding of where the problem lies, including the realisation that there is no “one-size-fits-all” recipe to pick the best privacy tool. One organiser illustrated this by emphasising that every participant has different needs when it comes to security measures [10] and that one needs to develop a security culture. [11] Security culture refers to the idea that security is always situational and is always both affecting other people and affected by their actions (see the discussion on relationality in Ermoshina & Musiani, 2018). My informants mentioned a variety of examples: needing help with data protection before travelling to China, needing help with a hacked Facebook account [12] or just needing to ‘start somewhere’ with thinking about personal security. [13] This corroborates previous research highlighting ‘how understandings

[9] This is also confirmed by the results of Kannengießer (2019).

[10] Cryptoparty 1, 2 and 3

[11] Cryptoparty 2.

[12] Cryptoparty 1

of “good” encryption, security and privacy emerge […] more often than not, in a non-academic and bottom-up fashion’ (Musiani & Ermoshina, 2017, p. 54).

What is striking, however, is that very specific legislation and events are rarely mentioned. For example, I expected the Snowden revelations to be a core event for most participants but when asked about it, they said that they were either already active at the time or only joined the CPs later. [14] A consistent reason given for activism at the CPs and the two hackerspaces I visited was a general concern that politicians, on the whole, do not have much tech expertise. It is striking that the concern seems to focus on politicians as a group and the general political context but not on specific people or events. The desire to learn about technological tools is thus motivated by the larger societal context rather than a reaction to a distinct experience. There is an observable set of diffused controversies and threat-scenarios around surveillance and privacy (for a discussion on the role of dispersion in surveillance society see Huysmans, 2016). CPs react to a type of *‘political situation’* (Barry, 2012) in which digital practices of internet security and practice become a matter of concern. Importantly, this political situation is not characterised by only one particular problem, but a constellation of security issues: government surveillance, data collection by private companies, phishing and targeted hacking attacks. CPs are a result of and deeply embedded in public controversies revolving around internet security, privacy and the roles of both global ICT companies and secret services.

The relevance of CPs for understanding internet governance lies in the way they illuminate the importance of mundane practices (and not only top-down steering) in the enactment of privacy and security on a broad scale. As discussed in the conceptual section of this paper, a bottom-up perspective gives us a more thorough understanding of the role CPs play in enacting a specific understanding of security and privacy. Activists and experts alike acknowledge that users need to account for their own personal threat-scenario. Hence there exist no universal ideal, technologies or practices, but only solutions appropriate to each individual situation (see Musiani & Ermoshina 2017, p. 69; Ermoshina & Musiani, 2018). Hence, internet security and privacy are not only seen as a function of legal regulation but also something that needs to be established anew by each individual in every situation. It also becomes clear that CPs are spaces in which diffused politics are enacted.

[13] Cryptoparty 3.

[14] In the context of the Snowden revelations, Gürses et al. (2018, p. 581) observed that while technologies were contested, the larger economic and socio-structural questions were hardly debated. Hence, they argue that ultimately the encryption debate after Snowden had depoliticising effects (for a different assessment see: Monsees, 2020).

Rather than constructing a centralised threat-scenario (the state! Facebook!), what emerges is both a diffuse and decentred image of prevailing threats and also its solution.

‘Experts’ and ‘participants’

One core issue for CP organisers is the relationship between those that teach tools during CPs and those that seek to learn them. The general idea underlying CPs is that anybody can organise one, and my conversation with the organisers revealed that they would prefer it to be the case. In practice, very few people organise CPs and they tend to be the ones with expertise in the field. This is relevant since the initial intention for CPs was not that a few ‘experts’ teach non-experts but that citizens come together in order to learn together. Asher Wolf, the founder of CPs, was not an expert herself. Those who teach tools are called ‘angels’, (Cryptoparty, 2019c) a term that emphasises their helpful, friendly manner rather than characterising them as ‘geeky’ experts. Currently, CPs are not as egalitarian as originally imagined. In reality, the organisers guide participants through the implementation and use of technology, sometimes even in a lecture-style format. [15] On a more fundamental level, founder Asher Wolf quit CPs because of the persistent misogyny that, she felt, devalued the perspectives of women and laypeople (mati & Wolf, 2012). Less drastically, Kannengießer observes that ‘there are strong hierarchies persisting between “teachers” and “students”’ (Kannengießer, 2019, p. 7). The tension between the ideal of a self-organised communal effort and the actual practice of learning in more hierarchical ways is crucial for understanding the rationale of CPs.

Whereas CPs cannot function without some kind of hierarchy, the organisers explicitly work against their status in order to create an open space, resisting the tendency CPs have of defaulting to experts. One informant told me he deliberately intends cryptoparties to ‘not look too professional’. [16] Another man, explaining the tenets of email encryption to a small group of people, fostered a discussion by deliberately limiting his lecturing. [17] One episode from the last CP I attended illustrates nicely how the original idea of CPs as a communal space of learning persists: a woman who had only attended a few CPs and otherwise did not have much prior knowledge announced in the opening round that she would be leading a small group on some issues she was familiar with. She said she could teach how to

[15] CP 1 and CP planning meeting.

[16] CP 2

[17] CP2

create secure passwords and some basic knowledge about how the internet works. In her own words, this was 'pure empowerment'. [18] This episode occurred at a CP that was only open to women, trans and non-binary people, and contributes anecdotal evidence that CPs provide an open environment for people from all kinds of backgrounds. CPs point us towards new ways to transfer knowledge and the diffusion of 'expert' knowledge.

CPs also demonstrate how political knowledge and issues circulate in the public. Issues concerning private cyber security and privacy are not only negotiated via governmental institutions and legal regulations. Decentred practices such as CPs that focus on the everyday practices of individuals and the knowledge, tools and technologies they use are equally important. The organisational methods of CP's might prefigure future activism in a technological society where expert knowledge is often required. Traditional forms of citizen engagement might be less equipped to offer a dynamic and personalised learning environment, while CPs offer all participants opportunities to receive knowledge tailored to their own needs and personal habits.

In the previous section, I showed how CPs contribute to the emergence of decentred threat-scenarios and simultaneously offer a solution. In this section, I looked at how ideas about relational risks also feature in how CP participants relate to each other. Again, the political relevance of CPs does not primarily lie in the way in which they feed back into governmental decision-making processes or their impact on new legal regulation. Rather, their relevance lies in the way they '[embed] concepts such as security and privacy' (Ermoshina & Musiani 2018, p. 18) in a wider context and thereby influence both our perception of these concepts and the practices we deem appropriate in enacting them. The next section zooms in on the issue of privacy.

Cryptoparties without encryption?

While privacy is consistently one of the core goals of CPs, the practices and tools used to achieve and improve it have changed over time. In order to understand the political significance of these technological changes, a short detour into the history of privacy and encryption is necessary.

Cryptoparties, as the name suggests, originally revolved mainly around encryption. PGP (Pretty Good Privacy; also GNUPG) is the traditional way to encrypt email, based on strong public-key cryptography. [19] However, PGP was not always legal

[18] Cryptoparty 3. Kannengießer presents a very similar story (Kannengießer, 2019, pp. 6-7).

since the US government tried to constrain its usage. The objective in regulating encryption is to determine who has access to what kind of information. Cryptography was first a military technology, but its applications multiplied with the emergence of the internet (Kahn, 1997; Singh, 2000). Governments around the world, but especially the US, tried to regulate the use of strong encryption (Diffie & Landau, 2007). Crypto Wars is the umbrella term for controversies around who gets to decide what kind of encryption is available for public use (FindLaw Attorney Writers, 2012; Levy, 1994). The primary question in these early debates was whether encryption should be strong enough to prevent government access to digital communication (Diffie & Landau, 2007; Levy, 2002). Diana Saco has shown that activists fighting for stronger encryption were part of a libertarian hacker scene that was interested in keeping the state out of the internet (Saco, 2002). Ultimately, the use and spread of email encryption programmes such as PGP was legalised. Even though regulations loosened, the hopes of activists for more widespread usage of encryption by end users did not materialise (Diffie & Landau, 2007). Today, there is renewed interest in encryption and data protection due mainly to the revelations by Edward Snowden (Schulze, 2017). [20] The resulting debates and pressure by end users have led to the establishment of new products and services such as encrypted messaging services.

This shift to a broader concern with privacy and data protection mirrors the conduct of CPs. Whereas early CPs focused heavily on email encryption and the use of PGP as an end user solution (CryptoParty, 2013), participants in the CPs I visited showed concern for a variety of vulnerabilities: the collection of data by corporate actors, secure internet banking and targeted hacking attacks. As discussed in the previous two sections, this shift dovetails with the way in which CPs enact decentred threat-scenarios. The changing societal context goes hand in hand with the changing availability of products. But there also seems to be a more technical reason for why PGP and email encryption are no longer a core privacy technology. If used incorrectly, PGP is harmful, and hence is not always taught at CPs. Indeed, email encryption does not constitute the main part of CPs anymore. Only two organisers still consider PGP the best (and only) tool to send email securely. According to them, despite PGP being complicated, it is still the most valuable tool for privacy in a digital environment. Even hackers consider PGP too complicated (Whitten & Tygar, 1999). During my visit at two hackerspaces only one person

[19] For a more in-depth description of the principle of public key cryptography, see Monsees (2020, pp. 61-63).

[20] That is why I expected the Snowden revelations would be identified as a crucial event by the activists. However, the importance of his revelations was played down in the interviews.

claimed to use PGP on a regular basis. Email encryption, while still considered to be crucial, is no longer central to debates on internet security. Rather, it is now included with other security and privacy tools that allow, for instance, for private messaging or anonymous browsing. Current discussions on email security focus on methods of server security and data mining by email providers. The original focus of CPs on PGP and email encryption has almost vanished, allowing for a more diffuse set of tools.

As a result, it becomes clear that CPs and their core idea has evolved considerably over time. Not only has the technological environment changed, the organisers have learned more about how end users can implement these tools. Several informants told me that over time they realised that teaching email encryption is too complicated and therefore decided to drop this tool and focus on other technologies. They learned from past experience and adapted their CP. At the same time, the political context and dominant technologies have changed. Today, users achieve privacy not mainly by personally encrypting their data, but by choosing services (social networks, messaging) that provide more privacy. In sum, we can see how technological change, societal change and individual learning processes alter CPs and the tools they teach.

This section showed how the political situation, the assessment of encryption technology and the diverse needs of participants all require comprehensive tools to enhance privacy and security. In contrast to earlier battles in the 1990s, the current issues can no longer be understood as a simple controversy about one particular technology such as PGP. Coming back to the insights from the first empirical section, we can see how learning and adapting to an ever-changing political and technological landscape is a core feature of CPs.

Conclusion

The present article is one of the few empirical studies on cryptoparties to date. The distinct focus on CPs as a political practice allowed a better understanding of a theme which receives only scarce academic and public attention. Based on participant observation of three CPs, informal interviews and additional document analysis, the study showed how CPs teach multiple tools to enhance privacy and prevent surveillance. The organisers of CPs strive for an egalitarian space for teaching and learning. Even though this goal is not always achieved, CPs can still serve as an example of citizen education in a technological society where every citizen needs to deal with complex technological issues.

On a more conceptual level this paper contributed to the emerging debate on 'doing internet governance'. Drawing on previous research which identified the need to look at micro-practices, I argued for the political relevance of CPs. Even though these practices might not have a direct impact on legislation, they are still politically relevant. I demonstrated that CPs work well in a political situation that is characterised by diffuse threats. Cyber threats do not only originate from centralised, top-down dynamics but might originate from a multiplicity of spaces and agents (states, hackers, private companies). I showed how CPs are able to react to this decentered threat-scenario by adapting the tools they teach. Indeed, encryption was a core issue of legal battles in the 1990s and threats to regulate it are still present in the current discourse (Schulze, 2017). Cryptoparties started with a strong focus on teaching email encryption, but my empirical observation revealed that current CPs focus on a multiplicity of issues. This shift coincides with observable technological changes. Presently, encryption is much more likely to be embedded as part of other tools. The focus is less on only email encryption (as it was in the controversies in the 1990s) but on how encryption can be part of, for instance, messaging tools. Indeed, encryption is only one part of the solution when thinking about safe surfing, private messaging or protecting one's anonymity.

This also means that a narrow focus on institutional aspects and legal regulations might miss the security and privacy maintenance done by end users on an everyday basis. Understanding this change in the *de facto* use of tools and their spread requires the study of mundane practices of end users. The focus on the practice of CPs revealed the importance of the idea of establishing a 'security culture'. For the organisers, the aim is not only to teach specific tools but to increase awareness about the multiple vulnerabilities that users might encounter. The organisers want to teach how a higher level of security is possible. Some participants were scared and overwhelmed, prompting the organisers to teach simple tools that will still help to increase privacy and security. In line with previous research, it becomes clear that the idea is not to teach some tools that establish security once and for all but make the participants aware of their own threat-model and the multiplicity of adversaries (see also Ermoshina & Musiani, 2018). This became especially visible in the small groups that discussed 'how the internet works'. Rather than teaching one specific tool, the idea was more to increase knowledge about technology and create awareness of one's specific threat-model.

This speaks to a similar observation William H. Dutton has made about the need for a 'security mindset'. According to him 'In cyber security, the risks are more difficult to communicate, given the multiplicity of risks in particular circumstances'

(Dutton, 2017, p. 3), requiring us to rethink how to communicate about these threats. In the cyber context the threats are more diffuse and often not directly felt. The core task is, then, to develop a 'mindset' about beliefs, attitudes and values concerning cyber security. While I do not think that Duttton's solution of using PGP everywhere is attainable for reasons described above, his plea for more encompassing research and policies for sensitising end users is certainly valid. Both future policies and citizen engagement practices can learn from CPs when negotiating the difficult terrain of teaching complex technologies in a political situation where threats to privacy and intrusion come from everywhere. The openness and adaptability of CPs are certainly helpful in an environment which is characterised by high complexity. Especially CPs that focus on women, transgender and nonbinary participants are able to create an open environment where a diverse ensemble of laypeople feel welcome. Mirroring these insights, it becomes clear that the conduct and the study of internet governance encompasses micro-practices and their evolution, and increasingly moves beyond a focus on institutions.

References

Barry, A. (2012). Political situations: Knowledge controversies in transnational governance. *Critical Policy Studies*, *6*(3), 324–336. https://doi.org/10.1080/19460171.2012.699234

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology*, *8*(2), 121–144. https://doi.org/10.1111/ips.12048

Bellanova, R. (2017). Digital, politics, and algorithms: Governing digital data through the lens of data protection. *European Journal of Social Theory*, *20*(3), 329–347. https://doi.org/10.1177/1368431016679167

Cetina, K. K., Schatzki, T. R. (2005), von Savigny, E. (Eds.). *The Practice Turn in Contemporary Theory*. Routledge. https://doi.org/10.4324/9780203977453

Christensen, K. K., & Liebetrau, T. (2019). A new role for 'the public'? Exploring cyber security controversies in the case of WannaCry. *Intelligence and National Security*, *34*(3), 395–408. https://doi.org/10.1080/02684527.2019.1553704

Coleman, G. (2010). The Hacker Conference: A Ritual Condensation and Celebration of a Lifeworld. *Anthropological Quarterly*, *83*(1), 47–72. https://doi.org/10.1353/anq.0.0112

CryptoParty. (2013). *The Crypto Party Handbook*. https://www.cryptoparty.in/learn/handbook

CryptoParty. (2019a). *Code of Conduct* [Wiki]. CryptoParty. https://www.cryptoparty.in/code_of_conduct

CryptoParty. (2019b). *CryptoParty* [Wiki]. https://www.cryptoparty.in/

CryptoParty. (2019c). *How to Organize a CryptoParty* [Wiki]. CryptoParty. https://www.cryptoparty.in/o rganize/howto

CryptoParty. (2019d). *Upcoming Parties* [Wiki]. CryptoParty. https://www.cryptoparty.in/parties/upcoming

DeNardis, L. (2010). *The Emerging Field of Internet Governance* (Yale Information Society Project) [Working Paper]. Yale University. https://doi.org/10.2139/ssrn.1678343

Denning, D. E. (1996). The Future of Cryptography. In P. Ludlow (Ed.), *Crypto Anarchy, Cyberstates, and Pirate Utopias*(pp. 85–101). MIT Press.

Diffie, W., & Landau, S. E. (2007). *Privacy on the line: The politics of wiretapping and encryption*. MIT Press.

Dutton, W. H. (2017). Fostering a cyber security mindset. *Internet Policy Review*, *6*(1). https://doi.org/10.14763/2017.1.443

Eeten, M. J., & Mueller, M. (2013). Where is the governance in Internet governance? *New Media & Society*, *15*(5), 720–736. https://doi.org/10.1177/1461444812462850

Emerson, R., Fretz, R., & Shaw, L. (2001). Participant observation and fieldnotes. In P. Atkinson, A. Coffey, S. Delamont, J. Lofland, & L. Lofland (Eds.), *Handbook of Ethnography* (pp. 352–368). SAGE Publications. https://doi.org/10.4135/9781848608337.n24

Epstein, D., Katzenbach, C., & Musiani, F. (2016). Doing internet governance: Practices, controversies, infrastructures, and institutions. *Internet Policy Review*, *5*(3). https://doi.org/10.14763/2016.3.435

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

FindLaw Attorney Writers. (2012, June 21). *30 Years of Public-Key Cryptography*. FindLaw. http://technology.findlaw.com/legal-software/30-years-of-public-key-cryptography.html

Flyverbom, M. (2016). Disclosing and concealing: Internet governance, information control and the management of visibility. *Internet Policy Review*, *5*(3). https://doi.org/10.14763/2016.3.428

Franke, U., & Roos, U. (2013). Einleitung: Zu den Begriffen 'Weltpolitik' und 'Rekonstruktion'. In U. Franke & U. Roos (Eds.), *Rekonstruktive Methoden der Weltpolitikforschung: Anwendungsbeispiele und Entwicklungstendenzen* (pp. 7–29). Nomos.

Gillespie, A., & Michelson, M. R. (2011). Participant Observation and the Political Scientist: Possibilities, Priorities, and Practicalities. *PS: Political Science & Politics*, *44*(2), 261–265. https://doi.org/10.1017/S1049096511000096

Gregory, M. A. (2012, August 23). Cybercrime bill makes it through – but what does that mean for you? The Conversation. *The Conversation*. https://theconversation.com/cybercrime-bill-makes-it-through-but-what-does-that-mean-for-you-8953

Guillaume, X., & Huysmans, J. (2013). Citizenship and Securitizing: Interstitial Politics. In X. Guillaume & J. Huysmans (Eds.), *Citizenship and security: The constitution of political being* (pp. 18–34). Routledge.

Gürses, S., Kundnani, A., & Van Hoboken, J. (2016). Crypto and empire: The contradictions of counter-surveillance advocacy. *Media, Culture & Society*, *38*(4), 576–590. https://doi.org/10.1177/0163443716643006

Herrera, G. L. (2002). The politics of bandwidth: International political implications of a global digital information network. *Review of International Studies*, *28*(1), 93–122. https://doi.org/10.1017/S0260210502000931

Herring, S., Job-Sluder, K., Scheckler, R., & Barab, S. (2002). Searching for Safety Online: Managing 'Trolling' in a Feminist Forum. *The Information Society*, *18*(5), 371–384. https://doi.org/10.1080/01972240290108186

Hofmann, J. (2016). Multi-stakeholderism in Internet governance: Putting a fiction into practice. *Journal of Cyber Policy*, *1*(1), 29–49. https://doi.org/10.1080/23738871.2016.1158303

Hofmann, J., Katzenbach, C., & Gollatz, K. (2016). Between coordination and regulation: Finding the governance in Internet governance. *New Media & Society*, *19*(9), 1406–1423. https://doi.org/10.1177/1461444816639975

Huysmans, J. (2016). Democratic curiosity in times of surveillance. *European Journal of International Security*, *1*(1), 73–93. https://doi.org/10.1017/eis.2015.2

Isin, E. F., & Ruppert, E. (2015). *Being Digital Citizens*. Rowman & Littlefield.

Jackson, P. T. (2011). *The conduct of inquiry in international relations: Philosophy of science and its implications for the study of world politics*. Routledge. https://doi.org/10.4324/9780203843321

Kahn, D. (1997). *The codebreakers: The comprehensive history of secret communication from ancient times to the Internet*. Scribner's and Sons.

Kannengießer, S. (2019). Reflecting and acting on datafication – CryptoParties as an example of re-active data activism. *Convergence: The International Journal of Research into New Media Technologies*. https://doi.org/10.1177/1354856519893357

Kubitschko, S. (2015). The Role of Hackers in Countering Surveillance and Promoting Democracy. *Media and Communication*, *3*(2), 77–87. https://doi.org/10.17645/mac.v3i2.281

Leander, A. (2017). From Cookbooks to Encyclopaedias in the Making: Methodological Perspectives for Research of Non-State Actors and Processes. In A. Kruck & A. Schneiker (Eds.), *Methodological Approaches for Studying Non-state Actors in International Security. Theory and Practice* (pp. 231–240). Routledge. https://doi.org/10.4324/9781315669830-16

Levy, S. (1994, November 2). Cypher Wars: Pretty Good Privacy Gets Pretty Legal. *Wired*. http://encryption_policies.tripod.com/industry/levy_021194_pgp.htm

Levy, S. (2002). *Crypto: How the code rebels beat the government, saving privacy in the digital age*. Penguin Putnam.

Loder, C. (2014). Something to Hide: Individual Strategies for Personal Privacy Practices. *IConference 2014 Proceedings*, 814–819. https://doi.org/10.9776/14403

Marx, G. T. (2015). Security and surveillance contests: Resistance and counter-resistance. In T. Balzacq (Ed.), *Contesting security: Strategies and logics* (pp. 15–28). Routledge. https://www.taylorfrancis.com/books/e/9780203079850/chapters/10.4324/9780203079850-9

mati, & Wolf, A. (2012, December 30). Dear Hacker Community—We Need to Talk [Blog post]. *Fachschaft Informatik*. https://www.fsinf.at/posts/de/2012-12-30-dear-hacker-community-we-need-to-talk/

Monsees, L. (2020). *Crypto-politics: Encryption and democratic practices in the digital era*. Routledge. h ttps://doi.org/10.4324/9780429456756

Mueller, M. L. (2010). *Networks and States: The Global Politics of Internet Governance*. MIT Press. https://doi.org/10.7551/mitpress/9780262014595.001.0001

Musiani, F., & Ermoshina, K. (2017). 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*, *12*(3), 51–71. https://doi.org/10.16997/wpcc.265

Myers West, S. (2018). Cryptographic imaginaries and the networked public. *Internet Policy Review*, *7*(2). https://doi.org/10.14763/2018.2.792

Poulsen, K. (2014, May 21). Snowden’s First Move Against the NSA Was a Party in Hawaii. *Wired*. https://www.wired.com/2014/05/snowden-cryptoparty/

Radio Free Europe. (2012, November 27). The Woman Behind Crypto Party. *Radio Free Europe*. https://www.rferl.org/a/the-woman-behind-cryptoparty/24782719.html

Raymond, M., & DeNardis, L. (2015). Multistakeholderism: Anatomy of an inchoate global institution. *International Theory*, *7*(3), 572–616. https://doi.org/10.1017/S1752971915000081

Reichertz, J. (2016). *Qualitative und interpretative Sozialforschung: Eine Einladung*. Springer. https://doi.org/10.1007/978-3-658-13462-4

Saco, D. (2002). *Cybering democracy: Public space and the Internet*. University of Minnesota Press.

Schulze, M. (2017). Clipper Meets Apple vs. FBI—A Comparison of the Cryptography Discourses from 1993 and 2016. *Media and Communication*, *5*(1), 54–62. https://doi.org/10.17645/mac.v5i1.805

Schwartz-Shea, P., & Yanow, D. (2012). *Interpretive research design: Concepts and processes*. Routledge. https://doi.org/10.4324/9780203854907

Selimovic, J. M. (2019). Everyday agency and transformation: Place, body and story in the divided city. *Cooperation and Conflict*, *54*(2), 131–148. https://doi.org/10.1177/0010836718807510

Singh, S. (2000). *The code book: The science of secrecy from ancient Egypt to quantum cryptography*. Anchor Books.

Solomon, T., & Steele, B. J. (2017). Micro-moves in International Relations theory. *European Journal of International Relations*, *23*(2), 267–291. https://doi.org/10.1177/1354066116634442

Tanczer, L. M. (2016). Hacktivism and the male-only stereotype. *New Media & Society*, *18*(8), 1599–1615. https://doi.org/10.1177/1461444814567983

Tanczer, L. M. (2017, April 6). *Digital skills in academia: Let’s CryptoParty! OpenDemocracy*. openDemocracy. https://www.opendemocracy.net/en/digital-skills-in-academia-let-s-cryptoparty/

Whitten, A., & Tygar, J. D. (1999). Why Johnny can’t encrypt: A usability evaluation of PGP 5.0. *Proceedings of the 8th Conference on USENIX Security Symposium*, *8*. https://www.usenix.org/legacy/events/sec99/full_papers/whitten/whitten.ps