Caring for IT Security: Accountabilities, Moralities, and Oscillations in IT Security Practices

LAURA KOCKSCH, Faculty of Social Science & SecHuman, Ruhr University Bochum, Germany
MATTHIAS KORN, Institute for Information Systems & iSchool, University of Siegen, Germany
ANDREAS POLLER, Fraunhofer Institute for Secure Information Technology, Germany
SUSANN WAGENKNECHT, Department of Social Sciences, University of Siegen, Germany

Despite being considered a fundamental issue in the design, use, and appropriation of digital technologies, IT security has found but little attention in CSCW so far. Approaches in Human-Computer Interaction and Software Engineering do not account appropriately for the weave of dispersed practices that it takes to 'do' IT security—practices that involve a heterogeneous set of actors and unfold at diverse sites and across organizational, legal, and professional boundaries. In this paper we propose to conceive of IT security through the lens of care, a notion that we draw from Science and Technology Studies. Caring for IT security requires continuous, often invisible work that relies upon tinkering and experimentation and addresses perennial oscillations between in-/securities. Caring for IT security, then, engages with established accountabilities and cultivates a moral stance that refrains from blaming insecurities upon single actors. We conclude with outlining a caring approach to IT security for CSCW.

CCS Concepts: • **Human-centered computing** → **Computer supported cooperative work**; • **Security and privacy** → *Social aspects of security and privacy*;

Additional Key Words and Phrases: IT security; care; maintenance and repair; tinkering; hacking; software development; Usable Security; Software Engineering.

ACM Reference Format:
Laura Kocksch, Matthias Korn, Andreas Poller, and Susann Wagenknecht. 2018. Caring for IT Security: Accountabilities, Moralities, and Oscillations in IT Security Practices. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 92 (November 2018), 20 pages. https://doi.org/10.1145/3274361

1 INTRODUCTION

> *"We should have more women on the board. They are good with the caring aspects of work."*
>
> — IT security professional at a software company,
> in personal communication with first author

Technologies, Annemarie Mol and colleagues write, "do not work and fail in and of themselves" but instead "depend on care work" [27, p. 15], forms of work that tend to be hands-on, piecemeal, badly

Authors' addresses: Laura Kocksch, Faculty of Social Science & SecHuman, Ruhr University Bochum, Universitaetsstr. 150, 44801 Bochum, Germany, laura.kocksch@rub.de; Matthias Korn, Institute for Information Systems & iSchool, University of Siegen, Kohlbettstr. 15, 57068 Siegen, Germany, matthias.korn@uni-siegen.de; Andreas Poller, Fraunhofer Institute for Secure Information Technology, Rheinstr. 75, 64295 Darmstadt, Germany, andreas.poller@sit.fraunhofer.de; Susann Wagenknecht, Department of Social Sciences, University of Siegen, Adolf-Reichwein-Str. 2, 57068 Siegen, Germany, susann.wagenknecht@uni-siegen.de.

2573-0142/2018/11-ART92 $15.00
https://doi.org/10.1145/3274361

accounted for, and feminized. Care is always ongoing, it never finds closure and hence demands affective commitment and dedication. In this paper, we propose the notion of IT security as *careful* practices, an approach that seeks to account for the nitty-gritty of keeping IT systems *secure*. IT security is typically framed in terms of technological fixes, such as updating software or introducing stricter password requirements. We, instead, characterize IT security as a matter of care, i.e., the object of continuous, often collaborative tinkering and experimentation—efforts that spread across sites and scales and involve a range of diverse actors.

When studying what it means to care for IT security, we complement recent research on the care of people, communities, organizations, and/or technologies in Computer-Supported Cooperative Work (CSCW) [6, 14, 16, 19]. We depart, however, from existing research on IT security in fields such as Usable Security or Software Engineering. In these research fields, IT security is commonly understood as the measures taken to prevent an 'adversary' from 'attacking' a computer system, i.e., gaining unauthorized access and/or corrupting the system. Insecurity, then, is framed as either technological shortcoming or mismatch between design and users' competencies. Within this framework, responsibilities for securing computer systems are delegated to developers [13] or individual users [12]. But such approaches, we find, are too limited to account for the ever-ongoing, multi-sited efforts that it takes to address IT security. Challenging Usable Security and Software Engineering, we follow existing research in CSCW [9] and re-frame IT security as a social phenomenon in the making. We examine how IT security is dealt with in professional practices of technology production and maintenance. In so doing, we suggest to understand IT security in terms of heterogeneous bundles of practices [38, 39], which interweave dispersed efforts that involve both collaboration and antagonism [21].

In this paper, we do what Puig de la Bellacasa calls "displac[ing] care", i.e., "involving it in issues and debates in which it has not frequently been addressed" [36, p. 12]. When we use the feminist concept for studying a male-dominated field not previously analyzed in its terms, we draw attention to the invisibilized, undervalued, and also unruly aspects of doing IT security. In so doing, we hope to expand and deepen the debate about what it means to secure computer systems. IT security is known to be treacherous, notorious for never being quite as solid as it seems. What would improve the security of computer systems? The epigraph above cites a male sales representative for IT security tools who, during an informal chat with a female ethnographer, tries to come up with a solution that would make corporate software developers write more secure code. It is revealing that in this conversation, the sales representative does not pitch his portfolio and refrains from advertising yet another of his products. Having closely cooperated with software developers throughout his professional career, he knows about the weak visibility of security issues and the often fuzzy accountabilities around them. So instead of blaming single developers or dated tools he makes an astonishing suggestion: "We should have more women on the board." With this suggestion, the sales representative embraces calls to increase the number of women in business leadership positions across the IT sector. He endorses a feminist cause but, at the same time, invokes an utterly sexist archetype—the "caring" woman who works to redeem male carelessness. While we reject such sexism, we do believe that his suggestion conveys important points: IT security demands care, and it demands a feminist perspective.

Aiming the lens of care at IT security, we unpack what it means to care for IT security. To do so, we present four vignettes, each of which describes a different site of practice and highlights different facets of caring for IT security. Thereby, we enrich care as an analytic notion, drawing attention to the ways in which care relates to dispersed accountabilities and alternate moral registers. We conclude with outlining a caring approach to IT security, an approach that, we believe, both benefits future research in CSCW and adjacent fields as well as interventions in practice.

2 BACKGROUND AND RELATED WORK

The practices and infrastructures that "hold the logics of (in)security in place" [42, p. 984] have recently re-entered the limelight of research in the social sciences. While much of ongoing research in Science and Technology Studies (STS) examines how sociotechnical systems are employed in the name of national or state security [3, 46, 50], Nissenbaum [30] points out how national security and IT security are distinct, yet closely related. In the following, we focus solely on IT security and the question what it takes to secure computer systems.

2.1 IT Security

Security and privacy have long been important research topics in the field of Human-Computer Interaction (HCI), where Usable Security has emerged as an interdisciplinary research area [12, 18]. Research in Usable Security focuses on the relationship between use and design, aiming to create human-computer interactions that meet pre-given security standards and procedures. In the perspective of Usable Security, users are considered in charge of using technology in secure ways, and technology, in turn, should support users in doing so. This view is challenged by Dourish and Anderson [9] who regard security as a sociocultural phenomenon, a collective endeavor that is formulated relative to social and cultural values. Security, Dourish and colleagues argue, is not a matter of predefined standards; it is rather a "practical problem" [10] that emerges from, and is addressed through, "collective information practice" [9].

However, by considering technology use and appropriation, Usable Security as well as its criticism still focus primarily on end-user settings. Only more recently has this focus shifted to technology production: Driven by the observation that users are supplied with information technology that is inherently insecure on its release, interdisciplinary researchers from HCI and Software Engineering have started to pay attention to the creation, operation, and maintenance of information technology [13]. New research interests have emerged including the material artifacts of software production such as tools for secure software development [47, 49], programming interfaces [2], and code analysis tools [40], as well as the practices of operating technology securely [11].

Notwithstanding changing research interests, the underlying rationale remains the same: Just as Usable Security examines how end-users struggle to use information technology in a secure manner, emerging studies on software production examine how developers struggle to comprehend and employ security tools and aids appropriately [2, 11]. But a range of recent studies of software production acknowledge that IT insecurity cannot be explained solely in terms of developers, their behavior, knowledge, skills, and perceptions, or their tools. Rather, IT insecurity is inextricably tied to questions of collaborative work practices and corporate management. In this vein, research on IT insecurity has studied how software developers are held accountable to consider technical security aspects [29], how their work benefits from opportunities for collaboration [47], and how security and development practices may impede each other [1, 28, 49]. Exploring these questions in connection, we argue, requires an understanding of technology production as bundles of interconnected, dispersed, and multi-faceted practices, shaped by organizational accountabilities, community commitments, and notions of good and bad.

Similar to Dourish and Anderson [9], we therefore frame IT security not as limited to tools, competencies, and perceptions but instead as a collective and dynamic social phenomenon. First steps to reframe IT security in this way have been taken in studies that examine the relationships among actors concerned with IT security. For instance, Ashenden and Sasse investigate how managers in charge of IT security are positioned within their company and how they interact with other employees [4]. Xiao et al. study how the diffusion of security tools depends on developers' social environment, e.g., the relationship between a company's security experts and software developers [48]. Poller et al. investigate the interplay of organizational structure and software developers' agency, stressing the role of narratives and tangibility of work results for corporate security programs [31]. Korn and Wagenknecht examine the tense relations between hacking communities and industry [21].

Following these lines of research, we want to propose a CSCW perspective on IT security by suggesting to explore security as care. We therewith take up recent conceptual shifts in STS, approaching IT security not as a matter of fact (and fabrication) but instead as a matter of concern (and worry), and more specifically as what Puig de la Bellacasa calls "matters of care": "The notion [...] is a proposition to think with. Rather than indicating a method to unveil what matters of fact are, it suggests that we make of them what is needed to generate more caring relationships" [34, p. 100].

2.2 The Lens of Care

In using care as a lens for examining IT security we approach IT security as brittle, frail, and messy, an ongoing achievement that involves continuous dedication. The work of care is what it takes "to meticulously explore, test, touch, adapt, adjust, pay attention to details and change them, until a suitable arrangement (material, emotional, relational) is achieved" [27, p. 16]—hands-on and piecemeal efforts that tend to be feminized, invisibilized, and are hardly ever considered a task in themselves. Care can be given, ostensibly, to people (as in nursing) but also to things (as in caretaking and maintenance). In attending to artifacts, systems, or infrastructures, caring means to work with materials and technologies as parts of more or less fragile networks, addressing them in their vulnerability while striving, ceaselessly, for stabilization—when stability must remain ephemeral [7]. Since this kind of work relies upon improvisation and can hardly be standardized [15], the work of care tends to fall between the cracks of organizational accountability.

The literature on care has grown immensely over the last years. For the purpose of this paper we draw particularly on the works of Mol and colleagues [27] as well as Denis and Pontille [7], all of whom compellingly argue that working technologies are, essentially, a matter of care. We furthermore rely on Puig de la Bellacasa's [34] work to uncover the moralities implied in caring for IT security.

It is important to note "the double significance of care as an everyday labour of maintenance that is also an ethical obligation" [34, p. 90]. While maintenance is a vital aspect of care, caring is often a kind of intervention aimed at changing the status quo 'for the better' ([36, p. 6], also [25]). Taking and giving care requires both material engagement and affective commitment. To care is deeply moral, but it is not normative in the sense of conventional ethics, i.e., to care is not about making judgments and holding people accountable against normative standards. It is also not so much about negotiating binding agreements or other forms of 'moral closure'. Rather, to care is about acknowledging moral heterogeneity and the open-ended, situated character of efforts to do good ([27, p. 15], see also [26, 35]). Precisely because the notion of care is fraught with goodwill and promise, the politics and limits of care require particular attention. Care is never all-encompassing; it is but one way of forging relations. And care is not innocent either; it is a compelling regime of power ([36, p. 11], also [25]).

The fact that the work of care is typically both invisibilized and feminized continues to have extraordinary consequences on gender inequality, women's pay and social status. But the feminization of care is not a women's issue only. In recent research, the notion of care has been applied in studying various forms of labor, investigations that have led beyond feminized occupations and for which a focus on female labor has proven too narrow [7, 25, 27]. To work with the notion of care in male-dominated, masculine fields has the potential to question cherished matters of course, raising challenging questions: What role does care play in these fields? Where and when does the ethnographer observe care? How do careful practices take shape in these fields? How is care brought up by the field itself—as presence or absence, in the complacent self-presentation of those who care or as allegation of carelessness?

2.3 Care in CSCW

In applying the lens of care, we take cues from a growing body of previous research in CSCW [6, 14, 16, 19, 22, 37, 43, 44]. Predominantly, CSCW research has concerned itself with interpersonal notions of care—the care of *people*. This includes service-oriented notions such as in health care, care for the elderly, care for other people in need, and so on [14, 19]. Parts of the research on the care of people has mobilized feminist care ethics to emphasize people's interdependence. Feminist-influenced accounts seek to go beyond a paternalistic view on care, emphasizing that care often goes both ways and encompasses caring for others as much as being cared for by others [22, 43, 44].

In CSCW, the care of people has become a central theme in research on communities and civic society [22, 44], in reflexive accounts of participatory research [22, 43], and in research on organizational settings [6, 14, 19]. In their study of philanthropic organizations, Harmon et al. [14] show the different scales at which care is enacted, ranging from individuals engaging in small and distinct acts of 'doing good' to collectives engaging in organizationally mediated forms of coordinated philanthropy. In their study of humanitarian help, Jack and Jackson [19] point out tensions between care and control in organizations where tasks associated with affective dedication confront confusing and challenging circumstances that need to be managed and controlled. Both studies illustrate how organization members, in the face of the perceived societal importance of the organization's mission or cause, develop an attitude of care also for the work itself.

The care of *things* (cf. [7, 27]), in contrast, is beginning to gain traction particularly in CSCW research on feminist hacking, maintenance, and repair [6, 16, 37]. In her research on a decaying space research infrastructure, Cohn observes how space researchers and engineers, slowly recognizing that the "machine is not what it once was" [6, p. 1514], positioning the spacecraft as "aged and in need of care" [6, p. 1515]. In their study of mobile phone repair, Houston and Jackson emphasize how "[c]are as applied to the world of things foregrounds the fragility of material objects and the wider social and technical worlds in which they circulate" [16, p. 10:2]. The notion of care, they argue, helps to "locate immediate forms of technical work within wider moral and political orderings" [16, p. 10:1], an insight we pursue below.

3 METHOD

This paper is a collaborative undertaking of the authors, drawing on fieldwork conducted both independently and in collaboration with one another. Building on research engagements with the field of IT security over the last six years [21, 31–33, 45], we gathered, compared, and discussed field notes from three different studies, all of which have been carried out in Germany: (1) from participant observations at Europe's largest hacking convention in 2015 and 2016 at four days each and the convention's associated online archival materials [21, 45]; (2) from participant observations and twelve semi-structured interviews at a global software vendor in 2014 and 2015 [31]; and (3) from three months of participant observations at a large utility company in 2017.

As recent research in CSCW has shown [17, 23], combining ethnographic data from diverse sites is key to examining the dispersion of sociotechnical phenomena [24]. For this reason, we bring together observations of four sites in each of which IT security is negotiated in a different manner: a talk given at a hacker convention, a security training for developers in a software company, a meeting with two of the developers who attended the training, and software developers configuring access control to a new data storage system in a utility company. At all four sites, various actors and multiple practices are involved in doing IT security, i.e., the ways in which IT security is created, maintained, challenged, undermined, and re-made. Taken together these four sites offer opportunities to explore IT security as a phenomenon that stretches across software development, software deployment in organizations, technology use and appropriation, and computer hacking.

The sites we have chosen to present are connected with one another in different ways. Some are immediately related as they are nested within the same organization. (Having observed a corporate IT security training, the first author went on to find out among training participants what might have changed in its aftermath.) All four sites are illustrative of specific ways of doing IT security, bundles of practices that relate to one another. As we will show, e.g., hackers and security researchers create the insecurities that software developers, sometimes with the help of external security consultants, are supposed to address. The sites, hence, are host to practices that can be connected through actors, materials, or meanings. It is not uncommon for security researchers, e.g., to present parts of their work at a hacking convention *and* make a living as external consultants, conducting training sessions with corporate developers. These connections, however, must not suggest that what is done about IT security at different sites is part of well-concerted action. Tension, friction, and disparities abound. Much of 'white hat' hacking, e.g., claims to work towards a vision of community-owned, not-for-profit knowledge, whereas corporate software development is concerned with the quality (and profitability) of a privately-owned product. Software developer or architect is an ordinary, well-paid, and relatively secure day job—hacker is not. Software development has to fit in with corporate management and tackles long-term projects—external consultancy does not. But note the apparent similarities, too. Across all sites, actors are overwhelmingly male, technology-savvy, well-educated, and middle class. (The hacking convention features mostly male speakers from Western countries. The software development company recruits internationally. The utility company employs predominantly Western European personnel.)

We convey our observations of different sites in the form of vignettes. As our empirical data stem from different researchers and research studies, the vignettes exemplify slightly different ethnographic techniques and modes of engagement with the field—from the ethnography of time-bound events to long-term and ongoing participant observations on company premises. Direct quotes used in the vignettes are drawn either from verbatim field notes, audio recordings of interviews, or online archival materials.

The vignettes, created from ethnographic data none of which has been analyzed previously, have been selected to convey motifs that we have observed recurrently throughout our data. Our ethnographic data have been coded collaboratively by all four authors in an open-ended, iterative process. In this process, we combined rounds of open coding with theory-guided codes. Open codes such as [*blaming*], [*oscillations of in-/security*], or [*control*] have sensitized us to the particular dynamics of what it means to 'do' IT security. Theory-guided codes such as [*invisible*], [*ongoing concern*], or [*experimentation/tinkering*] have enabled us to explore resonances with the notion of care as established in the literature.

We rely on care as an analytic lens to unfold the open-ended processuality of doing IT security, an understanding of IT security that all authors share and that has emerged from their previous work on IT security. The suggestion to conceive of IT security in terms of care surfaced early on in our collaborative research process, at a two-day workshop that explored how IT security can be fruitfully understood as ongoing collective achievement—a workshop that we organized to bring together social scientists, security researchers, and practitioners.[1] Proceeding from discussions among workshop participants, care as an analytic lens has subsequently informed our selection of data and their analysis.

[1] See https://it-security.wineme.fb5.uni-siegen.de/, last accessed on August 15, 2018.

As our analytic lens, the notion of care has shed a specific light upon our data, highlighting some aspects (temporality, accountability, morality) while backgrounding others (efficiency, confrontation, liability). In this manner, the lens of care has enabled us to formulate an account of IT security that does not emulate common narratives of faulty technologies, malevolent hackers, incompetent users, and negligent developers but instead comments upon such narratives. Any lens, however, has its bias, and we therefore also set out to probe its limits, paying particular attention to how aspects of IT security evade or confront the notion of care. We deliberately speak of care as a 'lens' to be conscious about how we position ourselves towards the field when we analyze our data, marking a difference between the observed and the observing, and emphasizing the relationality of what we present as the results of our study.

4 FOUR SITES OF IT SECURITY

Each of the following four vignettes sheds light on different aspects of doing IT security: hacking, teaching, organizing, negotiating, and tinkering. Yet drawn together, the vignettes convey a multi-faceted notion of what it means to care for IT security. Their combination allows to trace cross-cutting themes and connections, such as the ephemeral character of security, the moral registers implied in dealing with IT security, as well as issues of accountability and invisible work.

4.1 In-/Securities

The winter weather in Hamburg is grey, and it is dark inside the convention centre. The lamps are dimmed, LEDs are blinking, and the pale light of computer screens is reflected in people's faces. The Chaos Communications Congress, Europe's largest hacker convention, makes it hard to distinguish between day and night. The event, organized annually between Christmas and New Year's by the Chaos Computer Club (CCC) and legions of volunteers, is attracting more than 10,000 visitors per year. We are happy to have tickets for the 2016 event.[2] In fact, this is not the first time that second and fourth author visited the event. In 2015, the fourth author gave a presentation on the portrayal of hacking in social science at the convention. The second author is a long-time (if not active) member of the CCC. Both authors have been pursuing a research interest in hacking practices over the last years.

Once we enter the building, we find ourselves amid hackers, tech enthusiasts, media artists, and left-wing activists of all ages. Over the years, the number of small children present seems to grow constantly. There is also quite many people we recognize from media appearances and previous conventions—long time veterans of the CCC. The CCC, founded in 1986, describes itself as a 'white hat' hacking community seeking to promote 'freedom of information'. While a range of presentations at the convention cover digital art, global politics, and tech policy, so-called *security research*, i.e., the identification and exploitation of security weaknesses, remains at the core of the event. At the convention, security researchers will be admired and applauded for being able to demonstrate how to hack technologies—not, as presenters underline time and again, for profit or out of malicious intent, but to weed out insecurities and work towards a vision of 'open' technology.

The convention is an elaborate, well-rehearsed community ritual. Since a couple of years, all presentations given at the convention are recorded and stored in the CCC's media archive (media.ccc.de) so that we, months after the 2016 convention took place, are able to revisit a talk given by LaForge and holger, both renowned members of the CCC who are well known for their work on insecurities in mobile phone technology. This year, too, they promise to take on severe security weaknesses in a talk titled "Dissecting modern (3G/4G) cellular modems".[3]

[2] http://web.archive.org/web/20171031115221/http://events.ccc.de/congress/2016/wiki/Main_Page, last accessed 2018-08-16.
[3] See https://media.ccc.de/v/33c3-8151-dissecting_modern_3g_4g_cellular_modems, last accessed on April 18, 2018.

The talk shows how to reverse-engineer the computer code on state-of-the-art 3G/4G cellular modems (i.e., computer chips for broadband communication included in every smartphone, tablet, etc.), discussing property rights issues and security weaknesses. Understanding the talk requires quite some technical knowledge. But towards the end of their presentation, the speakers offer more general, programmatic remarks:

> *holger:* “But instead of just saying how bad it is we want to say what we expect them [industry] to do, and I’m handing over to [LaForge] again.”
>
> *LaForge:* “So, yeah, rather than saying oh this is all bad, this is all unlocked, it is insecure and so on... Well it’s fun for us of course because that’s what we wanted. We wanted a modem device, basically, where we could do whatever we want to and where we don’t have to break sophisticated security mechanisms that are designed to keep the user, or the customer, or the owner of the product out. So, yes, there are security issues, and those security issues must be fixed but we need security mechanisms that work without locking out the user or the owner of the device, of course. So, this is our public call to the manufacturers: If you fix those issues, keep in mind that the openness of the platform is interesting for all kinds of legitimate use cases. And while you want to protect against malicious attackers, you of course still want to enable the actual owners of the device and the users of those devices to use the flexibility that they provide because. . . ” (Applause starts.) (min 45-46.5)

What follows is information about the wiki the speakers have assembled and the release of the debugging and hardware tools they have used. Before they come to a close, the speakers are asking for support, calling upon fellow hackers to join their efforts of “experimenting” with mobile phone technology. There is a couple of minutes for questions from the audience; and then the chair closes the session: “Please join me in thanking [LaForge and holger] for presenting things I really didn’t want to know about 3G modems!”

Not unexpectedly, the presentation turns out to be one of this year’s highlights. LaForge is a widely-admired member of the CCC, known for his year-long investigations of corporate, ‘closed’ technologies—efforts that are largely *pro bono*. The presentation he gives with holger is a sequel to previous presentations in the last years in which LaForge and collaborators have, step by step, explored and reverse engineered the technologies that make up internet and mobile phone infrastructure. Their narrative is conventional: Making use of ingenious hacking techniques, the talk reveals widespread technology generally assumed to be secure—iPhones rely upon the examined modems as well—as insecure. The presenters ‘leak’ specific security vulnerabilities and call upon industry to ‘fix’ them, a maneuver that increases insecurity by publicizing it. They do so not because they would not care but in order to increase pressure upon tech corporations to improve security.

The vignette illustrates how issues of IT security are steeped in ambivalence: Curiosity and geeky enthusiasm for experimentation meet the notion that there are things you “really didn’t want to know.” Insecurity, if it concerns your private mobile phone, can be scary. But insecurity, for hackers, is also “fun”—it is their loophole, the material they play with. Nevertheless, holger and LaForge present themselves onstage as earnest, committed, and responsible, as professional security researchers who entertain crowds rather than as reclusive hacker-hobbyists. Dutifully, they report bugs and weaknesses to the public, calling upon industry actors to close the very insecurities they found to be “fun.” What is more, in the name of public good, they call upon industry to balance security against flexibility and accessibility. They warn against using security as a way to “lock out” users and instead promote the vision of open technology not black-boxed by proprietary, corporately-owned knowledge.

4.2 The Cure

In commercial software development it is common to contract external security consultants for what they call ‘ethical hacking’. Taking on the role of hackers, security consultants identify possible entry points *into* the system with the help of a penetration test. As results from the penetration test, consultants then translate found system entry points into vulnerabilities and vulnerability classes. These results feed into subsequent security training sessions for software developers. The training promises to give developers the knowledge and hands-on skills to fix security vulnerabilities on their own. The following vignette recalls a training session at a globally-operating software company that the first author visits in February 2015. The training convenes developers who collaborate on a specific software product but are situated in different offices around the world (Germany, the US, and India). The first author is part of an interdisciplinary team of researchers, led by the third author, that the company’s security officers had contracted to investigate the long-term impact of the penetration test and security training. Observing the training on site, the first author is one of only two women in the room together with 21 men. After the training, she conducts interviews and site visits over a 12-month period.

The external consultant enters a lively chatting bistro at the company and causes instant irritation, similar to when a teacher arrives after a break between lessons. All 17 developers, a second ethnographer, and I stream into an adjacent large meeting room with class-room like table rows, each with five chairs. Participants choose seats in every row of the room, except at the very front, leaving a respectful distance to the consultant, who appears considerably younger than most of the developers in the room. The atmosphere is apprehensive and tense. Developers expect to hear about their product’s in-/securities.

“Be paranoid and trust no one”, the consultant begins his presentation—this stance seems to be his first rule of secure software. It is his job in the next three days to promote this paranoia among developers, he explains, while skipping to a slide with a pharmaceutical jar labelled ‘awareness’. If you choose to inject it, he says, you are ‘cured’ from the disease called ‘insecurity’. He continues with IT security ‘war stories’ from other companies explaining that “attacks are everywhere” and “attackers are smarter, faster, and better motivated [e.g., to make money]” than developers are to write secure code. Under the tag line “attacker’s advantage and defender’s dilemma”, he points out that the defender “must defend all points [at the same time]”, “must be constantly vigilant”, and, worst of all, “must play by the rules”. He adds that defenders, meaning his audience, “can only defend against attacks that they know”. The impression that forms is that awareness of attack strategies, in his view, is the cure, a solution against an almighty and ubiquitous attacker. The attacker, on the other side, “can choose the weakest point” and “can probe for unknown vulnerabilities”, because they have more time and, worst of all, “can play dirty”. The developers listen to his explanations and laugh out now and then because of the apparent mistakes other companies make.

Later that day, the consultant shifts the focus of his presentation. Having raised awareness for the strategies of attack, he now addresses developers’ work, making them aware of their own mistakes. He starts with accusing developers, in general, by defining “[security] vulnerabilities [as] a quality defect resulting from bad coding [i.e., computer programming] habits”. And again, the consultant is quick to present his cure for bad coding—heightened awareness and knowledge of secure coding practices, calling upon the responsibility of individual developers.

When the consultant goes through each vulnerability found in the penetration test, a security officer intervenes: “Who did that, guys?” He looks around the room, waiting for an answer. One developer eventually gets up and takes the blame, immediately adding that he knows better now. The consultant replies laughingly: “This [mistake] is a clear don’t”, increasing the pressure on the developer. Some developers start giggling awkwardly. I perceive their laughter as the attempt to break out of an uncomfortable situation, whereas the consultant laughs because the mistake seems so obvious to him. The developer, who cared for his product enough to take the blame in front of everyone, sits back down. I feel his work was turned into a bad example rather than rewarding his bravery to admit his mistake.

In lunch and coffee breaks, developers from different teams stand together in little groups engaging in smalltalk and introducing themselves to each other. They have never met before in person and take the opportunity to get to know each other, but also to talk about some pressing development issues face to face. When I ask them for their opinion on the training they explain why they show attentiveness and interest: They consider themselves professionals who appreciate extending their expertise in training sessions and are proud of writing good code. They are not "in it for the paycheck", as one developer insists, but because they enjoy programming, care for their product, and want to do their work as good as possible.

The vignette illustrates how security is enacted in instructions, scare tactics, blame, and strict rhetoric of good and bad—there are, apparently, secure and insecure practices, healthy and sick code. The consultant assumes the code to be ill and developers' coding practices in need of a cure. He portrays IT security as solvable problem and individual awareness as matching solution. Carefulness, here, is the cure for insecure code. But it is a cure that leaves it to individual developers to care, neglecting team collaboration or organizational structures.

4.3 Invisible Work

Due to her interest in long-term effects, the first author returns to the software company to interview training participants about changes in their coding practices a couple of months later, in August 2015. She is invited to the office of two developers at a company outpost, Jens and Erik.

We sit down in their kitchenette and start talking about what security means in their everyday work. Jens, a senior software developer, explains that security must be made visible, e.g., in the form of issue reporting, to be a matter of everyday development work. Each security issue identified through the consultant's penetration test has been submitted to the company's issue tracking system and is now easily accessible to all developers. In the past, Jens says, external testing results were often just "thrown over the fence" and received little attention from developers or management. "Highest priority is only given when customers point to holes in the system", Jens adds. "The low priority of [security] issues means they do not pop up for the customer" and hence do not gain visibility or attention and are not allocated development resources.

In corporate software development, IT security remains largely invisible and dispersed across teams. Erik recalls a recent project that, even though one team was formally tasked with fixing security issues, caused a lot of work for developers outside the team as well. Time and again, the team tasked with security, was reaching out to Erik for his advice because he had written the original code.

"How can security become a more important factor in your development practices", I ask. "The development team", according to Erik, "simply does not have the upper hand [in steering development directions]." He wishes there would be a guideline to bring everyone up to speed and make other developers as attentive to security issues as he regards himself to be. Security issues are not automatically highly prioritized, which makes it "everyone's responsibility to write code conscientiously". "What has changed since the training?", I want to know. "Well, we received that pile of issues [from the consultant]", Jens replies. While the training brought to light which features of the product contained security vulnerabilities, "everyone coped with it on their own".

Security is also invisible in another way. "If you test for window scalability", Erik says and moves his hands up and down and from left to right, drawing an imagined browser window into the air, "you can manually test it with every browser available. You can *see* what does not work.

With security, this is different." He tries to grab something in the air, unsuccessfully, gesturing that security is not tangible. Testing in general, Jens points out, is "psychologically not very motivating". Security testing seems to be even worse, he indicates vaguely. "If you test, you will find something"—something you will most likely not like.

The conversation with Erik and Jens is symptomatic of their unhappiness with how security is delegated to individual efforts, invisibilizing work that they feel should gain more visibility throughout their company. At best, it seems, security is visible as a matter of only momentary insecurities. While Erik and Jens take pride in dealing with security issues, their care for security received no recognition, and training contents were not further discussed within the greater organization. Because of this, they fear that security is everyone's responsibility in general, and no one's in particular. They complain about a lack of control and guidance from above, and wished everyone else was just as conscientious as they are. What it takes to do IT security, they feel, should be made more visible in order to coordinate and recognize developers' efforts. Echoing the consultant's agenda, Jens and Erik call on others to care more, desiring a form of care that is better institutionalized and monitored.

4.4 Tinkering with Access Control

'Big data analytics' has proven a popular strategy in start-ups and internet corporations, and, quite recently, major traditional businesses also have started to invest in the promises of data-driven business decisions. Along with new techniques of data collection and building expertise in data analytics, companies are reviewing and rebuilding their data storage capabilities. A common strategy is the move to cloud technologies to support the storage and analysis of large quantities of data. The vignette, recalling observations made by the first author in a large utility company in 2017, offers a glimpse into negotiation and experimentation necessary to bring to life new technologies such as cloud storage into existing standards and regulatory frameworks of such a traditional business. As part of her dissertation research on IT security practices, the first author spent three months with the local big data analytics team, observing the security problems that arise when a new cloud storage infrastructure—the company's new 'data lake'—is built.

It is summer outside and I am sitting in an air-conditioned office with floor-to-ceiling windows. At one of the two desks in the middle of the room, two software developers, Georg and Karolin, and myself are squeezed together behind one screen. Georg calls himself the 'junior data lake architect', a term he made up for himself to indicate the new responsibilities that came along with the new technology. As such, he is responsible to give others permissions to a cloud service, the centrepiece of the company's data lake architecture. Karolin is a developer who had taken over several projects over the last two weeks that should use the cloud to store their data. Earlier in the week, she explains, she had been annoyed by the cloud service because of her missing permissions to it. "It is like running against a wall every two or three meters. There was nothing I could do. Since I had to wait for Georg to give me the permissions, I just went home." She laughs out loud. Georg asks "What do you need access to?" "Everything", Karolin replies and starts laughing. "But you do not need everything!", Georg replies, "Just bring me your laptop. Let's see what we can do." Karolin gets up and fetches her laptop from the other desk. She places it on her lap and enters her password asking, "What should I do?" "Open [the cloud interface] in the browser, please." She opens her e-mails instead and enters the cloud service name to search for the link that Georg had send her earlier together with her login credentials. She finds the mail, opens it, and clicks on the link. Her browser opens and I recognize the cloud service's interface. She enters her user name and password. With the page loading, she places the laptop on the desk and turns it to Georg. On his own computer, Georg is searching the web for the cloud service's permission guidelines. He opens another browser window that is full of links. He clicks on one, muttering to himself: "If I do this, I will give you that permission". He copies some code to a different browser tab, also in the cloud service's interface, looking for the right place to paste it, and eventually saves everything. He turns to Karolin's laptop, pressing F5 to reload the tab. An error message appears. "Mhm", he mumbles into the room, not surprised, "that does not work. Let's try something else."

He navigates back to the first window, copies a different code snippet, saves, and again uses Karolin's laptop to check whether his changes were successful. He needs to do so several times until eventually, instead of an error message, the (rather boring) usual interface appears with two folder icons. When she sees Georg had found the right permission code, Karolin shouts out: "Yay!"

"Now, can I try something?", Georg asks, requesting her permission to use her laptop for a little longer. "Sure, after I documented [the process] for Alex." She places the laptop back on her lap and starts taking screenshots and writing short descriptions, because among her colleagues she is the first to get access. "We need to play a little and learn how it works", Georg explains to me. He turns to his permissions window. "What if I put an asterisk in here, allowing everything?", he wonders. "The security people would kill me!", he says laughing, reflecting on the strict control by the department's security officer. "But we have to play around and learn", he addresses me apologetically. Karolin puts her laptop back on the table and jokes, knowing that Georg will play around using her laptop and credentials: "People will say I have deleted the cloud! I see where you are going!" All three of us laugh. He keeps tinkering in the permission code for another 15 minutes, occasionally checking Karolin's laptop and thinking aloud: "Oh, wow, now you can do what I can do, that is not good!"

In this vignette, security is negotiated in terms of access. The vignette illustrates how tinkering with access rules is necessary to find a secure working solution, and how this involves the violation of official guidelines and the crossing of boundaries of organizational control. Georg has good reasons to do so as he needs to familiarize himself with security mechanisms in order to make sound and safe decisions in the future. Apologetic jokes and mention of what the 'IT security people' would do are illustrative of the conscientious attention to security issues with which Karolin and Georg go about their work. They care for IT security—even if they have to bend the rules to do so.

5 DISCUSSION

Doing IT security comprises heterogeneous bundles of practices, dispersed across various sites, and involving a wide range of actors, materials, events, communities, and organizations. Taken together, our vignettes allow tracing connections between sites of research conventionally considered in isolation. In each of our vignettes, IT security is cared for—and care is called for—in different ways. In our first vignette on *in-/securities*, care of IT security emerges as a long-term commitment of hacking communities. In our second vignette on *the cure*, a consultant suggests to cure insecure code with awareness calling on developers to care. In our third vignette on *invisible work*, two developers talk about the lack of visibility for doing IT security in their company, and their personal dedication and attachment to take care of security in their product. In our fourth vignette on *tinkering*, two employees of a large utility company experiment with access rights and reveal, jokingly, the moral ambiguities of IT security. Using the vignettes as our starting point, we argue that caring for IT security means engaging with continuous oscillations of in-/securities, dispersed accountabilities, and intertwined moralities.

5.1 Oscillations

Doing IT security means caring for continuous and unexpected oscillations between in-/securities (cf. [42]), an ongoing effort that never finds closure and must rely on tinkering and experimentation. As the vignettes show, security is dynamically related to insecurity. Efforts to secure technologies typically bring about new insecurities. When Karolin and Georg tinker with access control for the cloud service of a large utility company, they complain about the rigid rules for data access that ‘the IT security people’ seek to implement. If they were to stick to these security rules slavishly, Karolin and Georg would not be able to help keep the company’s data storage secure. They knowingly engage in behavior that their company’s ‘security people’ would deem rather *in*secure when Georg, temporarily stepping over boundaries of organizational responsibility, gives Karolin access rights that she, officially, should not have. Security, here, emerges as a highly ambivalent notion.

At other sites, security is openly contested: Hackers such as holger and LaForge seek to reveal seemingly secure technologies to be insecure. As ‘security researchers’, they use hacking conventions as an arena to expose what they believe to be hidden insecurities in IT systems. Appealing to the common good, they publicize technical vulnerabilities to push corporate actors to fix them. But while holger and LaForge criticize corporations for producing insecure technology, they also are skeptical of overly rigid security measures that ‘lock out’ users. Corporate software development, in turn, may perceive such security research not as a way to secure vulnerable technologies but rather as illegitimate effort—‘attack’—to undermine the security of their products.

These oscillations between in-/security have their own temporal dynamics. In-/security transpires in a never-ending cycle of leak and fix: Once an attack, an in-house penetration test, ‘white hat’ security research or the dedicated scrutiny of a corporate software developer bring insecurity to the fore, measures are implemented to restore security. In this cycle of leak and fix, security remains always provisional and perennially requires the kind of continuous attention that we describe as care. Nonetheless, the security consultant in one of our vignettes promises software developers a ‘cure’ for security vulnerabilities. The ‘injection’ of careful attention, he contends, would solve the problem of insecure code finally. Here, the open-endedness of care contrasts the interventionist, once-and-for-all character of cure, two distinct temporalities that the consultant elaborately interweaves.

5.2 Accountabilities

Caring for IT security is, often, hard work not sufficiently recognized [10]—the reason being, in part, the very character of care. Typically, care is not a task in itself. It cannot be standardized and remains a matter of improvisation [7]. Thus, the work of care is typically invisible, undervalued, and badly accounted for [41]. Caring for IT security, then, grapples with questions of visibility and formalization: How can efforts to care for IT security preemptively be made tangible [48]? To what extent can, and should, doing IT security be made visible within the formalized accountabilities of, e.g., corporate organizations [31]? The external consultant in one of our vignettes gives visibility to the need for care by uncovering security issues, presenting to developers where they fail in enforcing product security. But because caring relies upon tinkering, experimentation, and affective commitment, genuine care can hardly be instilled in a two-day workshop alone. And while taking care of IT security means taking responsibility, caring for IT security is at odds with blaming and shaming. When a corporate security officer makes security something that individual developers are blamed for (‘Who did that, guys?’), care is jeopardized. Such finger-pointing undermines the collaborative practices in which IT security transpires as a shared commitment.

The care of IT security, however, is intricately interwoven with control. Quite fundamentally, caring for IT security requires a degree of technical command. Moreover, IT security, as an organizational achievement, relies on an intricate entanglement of care and organizational authority [19]. When Karolin and Georg seek to handle their company’s cloud services securely, they have to make do with the fact that they have but limited control of access rights and security rules. But caring for IT security not just requires control—it also affords control. Through careful experimental tinkering, hackers are able to gain technical control over systems and devices, a capacity that they leverage to re-negotiate issues of in-/security with large corporations.

Because security is not a well-defined functionality, it can hardly be confined to individual responsibility or the responsibility of a well-defined set of actors. For this reason, caring for IT security skillfully works with intertwined and distributed responsibilities, often crossing organizational, professional or even legal boundaries. When Karolin and Georg complain about the rigidity of access rules, they allocate accountability for security to the 'security people'—who might 'kill' Georg, they concede jokingly, if they ever found out about his playful, experimental approach to the security mechanisms they devised. At the same time, Georg claims accountability for security in his team. He has the most experience and acts as a gatekeeper. Only he is able to create the access Karolin needs; and Karolin, in turn, is not allowed to do what he does. Erik and Jens enact accountability, too, when they call for new team-wide guidelines on IT security, holding their management accountable while simultaneously asking for responsibility, and hence resources, for themselves. Here, caring for IT security means dealing with incongruence between who feels accountable (Erik and Jens), who is accountable (no one really knows), and who should be accountable (the team, the management).

Care and accountability are inextricably entangled in shifting relationships. Often, accountability undermines care. When, e.g., the security consultant holds single developers accountable for bad coding, he takes away pride, self-confidence, and dedication from developers such as Jens and Erik, who find their taking care of IT security issues not sufficiently appreciated. In other instances, however, carefulness may call for accountability. Because they care for the product they are working on, Jens and Erik are asking for more formal accountability within their corporation. Georg and Karolin, in turn, subvert formal accountabilities when they tinker with access rights, re-configuring responsibilities and organizational boundaries. And when hackers care to hold corporations accountable for security vulnerabilities, they create public accountability. Care and accountability, thus, continuously reconfigure one another.

5.3 Moralities

IT security is a deeply moral issue [30]. In our vignette about a corporate security training, developers claim that they are 'not in it for the paycheck'. Instead, they are proud and eager to write good—i.e., secure—code, both for the company and for the common good. In a similar vein, 'white hat' hackers and security researchers invoke notions of common good when they publicize security vulnerabilities and campaign for 'open' technologies. IT security is, not only in Erik and Jens' company, considered 'everyone's responsibility'. Undermining IT security is typically seen not just illegitimate or unlawful but also immoral. 'Attackers' of IT security, as the consultant at the training workshop puts it, 'can play dirty'. The disparity between the logic of warfare and the logic of care testifies to the distinct moralities at stake in doing IT security.

Since doing IT security must contend with the fact that security is never absolute nor final, many of the practices concerned with securing systems and devices pursue what Mol has called the "logic of care" [26]. Care "seeks to lighten what is heavy, and even if it fails it keeps on trying" [27, p. 13]. Care, Mol and colleagues emphasize, rests upon experimental perseverance: "try again, try something a bit different, be attentive" [27, p. 13]. Careful experimentation, then, "is not making value judgments, but engaging in practical activities" [26, p. 86]. As Mol argues, "'[g]ood and bad' are never settled in the logic of care" [26, p. 87]. Care, then, is not about locating the mistakes of the past: "The logic of care does not impose guilt, but calls for tenacity" [26, p. 91]. The morality of care is not about blame and shame [34, p. 95], but about morale and dedication.

But while we observe such 'carefulness' in the way in which Karolin and Georg handle their company's cloud services, other practices of doing IT security are more ambivalent. The kind of security research that is publicized at 'white hat' hacking conventions clearly relies upon tinkering and experimentation [45], but it foregrounds notions of 'attack' and 'defence', blaming security vulnerabilities on industry's negligence [21]. The security consultant in one of our vignettes also heavily draws upon such warfare rhetoric. More awareness for the 'dirty' ways in which attackers might think, he contends, would cure the company of insecure code.

Care and cure not only enact different temporalities, they also convey distinct moralities. In the context of hospital practice, Mol [26, p. 1] argues, the distinction between care and cure is untenable. Nonetheless, we find that it adds to a nuanced understanding of IT security, helping to parse differences in temporality and moral register. Care relies upon tenacity and sustained dedication; it is about provision, protection, and attachment. The morality of cure, in contrast, revolves around authority, expertise, and professional detachment. Cure is a time-bound intervention. Framing IT security in terms of cure means framing it as a problem from which, once solved successfully, one walks away. In doing IT security, the moral register of care exists alongside the register of cure, as well as the register of attack and defense. These registers do not thrive despite one another; rather, they overlap and complement one another.

Care calls for emotional support and reciprocity, fostering intimate relations. Care, as an ethos of proximity, however, can do but little to engage across distance. Instead, notions of attack and defence conjure up 'outside' threats, conveying a pitch for urgent, bold action across previous (organizational, professional) divides [21]. Security research, e.g., utilizes warfare metaphors to initiate forms of cooperation among hacking communities and industry actors. It is also not unusual for academic literature to make use of expressions such as pointing to a "battle" between system designers and attackers [8], or arguing that "developers are on the front line of the security battle" [1]. Here, the moral register of attack and defence helps to enlist actors in doing IT security, working to keep together and expand the weave of heterogeneous practices that IT security relies upon.

The care of IT security only gains profile against notions of cure, attack, and defense. In fact, what the lens of care brings to the fore is precisely the entanglement of care, cure, attack, and defense, all of which surface in doing IT security. As distinct moral registers, they challenge and complement one another, often going hand in hand. Faced with the limits of care, actors may invoke alternate moral registers in forging relations between people and things. That does not mean they would not care. It simply means that doing IT security involves a heterogeneous bundle of practices, invoking both care and cure, both the ethos of proximity and the pathos of defense.

5.4 A Caring Approach to IT Security

Seen through the lens of care, our vignettes afford an account of IT security that, we argue, calls for a caring approach towards the study of and interventions in IT security. Such an approach would benefit both research in CSCW as well as security research more broadly, academic as well as policy and activist interventions.

Both research and interventions in IT security have to address the fact that IT security is not a technicality that could be designed and implemented in any straightforward manner. Caring for IT security is rarely a task in itself. IT security, instead, is the outcome of efforts dispersed among a heterogeneous set of actors, a fragile, preliminary achievement that is taking place at diverse sites and across organizational, legal, and professional boundaries. Put differently, caring for IT security typically takes place *in-between*: It takes place between people and things because care is, inherently, a matter of forging relations. It cannot be confined to single actors, teams, departments, organizations, or communities. Its in-between character makes IT security a complex object of research and difficult target for intervention. Addressing—improving—IT security means to engage in a widely-spun nexus of practices [39]. 'Careful' design for IT security, hence, has to recognize how artifacts are incorporated in multiple, overlapping practices (cf. [5]).

Cognizant of the in-between character of doing IT security, a caring approach avoids delegating responsibility for IT security to single actors or specific groups of actors such as, e.g., users or software developers, and it refrains from blaming or shaming them. Rather, a caring approach is empathetic towards the different actors involved [43]; it seeks to understand and cultivate their respective skills and competencies, their ethos and morale. Such an approach acknowledges diverse forms of care for technology and its benefits for the common good [34]. In this approach, security training and workshops should offer space for forging bonds and attachments, fostering practices of experimentation rather than enacting standards, rules, and taboos. The approach neither aims at a sweeping, absolute notion of security nor at releasing yet another security tool or formulating yet another security guideline.

A caring approach to IT security has no ready answers but raises pressing questions: How do organizations grow a culture of care for IT security? What are 'careful' ways of relating to alternate moral registers, e.g., the logics of attack and defense? Is it possible for, e.g., external consultants to cure for care? And if so, how should consultants, when entering a company, best proceed? How can 'careful' design engage with attachment and dedication?

Lastly, we do not suggest to adopt a caring approach blindly or, worse, with feverish rigor. Care is not a matter of proselytizing. A caring approach is not dismissive of alternate moral registers such as, e.g., cure or attack and defense. Rather, it respectfully attends to differences in morality—knowing that it would be wrong, too, to shame actors for engaging in warfare rhetorics or mobilizing the logic of cure.

6 CONCLUSION

In this paper, we argue that IT security does indeed require care—i.e., a kind of work that is largely invisible, badly rewarded, and morally charged. A careful approach makes IT security a practical problem and moral obligation. It requires close attention and hands-on engagement, and it perceives security as fragile, gradual, scattered, relative, situated, dynamic, ambivalent, and contested. IT security, in this perspective, is never quite complete, never absolute. Caring for IT security, hence, is about tinkering with perennial oscillations between security and insecurity. *Secure* technology may tolerate carelessness (from Latin 'securus', literally 'without care' or 'without apprehension'; Source: Oxford Dictionary of English). But *keeping* technologies secure requires a great deal of carefulness.

While care is typically feminized, taking care of IT security remains, predominantly, a male preoccupation. Hackers, software developers, the external consultant, too, all care in their own way. But others, they feel, don't care enough. In our data, allegations of carelessness and demands for 'more' care occur time and again. They are directed not only at corporations at large, but also at (fellow) developers and management. There is, it seems, never sufficient care. However, demanding care rarely induces carefulness; and what it precisely would mean to care can hardly be explicated outside situated practice. For this reason, demands for care tend to appear helpless and vague. They ultimately convey a need for something that from an abstract, disengaged point of view must remain rather elusive. And it is this elusiveness of care—and of IT security—that finds its reflection in the sexist thinking, encapsulated in our epigraph, that "more women" on corporate boards, more female IT security experts in leadership positions, might help to better care for IT security. Clearly, to have more women on corporate boards is a crucial step in establishing gender equality. But declaring women the sole champions of care means undermining it. And our analysis suggests, in fact, that a focus on single actors' responsibility ("women") and top-down enforcement of accountability ("on the board") are rarely helpful in supporting care for IT security.

With this paper, we make several contributions: First of all, we draw attention to IT security as ongoing collective endeavor, an important though barely studied topic in CSCW. Secondly, we approach IT security as a heterogeneous bundle of practices that involve diverse actors and spread across organizational, legal, and professional boundaries. Many of these practices cultivate forms of carefulness. As we show, caring for IT security engages with dispersed accountabilities and entangled moralities. A caring approach to IT security, we suggest, fosters a moral stance that refrains from blaming insecurity upon single actors and instead attends to the networked character of IT security. Thirdly, we demonstrate how care as an analytic lens helps in tracing connections between various ethnographic fields, revealing not only different ways to care but also different ways in which care is complemented and challenged by alternate moral registers and organizational accountability.

To conclude, we suggest opportunities for future research. Quite apparently, our study is limited in scope, and ethnographic observation of further sites would enrich our findings. As we confined our study to professional practices of technology production, maintenance, and repair, future research will have to include lay practices of ordinary technology use and appropriation: How do (end-)users care, and how can they be adequately cared for? We also consider it worthwhile to further explore both the gendered and the relational character of caring for IT security: *For whom* is in-/security, *when* is it, and which relations does it forge? Care is crucial for maintaining social and economic relations. But care is not innocent. It can all too easily obscure power. Caring for IT security can quickly turn into paternalism when security mechanisms curtail use, privacy, and appropriation—and when gendered discourse suggests seemingly simple solutions.

Doing IT security is, in fact, making power. Doing IT security negotiates accountability and control, obligations and entitlements, risks and good(s) as well as, above all, access rights. Our study of the dispersed efforts to care for the security of IT systems is, hence, a study of power in the making. The relationship of care and power has many facets. Often, those who care would complain about a lack of recognition and power. Yet care, too, is powerful in its own right. Caring for something, for others is inextricably entangled with “hegemonic ethics” [36, p. 10]. There is always an aspect of domination, even usurpation to caring for IT security, especially when caring means ‘taking charge’, ‘taking responsibility’ rather than putting oneself into the service of empathetic dialogue. To engage in such dialogue remains a worthwhile challenge for scholars in CSCW and STS [20].

7 AUTHOR CONTRIBUTIONS AND ACKNOWLEDGEMENTS

Authors are listed alphabetically. All authors contributed substantially to the research and the writing of this paper. While the paper is the result of intense collective discussion, joint analysis, and collaborative writing, each author focused on different tasks, such as, e.g.: selection and formulation of ethnographic vignettes (LK), grounding the argument in the literature on care in CSCW (MK), anchoring the argument in the literature on IT Security (AP), and structuring the argument (SW).

The authors would like to thank the Center for Advanced Internet Studies (CAIS) and the participants of the workshop on The Practice Turn in IT Security: Martin Gilje Jaatun, Alexander May, Helmut Rother, Cornelius Schubert, Estrid Sørensen, Peter Mayer, and Christopher Lentzsch. We would also like to thank Felix A. Epp and Sven Türpe for their research contributions to the study at the global software vendor, Estrid Sørensen and Christine T. Wolf for helpful comments on drafts of the paper, as well as the anonymous reviewers for their thoughtful and constructive remarks. Lastly, we are deeply indebted to the informants and interlocutors in our field work for their generous trust and tenacity.

This work was partially supported by the German Federal Ministry of Education and Research (BMBF) and by the Hessen State Ministry for Higher Education, Research and the Arts (HMWK) within CRISP.

REFERENCES

[1] Yasemin Acar, Michael Backes, Sven Bugiel, Sascha Fahl, Patrick McDaniel, and Matthew Smith. 2016. SoK: Lessons Learned from Android Security Research for Appified Software Platforms. In *2016 IEEE Symposium on Security and Privacy (SP '16)*. 433–451. https://doi.org/10.1109/SP.2016.33

[2] Yasemin Acar, Michael Backes, Sascha Fahl, Simson Garfinkel, Doowon Kim, Michelle L. Mazurek, and Christian Stransky. 2017. Comparing the Usability of Cryptographic APIs. In *2017 IEEE Symposium on Security and Privacy (SP '17)*. 154–171. https://doi.org/10.1109/SP.2017.52

[3] Anthony Amicelle, Claudia Aradau, and Julien Jeandesboz. 2015. Questioning security devices: Performativity, resistance, politics. *Security Dialogue* 46, 4 (2015), 293–306. https://doi.org/10.1177/0967010615586964

[4] Debi Ashenden and Angela Sasse. 2013. CISOs and organisational culture: Their own worst enemy? *Computers & Security* 39 (2013), 396–405. https://doi.org/10.1016/j.cose.2013.09.004

[5] Pernille Bjørn and Carsten Østerlund. 2014. *Sociomaterial-Design: Bounding technologies in practice.* Springer International Publishing, Cham, Switzerland.

[6] Marisa Leavitt Cohn. 2016. Convivial Decay: Entangled Lifetimes in a Geriatric Infrastructure. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW '16)*. ACM, New York, NY, USA, 1511–1523. https://doi.org/10.1145/2818048.2820077

[7] Jérôme Denis and David Pontille. 2015. Material Ordering and the Care of Things. *Science, Technology, & Human Values* 40, 3 (2015), 338–367. https://doi.org/10.1177/0162243914553129

[8] Rachna Dhamija and J. D. Tygar. 2005. The Battle Against Phishing: Dynamic Security Skins. In *Proceedings of the 2005 Symposium on Usable Privacy and Security (SOUPS '05)*. ACM, New York, NY, USA, 77–88. https://doi.org/10.1145/1073001.1073009

[9] Paul Dourish and Ken Anderson. 2006. Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. *Human-Computer Interaction* 21, 3 (2006), 319–342. https://doi.org/10.1207/s15327051hci2103_2

[10] Paul Dourish, Rebecca E. Grinter, Jessica Delgado de la Flor, and Melissa Joseph. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing* 8, 6 (Nov 2004), 391–401. https://doi.org/10.1007/s00779-004-0308-5

[11] Sascha Fahl, Yasemin Acar, Henning Perl, and Matthew Smith. 2014. Why Eve and Mallory (Also) Love Webmasters: A Study on the Root Causes of SSL Misconfigurations. In *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security (ASIA CCS '14)*. ACM, New York, NY, USA, 507–512. https://doi.org/10.1145/2590296.2590341

[12] Simson Garfinkel and Heather Richter Lipford. 2014. *Usable Security: History, Themes, and Challenges.* Morgan & Claypool. https://doi.org/10.2200/S00594ED1V01Y201408SPT011

[13] Matthew Green and Matthew Smith. 2016. Developers are Not the Enemy!: The Need for Usable Security APIs. *IEEE Security Privacy* 14, 5 (Sept 2016), 40–46. https://doi.org/10.1109/MSP.2016.111

[14] Ellie Harmon, Matthias Korn, and Amy Voida. 2017. Supporting Everyday Philanthropy: Care Work In Situ and at Scale. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17)*. ACM, New York, NY, USA, 1631–1645. https://doi.org/10.1145/2998181.2998330

[15] Christopher R. Henke. 1999. The Mechanics of Workplace Order: Toward a Sociology of Repair. *Berkeley Journal of Sociology* 44 (1999), 55–81.

[16] Lara Houston and Steven J. Jackson. 2016. Caring for the "Next Billion" Mobile Handsets: Opening Proprietary Closures Through the Work of Repair. In *Proceedings of the Eighth International Conference on Information and Communication Technologies and Development (ICTD '16)*. ACM, New York, NY, USA, Article 10, 11 pages. https://doi.org/10.1145/2909609.2909658

[17] Lara Houston, Steven J Jackson, Daniela K Rosner, Syed Ishtiaque Ahmed, Meg Young, and Laewoo Kang. 2016. Values in repair. In *Proceedings of the 2016 CHI conference on human factors in computing systems (CHI '16)*. ACM, 1403–1414.

[18] Giovanni Iachello and Jason Hong. 2007. End-User Privacy in Human–Computer Interaction. *Foundations and Trends in Human–Computer Interaction* 1, 1 (2007), 1–137. https://doi.org/10.1561/1100000004

[19] Margaret Jack and Steven J. Jackson. 2016. Logistics As Care and Control: An Investigation into the UNICEF Supply Division. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 2209–2219. https://doi.org/10.1145/2858036.2858503

[20] Laura Kocksch, Katharina Kinder-Kurlanda, Andreas Poller, Estrid Sørensen, and Susann Wagenknecht. 2018. Caring, negotiating and tinkering for IT in/security. In *Panel at EASST 2018 Conference*. Lancaster University, England. https://nomadit.co.uk/easst/easst2018/conferencesuite.php/panels/6277

[21] Matthias Korn and Susann Wagenknecht. 2017. Friction in Arenas of Repair: Hacking, Security Research, and Mobile Phone Infrastructure. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17)*. ACM, New York, NY, USA, 2475–2488. https://doi.org/10.1145/2998181.2998308

[22] Ann Light and Yoko Akama. 2014. Structuring Future Social Relations: The Politics of Care in Participatory Practice. In *Proceedings of the 13th Participatory Design Conference: Research Papers - Volume 1 (PDC '14)*. ACM, New York, NY, USA, 151–160. https://doi.org/10.1145/2661435.2661438

[23] Silvia Lindtner and Seyram Avle. 2017. Tinkering with Governance: Technopolitics and the Economization of Citizenship. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW, Article 70 (Dec. 2017), 18 pages. https://doi.org/10.1145/3134705

[24] George E. Marcus. 1995. Ethnography in/of the World System: The Emergence of Multi-Sited Ethnography. *Annual Review of Anthropology* 24, 1 (1995), 95–117. https://doi.org/10.1146/annurev.an.24.100195.000523

[25] Aryn Martin, Natasha Myers, and Ana Viseu. 2015. The politics of care in technoscience. *Social Studies of Science* 45, 5 (2015), 625–641. https://doi.org/10.1177/0306312715602073

[26] Annemarie Mol. 2008. *The Logic of Care: Health and the Problem of Patient Choice*. Routledge, London and New York.

[27] Annemarie Mol, Ingunn Moser, and Jeannette Pols. 2010. Care: putting practice into theory. In *Care in Practice: On Tinkering in Clinics, Homes and Farms*, Annemarie Mol, Ingunn Moser, and Jeannette Pols (Eds.). transcript Verlag, Bielefeld, Germany, Chapter 1, 7–25.

[28] Patrick Morrison, Benjamin H. Smith, and Laurie Williams. 2017. Surveying Security Practice Adherence in Software Development. In *Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp (HoTSoS '17)*. ACM, New York, NY, USA, 85–94. https://doi.org/10.1145/3055305.3055312

[29] Alena Naiakshina, Anastasia Danilova, Christian Tiefenau, Marco Herzog, Sergej Dechand, and Matthew Smith. 2017. Why Do Developers Get Password Storage Wrong?: A Qualitative Usability Study. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17)*. ACM, New York, NY, USA, 311–328. https://doi.org/10.1145/3133956.3134082

[30] Helen Nissenbaum. 2005. Where Computer Security Meets National Security. *Ethics and Information Technology* 7, 2 (01 Jun 2005), 61–73. https://doi.org/10.1007/s10676-005-4582-3

[31] Andreas Poller, Laura Kocksch, Sven Türpe, Felix Anand Epp, and Katharina Kinder-Kurlanda. 2017. Can Security Become a Routine?: A Study of Organizational Change in an Agile Software Development Group. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW '17)*. ACM, New York, NY, USA, 2489–2503. https://doi.org/10.1145/2998181.2998191

[32] Andreas Poller, Sven Türpe, and Katharina Kinder-Kurlanda. 2014. An Asset to Security Modeling?: Analyzing Stakeholder Collaborations Instead of Threats to Assets. In *Proceedings of the 2014 New Security Paradigms Workshop (NSPW '14)*. ACM, New York, NY, USA, 69–82. https://doi.org/10.1145/2683467.2683474

[33] Andreas Poller, Ulrich Waldmann, Sven Vowe, and Sven Türpe. 2012. Electronic Identity Cards for User Authentication: Promise and Practice. *IEEE Security Privacy* 10, 1 (Jan 2012), 46–54. https://doi.org/10.1109/MSP.2011.148

[34] María Puig de la Bellacasa. 2011. Matters of care in technoscience: Assembling neglected things. *Social Studies of Science* 41, 1 (2011), 85–106. https://doi.org/10.1177/0306312710380301

[35] María Puig de la Bellacasa. 2012. 'Nothing Comes Without Its World': Thinking with Care. *The Sociological Review* 60, 2 (2012), 197–216. https://doi.org/10.1111/j.1467-954X.2012.02070.x

[36] María Puig de la Bellacasa. 2017. *Matters of Care: Speculative Ethics in More than Human Worlds*. University of Minnesota Press.

[37] Daniela K Rosner and Sarah E Fox. 2016. Legacies of craft and the centrality of failure in a mother-operated hackerspace. *New Media & Society* 18, 4 (2016), 558–580. https://doi.org/10.1177/1461444816629468

[38] Theodore R. Schatzki. 2002. *The Site of the Social: A Philosophical Account of the Constitution of Social Life and Change*. The Pennsylvania State University Press, University Park, Pennsylvania.

[39] Elizabeth Shove, Matt Watson, and Nicola Spurling. 2015. Conceptualizing connections: Energy demand, infrastructures and social practices. *European Journal of Social Theory* 18, 3 (2015), 274–287. https://doi.org/10.1177/1368431015579964

[40] Justin Smith, Brittany Johnson, Emerson Murphy-Hill, Bill Chu, and Heather Richter Lipford. 2015. Questions Developers Ask While Diagnosing Potential Security Vulnerabilities with Static Analysis. In *Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering (ESEC/FSE '15)*. ACM, New York, NY, USA, 248–259. https://doi.org/10.1145/2786805.2786812

[41] Susan Leigh Star and Anselm Strauss. 1999. Layers of Silence, Arenas of Voice: The Ecology of Visible and Invisible Work. *Computer Supported Cooperative Work (CSCW)* 8, 1 (Mar 1999), 9–30. https://doi.org/10.1023/A:1008651105359

[42] Lucy Suchman, Karolina Follis, and Jutta Weber. 2017. Tracking and Targeting: Sociotechnologies of (In)security. *Science, Technology, & Human Values* 42, 6 (2017), 983–1002. https://doi.org/10.1177/0162243917731524

[43] Austin Toombs, Shad Gross, Shaowen Bardzell, and Jeffrey Bardzell. 2017. From Empathy to Care: A Feminist Care Ethics Perspective on Long-Term Researcher-Participant Relations. *Interacting with Computers* 29, 1 (2017), 45–57. https://doi.org/10.1093/iwc/iww010

[44] Austin L. Toombs, Shaowen Bardzell, and Jeffrey Bardzell. 2015. The Proper Care and Feeding of Hackerspaces: Care Ethics and Cultures of Making. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing*

Systems (CHI '15). ACM, New York, NY, USA, 629–638. https://doi.org/10.1145/2702123.2702522

[45] Susann Wagenknecht and Matthias Korn. 2016. Hacking As Transgressive Infrastructuring: Mobile Phone Networks and the German Chaos Computer Club. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW '16)*. ACM, New York, NY, USA, 1104–1117. https://doi.org/10.1145/2818048.2820027

[46] Nina Witjes and Philipp Olbrich. 2017. A fragile transparency: satellite imagery analysis, non-state actors, and visual representations of security. *Science and Public Policy* 44, 4 (2017), 524–534. https://doi.org/10.1093/scipol/scw079

[47] Jim Witschey, Olga Zielinska, Allaire Welk, Emerson Murphy-Hill, Chris Mayhorn, and Thomas Zimmermann. 2015. Quantifying Developers' Adoption of Security Tools. In *Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering (ESEC/FSE '15)*. ACM, New York, NY, USA, 260–271. https://doi.org/10.1145/2786805.2786816

[48] Shundan Xiao, Jim Witschey, and Emerson Murphy-Hill. 2014. Social Influences on Secure Development Tool Adoption: Why Security Tools Spread. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '14)*. ACM, New York, NY, USA, 1095–1106. https://doi.org/10.1145/2531602.2531722

[49] Jing Xie, Heather Lipford, and Bei-Tseng Chu. 2012. Evaluating Interactive Support for Secure Programming. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12)*. ACM, New York, NY, USA, 2707–2716. https://doi.org/10.1145/2207676.2208665

[50] Elia Zureik and Karen Hindle. 2004. Governance, Security and Technology: the Case of Biometrics. *Studies in Political Economy* 73, 1 (2004), 113–137. https://doi.org/10.1080/19187033.2004.11675154

Received April 2018; revised July 2018; accepted September 2018