Replication Study: A Cross-Country Field Observation Study of Real World PIN Usage at ATMs and in Various Electronic Payment Scenarios

Melanie Volkamer, *Karlsruhe Institute of Technology* **(***KIT***)** *and Technische Universität Darmstadt;* **Andreas Gutmann,** *OneSpan Innovation Centre and University College London;* **Karen Renaud,** *Abertay University, University of South Africa, and University of Glasgow;* **Paul Gerber,** *Technische Universität Darmstadt;* **Peter Mayer,** *Karlsruhe Institute of Technology* **(***KIT***)** *and Technische Universität Darmstadt*

https://www.usenix.org/conference/soups2018/presentation/volkamer

This paper is included in the Proceedings of the Fourteenth Symposium on Usable Privacy and Security.

August 12–14, 2018 • Baltimore, MD, USA

ISBN 978-1-931971-45-4

Open access to the Proceedings of the Fourteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

Replication Study: A Cross-Country Field Observation Study of Real World PIN Usage at ATMs and in Various Electronic Payment Scenarios

Towards Understanding Why People Do, or Do Not, Shield PIN Entry

Melanie Volkamer
Karlsruhe Institute of Technology (KIT)
Technische Universität Darmstadt
melanie.volkamer@kit.edu

Andreas Gutmann
OneSpan Innovation Centre & University College London
andreas.gutmann@onespan.com

Karen Renaud
Abertay University
University of South Africa
University of Glasgow
k.renaud@abertay.ac.uk

Paul Gerber
Technische Universität Darmstadt
gerber@psychologie.tu-darmstadt.de

Peter Mayer
Karlsruhe Institute of Technology (KIT)
Technische Universität Darmstadt
peter.mayer@kit.edu

ABSTRACT

In this paper, we describe the study we carried out to replicate and extend the field observation study of real world ATM use carried out by De Luca *et al.,* published at the SOUPS conference in 2010 [10]. Replicating De Luca *et al.*'s study, we observed PIN shielding rates at ATMs in Germany. We then extended their research by conducting a similar field observation study in Sweden and the United Kingdom. Moreover, in addition to observing ATM users (*withdrawing*), we also observed electronic *payment* scenarios requiring PIN entry. Altogether, we gathered data related to 930 observations. Similar to De Luca *et al.,* we conducted follow-up interviews, the better to interpret our findings. We were able to confirm De Luca *et al.*'s findings with respect to low PIN shielding incidence during ATM cash withdrawals, with no significant differences between shielding rates across the three countries. PIN shielding incidence during electronic payment scenarios was significantly lower than incidence during ATM withdrawal scenarios in both the United Kingdom and Sweden. Shielding levels in Germany were similar during both withdrawal and payment scenarios. We conclude the paper by suggesting a number of explanations for the differences in shielding that our study revealed.

1. INTRODUCTION

People have been drawing cash from automated teller machines (ATM) for at least half a century [4]. The 21st century heralded an increasing use of card-based electronic payments [13]. Most bank cards are Chip & PIN based, allowing people either to withdraw money or pay for goods and services using the same card. To complete a transaction, the customer presents the card and provides a PIN to authenticate themselves. Exceptions are, for instance, Germany, where *Chip & Signature* is a common alternative to Chip & PIN, and the United Kingdom, where contactless payment (*tap only* for amounts less than £30) is gaining market share [39]. PINs are required during withdrawals in all countries, no matter how low the transaction amount.

PIN entry is not without risk, since thieves could observe the PIN (in person, or using a camera) and use the knowledge later, once they have managed to clone or steal the actual card. To prevent this, people are advised to take the precaution of shielding their PINs when they enter it (as well as being advised not to carry a note of their PIN together with the actual card).

In 2010, De Luca *et al.* investigated factors that impacted decisions related to taking security precautions when engaging in PIN-based ATM authentication [10]. The researchers observed how people entered their PINs at ATMs; in particular, whether people acted to protect their PIN entry from possible skimming attacks [3]. They conducted follow-up interviews to gain insights into the contextual factors affecting secure behaviors. We replicated their research study, and extended it as follows:

- *PIN usage scenarios:* Common electronic payment scenarios (i.e. in supermarkets or in restaurants / coffee bars) are very similar to withdrawing money from an ATM in terms of PIN authentication being required. We wanted to explore differences in PIN usage during payment scenarios, too. We also wanted to elicit explanations for shielding differences we observed. Similar research questions were suggested by De Luca *et al.* as a topic of future interesting investigations [10].
- *Countries:* While De Luca *et al.* [10] collected data in Germany and the Netherlands, they only reported overall observations. However, we believed that more detailed comparisons between different countries, particularly when considering different scenarios (payment/withdrawal), would de-

USENIX Symposium on Usable Privacy and Security (SOUPS) 2018.
August 12–14, 2018, Baltimore, MD, USA.

liver interesting insights in terms of shielding percentages and factors impacting PIN shielding.

Following the previous researchers' example, we commenced with an observational field study and then conducted interviews once the data from the first study was analysed. We collected data in Germany, similar to De Luca *et al.* We also extended the observation field study to both Sweden and the United Kingdom, and conducted interviews in all three countries.

De Luca *et al.* reported that 67% of the observed ATM users did not take any precautions against PIN skimming attacks. Almost a decade later, we observed the same high percentage of people *not* shielding PIN entry at ATMs (64% in Germany, 71% in the U.K, and 71% in Sweden). We discovered that the activity of either *withdrawing* or *paying*, as well as the observation country, were significant predictors of PIN shielding behavior. Further results are:

- In Germany, there was no significant difference in PIN shielding incidence during withdrawal and payment scenarios.
- In the United Kingdom and Sweden, we observed significantly fewer people shielding their PINs during payment, than during withdrawal transactions.
- Significantly more people shielded their PINs when paying with their cards in Germany, as compared to the United Kingdom and Sweden.
- Significantly more people shielded their PINs when paying with their cards in the United Kingdom, as compared to Sweden.

De Luca *et al.* identified a number of contextual factors from their follow-up interviews to determine why people did, or did not, shield PIN entry. One was that of being accompanied. We also recorded whether or not people were accompanied in our observation field study. However, our study did not reveal significant differences for this factor.

The interviews helped us to explain our findings; particularly with respect to the differences between shielding incidence during withdrawing and paying. Possible explanations are habituation (people engaging in more electronic transactions feel safer doing so, and are less likely to shield their PINs), lack of reminders to shield, the presence of hard cash during withdrawals, different goals (withdrawing means the primary goal is obtaining cash in hand; paying means the primary goal is obtaining desired products or services), and a lack of understanding of the actual attack scenarios. In terms of the latter, the primary threat might not be surrounding people, but rather strategically positioned security cameras which could easily record unshielded PINs.

Thus, we conclude that it seems particularly worthwhile to add opaque hardware shields to Chip&PIN devices which effectively removes the need for people to shield themselves. Just-in-time reminders might also reduce the risk of criminals gaining knowledge of people's PINs, as well as raising awareness of PIN shielding during payment scenarios.

2. METHODOLOGY

We commence by providing details of De Luca *et al.*'s study, and explaining how we went about replicating and extending it. In particular, we explain what precautions we took in order to ensure that the research was carried out in accordance with ethical requirements.

2.1 De Luca et al.'s Study

De Luca *et al.* [10] carried out a PIN observation study in 2010.

Goal: Their goal was better to understand PIN-based ATM authentication both with respect to taking any precautions against PIN skimming attacks and the time needed to authenticate. Furthermore, they wanted to determine how alternative authentication approaches could be evaluated and compared to existing ones.

Methodology: During their research, De Luca *et al.* observed ATM interactions at six locations in two cities in Germany and the Netherlands: a total of 360 observations. The observations (i.e. whether or not to shield the PIN entry and how long authentication takes) were recorded on a tally sheet during multiple sessions, by the same researcher "*to keep the data comparable, since different people might apply different standards during the observation, deliberately or not*" [10, p. 2]. After analyzing the collected data, several problems regarding the timing were identified. Correspondingly, two followup studies were conducted. To gain greater insights into the findings from the field evaluation, they subsequently carried out interviews with other people (not the ones they observed).

Findings: They found that the majority of the people they observed (65%) did not take any precautions against PIN skimming attacks (i.e. less than 65% shielded their PIN entry). In addition. the interviews revealed that contextual factors exerted a strong influence both on security behaviors and to the time required to authenticate. Example factors are distractions, physical hindrance (e.g. due to bags in peoples hands), and trust relations. Based on their findings, they suggested a number of "lessons learned" to inform subsequent field studies into the use of privacy-sensitive technologies, as well as a number of implications for the design of alternative ATM authentication systems. Their lessons learned section emphasised the importance of improving tally sheet designs during trial studies and adherence to strict rules during observations to ensure validity and comparability of the results.

2.2 Achieving Replication

We based the study design on De Luca *et al.*'s [10], and also incorporate design aspects from their lessons learned section.

Similar to De Luca *et al.*'s study, each location was visited at least twice during different time periods. By doing so, we ensured that the collected data was as diverse as possible. Replicating De Luca *et al.*'s study, we observed a variety of different bank ATM machines at different locations. We also observed a variety of scenarios during which PIN-based authentication was required during electronic payment.

We chose the locations similarly to De Luca *et al.* for their study. In effect, we chose locations that enabled us non-intrusively to observe the interactions with the corresponding devices. We identified scenarios where the devices were visible from public seating areas, such as street cafés. By so doing, we ensured that the observer did not arouse suspicion. Similar to De Luca *et al.,* the observation sessions were not prolonged so as to minimize the risk of raising suspicion and concern.

As reported by De Luca *et al.,* all observations were performed and recorded (in written form) by only one researcher. This eliminated inter-observer bias. Following De Luca *et al.*'s protocol, observations were only added to the data set if the observer was 100% sure about whether the subject had shielded their PIN or not. If his view was obscured, the observer did not record the event. The researcher did not observe any fraudulent incidents during the observation ses-

sions.

2.3 Observation Study

We now describe the variations we studied, for each of the two factors (PIN usage scenario, country/locations), and the content of the written protocol.

2.3.1 PIN Usage Scenarios

De Luca *et al.* investigated actions connected with ATM withdrawals. We studied interactions during this scenario and also studied payment scenarios during which PINs were required to authenticate: supermarkets and restaurants/coffee bars. Compared to withdrawing cash, the electronic payment process does not involve actual cash being handled. Furthermore, the subject's main task is to purchase something. Unlike ATM interactions, which is a solo activity, other people are often legitimately involved in payment interactions. For example, a shop assistant might be instructing a customer to insert their card and enter their PIN. We wanted to determine whether these different scenarios (withdrawing vs. paying) would make a difference to PIN shielding rates. We also considered two different types of payment scenarios, so as to reveal differences between payments in supermarkets at the cash register and payments in a restaurant/coffee bar setting.

Our 930 field observations were performed at different locations: 310 in each country. Besides ATMs, we observed people at various electronic payment scenarios involving a PIN authentication. The observation field study took place over a period of two weeks in each country. After the field observation study, follow-up public interviews were conducted in all three countries.

2.3.2 Countries and Locations

We conducted our observation field study in three different European countries, each with different profiles with respect to withdrawing cash and cashless payments. Based on data from the European Central Bank [13] and Eurostat [38], we identified three countries for our study: Germany, the United Kingdom and Sweden. People living in Germany, on average, withdraw money about as frequently as they pay electronically. People living in the United Kingdom use bank cards more frequently for both, to withdraw (smaller amounts of) money and generally pay for things electronically. Furthermore, in the United Kingdom, contactless payment (for payments under £30) is gaining market share [39]. This only requires PIN authentication for amounts over £30. In Sweden, "*cash is used relatively infrequently [...] while cards are used to a great extent*" [33] and also for very small amounts of money. For more details about the differences see Table 1.

We chose locations in each country to collect samples that are broad in range and comparable to each other.

Frankfurt, Germany. We included two ATMs in Germany (45 observations each). Both were located in train stations. Furthermore, observations were conducted in a supermarket (100 observations) and two restaurants (120 observations). A notable distinction between those restaurants was that customers at one restaurant paid before eating, while customers in the other restaurant paid just before departing.

Glasgow, United Kingdom. Our observations in the United Kingdom comprised a supermarket (100 observations), a fast food restaurant, and a coffee bar (both with 120 observations in total) as well as two ATMs in pedestrian precincts (45 observations each). The fast food restaurant provided multiple self-service kiosks, while customers in the coffee bar queued at a single teller.

	U.K.	**Germany**	**Sweden**
Withdrawals *per capita*	43.98	32.43	21.96
Avg. value of withdrawal (Euro)	83.00	128.21	108.88
Card payments *per capita*	178.99	33.21	235.47
Avg. value of card payment (Euro)	59.28	72.09	32.1
Avg. number of PIN entries per capita	222.97	65.64	257.43

Table 1: The number and value of withdrawals and card payments in the United Kingdom, Germany and Sweden in 2014 [13]. The average number of PIN entries *per capita* is based on the population on the 1st of January 2014 [38]. This presents an upper bound for Germany because Chip & Sign is commonly used [12] and for the United Kingdom because of the high usage of contactless payments [14].

Karlstad, Sweden. The observations in Sweden comprised two ATMs inside a building (45 observations each), a supermarket inside a mall (100 observations in total), a restaurant within a department store, and a payment terminal at the exit of the same department store (in total, 120 observations).

2.3.3 Written Protocol

The written protocol comprised the following information: country, scenario (including ATM vs. supermarket vs. restaurant/coffee bar), time of the day/date, shielded (or not), and whether accompanied by other people (or not). The fact that the latter might be important was suggested by De Luca *et al.*'s findings [10]. Their interviewees suggested that being accompanied negatively impacts people's decisions to shield due to social awkwardness.

2.4 Follow-Up: Public Interviews

We conducted public follow-up interviews, in order the better to interpret our observation findings. Interviews took place over a period of several days in the same cities where observations took place (while not necessarily close to the observation locations).

Similar to De Luca *et al.*'s protocol, people were first asked whether they would be available for a short interview. If they consented, they were informed that the interview was being conducted as part of a research project, and assured that no private data would be collected. Subjects were asked to be frank and honest in their responses. They were not interrupted as long as they felt like talking. Notes were taken manually. The interviews were conducted in English in the United Kingdom and Sweden, and in German in Germany.

The interview protocol was slightly different to the one from De Luca *et al.*'s . Because we had extended the observation field study by adding additional scenarios and countries, we wanted to address the differences we identified between these different settings in particular between the payment and the withdrawing scenario. We thus used the following protocol:

1. Describe, in detail, how you use your card to pay when shopping.
2. Describe, in detail, how you use your card to withdraw money at an ATM.
3. If PIN shielding has not been mentioned during the first two responses, ask:

(a) "You probably use only one hand to operate the device. What do you usually do with your other hand in both situations?"

(b) "Do you regularly shield your PIN entry?"

4. If PIN shielding is only mentioned in connection with ATMs:

   (a) What is the difference between withdrawing at an ATM and paying in a shop?

   (b) Why do you shield your PIN at one but not the other?

5. Have you heard about crimes related to PIN entry? If so, what did you hear and where did you hear it?

6. Do you sometimes see other people covering their hands when they enter their PINs? What do you think when you see them do this? Why?

7. Assume you are in a shop, or at an ATM, with a good friend, and he or she shields their PIN as they enter it. What would you think? Why?

Note that we decided to commence the interview with questions about scenarios, whereas De Luca *et al.* asked questions specifically about PIN security. We wanted to make sure we did not bias initial responses by mentioning security.

2.5 Ethical and Legal Considerations

When we investigate security behaviors, self reports often do not reflect actual behaviors, due to the social desirability effect [16, 36]. This makes surveys and interviews less than reliable in delivering insights into security-related behaviors. Observations reveal actual, rather than self-reported, behaviors, which is invaluable in understanding how to improve the design of socio-technical security systems.

Observational studies are a powerful tool for studying social worlds [23], and security behaviors in public places lend themselves to observational studies. Yet observational studies require researchers to take extra special care with respect to ethical and legal aspects of their studies. Before commencing the observations, we thus considered the ethical and legal aspects very carefully.

Ethical requirements and general recommendations provided by the American Psychological Association in their Ethical Principles of Psychologists and Code of Conduct [1] and the British Sociological Society Guidelines [6] were followed in planning this study. Ethics requirements and general recommendations provided by Technische Universität Darmstadt[1] [37] were strictly adhered to. However, two areas of concern merited special consideration and are therefore further discussed in the next paragraphs: (1) informed consent, and (2) deception.

(1) Informed Consent: The first issue was that it was not possible to obtain informed consent from the subjects we observed in our study. To seek consent would likely have changed behavior and compromised the integrity of the investigation [6, 34]. Spicker [34] explains that some studies simply cannot obtain consent. He cites three examples: "*Observing a crowd at a football match, watching drivers in moving cars, or attending a meeting of shareholders*" (p. 3). We believe our context to be similar to these, in the sense that requiring the researcher to obtain consent would have made it impossible for him to carry out the research in an ecologically-valid way.

Murphy and Dingwall [29], reporting on the ethics of ethnographic studies, argue that people in public spaces can expect to be scrutinized by anonymous others. They explain that, in the case of public behavior, people's consent to being observed is implied by their presence in the public place. Yet the researcher has to treat their subjects with respect and decency, which is what we sought to do. We considered that, in our study, consent was unachievable and would have invalidated our findings. Spicker [34] explains that where there is a need to carry out research that is minimally intrusive, in public, it is often not possible to obtain consent from those being observed. We thus did not obtain informed consent from our observed subjects.

(2) Deception: The second potential concern is that subjects in observation studies are often subject to deception. We designed our study to be a *covert non-participant observation* study instead of a *researcher-as-participant* study, which is much more deceptive, and makes it more difficult for researchers to preserve anonymity of subjects. This is harder to justify ethically than the kind of non-intrusive study we carried out [29, 11]. Our subjects were not deliberately deceived at all, so this was not an ethical concern.

However, there are some *limitations* and *challenges* to consider when carrying out non-participant covert observation studies [25, 31]:

(a) **Observer Effect:** the observer's presence could affect the actions of the subject.

(b) **Objectivity:** the observer needs to ensure that he/she maintains objectivity during observation.

(c) **Selectivity:** ensuring that observations are captured in a variety of situations to offset selectivity bias.

(d) **Hearing the subjects' voices:** ensuring that the final account does not only reflect the researcher's voice.

(e) **Unobtrusiveness**: not standing out in the environment when recording observations.

The limitations were addressed by the following precautions, replicating all of those applied by De Luca *et al.* [10] (Table 2 shows the mapping between the limitations and the precautions.)

(1) **Privacy:** PIN entry is a secret and sensitive issue. It was essential to ensure that we did not gain knowledge of anyone's PIN while carrying out the observations. The observation locations were selected so that, in order to respect the privacy and secrecy of our unwitting subjects, we were always able to observe from a vantage point that allowed us to see whether people were shielding PIN entry, but not to be able to observe the PIN itself. This was achieved either by positioning the observer to the side of the device, at an obtuse angle, or to position the observer too far away to be able to observe anything more than the use of a hand or wallet to shield PIN entry.

[1] Relevant for the research reported here (observational study without any interaction with the participants) are the avoidance of damage, stress, fear or other aversive effects on the subjects of the study, i.e. the observed, the avoidance of the collection of personal data, if this is not necessary, and the preservation of subject anonymity, especially in the collection of data related to minorities, which could be deanonymised unintentionally by statistical linking of data.

(2) **Location Accessibility & Variety:** the observation locations were selected in such a way that the observer could not see the device's screen, and were easily accessible. Moreover, observations were carried out at a range of locations.

(3) **Anonymity:** We did not collect any personal data such as names, contact data, photos or videos, so as to grant our subjects full anonymity.

(4) **Respect:** we interviewed *other* Chip&PIN card holders, who were not observed subjects, after we had carried out all the observations, in order to hear their explanations for shielding decisions.

(5) **Inconspicuousness:** the observer acted as required by the environment so that he did not stand out unduly. For example, if he was observing in a coffee shop he ordered a coffee, if he was observing out in the street he sat on a bench and appeared to be resting. He engaged in no interaction with the subjects, so as not to occasion any disquiet.

(6) **Recording Protocol:** the observer manually recorded the data related to the subject's shielding actions.

Limitation	**Precaution**
(a) Observer Effect	(1) Privacy, (3) Anonymity
(b) Objectivity	(6) Reporting Protocol
(c) Selectivity	(2) Location Accessibility & Variety
(d) Hearing the subjects' voices	(4) Respect
(e) Unobtrusiveness	(5) Inconspicuousness

Table 2: The mapping from the aforementioned limitations to the precautions we took in designing our study.

We informally consulted lawyers and experts from data protection authorities in the respective countries. We also asked Karlsruhe Institute of Technology's legal department to provide feedback regarding the legal aspects of our study design. Given the precautions we designed into our study, as detailed above, they could not identify any legal issues with our study design. This included observations carried out in indoor locations, such as restaurants. None of the lawyers we consulted could see that we needed to get in touch with the owner/manager of these locations beforehand, given the precautions we took. In particular, we respected the privacy of the subjects we observed and did not not interact with, or impede, anyone. They also confirmed that, given these precautions, we did not have to obtain signed consent from the subjects. Again, the most important aspects were that subjects were essentially anonymous for research purposes, and that the researcher did not interact with them in any way.

In conclusion, we planned our study activities carefully in order to ensure that we did not harm the safety, dignity, or privacy of the people we observed, as advised by the European Commission [19].

2.6 Methodology Limitations

Following the De Luca *et al.*'s [10] methodology means facing the same limitations. As explained by De Luca *et al.,* it was important not to interview subjects after observing their actions. Instead, an independent set of people was interviewed. That being so, the same limitation holds: the explanations provided by our interviewees were not directly provided by the observed subjects and thus cannot be considered to be reliable causatives.

It is also possible that people falsely represented their usual PIN-related actions during interviews due to social desirability of making a good impression, or to please the interviewer. We have no indication that this happened but this limitation must be acknowledged.

3. FINDINGS

We first present the findings from the observation field study and then those from the follow-up interviews.

3.1 Observation Field Study

The details of the study are provided in Table 3 and summarized in Table 4.

Results from Replication. De Luca *et al.* [10] reported that 120 out of 360 (33.3%) of the people they observed at ATMs did observably shield their input. We recorded that 39% of the people being observed at ATMs in Germany shielded their PINs, with 29% in both Sweden and the United Kingdom shielding.

We compared the shielding behavior at ATMs in all locations with that reported by De Luca *et al.* [10] on pair-wise significance with two-proportion z-tests. This method is appropriate for single characteristics (binary data) of two independent groups sampled at random [7]. The tested hypothesis is that shielding incidence at each of the three locations differ significantly from that reported by De Luca *et al.* . The null hypothesis is that there is no difference. The results of all tests reveal no significant differences at $p<.05$ (see Table 5), therefore the alternative hypothesis is rejected, although this does not mean that the null hypothesis would be accepted.

Regression Modelling. We tested the collected data (see Table 3) with regression modelling techniques and set the shielding behavior as the dependent variable. Categorical variables, e.g. the country of observation, were coded into indicator variables before performing the regression modelling. We identified the person's activity of either withdrawing or paying, as well as the country in which the sample was collected, as significant predictors of shielding behaviors (see Table 6). The linear regression model accounts for about 10% of the variation (R^2 =.100, corrected R^2 =.0956, and standard error =.382). The model provided a significant prediction of the criteria 'shielding behavior' with F=20.636 and $p<.001$. The regression model identified two significant predictors for shielding behavior: the country in which the sample is collected and the activity of either withdrawing or paying. It does not indicate whether the combination of both significant predictors is a significant predictor as well, i.e.

- It is more likely that people shielded their PINs when withdrawing money, as compared to paying.
- It is more likely that people shielded their PINs in Germany, as compared to the United Kingdom and Sweden. It is also more likely for people in the United Kingdom to shield their PINs, as compared to Sweden.

Post-hoc ANOVA comparison. We tested the between-subjects effect of independent variables 'country' and 'scenario' (i.e. paying versus withdrawing at ATMs versus supermarket versus restaurant/coffee bars (labelled 'others' in Table 3)) on the dependent variable 'shielding behavior' with two-way ANOVA. We have applied the Sidak correction to compensate for the accumulation of

	United Kingdom				Germany				Sweden			
	ATM	Pay	*Sup*	*Others*	*ATM*	*Pay*	*Sup*	*Others*	*ATM*	*Pay*	*Sup*	*Others*
Total	*90*	*220*	*100*	*120*	*90*	*220*	*100*	*120*	*90*	*220*	*100*	*120*
Shield	29%(26)	14%(30)	13%(13)	14%(17)	36%(32)	34%(74)	34%(34)	33%(40)	29%(26)	0%	0%	0%
Company	13% 12)	35%(79)	47%(47)	27%(32)	3%(3)	30%(65)	42%(42)	19%(23)	8% (7)	–	–	–
↳ shield	58%(7)	15%(12)	15%(7)	16%(5)	0%	31%(20)	33%(14)	26%(6)	14%(1)	–	–	–

Table 3: The percentages and total amounts for the observations, per scenario, and per country. Note that "Others" refers to restaurants and coffee bars. A long dash denotes irrelevance of the data field due to '0%' in the row above. 'Sup' is used as shortcut for supermarket due to space constraints.

	ATM	Pay	Supermarket	Others
Total	*270*	*660*	*300*	*360*
Shield	31% (84)	16% (104)	16% (47)	16% (57)
Company	8% (22)	31% (206)	45% (129)	23% (77)
↳ shield	36% (8)	16% (32)	16% (21)	14% (11)

Table 4: The percentages and total numbers for the observations per scenarios for all three countries. Note that "Others" refers to restaurants and coffee bars.

	United Kingdom	Germany	Sweden
z-score	-0.81	0.4	-0.81
p value	.42	.69	.42

Table 5: The results of the two-proportion z-test on data reported by De Luca et al. [10] and our ATM samples.

	Standardised beta	T	Significance
Germany	.303	8.409	<.001
ATM	.174	4.961	<.001
United Kingdom	.113	3.124	.002
Company	.010	.289	.773
Supermarket	-.004	-.117	.907

Table 6: The regression model data, with coefficients for dependent variables of whether subjects shielded the PIN entry, or not.

type I error. Both major effects as well as the interaction were significant. Since there were no *a-priori* hypotheses, we calculated post-hoc comparisons, comparing behavior in the three countries across all scenarios. The results are presented in Table 7. The most important findings are:

- For the *withdrawal* scenarios, there were no significant differences between shielding across the three countries.
- For the *payment* scenarios, there are significantly more subjects in Germany who shielded their PINs, as compared to the other two countries.
- For the *payment* scenario, significantly more United Kingdom subjects shielded their PINs, as compared to those in Sweden.
- In Germany, there is no significant difference between shielding while either withdrawing or paying.
- There are significant differences between the three scenarios (withdrawing and supermarket/coffee bar) in the United Kingdom and Sweden (with fewer people shielding their PINs during payment, as compared to withdrawing).
- No differences, in terms of PIN shielding, manifested between the two different payment scenarios: supermarkets and others (restaurants/coffee bars), across all three countries.

We did not find any differences in terms of 'being accompanied during PIN entry', neither for the whole sample nor for the three different country-specific samples.

3.2 Follow-Up: Public Interviews

The focus of our interviews was on explaining the differences between withdrawing and paying in the different countries. We conducted a total of 27 interviews: ten in Sweden, ten in the United Kingdom and seven in Germany. The written notes were coded by two of the authors. We used structural coding [27] for initial segmentation of the data and magnitude coding [28, 42] on the collected segments. A three-level magnitude code was applied: several > some > few. The following categories, as possible explanations for shielding, were identified.

3.2.1 ATM Environments Considered More Risky

Several subjects said that they considered the ATM environment to be less safe. One reason, cited by several interviewees, is that there was little to no media coverage of PIN-related crime elsewhere than at ATMs. During some interviews, it was reported that ATMs were often in less secure environments, especially when they were outside banks. Several participants mentioned that strangers hanging around ATMs were mistrusted more than in other scenarios "*...at an ATM anyone could stand behind you. But people in a supermarket are there to buy something*"). Actually, in payment scenarios, the subjects perceived strangers as a 'protector', and assumed that they would implicitly provide protection by spotting external threats. In particular, the cashier and accompanying friends are perceived to be another person who can 'exercise care'. In Germany, in particular, customers commonly hand over the card to the cashier, who then puts the card into the device, prepares everything and asks the customer to enter their PIN. Few interviewees mentioned that the cashier or waitresses are usually discreet enough to turn their bodies away, or avert their eyes, when a customer is entering their PIN.

Thus, other than the withdrawal scenario, people did not consider co-located people a threat in supermarkets, restaurants and shops. Few subjects were not particularly specific but just commented: "*You're not supposed to get robbed in stores*" or "*Not something you usually think about in a store*"

3.2.2 Reminded by Displayed Advice

During some interviews, subjects mentioned that they shielded their PINs when they were visibly reminded to do so. It was acknowledged that only ATMs display such advice: "*There are warnings*

			Mean diff.	Standard error	Sign.	95% conf. interval for the difference	
						Lower boundary	upper boundary
ATM	Germany	U.K.	,067	,057	,559	-,069	,202
	Germany	Sweden	.067	.057	.559	-.069	.202
	U.K.	Sweden	<0.01	.057	1.000	-.135	.135
Supermarket	Germany	U.K.	.210*	.054	**.000***	.082	.338
	Germany	Sweden	.340*	.054	**.000***	.212	.468
	U.K.	Sweden	.130*	.054	**.046***	.002	.258
Others	Germany	U.K.	.192*	.049	**.000***	.074	.309
	Germany	Sweden	.333*	.049	**.000***	.216	.451
	U.K.	Sweden	.142*	.049	**.012***	.024	.259
Germany	ATM	supermarket	.016	.055	.989	-.116	.147
	ATM	Others	.022	.053	.966	-.104	.149
	Supermarket	Others	.007	.051	.999	-.116	.130
UK	ATM	supermarket	.159*	.055	**.012***	.027	.291
	ATM	Restaurant / Cafe	.147*	.053	**.016***	.021	.274
	Supermarket	Others	-.012	.051	.994	-.135	.111
Sweden	ATM	supermarket	.289*	.055	**.000***	.157	.421
	ATM	Others	.289*	.053	**.000***	.162	.415
	Supermarket	Others	<0.01	.051	1.000	-.123	.123

Table 7: Results of post-hoc comparisons for the three countries, in terms of the scenario, and for the three scenarios for the three countries. Those that are significant are starred.

at ATMs, thus I cover automatically. Else I wouldn't because there is no need". Indeed, in our study only the ATMs displayed such reminders.

3.2.3 Cash Perceptions

Few interviewees expressed their views that ATMs would be more strongly connected to bank accounts and to hard cash ("*Because the ATM is, like, about money*"). In their opinion, this perception would frame actions in the vicinity, implicitly prompting security precautions.

3.2.4 Habitual Protective Actions

Some subjects merely said shielding was a habit, perhaps prompted some time ago because they had observed others doing it (social norm), or because their parents taught them to do it. This type of argumentation was actually used in both ways: some participants said others are doing it (in particular friends or parents), which is why they shield their PIN without really thinking about it: "*This is just normal"*. But few others argued that it is normal to enter the PIN, as "*fast as possible"* as no one else shields. A few also considered that the shopping scenario exerts more time pressure than the ATM scenario: at ATMs people generally stand back and the activity is essentially solo, whereas payment scenarios usually involve at least one other person who is somehow involved in the transaction.

3.2.5 Social Awkwardness

Some people were put off by impressions of social unacceptability. Some participants reported that shielding might signal mistrust to people around you: "*I don't want to look like a freak*", "*Only old people cover*", "*Covering feels stupid*", "*People who cover are paranoid*". While these reasons may hold for both scenarios, it might be worse for paying. These subjects mentioned that they are often accompanied by friends or relatives during payment scenarios. On the other hand, they usually withdrew money on their own. One mentioned situational differences: at the supermarket, friends usually go to the cash register together while someone usually breaks away from the group to withdraw money.

3.2.6 Further Findings

While the sample is clearly not representative, we can conclude the following:

- Very few interviewees specifically mentioned attacks. For example, it is easier to install a skimmer on an ATM. Some mentioned the risk related to strategically-placed surveillance cameras that are able to record unshielded PINs. However, such threats were only mentioned as related to the ATM context. Some subjects only considered shielding necessary at ATMs if strangers were standing too close for comfort. Similar findings were reported by De Luca *et al.* [10]. They, too, reported subjects securing their PINs by entering them as quickly as possible. Others checked the surrounding area before approaching an ATM machine or blocked the ATM with their bodies.
- No interviewees mentioned that the actual behavior is affected by an installed plastic shield over the PIN pad. They did not mention the presence of these, nor whether these were considered helpful and/or effective.
- Physical hindrance was not mentioned by our subjects. This

was identified as factor influencing shielding likelihood by De Luca *et al.* [10] during their observations.

- In Germany, of the seven people we interviewed, six mentioned PIN shielding in their initial descriptions of what they did in the two scenarios. In the United Kingdom, and particularly in Sweden, interviewees explicitly distinguished between ATM withdrawal and payment scenarios in this respect.

4. DISCUSSION

Our study replicated and extended one particular aspect of De Luca *et al.*'s ATM study. We focused primarily on the PIN entry aspects of the original study, and then extended the study to different card usage environments.

4.1 Country Differences for Payment Scenarios

The interesting differences here are *firstly* that there was almost no difference in shielding between withdrawal and payment transactions in Germany. The *second* interesting finding was that no subjects in Sweden shielded during payment transactions. The *third* is the difference in payment shielding between the three countries.

A number of explanations can be advanced for these relative outliers. In the first place, there might be significant differences in the frequency of card use and the amount of money involved in each transaction. The Swedish population uses their cards to pay far more than the German population at large (Table 1). Thus, in Sweden, paying by card seems to be *de rigeur* i.e. nothing out of the ordinary requiring special attentiveness.

Moreover, there is also a difference in amounts paid using cards. In Germany, the average amount is more than twice that of Sweden, while the amount in the United Kingdom is in-between the German and Swedish averages. Hence the risk associated with the transactions is greater in Germany, and subjects might well be behaving in accordance with heightened risk perceptions. The *status quo* might well change over the next few years as Germany, for example, has recently introduced PIN-less payments for amounts less than €30.

These numbers accord with our insights from the follow-up interviews: The number of payment instances (both paying oneself using Chip & PIN, as well as observing others doing so) make people less likely to shield. The extreme observations (no one shielding in the payment scenario) in Sweden might also be due to the high level of trust and transparency in Swedish society [32].

4.2 Differences Between Payment and ATM Withdrawal

Our United Kingdom and Swedish subjects were more likely to shield their PINs when withdrawing money than when paying. The following findings from our follow-up interviews suggest explanations for this:

- In one scenario, people receive **cash in hand**, and for the other the transfer of money happened invisibly. People associate security measures with cash and therefore are more likely to shield in the withdrawing scenarios, as compared to the payment scenarios. Similar findings can be found in the literature: Bijleveld and Aarts [5] explain that "*Money [...] activates knowledge structures that are incompatible with the pursuit of social harmony*" [5, page 16]. Related to this is also the following finding from the literature: There is a substantial difference in terms of goal satisfaction. As opposed to obtaining cash, the primary goal of *buying* something is to obtain an object or experience. The underlying purpose is to maximize happiness [8]. Money becomes a secondary concern, a mere facilitator.

- People say they are more likely to shield during withdrawals because ATMs often display reminders to shield. There is more space to place a sticker or to display the reminder on the screen.

- People perceive ATM environments as being more risky than payment contexts in supermarkets, coffee bars, or restaurants. This explanation suggests the existence of misunderstandings or a lack of awareness of the full range of attack vectors. In both cases, there is a risk of manipulated devices and cameras recording PINs, without a human needing to be anywhere near the person using the card.

- People are more 'alone' at ATMs, thus social awkwardness, which would perhaps prevent them from shielding, is less of an issue.

4.3 Comparing to De Luca's ATM withdrawals

We replicated De Luca *et al.*'s [10] results with respect to the percentages of people shielding their PINs at ATMs. The explanation for the relatively low percentages might still be the same as those advanced by De Luca *et al.* i.e. lack of awareness of actual attacker tactics and, corresponding misconceptions regarding the effectiveness of the security measures that they currently take (e.g. checking that nobody is loitering close by).

This low number also indicates that effective protection can only be assured when the PIN pad has pre-installed shields that prevent PIN leakage. However, it is still important to ensure usability for a wide range of people, including those with disabilities.

4.4 Impact of being Accompanied

We did not uncover any differences in terms of 'being accompanied by other people' (e.g. friends, relatives) during PIN entry. Both the interviews by De Luca *et al.* [10] and ours may create the impression that being accompanied makes a difference. A number of interviewees mentioned the social awkwardness that arises from shielding when accompanied by friends or acquaintances.

It is worth mentioning that in all three countries only very few observations recorded subjects being accompanied at ATMs. The lack of a finding might be a consequence of the low numbers. On the other hand, it looks as if this situation is not very typical because our interviewees suggested that cash withdrawal is generally a solo activity. While friends often accompany each other at the cash register, they do not, as a rule, join each other at the ATM.

It looks as if those Germans who do shield make a habit of shielding: those who have this habit always shield when using their cards, with no differences between withdrawal and payment transactions. They either always shield, or never shield. The context does not seem to influence them, nor does the presence or absence of any other people around them.

In the United Kingdom and Sweden, people shielding their PINs are already in such a minority that the cultural norm of not shielding might well perpetuate not shielding, even when accompanied.

4.5 Limitations

The observation field study, as well as the follow-up interviews, took place in three medium-sized cities in three European countries. Thus, the results have only limited validity with respect to large European cities, small towns, or cities in other countries.

We observed PIN shielding from some distance to guarantee anonymity and privacy. This comes with some limitations. A subject was counted as having shielded the PIN as soon as this person used his/her hand, or some other object to shield the PIN pad. However, even if they did shield their PIN entry, they might not have entirely prevented observation from some other vantage point than the one taken by our observer. What we recorded was shielding *attempts*, not efficacy. Moreover, by only observing whether or not someone acted to shield PIN entry, we did not record other protective activities such as checking for surveillance cameras or ensuring that nobody in the vicinity was trying to observe their PIN entry. It might be that subjects did engage in some situational awareness activities and made a perfectly valid low risk assessment. Even if they did realize that someone was close enough to observe their PIN, they might well have interposed their own body between that person and the PIN pad. These kinds of precautions might have been effective in a pre-surveillance era, but with cameras in inner cities, and especially at ATMs, recording people all the time, such precautions are less than effective.

We compared our results to De Luca *et al.*'s. We were able to replicate their results with respect to people shielding their PINs at ATMs. We are aware that the criteria we used for shielding might be slightly different in the two studies because the observers were different people. Yet we did attempt to replicate the study as exactly as possible, based on the information reported in the paper.

The follow-up interview responses might have elicited social desirability responses, but this is a common issue for any interview situation in the security context. We tried to address this limitation by commencing with an innocuous question asking them to detail their own actions in withdrawing and paying with their Chip & PIN cards. Only after this did we focus on the real issue, i.e. shielding, exploring their perspectives on the need for this action.

5. RELATED WORK

We set out to replicate De Luca *et al.*'s study and another two researchers also recently carried out a non-participant observation study of PIN-related behaviors at ATMs. Ashby and Thorpe [2] observed people entering their PINs at a number of different locations of one bank's ATM machines in London. They focused on "hot spot" areas, those where ATM crimes were highest in the London area. Their study revealed that 47% of subjects attempted to cover the PIN pad when they entered their PINs. Unlike our study, they observed only ATM usage, and only in one country. The higher shielding percentages might well be due to the fact that they focused specifically on crime hotspots. This intuition gains some confirmation from the fact that when they interviewed a subset of their observed subjects, and asked them what kinds of precautions they took, the most common one was to use only ATMs that were in safe areas.

A number of papers exist on usable security ATM research. For example, in [9], the authors studied and discussed the idea of biometric authentication at ATMs. Their research revealed a number of non-trivial issues with the introduction of this type authentication for ATMs. Little [24] examined the influence of external factors on ATM use in general. Privacy was one identified factor that aligns with our findings.

Other observation studies of visibly revealed security-related behaviors appear in the research literature. Von Zezschwitz *et al.* [41] studied real-world behavior related to Android authentication patterns. This helped them to compare the real life usability of these patterns to the more traditional PINs. Machuletz *et al.* [26] observed people working in public, to see how prevalent webcam covering behavior was. Greig *et al.* [18] carried out an observation study of one particular branch of a chain store to monitor security-related behaviors. Despite regular information security training and general awareness, they observed passwords written on blackboards, sharing of credentials and staff taking photos of till screens.

Other researchers left USB sticks lying around to see how many people would plug them in [40]. The visible behavior, here, was plugging the stick in the USB port of a PC, and half of their subjects did so. A number of researchers have proposed sending out fake phishing messages to employees to test actual resilience after phishing awareness training [20, 21, 35]. These kinds of exercises seem to be becoming popular in industry [15, 30]. Finally, Forget *et al.* [17] propose a security behavior observation infrastructure to effect long-term monitoring of user behaviors on client machines and Lévesque *et al.* [22], along the same lines, propose a methodology for a field study of anti-malware software.

6. CONCLUSION & FUTURE WORK

We carried out a field study, during which we observed 930 Chip & PIN card uses, in three countries and in different scenarios, with people either withdrawing or paying. There were significant differences with respect to the scenario, with people shielding their PINs significantly less often when they withdrew cash than when they paid in two of the countries (the United Kingdom and Sweden). In Germany, shielding occurrence was equal in both situations. In addition, we carried out interviews to identify factors that may explain what we observed. These include habituation, lack of reminders, the influence of cash in hand, and a lack of awareness of actual attack scenarios.

In general, the percentage of people shielding is surprisingly low, given that they could lose their hard earned money. We were able to confirm De Luca *et al.*'s findings with respect to the low percentage of people shielding their PINs when withdrawing money at ATMs.

Based on our findings, a number of interesting future research questions emerged:

- What influence does the amount of money that someone withdraws or pays have on the decision to shield? In Germany and the United Kingdom / Sweden the average transaction amounts are different. Is this one possible explanation for the identified differences between these countries?
- Based on the identified explanations, it would also be advisable to study the influence of the type and size of plastic shields over PIN pads, and the actual impact of reminders, as also suggested by [2].
- What is the influence of the actual/perceived liability of cardholders on the decision to shield? Initial investigations suggest that mixed messages are sent by different banks we contacted and information provided on their websites. We informally polled a number of people in our respective countries about their understanding and discovered that people have different ideas about whether, and what types of, consequences they might have to face if their PIN is covertly observed and their card subsequently stolen without their knowledge.

- In the interviews, the scenario of the cashier or waitress putting the card into the device for the payee emerged. This is an additional scenario to study as future work. A similar extension would be to study behavior at ticket machines, which are somehow inbetween pure withdrawal (ATM) and the usual store payment scenarios.

However, the long-term goal must be to replace existing devices with those that have opaque shields pre-installed. In the meanwhile, another area of future work could be awareness raising, because one of the findings that emerged from the interviews was that people were not aware of the surveillance camera attack scenarios. They tend to rely on their innate yet inaccurate sense that humans are the greatest threat in these scenarios.

Acknowledgments

This work was supported by the German Federal Ministry of Education and Research (BMBF) within the Competence Center for Applied Security Technology (KASTEL), the Center for Research in Security and Privacy (CRISP), and has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675730.

Four of the authors changed institutions between the time this research was started and this publication. When the research was started:

- Melanie Volkamer, Andreas Gutmann, and Peter Mayer were employed by the Technische Universität Darmstadt in Germany.
- Karen Renaud was employed by the University of Glasgow in Scotland.

7. REFERENCES

[1] American Psychological Association. Ethical Principles of Psychologists and Code of Conduct. http://www.apa.org/ethics/code/ (Accessed: 20 May 2018).

[2] M. P. Ashby and A. Thorpe. Self-guardianship at automated teller machines. *Crime Prevention and Community Safety*, 19(1):1–16, 2017.

[3] G. Baltistan. Rising number of ATM-skimming frauds must not be taken lightly, 2018. 17 January http://gbherald.com/index.php/2018/01/17/rising-number-of-atm-skimming-frauds-must-not\-be-taken-lightly/ (Accessed: 15 February 2018).

[4] B. Bátiz-Lazo and R. J. Reid. Evidence from the patent record on the development of cash dispensing technology. In *History of Telecommunications Conference, 2008. HISTELCON 2008. IEEE*, pages 110–114. IEEE, 2008.

[5] E. Bijleveld and H. Aarts. A psychological perspective on money. In *The Psychological Science of Money*, pages 3–19. Springer, 2014.

[6] British Sociological Association. Statement of ethical practice, 2017. www.britsoc.co.uk (Accessed: 20 May 2018).

[7] B. L. Brown, S. B. Hendrix, D. W. Hedges, and T. B. Smith. *Multivariate analysis for the biobehavioral and social sciences: a graphical approach*. John Wiley & Sons, 2011.

[8] T. J. Carter. The psychological science of spending money. In *The Psychological Science of Money*, pages 213–242. Springer, 2014.

[9] L. Coventry, A. De Angeli, and G. Johnson. Usability and Biometric Verification at the ATM Interface. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '03, pages 153–160, New York, NY, USA, 2003. ACM.

[10] A. De Luca, M. Langheinrich, and H. Hussmann. Towards understanding ATM security: a field study of real world ATM use. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS)*, page 16, San Fransisco, 2010. ACM.

[11] Department of Sustainability and Environment. Effective engagement: building relationships with community and other stakeholders, 2005. The Community Engagement Network Resource and Regional Services Division Victorian Government Department of Sustainability and Environment. Book 3: The Engagement Toolkit. Retrieved from http://www.dse.vic.gov.au/__data/assets/pdf_file/0003/105825/Book_3_-_The_Engagement_Toolkit.pdf (Accessed: 20 May 2018).

[12] Deutsche Bundesbank. Payment behaviour in Germany in 2014. https://www.bundesbank.de/Redaktion/EN/Downloads/Publications/Studies/payment_behaviour_in_germany_in_2014.pdf, 2015. (Accessed: 15 February 2018).

[13] European Central Bank. Payment statistics. http://sdw.ecb.europa.eu/reports.do?node=1000004051, October 2015. (Accessed: 15 February 2018).

[14] D. S. Evans, K. Webster, G. K. Colgan, and S. R. Murray. Paying with cash: A multi-country analysis of the past and future of the use of cash for payments by consumers. *Available at SSRN 2273192*, 2013.

[15] J. Eyers. Banks test staff with cyber security 'fire drills'. http://www.afr.com/technology/banks-test-staff-with-cyber-security-fire-drills-20160914-grg2e8. (Accessed: 15 February 2018).

[16] R. J. Fisher. Social desirability bias and the validity of indirect questioning. *Journal of Consumer Research*, 20(2):303–315, 1993.

[17] A. Forget, S. Komanduri, A. Acquisti, N. Christin, L. F. Cranor, and R. Telang. Security behavior observatory: Infrastructure for long-term monitoring of client machines. Technical report, Carnegie-Mellon University Pittsburgh PA United States (CMU-CyLab-14-009), 2014.

[18] A. Greig, K. Renaud, and S. Flowerday. An ethnographic study to assess the enactment of information security culture in a retail store. In *2015 World Congress on Internet Security (WorldCIS)*, pages 61–66, Dublin, 2015. IEEE.

[19] R. Iphofen. Research ethics in ethnography/anthropology, 2013. European Commission http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/ethics-guide-ethnog-anthrop_en.pdf.

[20] K. Jansson and R. von Solms. Phishing for phishing awareness. *Behaviour & Information Technology*, 32(6):584–593, 2013.

[21] P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. A. Blair, and T. Pham. School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, page 3. ACM, 2009.

[22] F. L. Lévesque, C. R. Davis, J. M. Fernandez, S. Chiasson, and A. Somayaji. Methodology for a field study of

anti-malware software. In *International Conference on Financial Cryptography and Data Security*, pages 80–85. Springer, 2012.

[23] A. Lindesmith, A. Strauss, and N. Renzin. *Social Psychology*. New York: Holt, 1975.

[24] L. Little. Attitudes Towards Technology Use in Public Zones: The Influence of External Factors on ATM Use. In *CHI '03 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '03, pages 990–991, New York, NY, USA, 2003. ACM.

[25] F. Liu and S. Maitlis. Nonparticipant observation. In A. J. Mills, G. Durepos, and E. Wiebe, editors, *Encyclopedia of Case Study Research*, pages 610–612. Thousand Oaks, CA: SAGE Publications, 2010.

[26] D. Machuletz, H. Sendt, S. Laube, and R. Böhme. Users protect their privacy if they can: Determinants of webcam covering behavior. In *EuroUSEC*, Darmstadt, Germany, July 2016. Internet Society.

[27] K. M. MacQueen, E. McLellan-Lemal, K. Bartholow, and B. Milstein. Team-based codebook development: structure, process, and agreement. *Handbook for Team-Based Qualitative Research*, pages 119–135, 2008.

[28] M. B. Miles and A. M. Huberman. *Qualitative data analysis: An expanded sourcebook*. Sage, 1994.

[29] E. Murphy and R. Dingwall. Informed consent, anticipatory regulation and ethnographic practice. *Social Science & Medicine*, 65(11):2223–2234, 2007.

[30] D. Pauli. Go phish your own staff: Dev builds open-source fool-testing tool. `http://www.theregister.co.uk/2016/02/04/no_more_excuses_dev_builds_dead_easy_open_source_antiphishing_app/`, 2016. (Accessed: 15 February 2018).

[31] M. Petticrew, S. Semple, S. Hilton, K. S. Creely, D. Eadie, D. Ritchie, C. Ferrell, Y. Christopher, and F. Hurley. Covert observation in practice: lessons from the evaluation of the prohibition of smoking in public places in Scotland. *BMC Public Health*, 7(1):204, 2007.

[32] N. Sanandaji. Trust not taxes have made Sweden a success, 2015. `https://www.thelocal.se/20150711/trust-not-high-taxes-have-made-sweden-a-\success-opinion` 11 July (Accessed: 21 May 2018).

[33] B. Segendorf and A.-L. Wretman. The Swedish retail payment market. *Sveriges Riksbank Economic Review*, (3):48–68, 2015.

[34] P. Spicker. Research without consent. *Social Research Update*, 51:1–4, 2007.

[35] T. Steyn, H. A. Kruger, and L. Drevin. Identity theft. empirical evidence from a phishing exercise. In *IFIP International Information Security Conference*, pages 193–203. Springer, 2007.

[36] R. M. Sutton and S. Farrall. Gender, socially desirable responding and the fear of crime: Are women really more anxious about crime? *British Journal of Criminology*, 45(2):212–224, 2004.

[37] Technische Universität Darmstadt. Webpage of the Ethics Commission of the Technische Universität Darmstadt. `https://www.intern.tu-darmstadt.de/gremien/ethikkommisson/zustndigkeit/zustndigkeit.en.jsp` (Accessed: 20 May 2018).

[38] The Statistical Office of the European Union. Population on 1 January (tps00001). `http://ec.europa.eu/eurostat/tgm/table.do?language=en&pcode=tps00001`, 2016. (Accessed: 15 February 2018).

[39] The UK Cards Association. UK Card Payments 2015. `http://www.theukcardsassociation.org.uk/wm_documents/UK%20Card%20Payments%202015%20taster%20for%20website.pdf`, 2015. (Accessed: 15 February 2018).

[40] M. Tischer, Z. Durumeric, S. Foster, S. Duan, A. Mori, E. Bursztein, and M. Bailey. Users Really Do Plug in USB Drives They Find. In *IEEE Symposium on Security and Privacy*, pages 306–319, Fairmont, San José, CA, MAY 23-25 2016. IEEE.

[41] E. Von Zezschwitz, P. Dunphy, and A. De Luca. Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices. In *Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services*, pages 261–270. ACM, 2013.

[42] C. Weston, T. Gandell, J. Beauchamp, L. McAlpine, C. Wiseman, and C. Beauchamp. Analyzing interview data: The development and evolution of a coding system. *Qualitative Sociology*, 24(3):381–400, 2001.