Digital Enlightenment Yearbook 2014
K. O'Hara et al. (Eds.)
IOS Press, 2014

doi: 10.3233/978-1-61499-450-3-147

Watching You Watching Me: The Art of Playing the Panopticon

Lizzie COLES-KEMP [a,1], Alf ZUGENMAIER [b] and Makayla LEWIS [a]
[a] *Possible Futures Lab, Information Security Group, Royal Holloway University of London*
[b] *Munich University of Applied Sciences*

Abstract. As governments increasingly deliver services over the Internet, the opportunities for monitoring and surveillance of society increase. In public services to support the vulnerable, such as welfare, monitoring and surveillance functionality is often regarded by system designers as important components in defences against fraud and system misuse. However, the responses from the participants in this study demonstrate the potential difficulty of deploying such approaches when the systems themselves are perceived as working against not with the communities and indicate that supportive social networks are a prerequisite for these the technological systems to be secure. We explored the case of the use of the Internet to deliver parts of the UK welfare system from the perspective of an economically and socially deprived community in the North East of England. The findings show that, in the views of the research participants, reliance on technological security mechanisms makes the underlying administrative processes less rather than more secure. The findings also show that a focus on system security and monitoring rather than benevolence and user empathy is a barrier to the successful delivery of 'digital by default' services and can increase the overall feelings of insecurity in everyday life for service users. Our conclusion is that rather than being regarded as a technical system, such a service is better conceptualised as a social system with technological elements embedded within it. We therefore also argue that if such technological systems are to be secure, then the service design must also support the social networks that interact with these systems. We further argue that service providers must work with individual communities to develop and support the social networks in order for the technological security controls to be effective.

Keywords. security in the wild, service design, community, digital civic

Introduction

Over the last 10 years, there has been a considerable amount of research undertaken to understand how employee attitudes, values and beliefs influence the degree to which they comply with the security goals of an institution. In this study, we ask two research questions. 1) What is the possibility for positive service engagement when service users feel that a service adversely affects the security of their everyday lives?

2) Is data security possible in any practical sense without the support of the social networks that reside within the service user community?

[1] Corresponding Author.

In order to explore this topic, we focus on online services used to support the assessment and payment of welfare/social security in the UK. In the UK, such a system is often termed the 'benefits system' and claimants are paid 'benefits'. The use of online services emphasises the shift in the UK benefits system towards a largely transactional service that does not accommodate the social and relational aspects of support for those relying on welfare. When the welfare system was originally conceptualised, there were many more service mechanisms for individual support, both within the system and within the community, that are absent in the current service design.

In summary, our findings show that for the participants in this study welfare changes did increase feelings of insecurity in everyday life. Technical controls to protect data might increase this overall feeling of insecurity unless a social system is in place to tend to these wider feelings of insecurity and articulate the value of the technical controls. The main conclusion from this study is that social contact is key to influencing cooperative behaviours and that a service design built on cooperation and active participation rather than coercion and pacification will achieve better engagement with these services. Therefore, careful attention must be paid to the design of the social system into which technical controls are deployed. Traditionally, value alignment, positive role models and trust are used within a social system to support the overall goals of the system. The work presented in this chapter explores what system security roles such attributes play in the context of societal insecurities.

1. The Context – Welfare and Digital by Default

Mark Neocleous [1] underlines the significance of understanding social security as another form of control and [2] presents the argument that recent changes to welfare in many countries represent a further securitising of society. Recent welfare reform in the UK could be interpreted as a political desire to bring under control that part of society that is reliant on the receipt of benefits. As is often the case with reforms to essential systems such as welfare, there has been controversy[2,3] – particularly in light of the use of benefit sanctions and the speed and method of change [3]. The use of technology is linked to this controversy, as it is a highly visible instrument of change and has an explicit role in the benefit sanctions process.[4] The UK has introduced a 'digital by default' agenda that has online service delivery as the mechanism of choice when implementing central and local government services in the UK.[5] In 2012, the UK's Welfare Reform Act[6] heralded the extension of 'digital by default' to the delivery of welfare assessments and payments in the UK. Whereas previously the delivery of welfare services has relied on much face-to-face contact between Benefits Officers and claimants, the plan is now to primarily deliver this using online means.[7] This type of approach places systems security mechanisms at the forefront of this perceived drive to re-order parts of UK society, and also aligns the use of security mechanisms with algorithmic means of assessing claimant requirements,

[2] http://www.theguardian.com/society/2013/jan/25/spare-bedroom-tax-contradiction-impossibility

[3] http://www.theguardian.com/commentisfree/2013/jan/08/welfare-state-1942-2013-obituary?CMP=twt_gu

[4] http://www.bbc.co.uk/news/uk-24104743

[5] https://www.gov.uk/government/publications/government-digital-strategy

[6] http://www.legislation.gov.uk/ukpga/2012/5/pdfs/ukpga_20120005_en.pdf

[7] http://central-government.governmentcomputing.com/news/2012/feb/03/universal-credit-digital-by-default

potentially giving the impression of a coercive rather than cooperative use of security controls. It follows, therefore, that if the benefits system is regarded as contributing to increased feelings of general insecurity (financial, emotional and relationship insecurity) then the technological security controls will also contribute to such feelings and reduce the likelihood of positive system engagement.

1.1. Contribution

Our work contributes to an understanding of the relationship between technological controls, service delivery and general feelings of security. This chapter makes a contribution to our understanding of the role of cooperation in system security and the implications for system security when this cooperation breaks down. It also illustrates the difficulty of replacing cooperation with surveillance as a means of instilling end-user control.

2. Bridging Two Literatures

In order to contribute to the understanding of technological control in the wider discourse of societal security and insecurity, we must bridge two academic literatures: the literature of critical security studies, which is largely the domain of social scientists and humanities scholars, and the literature of system security, which is largely the domain of technologists and mathematical scientists. By using critical studies as a lens through which to survey the technological service design, we can see that if we consider information and systems security as part of, and not separate from, the field of security studies, then technological security mechanisms might be characterised in critical security studies as an instrument with which to carry out a security doctrine of ordering and re-ordering society [1] where security technologies are used as a means of user community management. This technological approach focuses on the ability of service providers to be able to identify service users and to use this identification to determine levels of service access.[8] The identification and verification of system users has long been a fundamental theme of computer and network security studies [4]. In the mid-1990s, technological approaches to identifying and verifying users also became a focus of usability and security studies [5]. Encouraging user cooperation [6] and the gaining of user trust [7] are frequent usable security design messages, albeit a difficult concept to operationalise through traditional security design thinking [8]. The focus of usable security studies is typically the relationship between the service user and the service and its technologies, rather than a focus on the effect a service and its deployment might have on the user's general feelings of security [9]. An understanding of a societally situated user experience is still relatively new in security design [10], and in security design, users are rarely understood in the context of their everyday lives and the aspects of those lives (relationships, emotions, health, finance, employment, housing etc.) that affect a person's general feelings of security. By placing a critical security studies lens on technological service design, the work presented in this chapter brings the wider societal perspective to those who, hitherto, have primarily focused on the technological design rather than the interaction between social systems and technology.

[8] Cf. Footnote 5.

2.1. Related Work on Social Responses

System security research on goal alignment has been undertaken to better understand how alignment of organisational goals with thepersonal goals of users results in greater compliance with information security policies [11,12,13,14]. In this organisationally-focused system security literature, the service provider is not characterised as a threat actor and there is a degree of benevolence assumed on the part of the service provider. The issue of benevolence is important, as studies indicate that sanctions [12] do not affect the intention to comply, whereas the attitude, practices and values of the user do. Linked to this, research also points to the importance of social bonds [11] within a community and results indicate that where computer misuse occurs there is often an absence of role models representing compliant behaviours. Willison's work also makes clear the importance of theories of environmental criminology, where prior knowledge of the organisational processes at work is necessary for system abuse to take place. The importance of workflow and process knowledge is further emphasised in the 'insider threat' literature [13,15], which shows the difficulty of identifying workflow and process misuse by users who are authorised to use those processes. In our study, we explore how the user community might appropriate insider knowledge, and the impact that the threat of benefit sanctions and system imposition has on the potential types of appropriation.

Mishra and Dhillon [13] advocate informal management as an important instrument for nurturing and managing information security compliance, and emphasise that informal structures are as important as formal ones in terms of influencing compliance behaviour. This perspective further underlines the importance of social networks and relationships and the importance of role models in influencing the management of information. The acknowledgement of the importance of social relationships and informal networks contrasts with the more formalised approaches of access control studies [16,17] and of security management [18] and indicates that cooperation is a fundamental principle in the management of information. In our study, we therefore explore the role of informal management and consider how the user community constructs informal management and for what purposes.

The issue of trust has been a dominant area of study in e-commerce [19] and security design [6,7], and the implications of lack of trust in either the technology and infrastructure, the mediating agents, the partners or the institutions are shown to result in a lack of cooperation with the system and can result in non-engagement or resistance activities [8,7]. This focus on trust further speaks to the importance of social relationships and role models. In our study we therefore consider both how the user community might appropriate the surveillance and monitoring functionality, and whether trust can still be brokered when surveillance and monitoring are dominant system security features.

2.2. Situating this Study

Our study looks at the traditional information systems themes of goal alignment, role models and process misuse through the lens of critical security studies by exploring the themes of value alignment, role models and trust within security practices in the wild [20–23] and considers the impact of political and social hostility between the service user and service provider on these practices. In summary, the motivation of our study is to understand how traditional system security controls fare in a hostile environment

where there is an absence of cooperation between service provider and service user and what role such controls play in overall feelings of security. The focus of our study is the user community consisting of long-term benefits claimants who had started claiming benefits when the system was analogue and paper-based and who now use online services as part of their method of claiming benefits. The goal of our study is to understand whether value alignment, positive role models and a culture of trust play any part in system security when the system deploys a public policy regarded by users as coercive. As this is a user community that is not typically the focus of system security studies, it was decided that inductive reasoning within a grounded research approach [24] would be used. The structure of this study has its roots in the traditional methods of social, community-focused research [25,26] used to explore the effects of social policy change on marginalised communities.

3. Study Structure

In many senses, socially and economically deprived areas represent 'hard to reach' communities in research terms. Academic researchers rarely come from such communities, and often such communities are wary of outsiders. The employment, financial, educational, health, food and housing deprivation found in such communities often give rise to a mistrust of outsiders and also make it difficult to find a shared conceptualisation and language with which researchers and community members can explore technology-related research topics. Therefore, such studies require an element of trust building and researcher socialisation within the community. Researchers must first build a relationship with the community using ethnographic research so that they gain a feeling for the community narratives related to the research topic. Being aware of these research challenges, we designed a three-part study structure in which we began with an ethnographic study, then, using the findings of the ethnographic study we designed and implemented a community consultation, and finally we completed the study with a focus group. The output of the study is a consolidated community narrative.

3.1. Ethnographic Study

Our initial ethnographic work took place for nine months, in a Community Centre providing a range of community services within a socially and economically deprived community in the North East of England, and explored the attitudes of the community towards welfare change. As part of this ethnographic study, we learned the community language used to describe the welfare system, and we learned that system 'twisting' (circumventing system security) was a relevant focus for our study – because twisting represented a rejection of the technological controls – and that during the observational work it was seen that the nature of the social network within the community influenced the extent and the nature of the twisting. Twisting is therefore an important concept because it is influenced by a service design that reduces the amount of social network support, which is one of the key differences between the benefits system as it was originally conceptualised and that which prevails the changes brought in from the 2012 legislation.

The ethnographic study revealed a complex set of feelings towards the benefits system, including anger, frustration and alienation. Community members often expressed

feelings of helplessness, and for some the Community Centre was an empowering space where they acquired knowledge which helped them to regain some control of the benefits process. At times the frustration was articulated as a desire to 'strike back'. The use of technology to strike back is a phenomenon that has been seen in other digital interactions between economically deprived communities and the State [27] and is one explanation for the potential use of system twists. The studies were carried out under the standard institutional ethical policy and underwent an approval process; no system twists were witnessed during the study and participants only talked about such activities in terms of hypothetical scenarios.

In order to move beyond the ethnographic study and work with the community to better understand how security practices in the wild manifest themselves in this context, we deployed two further elements of the study: community consultation and focus groups.

3.2. Community Consultation

In the centre where this study took place, the community workers routinely conducted consultations with community members on matters of local policy. To extend our understanding and to focus specifically on the views related to benefits systems and their online deployment, we used lay research through consultations to gather data from welfare claimants using the Community Centre. Lay research uses community members as co-investigators [28] and provides a contextually sympathetic method of data gathering that of particular use when working with hard to reach communities not used to academic research engagements. The use of lay researchers has a long history in social research [25,26], and is a valuable means of deepening the nature of community engagement. The biases of lay-researchers were identified as part of the initial ethnographic study, and these biases were accounted for in the analysis of the data collected during the community consultation. Lay research provides a useful means of checking the consistency of the interpretation of the ethnographic study, as lay research is, in a sense, the response of the community to the themes initially identified by the academic researchers.

The consultation extended to 12 participants with profiles representative of long-term benefits claimants in this region. Participants were male and female; all benefits claimants were aged over 18 years, with similar social and financial backgrounds. The consultation was structured around a set of carefully predetermined questions that were co-designed with the lay researcher. The questionnaire was designed using the results of the ethnographic study. The following questions were asked.

- Do you feel comfortable using the current benefits system?
- What are the sorts of ways in which people might twist the benefits system?
- Are there situations in which the system might be twisted for someone else by family, friends, or other people in the community?
- Do you think moving to an Internet benefits system will make it harder or easier to twist the system?

The lay researcher deployed the questionnaire and provided a summary of participant responses to protect participant anonymity. The summary was compared with the findings of the ethnographic study to check for authenticity and representativeness. The summary was closely read and key themes were identified. The following themes emerged 'feeling powerless', 'system twisting based on claims', 'manipulation', and 'technology'. Within the technology theme, the following points were summarised by the lay researcher:

> Everyone agreed it was going to be easier to twist the system, . . .
> Everyone asked thought it would be easier to manipulate more vulnerable people like the elderly/special needs [person with a disability] as they may not have the skills or understanding to know what they are agreeing to. They feel that anybody could benefit from others, for example loan sharks, abusers, family members and scammers could take advantage of vulnerable people.
> Also people were very vocal that there is no evidence/proof of who is on the computer completing the form; it could be anyone with access to the computer.

As can be seen, it was understood by the participants that not only system monitoring took place, but also that the monitoring offered no proof of the source of the action. The theme of safety and general insecurity was raised, in particular the sense that identification and verification is liable to attack from those within the community, thus offering the claimant no protection. The responses indicated the potential for system twisting to contribute to feelings of insecurity about the benefits system itself as well as the potential for feelings of insecurity in the home and in the community.

3.3. Focus Group

In order to better understand the relationship between system twists and feelings of insecurity, a focus group was brought together. The membership of the focus group was carefully selected to accurately represent the segmentation within the claimant community. Participants comprised two males and three females, all aged over 18 years, with representative experience of claiming benefits, namely: 3 participants were long-term unemployed, 2 participants were working in the third sector, and 2 of the participants received a disability living allowance. The focus group participants represented the background of the participants in both the ethnographic study and the consultation. The focus group was given the following four questions in advance by the lay-researcher.

- How easy is it to twist the system?
- How can the system be twisted?
- Who is on the computer completing the form?
- If someone else is completing the form, why is this person required?

The four questions were followed by a problem statement quoted from the remote consultation study:

> There is a concern that we are getting to an age where face-to-face contact is becoming less and less and people can easily manipulate [‘twist’/circumvent] systems and vulnerable people for their own financial gain.

The problem statement was derived from the findings of the previous parts of the study and was used to encourage group discussion that might lead to a greater depth of understanding.

The total duration of the focus group was 82 minutes. The focus group was audio recorded with the permission of the participants. The raw data was transcribed verbatim and cleaned by removing nonessential utterances, adding quotation line numbers, and assigning unique identifiers to each participant. The transcript was then coded by assigning labels or themes to phrases, whereby a phrase could have multiple codes. A codebook was developed during the coding process. The coding was repeated several times until the coding and codebook were stable. New codes were added as required. We chose to use the

general inductive approach (GIA) [29]. The GIA approach systematises the process for analysing qualitative data and is more easily understood by security specialists who are more familiar with deductive, quantitative analysis. The GIA approach creates space for research findings to emerge from the frequent, dominant, or significant themes inherent in the raw data, arguably without the restraints imposed by more structured methodologies [29]. The frequency and clustering of the codes indicate the importance that participants give to particular points.

4. Findings

One of the most prevalent codes (40 instances, average 300 characters per code) is that of security practices; defined as text units referring to interactions with a real or hypothetical security feature of a system. Given the problem statement, as expected, the most dominant code was that of the system twist or system manipulation.

These security practices can be grouped into those relating to identification and authentication of identity (25 instances), those relating to verification of attributes such as the existence of a disability (12 instances), those relating to physical security (3 instances) and those dealing with security incidents (2 instances). Some text units were coded as relating to multiple concepts.

In this section we will present some examples of uses and misuses of the identification and authentication system. The given quotes were cleaned of off-topic remarks (such as: 'sugar, please' in response to tea being poured, and fillers such as 'you know, like') when they were distracting from the main topic and replaced by square brackets [. . .].

Initially, the participants talked about the benefits system in general and highlighted the importance of cooperation and the significance of role models. In line with existing systems literature, the importance of playing by the rules and the ease with which rules could be twisted if cooperation was not present was the focus of the first part of the discussion.

4.1. No Control without Cooperation

All the twists identified by the participants related in some way to subverting the means of user access to the system. One way to secure access to a system is to design robust identification and verification processes (often termed authentication) for a user. The robustness of the authentication processes is largely dependent on the robustness of the initial registration process that sets up user accounts on the system and links the system identity to the biological identity of the user, and this process is largely one that relies on the social network that supports the service.

The participants in the focus group showed little respect for the registration, identification and verification processes that they were faced with, and twisting is sometimes presented as an act of empowerment, sometimes as an act of coercion, and typically an act driven by financial need. The responses showed that twisting could both increase and decrease feelings of insecurity. The participants gave detailed examples of how they might expect to be able to twist the system. It is striking that the participants gave examples of how organisational processes, rather than technologies, might be attacked, and illustrated that the best defence of organisational processes is face-to-face contact with a service provider where respect is built for those processes through that face-to-face contact.

4.1.1. Identity 'Theft'

Superficially, much of the potential system twisting described by the participants could be labelled 'identity theft'.

> Participant 1: . . . on the computer completing the forms: I'm the benefits officer and you [are] sending them to me, [participant 1] name sign it, you could be anybody Tom, Dick or Harry.

We can see from this example that participants felt that it would be fairly straightforward to manipulate identification. Underlying this assumption is the knowledge that in less affluent socio-economic groups, verification documents such as driving licences and passports are less likely. Added to which, proof of housing is also less reliable, because housing is often temporary, and the individual is not an owner-occupier. The participants knew the lack of verification documentation is problematic for registration on a new system, and saw this as a potential weakness which could be exploited.

The initial registration process was not the only aspect that was regarded as weak – easy access to personal data within a family or social setting was also regarded as a vulnerability. For example, one scenario given is where the person interacting with the system is pretending to be a different person, with the impersonated person not being aware that this impersonation is happening. The person interacting with the system has enough information to authenticate themselves as the intended user. This could be considered as a clear case of identity theft. The success of this twist depends on the ability of the impersonator to gather data.

Different variations of how the identity thief might gather the information, requiring them to pass themselves off as the victim, were described by the focus group, and the range of approaches demonstrates how difficult it is to design a robust registration process.

One way would be to get hold of the required information by dumpster diving or by chance, as this participant describes:

> Participant 1: [you] might toss a letter around with your name and address on it. I can, I can go into the benefits and I can get, now you can get what they call them loans, crisis loans. . .

This example reveals the insight that the request dor a crisis loan puts the process under pressure to issue money quickly, and verification is therefore likely to be less robust – this reflects astute situational awareness. (A crisis loan is an emergency loan to cover an essential cost.)

However, the concept of identity theft is inadequate to explain the tight, interwoven relationships that occur within families. Sharing technology access, relying on support from family members and providing support to those who need help with engaging with the benefits system were all themes, and participants explained how this scenario offers further opportunity for more complex twists.

Delegation systems, such as power of attorney, are set-up to take into account the role of the assister. However, formal delegation is not always used as the process for setting up ad-hoc delegation is regarded as unwieldy or inaccessible. Examples were given of where a typical response might be for the delegatee to impersonate the delegator in order to authorise an ad-hoc delegation of access.

Examples given by the participants illustrated how easy it might be to impersonate another, especially when the impersonated person and the impersonator are from the same

family or close community. The difficulty here is that there is no way of knowing whether this is approved or unapproved by the claimant. If the delegatee is acting in the best interest of the claimant, this could be considered tacit approval of delegation, or a 'break the glass' overriding of access control [16,17] but requires agreement as to what is 'best interest'.

In conclusion, the participants reflected that technological controls for identification and authorisation are not perceived as protecting either the user or the system, and might increase rather than decrease feelings of insecurity if users already feel vulnerable.

4.2. Benevolent or Malevolent Twist

As can be seen from the previous section, as well as being driven by financial need, at times system twisting is driven by a desire to empower, but at times it is driven by coercion. The following example describes this type of ambiguity:

> Participant 5: . . . My daughter gets disability benefits and I'm her power of attorney and I never once [...] [but] I could claim anything for her; and the money gets paid into my bank account; and I could do anything.

The sense of insecurity when using such controls becomes apparent when considering delegated authorities. The following examples were given of instances where social and organisational processes and protocols might be twisted:

> Participant 4: I know people who [have] given their cards to people to get the money out of the banks, [. . .] and they just went and took the money and everything.

> Participant 5: There are people, who are a little bit unscrupulous, and you got more vulnerable people. You got people maybe in care homes.

Assisted use of technology is another category of delegated or shared authority that gives rise to its own set of problems, such as a family member who is normally trusted turning against the person they are helping.

> Investigator: Would you let your grandchild help you?
> Participant 2: But [. . .] what if your child is a drug dealer? They are all into drugs and they want money? That's your money, and that helping you, or you think it is helping you, if not, they're just robbing you. [. . .]

System access and system monitoring would seem to offer no defence against these potential causes of insecurity without the support of social relationships.

4.3. Fluid Meaning

The examples in the previous section highlight how events can be re-interpreted over time and how fluid the interpretation is. As a result, differentiating between benevolent and malevolent twists can only be achieved with close knowledge of the claimant and their situation. This is a particular problem when reliance is moved from face-to-face engagement to a system focusing on technological transactions. For example, in the case below, the system must differentiate between a voluntary and an involuntary cash withdrawal.

> Participant 2: I'm her loan shark and she owes me like thirty quid a week, and then I [let her] get another loan out, and another loan out. So I just take her card off her, [and say] "Give us the code". And I go and try it once, and if it works, I just keep the card.

Alternatively, a more subtle method of coercion was described, where the coercer pretends to represent the benefit system and plays on the vulnerability that some benefits claimants feel in not being confident online service users:

> Participant 5: A women or a man and a women in a suit, going to have a portable laptop with them, [. . .] knock on the door: 'Hello we [are] from the [benefits office], have you got a computer access? You know, the benefits [are] online. Would you like to give me your details, and I'll fill it in all for you.' [. . .] : 'Oh, it might take 6 to 8 weeks for the changes.' [. . .] So [go] by 6 to 8 weeks before they even think about reporting it.

We would argue that what is required is the strengthening of the social network so that those who lack confidence can rely on the social network to help them engage with the online service and take advantage of the technological protection measures.

4.4. Playing to the Panopticon

Privacy concerns have often been raised when presenting a 'digital by default' agenda. The idea of using online systems that can track and trace many of your actions is often seen as another move towards a surveillance state. However, participants in the focus group indicated that surveillance was a fact of life, and could be used by the would-be system twister as much as by the service provider. The participants' comments reflected the view that being observed had always been a feature of the benefits system, and the more you understood the system, the easier it was to use the monitoring and surveillance to your advantage.

Participants gave examples of how, under the face-to-face system, knowing that they were being watched, a claimant might try to maximise their chances of a positive assessment during a face-to-face assessment by adapting their appearance by not shaving or washing to convey a particular impression as described in the following quotation:

> Participant 1: [. . .] they done fuck all [and] don't shave for like 23 days go around dirty and then they go look and all that and they sit like that.

In another example, participants explained how they might adapt their behaviour to what they believe is expected of someone with a mental health issue, if that is what their benefit calculation is based on.

> Participant 1: When you go into the lift make sure that [you are seen to say that] you can't go [. . .] if you're saying that you got anxiety or whatever.

Principles of behaviour modification are also extended to electronic surveillance. For example, participants expressed the belief that CCTV cameras on premises are used for supervising their behaviour. Therefore they explained that a claimant could adapt their behaviour accordingly, in order to not leave any evidence that could be interpreted as contradicting their story.

> Participant 5: Well the other ones will say like: "When you go in there's a camera that that you are on [C]CTV walking down so make sure you're limping."

Importantly, these observations reflect the point that system users are not static objects and that users adapt behaviours in response to experience and knowledge, potentially making surveillance problematic. It is not inconceivable that more sophisticated surveillance will simply result in more sophisticated user responses. The comments also illustrate the importance of the word of mouth networks and how system knowledge is shared and updated through these networks.

5. Concluding Design Discussion – Security that You Can Respect

When considering the security of digital systems, the focus group concluded that online systems reduce the unpredictability of a process and potentially make it easier to compromise the underlying weaknesses of the administrative system. In the view of the focus group, the technological controls did not offer any protection to the claimant and at times could exacerbate the general feelings of insecurity. They put forward the view that protection of the data and the individual was instead provided through social contact and social relationships, and this raises the question of how role models and value alignment might help in this respect.

5.1. Re-conceptualising the System as a Social rather than Technocratic System

The participants responses reflect that, no matter how much effort is placed in technological controls and surveillance methodologies, the determining factor in user behaviours is the relationship to the social networks around them, located in the physical spaces that they inhabit. This conclusion is reminiscent of early social research [26], and perhaps therefore unsurprisingly, the findings of this paper echo the findings of these early social studies.

As changes to the benefits system are being rolled out, there is increasing concern about the security of the system, and yet digital by default continues unabated. The findings from this small study indicate that standard end-user system security techniques of identification and verification and monitoring and surveillance do not result in the protection of the data on the system, because these mechanisms on their own do not encourage positive user engagement. Therefore, this study concludes that the focus should be given to community cooperation and the development of supportive role models, and that technological controls should be seen as sitting within such networks. It is then for the social networks to engage with and make sense of the technological support, thus offering greater levels of support to the service users.

One tangible approach might be the development of a community-based component to a centralised system, where local community members are an active part of the social system surrounding the technical controls. The typical criticism towards such an approach is that community members can also be malevolent. However, this ignores the importance of the word-of-mouth networks and their ability to vouch for people and groups, and the willingness to only cooperate with those who are working with, and not against, the user community. Given that claiming welfare is linked to physical location and that local community groups, separate from local and central government, already provide technology

and welfare rights advice and training, this activity could be a natural extension. This model would not only re-align the system to the goals and values of the user community, thus encouraging positive use of the system, but would also provide a better set of local protection mechanisms from coercive behaviours. This proposal is an extension of the concept of multi-lateral security [14], where community members cooperate to achieve a balance in the data protection goals and in so doing act as defence against malpractice by other community members. Community models of this type should be better able to create empowering spaces that help benefits claimants to develop strategies for feeling more secure in their ability to engage with the welfare services, and to manage these interactions on their own terms. The study indicates that the two underpinning principles of a cooperative approach are the need for social contact and the importance of fairness.

5.2. The Need for Social Contact

Social contact and the need for human to human interaction were regarded as important by the focus group participants. An example of this view is articulated in the following quotation.

> Participant 1: It might [be] better off having someone actually going you like somebody like community person going out to do the benefits because they are seeing people.

This suggests that the social relationships between community workers and claimants reinforce trust and reduce vulnerabilities in the system. This insight converges with the observations made during the ethnographic study, where community workers could be seen to assume the role of positive role models guiding people to make system choices that were in the claimant's best interests. Community workers were heard to use the narrative of value alignment, where the goal of the benefits process became to find the best outcome for the claimant. In each case, the community worker built a trust relationship, and through this relationship the individual regained some control.

In line with the organisational literature, participants often indicated that it was the processes and the frailties in human practices that could be leveraged in order to perform a twist. The participants put forward the view that the unpredictability of face-to-face communication makes it harder to generate accurate answers, whereas online responses are easier to control. The following example shows the difficulty of designing a service that is both usable and secure for wide cross-section of the community:

> Participant 5: It's more easily manipulated, because it's anonymous [...] you can open another tab bar and Google something and thing, you can have the information all down in front of you.

Participants often commented that these administrative processes needed to be vulnerable in order to respond to the different needs of claimants, and that face-to-face contact was the only way to make these processes secure. The participants also clearly highlighted that, in their opinion, it is unpredictability that makes a system harder to twist and therefore an economically efficient architecture, which is designed on the economies of repetitive tasks, potentially makes a system more insecure. In both cases a multi-lateral security approach instantiated within a social network can contribute to the mitigation of these risks.

5.3. Fair Game or Just Fair?

During the focus group, respect for the welfare system was a recurring theme. There was a general lack of respect and trust expressed for the administrative processes. In particular, the participants reflected that digital by default does not necessarily make fraud detection easier unless the administrative processes are in place to support it.

> Participant 1: So, now, get all that information, get all information for their sickness, marry it together and go like, right, ok then, all these people with registered dis[ability], [...] so you wiped all of them off, now you got a list a million people who were not registered disabled, but they are claiming disability then these are the first ones you look at.

During the ethnographic study and as part of the consultation, anger at the system of benefit sanctions was often expressed, and the sense of the system being unfairly administered was frequently articulated. This anger could potentially fuel the practice of system twists. One conclusion from this study is that a combination of a system regarded as unfair and administrative processes being viewed as alienating, ineffective and mistrusted results in a system regarded by many as fair game rather than fair. The ethnographic work also indicated that this interpretation can be adjusted by positive role models and a re-direction of user focus towards more positive service use goals.

6. Conclusion

Throughout this study, participants voiced feelings of anger, frustration and alienation. These are feelings which are often expressed in socially and economically deprived communities such as the one described in this chapter. These feelings combine with the realities of relative poverty to foster an environment in which twisting the system is a constant part of the landscape if the social network that supports the service user community does not in some way 'design out' such practices. Technological responses can create more insecurity unless they are embedded within a wider social system that works fairly and cooperatively with the user community. Re-conceptualising the system as a social system that works with, rather than against, users and that offers users protection and a means of reducing general feelings of insecurity may be a more effective means of system security.

Acknowledgements

We would like to thank the study participants for their time, patience, trust and invaluable insights. We would also like to thank the numerous proof readers and supporters of this chapter for their interest and commitment to our research.

References

[1] M. Neocleous, *Critique of Security*. Edinburgh University Press, 2008.
[2] M. Neocleous and G.S. Rigakos, *Anti-Security*. Red Quill Books, Ottawa, Canada, 2011.

[3] A. Tarr and D. Finn, *Implementing Universal Credit: Will the Reforms Improve the Service for Users?* Findings (Joseph Rowntree Foundation). Inclusion, London, UK, 2012.
[4] J.H. Saltzer and M.D. Schroeder, The protection of information in computer systems, *Proceedings of the IEEE* **63**(9) (1975), 1278–1308.
[5] M.E. Zurko and R.T. Simon, User-centered security. In *Proceedings of the 1996 Workshop on New Security Paradigms*, NSPW '96, pages 27–33, New York, NY, USA, 1996. ACM.
[6] A. Adams and M.A. Sasse, Users are not the enemy. *Commun. ACM*, **42**(12) (1999), 40–46.
[7] A. Beautement, M.A. Sasse and M. Wonham, The compliance budget: Managing security behaviour in organisations. In *Proceedings of the 2008 Workshop on New Security Paradigms*, NSPW '08, pages 47–58, New York, NY, USA, 2008. ACM.
[8] S. Bødker, N. Mathiasen and M.G. Petersen, Modeling is not the answer!: Designing for usable security, *Interactions* **19**(5) (2012), 54–57.
[9] N.R. Mathiasen and S. Bødker, Threats or threads: From usable security to secure experience? In *Proceedings of the 5th Nordic Conference on Human-computer Interaction: Building Bridges*, NordiCHI '08, pages 283–289, New York, NY, USA, 2008. ACM.
[10] M.M. Lewis and L. Coles-Kemp, Who says personas can't dance?: The use of comic strips to design information security personas. In *CHI '14 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '14, pages 2485–2490, New York, NY, USA, 2014. ACM.
[11] R. Willison, Understanding the offender/environment dynamic for computer crimes. Working Papers 2005-4, Copenhagen Business School, Department of Informatics, 2005.
[12] S. Pahnila, M. Siponen and A. Mahmood, Employees' behavior towards is security policy compliance. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, pages 156b–156b. IEEE, 2007.
[13] S. Mishra and G. Dhillon, Information systems security governance research: A behavioral perspective. In *1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference*, pages 27–35, 2006.
[14] K. Rannenberg, Multilateral security a concept and examples for balanced security. In *Proceedings of the 2000 workshop on New security paradigms*, pages 151–162. ACM, 2001.
[15] G. Magklaras and S. Furnell, A preliminary model of end user sophistication for insider threat prediction in it systems, *Computers & Security* **24**(5) (2005), 371–380.
[16] A. Ferreira, R. Cruz-Correia, L. Antunes, P. Farinha, E. Oliveira-Palhares, D. W. Chadwick and A. Costa-Pereira, How to break access control in a controlled manner. In *Proceedings of the 19th IEEE Symposium on Computer-Based Medical Systems*, CBMS '06, pages 847–854, Washington, DC, USA, 2006. IEEE Computer Society.
[17] E. Rissanen, Towards a mechanism for discretionary overriding of access control (transcript of discussion). In *Proceedings of the 12th International Conference on Security Protocols*, SP'04, pages 320–323, Berlin, Heidelberg, 2006. Springer-Verlag.
[18] S.L. Erete, Protecting the home: exploring the roles of technology and citizen activism from a burglar's perspective. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '13, pages 2507–2516, New York, NY, USA, 2013. ACM.
[19] C. Castelfranchi and Y.-H. Tan, The role of trust and deception in virtual societies. In *HICSS*. IEEE Computer Society, 2001.
[20] P. Dunphy, A. Monk, J. Vines, M. Blythe and P. Olivier, Designing for spontaneous and secure delegation in digital payments, *Interacting with Computers*, page iwt038, 2013.
[21] P. Dourish, E. Grinter, J. Delgado de la Flor and M. Joseph, Security in the wild: User strategies for managing security as an everyday, practical problem, *Personal Ubiquitous Comput* **8**(6) (2004), 391–401.
[22] S. Singh, A. Cabraal, C. Demosthenous, G. Astbrink and M. Furlong, Password sharing: Implications for security design based on social practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '07, pages 895–904, New York, NY, USA, 2007. ACM.
[23] C. Herley, So long, and no thanks for the externalities: The rational rejection of security advice by users. In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, NSPW '09, pages 133–144, New York, NY, USA, 2009. ACM.
[24] B.G. Glaser and A.L. Strauss, *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Aldine de Gruyter, New York, NY, 1967.
[25] A.P. Jephcott and H. Robinson, *Homes in High Flats: Some of the Human Problems Involved in Multi-storey Housing*. Occasional papers. Oliver and Boyd, Edinburgh, UK, 1971.

[26] P. Jephcott, *Some young People*. George Allen and Unwin, London, UK, 1954.
[27] K. O'Hara and D. Stevens, *inequality.com : power, poverty and the digital divide/Kieron O'Hara and David Stevens*. Oneworld Oxford, 2006.
[28] A.C. Macaulay, L.E. Commanda, W.L. Freeman, N. Gibson, M.L. McCabe, C.M. Robbins and P.L. Twohig, Participatory research maximises community and lay involvement, *BMJ* **319**(7212) (1999), 774–778.
[29] D.R. Thomas, A general inductive approach for analyzing qualitative evaluation data. *American journal of evaluation* **27**(2) (2006), 237–246.