THEATRES OF FAILURE: DIGITAL DEMONSTRATIONS OF DISRUPTION IN EVERYDAY LIFE

Jessamy Perriam

Department of Sociology

Goldsmiths, University of London

Thesis submitted for the degree of Doctor of Philosophy (PhD) 2018

Declaration of Authorship

I, Jessamy Louise Perriam hereby declare that this thesis and the work presented in it is entirely my own. Where I have consulted the work of others, this is always clearly stated.

Signed: ______________________ Date:

Acknowledgements

Firstly, many, many thanks goes to my supervisors. Noortje Marres, who replied to a vague email from her former Digital Sociology student who just wanted to keep researching with encouragement to apply for a PhD studentship. And Daniel Neyland, who has been a source of wisdom, wit and support throughout this process. Thank you both for being my trusted guides through STS and for pushing me to be a better sociologist and researcher.

Thank you to the Centre for Invention and Social Process at Goldsmiths, University of London who gave me the opportunity and funding to take up this PhD. Thank you to all CISP members and the current directors, Michael Guggenheim, Marsha Rosengarten and Alex Wilkie for supporting my endeavours.
The genesis of Chapter Six's selfie stick research came from a C(S)ISP Salon on *Methods Out of the Box* in early 2015. Many thanks to my collaborators Noortje Marres, Dave Moats and Ana-Maria Herman.

Thank you to my upgrade examiners Evelyn Ruppert and Kat Jungnickel for helping clarify my ideas and solidifying my standpoints.

Many thanks to the Goldwig writing group, where much of this thesis was written in 20-minute increments. In particular, thank you to Baki Cakici, Katherine Robinson, Hanna Sjogren, Francisca Grommé, Funda Ustek-Spilda, Rasmus Birk Hoffman and Francisco Calafate-Faria for their moral support. Thanks to Andy Freeman for technical support and discussions on APIs.

Thanks to the many PhD students and post-docs I have had the pleasure of sharing ideas and the 12th floor of Warmington Tower with: Dave Moats, Irina Papazu, Andreas Birkbak, Nele Jensen, Laurie Waller, Vera Ehrenstein, Sveta Milyaeva and Mario Trifuoggi. Thank you for your conversation and camaraderie in the face of patchy wifi and erratic heating.

Thanks to my fellow PhD students who have shared the ups and downs of the PhD experience and become firm friends: Sian Gouldstone, Adam Carter, Louise Rondel, Claire Levy, Emily Nicholls, Alice Corble, Ming-Der Peng, Macarena Bonhomme, Vanessa Hughes, Ville Takala, Kaoru Takahashi, Chloe Peacock and Ignacio Rivera.

Throughout my PhD, I have been fortunate to participate in workshops and summer schools which have been formative in both my thinking and practice. Thank you to organisers and interlocutors from the How to Map Issues workshop, the Ethnographies of Objects in STS summer school, the Big Data and Ethics summer school, the Mapping Controversies and Conspiracies summer school, the Digital Ethnography summer school and the Sprinting Obesity Data Sprint.

This thesis couldn't have been completed without the support of:
Friends in London: Alex, Andrew, Nat, Kate, Colette, Beth, Guido, Kerry, Barton, Jaime, Callum, Dan, Lizzie, Orrin, James, Antonio, Kat, Lisa and Tim.
Friends in far flung places: Astrid, Francesco, Johannes, Sarietha, Laney, Emma, Daniel, Sarah and Marianne. And the support of colleagues: Dave, Harry, Vita, Hilary, Leeky, Vee, Stacey and Sammy.
Lastly, thank you to my family in Australia: Peter, Carolyn, Steven, Avril, Freya, Morrigan and Dion. Thanks for cheering me on from afar.

This thesis is dedicated to:
David George Perriam (1924 - 2016)
Cynthia Wilson Perriam (1927 – 2016)
Stella “Ms Mac” McLoughlin (1970 - 2017)

Table of Contents

List of images

Abstract

Disruption regularly occurs in everyday life: public transport runs late, online accounts get hacked or faddish technology interrupts our experience of public spaces. These disruptions are sometimes called 'speed bumps' in our daily experience, giving insight into our expectations of a normal working order of everyday life. But mundane disruptions are not only events that occur and are then forgotten about. As I discuss in this thesis, we also demonstrate our disruption to those responsible as a form of problematisation (Callon 1986a), enrolling others into the disruption. As far as direct communication is concerned, these disruptions were once demonstrated between the disrupted party and the responsible entity via personal media such as letters, telephone conversations or emails. However, the uptake of social and digital media devices in recent years has meant demonstrations of mundane disruption have become networked, enlisting participation from broader audiences beyond those directly responsible. This leaves us with questions about the ontology and agency of the digital: is the digital a setting, an actor or an assemblage in the demonstration of disruption, or many other entities in addition? This thesis investigates how demonstrations of disruption are being reconfigured in light of the digital. I examine this phenomenon through theoretical standpoints in Science and Technology Studies, the emerging field of digital sociology and, ethnomethodology, which I bring to bear on demonstrations performed in three different field sites. The first is an ethnographic study of the situated practices of Transport for London’s social media customer service team. The second analyses blogs and YouTube videos that attempt to enrol publics in issues of cyber security. The last empirical chapter combines digital ethnography with an

in situ breaching experiment to describe and analyse how people use social media to demonstrate a particular disruptive digital object, the selfie stick, in public places.

Introduction

Why study demonstrations of disruption in digital settings?

In August 2016 I was standing in Transport for London's First Contact Customer Service Centre in North Greenwich, a large, modern, open plan office. I was talking to the manager of the social media customer service team who was a veteran of the public transport organisation. He hadn't worked for any other organisation. As he was making me a cup of tea, he described what his role was like when he joined Transport for London (TfL) straight out of secondary school in the mid-1980s. He was telling me about the process that London commuters had to go through to receive refunds for disrupted journeys. One of his first tasks in the role was to read the handwritten or typed letters from commuters to determine whether to issue them with a refund cheque. These letters went into quite some detail: times, dates, the stations they started their journey, where they intended to travel, along with the ticket they wanted a refund for. It was all potential proof that the disruption had occurred and the commuter was entitled to a refund. This evaluative process was an affair that involved a member of the public and the institution; the broader public was not involved.

Thirty years later, and this TfL employee's role had been reconfigured in ways he could not have imagined as a school leaver. To be sure, he was still dealing with commuter disruption but rather than solely issuing refunds for disrupted journeys, the role of a customer service agent has been respecified in the past five years as commuters have been making their way to social media platforms such as Twitter and Facebook to ask about disrupted journeys in real time, and often, in public. What was once a relatively private negotiation for a refund was a now a public demand for information, with the risk of TfL losing credibility amongst commuters and wider audiences. This TfL employee now spends his days managing a team of people who proactively communicate about disruptions in real time to the commuting public specifically to avoid issuing refunds.

This account provided by a TFL employee highlights two digitally enabled shifts in demonstrations that inform the research question that I address in this thesis. Firstly, a shift in the temporal structure of a disruption. The focus now rests not just on ascertaining what *has happened* but also on demonstrating what *is happening.* And secondly, a shift in the audience of demonstrations of disruption. What was once a small, targeted demonstration via letter, telephone or email between the commuter and the responsible institution has now become a public[1], potentially large, distributed demonstration between the commuter, the responsible institution and a larger audience of 'followers' or 'friends'. These two shifts change the nature and dynamics of demonstrations of disruption. They open up questions about how demonstrations can be configured to enrol actors into the formulation of a response to a disruption.

But why refer to this as a digital demonstration of disruption? And why is this worthy of study? How does it contribute to sociology and, more specifically, Science and Technology Studies (Pinch 1993, Star 1999, Grommé 2015)? A demonstration of disruption could take many forms. It could be similar to the

[1] By way of clarification, in this thesis, unless otherwise specified 'public' and 'private' are meant in terms of audiences and who is able to be involved in a demonstration of disruption. This is not to be confused with other uses of the terms public and private such as with public and private sectors or, publicly listed companies.

demonstrations described by the TfL customer service staff that involves an organization publically broadcasting information about a disruption to a service or conversely, a service user enquiring about a disruption that they are experiencing. But is there scope for demonstrations of disruptions to encompass more than service notifications or enquiries about disruptions presently happening? In this thesis, I will also examine demonstrations of potential cyber security disruptions. These demonstrations raise questions about the role of the experts in demonstrating possible disruption and the effective use of digital means to those impacted. It also raises questions about the consequences for not effectively enrolling people in the demonstrations, or excluding people from demonstrations. For example, what happens if an audience does not have enough expertise to understand demonstration of disruption about cyber security? What responsibility do demonstrators have to ensure their demonstration is comprehensible and relevant to their audience?

This list of examples of demonstrations of disruption is by no means exhaustive, nor are they strictly defined. In fact, my thesis also explores demonstrations that attempt to convince an audience that an object or actor recently added to a setting is disruptive. In these circumstances, the actors responsible for deciding whether something is disruptive may not have yet been enrolled in the demonstration. The demonstration of disruption may consist of social media users describing instances where they have encountered a disruption. An example of this can be found in Chapter Six where I attempt to locate digital demonstrations of selfie sticks disrupting public spaces such as galleries and museums. During the next part of this chapter, I will take on a brief tour of the thesis: its theoretical standpoints, its methodological approaches and, to the field sites where digital demonstrations of disruption are witnessed.

An STS approach to researching demonstrations, disruption and, the digital

In Chapter Two, I will discuss the Science and Technology Studies literature about demonstrations, disruption, the digital and, devices.

Demonstrations have a rich history in Science and Technology Studies and related literatures. In the former field, the work of Shapin and Schaffer (1985) on public science demonstrations in the era of the Scientific Revolution contributes to a conversation about the performative work that demonstrations do in creating and stabilising new knowledge. The works of Pinch (1993) and Downer (2007) show how public demonstrations in the late 20th Century and early 21st Century have been used to persuade or reassure the public of safety. More recently, the studies of Coopmans (2011) on demonstrations of medical imaging software and Smith (2009) in IT demonstrations begin to bring the digital into this conversation and its increasing role in demonstrations. In this thesis I use 'the digital' as a descriptor for the multiple ways the technology might be conceived: as a setting, an actor or assemblage and, as a research instrument (Marres 2017. This leads me to discuss the increasing role of digital technologies and settings - and more specifically, social and digital media - in demonstrations to do performative, persuasive work.

When discussing demonstrations, I will also use terms related to the notion of demonstrations, namely the 'theatre of proof' (Latour 1988) and the 'theatre of use' (Smith 2009). I will argue that some demonstrations of disruption may also be understood in terms of a 'theatre of failure'. Each of my empirical chapters attempts to describe how demonstrations occur within digital 'theatres of failure'.

However, for this to make sense the digital must also be better defined. A great wealth of STS literature and empirical work reminds us that the digital is not a new phenomenon or concept or indeed, terribly novel. However, it seems to me that, while STS as a field deals well with describing the socio-technical, it begins to falter around ontological understandings of the digital. Is it an actor? Is it an assemblage? Is it a setting? Indeed, could it possibly be all of the above and many more (Marres 2017)? In Chapter 3, I will discuss some of the ways in which the digital has been conceptualised with a view to specifying what the digital refers to in my discussion of my field sites.

In exploring ontologies of the digital, my aim is to outline ways in which we might mobilise approaches to the digital as analytical frameworks within empirical studies. For instance, how does the digital provide *a setting* for demonstrations? But the digital may also participate as *an actor or assemblage* in a disruption. How does the digital *enrol us* in disruption? And how might we use the digital as *a research instrument* to detect, observe and analyse demonstrations of disruption? By acknowledging these multiple configurations and implications of the digital, we are able to determine how it is deployed and/or invoked by members in each setting. This heuristic approach allows me to engage empirically with demonstrations of disruption without placing boundaries on the digital and to acknowledge how its role and specificities may change according to the situated practices of the actors involved (Marres and Lezaun 2011). This allows reflexivity and acknowledgement of the recursive nature of many configurations of the digital.

Further in Chapter Two, I will discuss devices with a view to having working definitions of what might be meant by ‘devices’ in the context of my research. In common parlance, the word ‘device’ is almost an immediate suffix to ‘digital’ when talking about objects that are digitally enabled. But in social sciences, devices are not understood or engaged with in such simple ways. In order to understand what might be meant when devices are discussed, I examine concepts of the dispositif (Foucault 1980), apparatus (Ruppert, Law & Savage 2013), and inscription devices (Latour and Woolgar 1986).

Finally, I will also engage with theoretical understandings of disruption. When talking about disruption, I am not referring to it in the sense of ‘cyberbole’ (Woolgar 2002), technological utopianism and, the project of disrupting existing industries by reorganising and moulding them for the gig economy. Although this is indeed a form of disruption to power relations and relations of rights and responsibilities between business owners and people working for them - as the gig economy forces drivers, delivery people and labourers to forgo sick leave and holiday entitlements (Cotton 2016) - this is *not* the definition of disruption I will be working with. Rather, I approach disruptions as everyday, mundane interruptions through the examples of the use selfie sticks in public places, public transport disruptions and, cyber security incidents. I will use my case studies to further explore what disruption can tell us about how things *aren’t* and how things *ought to be*. But most importantly, I will discuss the relationship between disruption and demonstrations. My aim is to understand how demonstrations are used to enrol actors in an unfolding disruption. In talking about disruption in the everyday, I will be making use of the literature around ethnomethodology (Garfinkel 1967/1991) and explore how disruption can be conceptualised as an opportunity to explain or create a social order that would otherwise be difficult to articulate.

This standpoint also enables me to use theories about problem-solution relationships (Garfinkel 1967/1991)[2] that arise out of disruptions.

Observing and describing digitally demonstrated disruptions, a mixed methods approach

But how then to research digital demonstrations of disruption? How might we attend to the digital in the light of my conception of it as a setting, actor and research instrument? In Chapter Three, I will detail the methodological approaches I have taken up to gather and analyse empirical instances of digitally demonstrated disruption: ethnomethodology, Actor-Network Theory (with Post-ANT) and digital sociology. Each of these methodologies informs my way of observing the digital, and attending to the different settings and requirements encountered in each of my field studies. In order to examine demonstrations of disruption within these different heuristic frameworks, I employed a number of ethnographic and digital methods to capture different ontologies of the digital.

As I will discuss in Chapter Three, I used ethnography in the form of semi-structured interviews, observations and field visits to explore how Transport for London (TfL) uses social media *as a setting* for demonstrations of disruption for both commuters and social media customer service agents to take place.

Additionally, I used participant observation within the setting of a corporate conference workshop, in order to understand how the company supplying the software configures workshop participants to use social media management

[2] While Garfinkel is one of the first to describe this concept of a problem-solution relationship, he does so only by briefly mentioning it in *Studies in Ethnomethodology* (1967/1991) and not elaborating further on it. Other researchers such as Neyland and Milyaeva (2016) take up this concept and work with it in more detail within STS.

software in preferred ways.

The use of observation in each of these field visits take their cues from Lucy Suchman (1987/2007, 1997) and her work with the situated practices of operating photocopiers and coordinating airport operations. By using observation and participant observation in the settings of Transport for London's customer service office and at a conference workshop, I am examining the situated practices of TfL staff demonstrating infrastructural disruption with the aid of social media management software.

I will discuss the use of more structured interviews to gather understandings around the concepts of the Internet of Things and cyber security from experts in the area. This method gathers empirical data around the entities that make up assemblages such as the Internet of Things. Additionally, I discuss the use of elicitation devices (Laurier 2004) such as online videos to provoke participants' understandings of the Internet of Things and cyber security more generally. In particular, I use these elicitation devices to provoke their professional vision (Goodwin 1994) based on their standpoint as either ethical hackers or cyber security experts attempting to engage publics.

In addition to discussing the use of structured interviews and elicitation devices, I will discuss the collection of digital demonstrations of cyber security disruptions from YouTube, Twitter and blogs in order to analyse how people demonstrate breaches to digital assemblages, and crucially, who they enrol through these demonstrations. This analysis will also look at the entities used by different people to demonstrate not only the risk or results of disruption, but also their own expertise in this area.

I will discuss the challenges of deploying methods to research digital objects as actors. I will examine the use of social media data scraping and visual analysis of social media to describe the use of and discourse around the use of the selfie stick in public places. But data scraping comes with some problems and opportunities, which I will briefly touch upon. I will also describe how ethnomethodology - in the form of breaching experiments - might be deployed to further investigate the reasoning for selfie sticks being banned in public venues such as art galleries and sporting venues.

In addition to discussing methods, I will briefly review some of the ethics around conducting research in both digital and material settings. This will take into account discussions on situated ethics, ethics of care and, ethical guidelines set out by the British Sociological Association (2017) and the Association of Internet Researchers (AoIR), along with viewpoints from other academics.

Configuring the commuter, Transport for London's use of social media.

In Chapter Four, I will take you to Transport for London's social media customer service centre to investigate the concept of *the digital as a setting* for demonstrating public transport disruption to commuters. In this chapter I discuss how Transport for London (TfL) started using Twitter in 2012 to broadcast transport updates to those attending the London 2012 Olympics. I discuss the ways in which TfL has developed their social media use: from a form of broadcasting disruption, they went on to engage with commuters about disruption, and to create self-service information about disruptions in the form of direct message notifications of disruption and Twitter bots[3]. This evolution in demonstrative practices, I will argue, highlights the performativity of these digital demonstrations of disruption. I explore how TfL has configured the commuter (Woolgar 1990) to expect disruption to be demonstrated in this social media setting. Additionally, we see how TfL also configured the commuter to carry out tasks that they were previously responsible for.

Similarly, how have social media innovations reconfigured TfL's customer service interactions to incorporate non-human actors carrying out digital demonstrations of disruption to commuters? I outline TfL and Twitter's recent collaborations on direct message notifications and chat bots as an example of how TfL have shifted common disruption enquiries to an automated and/or self-service provision. I propose that innovation within social media and social media management technology along with the evolving practices of both TfL staff and commuters over the past five years has produced a problem-solution relationship whereby actors adapt to the methods of demonstrating disruption and amend them when social media attributes are modified. This ongoing problem-solution relationship is important to studies of digital demonstrations of disruption because it is where we see accountability allocated between TfL and commuter. As a result, these innovations configure the commuter to demonstrate disruptions that require more customer service agent interaction. This shows that actions within the digital setting shift in response to changes in attributes and processes adopted by TfL.

[3] The bots discussed in this research are not to be confused with spam bots that feature in other scholarly work about Twitter. Rather, I will be discussing the growing use of chat bots on Twitter that follow an automated script with Twitter users. In the case of TfL, they use Twitter bots for commuters to make enquiries about the current status of a particular tube line.

Configuring the customer service agent. Social media management platforms and problem amplification

Visiting the field site at TfL not only allows us to examine the digital setting available to commuters when demonstrating disruption. It also allows us to examine the intervention of social media management platforms as a setting for customer service. This is a digital setting that is part of the customer service apparatus, and yet it is not visible to the commuter. I will spend some time in Chapter Four examining this setting because it forms part of the accountability process of these forms of public transport demonstrations of disruption. To do this, I visit a conference workshop session for a social media management software company to observe how they configure their users - in our case, the social media managers at Transport for London. This empirical participant observation provides data that is not too dissimilar to that encountered by Coopmans (2011) in her ethnography of medical imaging software companies. However, the difference here is that while Coopmans was a participant observer as an employee of a software company, I was a participant observer as a conference attendee. I was being configured rather than doing the configuring. By conducting this participant observation as a conference attendee, I was able to examine how users were being configured outside of the situated practices of Transport for London. I was also able to reflexively use this experience of being configured to return to the Transport for London field site and observe how these attempts by the software company to configure their users had succeeded or failed in different situated practices. To do this, I use the examples of the software’s capabilities to enact sentiment analysis - which Transport for London resisted using - and data analysis, which they used for performance management and demonstrating trends within their team and more broadly throughout the organisation. In particular, the data captured by the software allows Transport for London to observe trends in demonstrations of disruption and then do the performative work of amending staff and workloads in response. This part of the chapter looks at the uses of data generated by demonstrations of transport disruption and how that produces problem amplification (Latour 1999).

Problematising cyber security through demonstrations

Chapter Five shifts the focus from the digital as a setting for demonstrations of disruption to take place within, to *an assemblage or actor*[4] that can be breached through cyber attacks. I will describe how hackers and government agencies use the digital to demonstrate the potential disruption caused by public inattention to cyber security. This raises an interesting question as how some demonstrations succeed in problematising cyber security issues and enrolling the public in adopting better security practices, whereas others attempt to do this but find it difficult to capture the public imagination. How to enrol the public in taking an active role in ensuring their own cyber security? To take this further, I explore how cyber security could be considered as social and material arrangement (Law and Ruppert 2013) that actors work towards producing and maintaining.

In this chapter, I describe four ways in which both the hacking community and the Sociotechnical Security Group (StSG) in the UK's National Cyber Security Centre (NCSC) attempt to enrol the public in issues around cyber security. The examples are demonstrations from Twitter, YouTube and blogs.

[4] For Chapter Five, the digital is described as an assemblage or an actor that can be breached because there are situations where hackers may exploit a vulnerability in an actor (such as an internet enabled toy) to gain further access to an assemblage which may contain valuable data (such as a database of usernames, passwords, credit card details, addresses, etc).

The two demonstrations I refer to on YouTube present both extremes of narratives around digital assemblages in everyday life. On one hand, I examine how corporations frame the Internet of Things as a digital assemblage that helps deliver a convenient lifestyle (Shove 2004) through the use of overly simplified cartoon videos. I also compare the use of blogs to communicate cyber security risks to the consumer public. In particular, I analyse a cyber security blog post that gives a post-mortem of sorts of an Internet of Things enabled children's toy that was hacked. In this analysis, I focus on the ways in which the evidence for the hacking event is presented through screenshots of breached databases and emails to the company responsible for producing the toy and securing the databases that hold customer information. However, in this analysis, I argue that the digital evidence presented in the blog requires such a high level of expertise or professional vision (Goodwin 1994) to understand how the disruption occurred, that it is less effective in educating the consumer public about ensuring their Internet of Things devices and inscriptions are kept secure. I also argue that while the blog does a good job of problematising cyber security, it struggles to enrol Internet of Things users in ensuring good practices. These two demonstrations challenge how digital infrastructure is made visible. One focuses on describing what the infrastructure can do to achieve convenience. The other demonstrates just how mundane the infrastructure is and how easily it can break down.

But how effective are these demonstrations - both simplified cartoons and complex blog posts - in amplifying the problem (Latour 1999) of inadequate cyber security?

I argue that they are not effective digital demonstrations for the purposes of enrolling citizen-consumers[5] in the potential for mundane cyber security disruption. At one end of the spectrum, citizen-consumers are lulled into a false sense of security by cartoons that describe the positives of Internet of Things technology, without addressing the risks. On the other, the risks are demonstrated with such complexity that citizen-consumers without technical expertise could not understand or act upon the demonstrations. I will take up this important question by attempting to find demonstrations that sit between the simple cartoons and the complex blog posts.

To do this, I analyse blog posts of the Sociotechnical Security Group in the National Cyber Security Centre. The StSG are tasked with researching how lapses in cyber security occur in every day settings with the objective of doing reflexive work to inform consumers, product developers and business owners of cyber security best practice. Rather than focusing on one hacking event, the StSG examines the situated practices (Suchman 1987/2012) and pressures of people using digital devices and those developing them. Their argument is that the cognitive load on people in workplaces or home environments is quite often too strained to remember the volume of passwords required to access services we use on a daily basis (Beautement et al 2008); therefore, our situated practices involve workarounds that create cyber security risks. They further develop this observation that companies do not take this cognitive load into account when designing cyber security solutions for products and, they challenge them to reconsider how they design the security elements of a digital assemblage. However, the StSG also acknowledges that the developers creating digital products face economic, time, legal and design constraints from

[5] I take up the term ‘citizen-consumer’ to describe actors who are deemed by manufacturers to be ‘consumers’, but who are also labeled as ‘citizens’ by government organisations such as the National Cyber Security Centre.

other people in the actor-network responsible for creating a device.

In analysing these two types of blog posts from the cyber security industry and the StSG, I examine how one blog post informs other cyber security professionals and demonstrates expertise around the digital and, the other demonstrates these difficulties faced by user and producers. By doing so they are problematising more than just the end result of cyber security breaches. They are also problematising and encouraging users and producers to be reflexive about their practices in order to enrol them in different methods of ensuring cyber security in their workplaces and everyday life.

As a result of the empirical research and analysis of digital demonstrations in this chapter, I show the digital as an assemblage that can be disrupted through cyber attacks. However, I also examine the recursive benefits of demonstrating this type of disruption through digital means so as to enrol publics in adopting cyber security best practices.

Searching for the 'theatre of failure'

Chapter Six, the final empirical chapter, frames the selfie stick as a digitally disruptive actor in public settings. But from the outset, the question remains: just *how* is it disruptive? This chapter takes the analytic framework of the digital as an actor in cultural disruption while also using the digital as a research instrument to observe demonstrations of selfie stick related disruption. When the selfie stick was introduced as the newest popular culture fad in 2014, it was disruptive in a few ways. Some people in public, cultural institutions such as art galleries found them to be a nuisance in the space, antithetical to the activity of engaging with art and sought to have them banned, while some amateur photographers using visual social media platforms such as Instagram welcomed the selfie stick and found it a positive disruption that enhanced their photographic practices and images.

This chapter uses social media ethnography to determine how the selfie stick was being configured as an actor within amateur photography practices. I also used the ethnomethodological method of the breaching experiment (Garfinkel 1967/1991) to use a selfie stick in the National Gallery - a setting where the selfie stick had been banned - in order to produce an account of the expected social practices within the gallery setting. As will be explained further in the chapter, the breaching experiment did not go according to plan; there was no reprimand for using the selfie stick in a gallery setting.

However, I compare this with demonstrations of disruption in digital settings such as the comment sections of blog posts that discuss the disruptive attributes of the selfie stick and produces accounts of social practices within a gallery setting. Surprisingly, these comments are accounts of the reasons why people choose to use selfie sticks in the space, and accounts for their awareness both of their own behaviour and of the selfie stick as a disruptive actor in the gallery or museum setting. How might we analyse the in-situ results of a breaching experiment in a gallery on one hand and the comments section of a blog about gallery etiquette on the other? Exploring this question helps answer the overarching question of this chapter of how the selfie stick is demonstrated as disruptive in differing ways.

But in exploring the ways in which the selfie stick is considered to be both a positive and negative disruption, we encounter a discourse around perceived acceptable and unacceptable practices in public settings. In the analysis, we observe that these demonstrations act to mediate actors and enrol them in the practice of being a rule-abiding appreciator of art.

The research of demonstrations of selfie-stick related disruptions sits counter to the research in previous chapters. Where the previous chapters talk about demonstrating disruption by digital means for the purpose of updating people on disruptions in progress, or prevent future disruptions, this chapter deals with *the negotiation and problematisation of an object's disruptiveness* by way of demonstrations. In this sense, I observe the selfie stick as an actor. I seek to understand whether - much like the gun referred to by Latour (1999) - it is the selfie stick as a non-human actor that is disruptive, or the 'selfie-stick-in-hand' that makes disruption.

The work(s) of digital demonstrations of disruptions.

Evolution of demonstrations of disruption

This thesis shows how demonstrations of disruption evolve over time, and the shifts in how chains of accountability become shorter or more visible as a result of occurring in a digital setting. In the chapters about Transport for London, we see their demonstrations of disruption evolving from a one-way broadcast to a device that allows both commuters and TfL to demonstrate disruptions to one another. In the other case studies, we see less traceable, less stabilised accounts of demonstrating disruption. The research chapter about cyber security disruptions has shown the difficulties of enrolling publics in the work of *preventing disruption* merely by showing the disruption itself and the impacts of it. As shown in the discussions with the NCSC's Sociotechnical Security Group, demonstrating potential disruption is not enough to enrol a public. However, demonstrating that you understand the situated practices and limitations to people adopting safe cyber security practices *does* help towards enrolling publics into the potential for disruption by engaging them in reflexively thinking about their own struggles in situated cyber security practices. In the chapter about the selfie stick, we see the performativity of these demonstrations emerge subtly. Demonstrating disruption via digital means allows us to tinker with those demonstrations; adjusting and iterating over time, allowing new actors to demonstrate who previously may not have had such a public voice as experts. This performativity of digital demonstrations of selfie stick disruption also contributes, in part, to a ban on the object. How might demonstrations of disruption further evolve along with advances in socio-technical developments? Similarly, what might demonstrations of mundane, everyday disruptions teach us about researching and analysing demonstrations of political, social or economic disruption?

I also describe further research into digital demonstrations of disruption in light of transitions from private, to public to personalized demonstrations. In particular, the potential for future research into the scripting of digital demonstrations of disruption in light of a progression towards human actors demonstrating their disruption to non-human chat bot representatives of organisations.

I ask: Might we take a feminist approach to demonstrating disruption, and the potential of disruption, in light of the research into demonstrating cyber security disruption? What might a feminist approach to demonstrating disruption look like and how might that change the ways we think about enrolling people into these disruptions?

What I wish to show in this thesis, then, is that everyday disruption can be more than just having a train delayed. We will see demonstrations of disruption that appear to be rather frivolous with much digital ink spilled over disruptive, narcissistic selfie sticks. And yet we will see demonstrations of potential disruptions such as those detailed in the chapter about cyber security disruptions that struggle to enrol the imagination of the public. C. Wright Mills (1959) and Marres (2007) might argue that because we have not personally experienced a disruption, it is not a personal problem, and therefore, not yet a public issue. Does this make it any less worthy of demonstration? This opens the door to studying how more disruptions - such as political disruptions, consumer disruptions and yes, even the cyberbolic 'disruption' of the gig economy - are demonstrated online

Stabilising disruption

Perhaps the most exciting aspect of digital demonstrations is that we are able to witness the recursive work of stabilising disruption in great detail. Because of the public records created online, we feel we are able to see the work that is done in demonstrating, enrolling, acknowledging and responding to any given disruption. Where previously, it may have been difficult to account for each of the points in the process, we are now able to access and observe these demonstrations and the work that they do. I will describe this in greater detail in my empirical chapters, with a view to exploring how this may be deployed in future research of disruptions. Of primary interest is how the specificities of digital demonstrations of disruption allow for this stabilisation process to be fast and public in comparison to non-digital demonstrations. It also shows how the agency of human and non-human actors in the process of demonstrating disruption is distributed and shifting through a problem-solution relationship.

While this thesis is firmly situated in STS, there are aspects that could be of particular value to other disciplines. I will describe how other disciplines such as media studies, cultural studies, human computer-interaction and workplace studies may find the thesis useful or provocative. I am hopeful that this thesis is itself a demonstration of how disruption can be studied by digital means with an STS standpoint. In any case, it is a starting point of a conversation about the role of the digital in everyday disruptions that I hope will continue as digital and social media continues to configure and reconfigure the entities involved.

So why study digital demonstrations of disruption?

By studying digital demonstrations of disruption I want to observe and analyse the how digital and social media have shifted the chains of accountability between publics and institutions. Further, I want to observe these digital demonstrations of disruption in this fleeting moment where the specificities of social media platforms mean that these chains of accountability are very public and quite short. Before making these observations, I will examine the STS and sociological literature on the component parts of my research question - demonstrations, the digital and, disruption – in order to further develop the theoretical standpoint for this thesis.

Chapter Two: An STS approach to demonstrations of disruption

Introduction

If you're attentive to them, examples of digital demonstrations of disruption seem to be everywhere you look. There will be the old school friend complaining to a company on Facebook, the colleague tweeting about being stranded on a train platform and, a blogger or vlogger giving how-to advice about common household problems on YouTube. But although it is easy to notice these digital demonstrations of disruption, it is not immediately obvious how to analyse and conceptualise what is specific or important about demonstrations of disruption produced by digital means.

Before social media were part of everyday life, when our everyday life was disrupted we had to make do with less publicly visible and accountable methods such as time consuming emails, phone calls, letters, face to face appointments or, keeping one ear on the radio. In my research, I therefore sought to examine the different forms of disruption that people feel compelled to demonstrate in public, digital spaces, whether that is an infrastructural disruption or a disruption to expectations in a public social setting. These reconfigurations in the ways disruption is demonstrated via the digital poses two major research questions to be explored in further detail: 1) what reconfigurations of humans and non-humans in demonstrations of disruption can we observe in light of the addition of digital and social media in demonstrational assemblages? And, 2) what ontologies of the digital emerge when we begin to observe these demonstrations of disruption in situ and in networked media? How might we know the digital in different ways? In this chapter, I will contextualize these questions by examining literature in STS and related fields associated with three key concepts: demonstration, the digital (including devices) and, disruption. In exploring literature around the digital, I will also describe my chosen heuristic of framing the digital as setting, actor/assemblage and, research instrument.

Demonstrations and the bias towards success- from 'theatre of proof' to 'theatre of failure'

In this section, I examine the Science and Technology Studies literature around demonstrations. I will describe three distinct historical points in time in which STS scholars have studied demonstrations. Firstly, public science demonstrations of Hobbes and Boyle in the age of the Scientific Revolution, which aimed to enrol publics in new knowledge. These scientific demonstrations influenced 20th Century demonstrations concerned with proving the safety of new technologies and processes. Both of these demonstrations are examples of what Latour (1988) describes as the 'theatre of proof'. I then turn to demonstrations of IT hardware and software in the early 21st century, which are aimed at convincing an audience to purchase a product. Demonstrations of this type fall into the 'theatre of use' (Smith 2009). Finally, I will discuss how digital demonstrations of disruption challenge these conventional aims of showing proof or use. I will do so by discussing the 'theatre of failure' (Grommé 2014) that often comes about when demonstrating disruption. Finally I will reflect on the use of the digital as a setting for demonstrating disruption and the ways in which this affects the scripting (Goffman 1959) - rather than framing - of a demonstration, allegedly letting those previously seen as spectators *speak* for themselves.

Classic studies of demonstrations of scientific knowledge

To understand demonstrations from a Science and Technology Studies standpoint, we need to return to Shapin and Schaffer's study of the Scientific Revolution to observe the public demonstrations from early modern scientists such as Robert Boyle. In their description of Boyle's air-pump demonstrations, Shapin and Schaffer (1985) show how the decision to conduct these (by now stabilised) experiments to a select public of gentlemen scholars and privileged members of society was done to transform knowledge creation into a public, witnessed event. The public experiment allowed its 'public' to see with their own eyes (Smith 2009). While this may be taken for granted in 21st Century, Western settings, in 17th Century London, knowledge was something previously only generated by philosophers and accepted by audiences without expecting reproducible evidence of that new knowledge. To allow a public to see a demonstration of a new knowledge proposition was extraordinary.

Shapin and Schaffer show how these public demonstrations of new scientific discoveries became institutionalized, as it became common for scientists to demonstrate newfound knowledge in public, albeit controlled settings[6] as a form of knowledge transfer. These public demonstrations of scientific discoveries continued in various forms throughout the Western world until the 20th Century. These demonstrations include Pasteur's public trial of the anthrax vaccine, which has been studied in great detail by Latour (1988). How might we use STS to further understanding the performativity of demonstrations? And is a scientific discovery only as good as its demonstration? Latour seems to think so when he describes Pasteur's work as 'genius' but qualifying that as within 'what might be

[6] The public that comprised these 17th Century audiences were not as representative of the general public that we would expect in the 21st Century. The public were considered able to attend a demonstration such as Boyle's would consist of white men of good socio-economic status.

called the theatre of proof.' It raises the notion that the scientist is not merely a scientist. The scientist also takes on the role of a demonstrator or a performer. They not only make new discoveries, but they do the performative labour involved in demonstrating the new knowledge and enrolling their chosen public in that.

Demonstrations of public safety

This performative notion of the 'theatre of proof' is taken up by social studies of technology researchers examining demonstrations in the 20th Century. Harry Collins (1988) describes the theatre of proof and demonstrations within the context of public demonstrations of controlled technology experiments in the 20th Century. In particular, he describes a televised experiment of a collision between a train and a nuclear flask in order to demonstrate the safety of transporting nuclear materials by rail. Collins writes that the televised nature of the controlled experiment constitutes a 'distanced demonstration', as - due to the nature of televised demonstrations - the audience was only present in a temporal sense, and not in a spatial sense. But does this distance make the demonstration any less capable of enrolling the television public in the proven safety of transporting nuclear materials? Smith (2009) argues that the televised nature of the demonstration doesn't detract from its performativity because it is still 'letting spectators see for themselves'. What these demonstrations of public safety have in common with the public scientific demonstrations mentioned earlier is that they are in fact, controlled replications of the experiments that have resulted in the new discovery or, confirmation of the safety of an activity. How might demonstrations of disruption be different due to the uncontrolled, non-experimental nature of the demonstration? But also, what commonalities might these 'distanced demonstrations' share with digital demonstrations of disruption?

From 'theatre of proof' to 'theatre of use' - IT demonstrations in the 21st century

In the early 21st Century there is a marked shift in the demonstration literature as scholars begin to examine the information technology sector. Both Wally Smith (2009) and Catelijne Coopmans (2011) focus on information technology demonstrations as an economic activity, where the focus is on selling a product to the prospective customer. However, each scholar has a differing theoretical take on these demonstrations. Smith uses Goffman's dramaturgical analogy (1959) along with his work on framing and keying (1974) to describe IT demonstrations as a 'theatre of use', in comparison to Latour's 'theatre of proof'. The purposes of these theatres differ in terms of what is being demonstrated. Latour's theatre of proof exists to persuade the audience of a scientific proposition and its performative transformation of the world while Smith's 'theatre of use' exists to show the audience how they might apply that new knowledge or new product to their everyday, situated practices. In his research into demonstrations of enterprise level software to small to medium size businesses, Smith argues that there are similarities between these demonstrations and the vacuum cleaner demonstrations in Goffman's *Frame Analysis* (1974). Both the audience and the demonstrator know that there is some level of artifice in the demonstration. As Smith describes:

> "Both the salesman and the householder would agree that, in an important sense, he is not *really* cleaning the floor but just showing how somebody *would* do so with his machine. This re-framing brings new meaning and rules of engagement, but the original activity is still relevant for understanding the new one." (Smith, 2009: 453)

Smith connects this to the prior literature of demonstrations by explaining that ‘a *demonstration frame* constructs a presentable copy of the messy private experiment.’ (Ibid.).

Coopmans’ ethnography of a medical imaging software company (2011) largely supports Smith’s observations of IT demonstrations. But she goes a step further by becoming part of a medical imagining company conducting the demonstrations rather than merely observing these demonstrations. This enables her to examine demonstrations from a different viewpoint from previous scholars, who have had more affinity with the audience of the demonstration. Coopmans describes the process of determining *what* is to be demonstrated and almost as importantly, *to whom* it is demonstrated*.* She describes the setting of medical conferences, in which these demonstrations of mammography imaging software occur. These settings differ from those discussed thus far because the audience is quite narrow and must choose to visit the company’s stand in the conference exhibition space and then display enough interest and expertise in the product to warrant a demonstration. Coopmans explains how demonstrations are finely tuned to give enough information to generate interest from potential clients in some instances and then less information to competitor companies in that setting in order to protect intellectual property. In other circumstances, her standpoint as an employee allows her to see when demonstrations are amended to conceal software features that do not yet exist or are not of a standard that the company was happy with. Coopmans helps to show that what isn’t demonstrated is as important as what is *chosen* to be demonstrated. In comparison to Smith’s work on IT demonstrations, Coopmans’ ethnography of a software company describes a situation where the mess doesn't yet exist in order for a presentable copy to be demonstrated to an audience. This challenges our perception of demonstrations as a representation of a concept or a product that is complete or certain.

More recently, academics have been discussing a short history of demonstrations in projects. Researcher danah boyd (2017) describes the 'demo-or-die' ethos of MIT's Media Lab[7] as 'most likely because of Nicholas Negroponte's dismissal of "publish-or-perish" in academia. So the idea was to focus not on writing words but producing artefacts.'[8] Boyd goes on to describe the process of being on a rota to conduct demonstrations of projects to lab visitors, some of whom gave no warning of their visit. This lead to improvised demonstrations, rather than the well-rehearsed ones described in other literature. This challenges Smith's notion that demonstrations are a completely presentable copy of the mess. However, in her article boyd questions the benefits and the epistemology of these demonstrations, which are similar to the purpose of the early scientific demonstrations:

"…as I developed in my career, I realized that "demo-or-die" wasn't really about the demo itself. At the end of the day, the goal wasn't to pitch the demo — it was to help the visitor change their perspective of the world through the lens of the demo. In trying to shift their thinking, we had to invite them to see the world differently. The demo was a prop. Everything about what I do as a researcher is rooted in the goal of using empirical work to help challenge people's assumptions and generate new frames that people can work with. I have to understand where they're coming from, appreciate their perspective, and then strategically engage them to shift their point of view." (Boyd, 2017, LinkedIn article "*How "Demo-or-Die" Helped My Career"*)

[7] Rather than making these observations of her time at the Media Lab in a formal scholarly setting, boyd chose to write this as an article on the professional social media platform LinkedIn. This decision to demonstrate academic process in a non-academic setting is quite an interesting choice.

[8] The temptation to draw parallels between the history on demonstrations and the 'publish or perish' culture in academia while writing this thesis has been great at times. I am glad to have these words coming from someone else, as a sense of confirmation.

For boyd and her colleagues at the Media Lab at the time, the demo-or-die approach has similarities with Latour's description of the 'theatre of proof' in that the demonstrators were trying to encourage their audience 'to see the world differently.' However, the approach is also a theatre of proof of academic labour and productivity; and like Smith's take on IT demonstrations, it was also a 'theatre of use' to help the audience imagine how the new technological advancements could be applicable to their life. But perhaps because this is a first-hand account of conducting a demonstration, boyd describes the roles audiences have in demonstrations, and the need that demonstrators have to account for them and their standpoints in order to enrol them in new knowledge or a new product or practice.

The theatre of failure

How might we read demonstrations that don't seek to demonstrate new knowledge or convince a public of the value of an object or procedure? There are also demonstrations that invoke not a 'theatre of proof' or a 'theatre of use', but a 'theatre of failure.' While there hasn't been much written about this thus far, Francisca Grommé (2015) offers this notion of demonstrating failure in her analysis of the piloting of aggression monitoring technology at a Dutch bus station. The aggression monitors were part of an audio-based system that listened for any noises that could be considered aggressive. When the monitors picked up noise that it perceived as aggressive, it would sound an alarm in the control room of those responsible for the security in and around the station. However, the monitors were too sensitive and control room staff were being alerted to sounds that were not indicative of aggression, and led them to waste time investigating the false alarms. Worse still, staff found that the aggression monitors diverted their attention from watching CCTV monitors. As Grommé discusses, this resulted in an antagonism towards the new system, with staff tinkering with the device in order to quieten or disable it, thus demonstrating to the installers that the experiment had failed. What we learn from Gromme's study is that non-scientists are capable of carrying out demonstrations; and they may not need to be part of a core set of experts to do so.[9]

Keeping in mind this idea of demonstrating failure, how might Smith's idea of a presentable copy of mess be challenged by the phenomenon of these digitally demonstrated disruptions, when we are now witness to the mess itself being demonstrated? In this thesis, I argue that these digitally demonstrated disruptions occur as a form of 'theatre of failure'.

Commonalities of non-digital demonstrations

The demonstrations I have discussed until now have four attributes in common. Firstly, they occur in *public settings* such as lecture theatres, meeting rooms, conferences or, in the case of the safety demonstrations described by Collins, they are simulcast on broadcast media from public settings. Secondly, each of these demonstrations occur within the framework of a 'theatre of proof, 'theatre of use' or, 'theatre of failure'. These concepts assume that the demonstrator's primary concern is to show good working order, concealing the mess and the hard work that has culminated in demonstration. Thirdly, the analysis of these demonstrations - especially those of IT demonstrations - relies on framing as a theoretical standpoint. And lastly, as Smith describes, demonstrations of this variety are a means of 'letting spectators see for themselves.'

[9] One could argue that these publics are experts of their own lived experiences and situated practices. Perhaps that's a helpful way to understand this.

The literature around demonstrations thus far suggests that the attributes of demonstrations in science and technology are stabilised and that we as an audience know what to expect when faced with a demonstration. One of the questions that animate this thesis is whether digital demonstrations of disruption challenge these once stable understandings of demonstrations. To be clear, when discussing the digital demonstrations, I am describing demonstrations made *with* digital technologies and/or which occur *in* digital settings. As discussed, there have been several studies of demonstrations *of* digital products, but as the digital is today also serving as a setting for demonstration, we need to consider the differing ways in which the digital presents both an object and setting of study, and an instrument with which to study. Indeed, I want argue that digital demonstrations are worthy of study because they challenge previously held notions of what a demonstration ought to be and consist of. I argue that digital and social media allows the public audience to be broader, dispersed and unknown or unseen to the demonstrator.

When examining demonstrations in a digital setting, it is noticeable that the spectators are no longer merely able to see for themselves, they are now apparently able to *speak for themselves* if they desire. It follows that the attributes of the digital as a setting for demonstrations, may also affect the scripting of a demonstration. To explore this in more detail, I will move away from the often used analytic framework of framing and call on one of Goffman's other dramaturgical devices of scripting (Goffman 1959) to examine how the digital may reconfigure demonstrations between the public, experts and the broader audience.

Scriptings rather than framings

At first it may seem odd to draw the attention towards the scripting of demonstrations, rather than draw on a seam of literature on framing and the digital which takes into account Smith's work on framing for IT demonstrations (2009) and Tkacz's analysis of framing of Wikipedia editing negotiations (2015). Indeed, Tkacz makes a compelling case for utilising Goffman's frame analysis in STS research, remarking:

> "…the question of organization remains central. In ways that anticipate methodological developments in actor-network theory (ANT), Goffman's method is to begin with the situation and pose the question of organization, or indeed structure, second - but it is posed nonetheless. It is an attempt to pose the question of structure without bringing a structural answer." (Tkacz 2015 p73)

But when shifting attention to demonstrations of disruption there is a problem with framing that is not encountered in the case of demonstrations of knowledge. In the theatre of proof or the theatre of use the audience witnesses a simulacrum of a successful experiment. However, in a digital demonstration of disruption, the audience or addressee is often presented with the situated action of the problem that is currently occurring or has previously occurred. This reconfigures the sequence of demonstration along with the scripts of each actor to an extent as we may not have the expert or the 'core-set' (Collins 1988) of experts with specialist knowledge making the demonstration. Instead, the disrupted party may end up making a demonstration because while they are *not* the experts in resolving a disruption, they *are* the experiential experts in the disruption that they face.

While the case studies in this thesis could be analysed using Goffman's work on framing and the literature and empirical work that draws on it, but to examine the framing of digital demonstrations would be to leapfrog over some reconfigurations of demonstrations in a digital age that are worth examining.

This standpoint of paying attention to the experiential experts is similar to Akrich's assertion about scripts and de-scription when dealing with designing objects. Akrich (1992) argues that when observing an innovation, 'we have to go back and forth continually between the designer and the user, between the designer's projected user and the real user, between *the world inscribed in the object* and *the world described by its displacement.*' (pp. 208-9, emphasis original) This concept is relevant in digital settings, because we are observing how social media are available to the 'real user' to demonstrate disruption. In particular, I focus on how the digital may reconfigure the scripts of demonstrations.

Scripting demonstrations of disruption

In taking on a dramaturgical view of demonstrations, it is helpful to consider the scripting of the demonstration. Examining demonstrations of disruption through Goffman's performances with teams (1959) - where two or more actors with different roles perform together towards a common goal - helps us to understand how the digital may reconfigure demonstrations.

Goffman describes the idea of teams and scripting in *The Presentation of Self in Everyday Life*:

> 'Whether the members of a team stage similar individual performances or stage dissimilar performances which fit together as a whole, an emergent team impression arises which can conveniently be treated as a fact in its own right, as a third level of fact located between the individual performance on one hand and the total interaction of the participants on the other.' (Goffman, 1959: 85)

How might a team be encountered in digital demonstrations of disruption? In my field studies of disruption, I also observed the emergence of a team. We see both the core-set (or addressee) and the lay person (the audience) experiencing the disruption come together as a team in order to problematise and enrol others in the problem. A layperson may first perform the role of someone who has experienced a disruption and then demonstrate that the failure is worthy of attention from the core-set. I present instances of this in Chapters 4 and 6 when I discuss commuters asking TfL for a status update on a tube line and a member of the public complaining about the selfie stick being used in a certain venue.

In this situation, the core-set are audience members who are able to respond to the performance. At this stage, we should consider them to be the demonstrator and the addressee. With the demonstrator taking quite an active role and the addressee taking on a passive role. This passivity doesn't mean to say that the addressee is diminished in agency. Rather, their agency lies in the fact that they have the means to resolve the disruption and, they need to be convinced by the demonstration.[10] Goffman describes this as *dramatic dominance* (1959, 105). Goffman uses the example of a funeral setting where the deceased holds dramatic dominance - even though they are not alive - because the activity of the attendees is centred around mourning their passing. Goffman also describes the concept of *directive dominance,* which refers to the actor who may not be dramatically dominant, but instructs the other actors in the activity. In his analogy of the funeral setting, the undertaker is considered to have

[10] Similarly, in ethnomethodology this is described as mutual accountability.

directive dominance because he has the most experience in this setting and can lead the attendees through the mourning process.

Connecting the dramatic and the digital

But how can these concepts of dramatic and directive dominance be used to understand digital demonstrations of disruption? While the demonstrator of disruption may have dramatic dominance in a team performance, especially at the beginning, this does not necessarily represent the power or agency they have in the situation at hand. Indeed, their dramatic dominance is as a direct result of being witness to the disruption - a delayed train, a hacked computer or a selfie stick. It has forced itself upon them (Graham and Thrift 2007, Verbeek 2004). They now need to force the disruption upon someone with expertise - or directive dominance - in order that they might be able to carry out the task at hand.

However, the uncertain or non-specific nature of the digital gives us an edge case that challenge this, requiring us to be flexible in our analytic approach to teams and demonstrators and audiences. For example, in the Transport for London chapter, we encounter a team that could also be reconfigured with a chatbot or a direct messaging service and a commuter. No longer are the team and the ensuing script purely human; so how might we understand demonstrations that occur between humans and non-humans?

While I am keen not to take the dramaturgical analogy too far, when proof of failure has been achieved we begin to see the audience and the actors become a team - not too dissimilar to an improvisational theatre troupe - where the layperson declares the failure to be a problem and the core-set are forced to respond on the fly to these problems. As we will see in the research chapters, framing demonstrations of disruption as configuring a ‘theatre of failure’ allows for a demonstration to take place as both the demonstrator and the audience work through the disruption in a discursive way.

In the non-digital theatre of failure that Goffman describes, the team is small. The layperson and the core-set are in dialogue, often with a small audience as this dialogue occurs over the phone or by email or in person at a help desk. The layperson is an expert in the failure they are experiencing and the core-set representative is an expert in its ideal state and may have experience of resolving previous failures. Through this process of negotiation, the layperson and the core-set representative arrive at the cause of the failure in order to arrive at a course of action ending in a solution. In some instances, the core-set representative may need to co-opt another member of the core-set with more expertise in this certain type of failure to join the team, as it were. An example of this that we will see in the Transport for London research is where social media customer service agents specialise in responding to certain commuter problems, such as problems with a particular payment method. In situations where commuters are having payment related problems, these experts are called in to take over in responding to the demonstration.

Demonstrations and the digital

Goffman emphasises the importance of setting when describing these team performances. Returning to the description of dramatic and directive dominance, he uses the funeral home example to illustrate how ‘both the bereaved team and the establishment’s team, will be arranged so as to express their feelings for the deceased.' (1959: 105) While the bereaved team perform their grieving, the funeral staff's team perform sympathy and emotional stability towards the bereaved team. This team and their performance are constrained to the setting of the grieving process within the funeral home. At the end of the grieving process and outside of the walls of the funeral home, the teams are disbanded. Some of these people may meet again in another location and in a vastly different context - such as bumping into one another in the supermarket - and they will not form those same teams from the funeral because they are not in the setting that encourages them to take on these roles.

In examining digital demonstrations of disruption, we need to consider the possibility of multiple settings, along with the specificities that each of these settings bring. The setting of the demonstration dictates whether it will be a distanced demonstration (Collins 1988) or an in-situ demonstration. Take a public transport delay for example; one could demonstrate the disruption in many settings. A member of the public could demonstrate the delay in-situ by asking a member of station staff about it while using nearby objects such as a departure board and the absence of the train as proof. However, there may not be station staff around to ask, so a commuter could demonstrate the delay in a digital setting via Twitter to Transport for London's customer service agents. Although these demonstrations occur in different settings, they elicit a similar outcome. However, while commuters are well versed in asking about disruptions within in-situ settings, how might they have learned that they are able to demonstrate disruptions and gain responses within digital settings?

Audiences of digital demonstrations

The ramifications of this for the study of digital demonstrations of disruption include the difficulty of pinpointing exactly where the demonstration occurs, and precisely who is party to it. Returning to our 17th century scientific demonstrations, we know exactly who is demonstrating and to whom: scientists are the ones who discover new knowledge and are therefore fixed in the role of demonstrator, while the public who seek new knowledge comprise the audience. In comparison, the actors in digital demonstrations of disruption are not as fixed in their roles, and likewise, the setting is also not as fixed. In theory, a disrupted member of the public can just as easily demonstrate a disruption in a digital setting as an expert who is pre-emptively demonstrating a disruption to a public. Anyone with the economic means and internet connectivity to take part in the digital setting - that is, someone with a digital device and internet access - could be a modern-day Hobbes, Boyle or Pasteur, creating an account of their disruptive experience and sharing it with others via social media. Similarly, anyone who has the motivation to choose to take part in social media can act as the public. However, in practice, this seemingly level playing field of digitally demonstrating disruption is weighted by social media platforms themselves and their algorithmic displays of content. I propose that there are two audiences for digital demonstrations of disruption. The first is usually a 'core set' of actors who have the agency (or directive dominance to borrow from Goffman) to resolve the disruption; this could be a corporation, an institution or a high profile person. The second audience is comprised of digital or social media users who see the demonstration via the algorithmic attributes of the settings. In simpler terms, a social media user may see a commuter demonstration to TfL on Facebook because they are friends with the commuter and platform's algorithm has determined that this user would be interested in seeing this post[11]. This second audience is a *collateral audience* of sorts. But this collateral audience is vital to the dramatic dominance of the demonstrator. Without this audience, the core-set being demonstrated to has no incentive to demonstrate their responsibility or accountability. But the presence of this audience compels the core-set to demonstrate their competence by providing an adequate response (Garfinkel 1967/1991). These two audiences place us in a position where the disruption is demonstrated to someone of agency but for all the world to witness their response to the demonstration, causing a dynamic whereby the response is a demonstration of their ability to use their agency in a socially accepted way. This dual demonstration dynamic forces the addressee to become accountable to the collateral audience, lest the addressee becomes diminished in the eyes of the residual public.

A multiple 'digital as…' approach amongst critical digital standpoints

My engagement with historical and sociological literature on demonstrations raises the question of how we should understand demonstrations undertaken within digital settings. To address this, I will discuss concepts of the digital in order to specify the role it plays in my project, as both an object and a setting that has the potential to reconfigure the role of scripts and actors within a demonstration, but also as an instrument for studying the phenomenon. To account for the digital as an element in demonstrations of disruption, I adopt the post-ANT standpoint of multiple ontologies (Mol 2002) alongside a digital sociological (Marres 2017) standpoint. This allows me to recognize the relative instability of 'the digital' as an empirical category: it may present itself as both or

[11] The user probably isn't interested in seeing this post unless they share a similar commute to their Facebook friend. But due to the algorithms of social media platforms being opaque, we don't know precisely how a demonstration such as this would be elevated within their feed.

either a setting in which social life occurs, an object of social research, and/or an instrument with which to conduct research.

The digital has been conceptualized in many ways in recent decades (Woolgar 2002, Hine 2000, Miller and Slater 2001, Suchman 1987/2012, Savage and Burrows 2007). While critical and theoretical approaches to the digital highlight core features of how the digital is present and operative in social settings, I will propose that definitional approaches to elucidating the digital are not the most helpful when researching digital demonstrations of disruption. I will then describe an alternative, empirical approach to the digital that recognizes multiple ontologies – such as the digital as setting, assemblage or research instrument - and how this can be fruitful when examining digital demonstrations of disruption. I will consider the practicalities of this approach in Chapter Three when discussing methods and methodology.

At its simplest level, the digital has been defined as data depicted in binary form - zeroes and ones - that allows for it to be calculated and manipulated with machines, primarily computers (Galloway 2004, 2016). While at a base level, this is an accurate definition of the digital, my focus in this section is on how other scholars on the borders of STS and (new) media studies conceptualise the digital in order to study it.

For these purposes, the digital could be understood as an aggregation of large volumes of literature or data than can tell about society rather than the technical, computational definition of the digital described above. This definition and understanding of the digital has the potential to reshape how social researchers go about their craft, as described by Venturini and Latour (2010) below:

“… the social sciences have never had methods to reconnect micro and macro and show how global phenomena are built by the assemblage of local interactions. Digital technology promises to revolutionize this situation, providing the social sciences the possibility of following each thread of interaction and showing how social life is woven together by their assemblage.” Venturini and Latour (2010)

While the promise of revolutionised research with the micro and macro reconnected is appealing, I would like to argue that although these visualisations are fruitful inscriptions of interactions, they help us understand the topology of an assemblage but do very little to help us understand how actors came to be in this topology and how they understand their place within it. Put simply: the promise that Venturini and Latour put forward is still too focused on global phenomena and not enough on the situational. It is phenomena-first, not assemblage-first. This is a problematic premise that carries through a number of other conceptualisations of the digital specific to media studies

Richard Rogers (2013) proposes that natively digital data - that is data that is created within digital settings by digital actors - can tell us about society. He develops this argument by detailing the empirical affordances of the digital objects such as hyperlinks, showing how they can depict connections between actors around issues and politics. As such, this approach focuses on the specificities of the digital objects and the networks they can reveal. This results in research via methods such as issue mapping, associational profiling and network visualisation. Although there are attempts at using this approach within Chapter Six, it is largely incompatible with the research question at hand for a few reasons.

Rogers' approach is incompatible because my research question centres on mundane disruption, which is not easily rendered traceable as an issue. Mundane disruptions are ephemeral, fleeting, and negotiated relatively easily whereas issues are sustained and often develop over far longer periods of time.

Similarly, digital demonstrations of mundane disruption are likely incompatible with Rogers' approach because it concerns itself with networks that focus around political issues or events (Rogers 2004). Digital demonstrations of disruption are more concerned with situated practices that arise from enrolling actors into disruptions via the digital. Simply, digital demonstrations of disruption are concerned with what is being communicated between actors *and what happens next,* rather than who is connected to whom in a particular issue.

Rogers' approach is also incompatible because there is often a singular understanding of digital objects such as a hyperlink, a 'like' or a tweet. Rogers and others (Gerlitz and Helmond 2013, Rieder 2013) create historiographies of these objects by comparing their behaviour over time. This suggests that these objects are relatively stable with a common understanding and use amongst users until those responsible for the design of platforms make alterations. As I will describe in the Chapter Four, digital demonstrations of disruptions do not assume that a digital object such as a tweet behaves continuously in a uniform way to all actors, rather it changes in meaning as actors encounter them and apply their own situated needs to them.

The theoretical approach of digital methods[12] (Rogers 2013) is hampered by natively digital devices and their outputs: networks and visualisations. Chun (2016) picks up on the prevalence of the use of networks in media studies and critical digital studies. She critiques the use of the digital and network analysis in the context of neoliberalism to attempt to simplify and render visible the effects of globalisation. "… 'Networks' render the seemingly complex and unmappable world of globalization trackable and comprehensible by transforming time-based interactions and intervals into spatial representations." (Chun 2016, p2) Additionally, Chun asserts that attempts to understand the digital through the study and use of networks generate more networks, "the examination of networks leads to the formation of ever more networks, making it difficult to separate network analyses from networks themselves." (Chun 2016, p 25)

While I agree with Chun's critique of networks - especially their use to attempt to visualise and simplify neoliberalism, globalisation and their respective entangled actors - my critique of networks in understanding and researching the digital specifically addresses its incompatibility with studying digital demonstrations of disruption. Similar to the critique of Rogers' digital approach with a focus on networks and visualisations as an output, my research has less to do with mapping nodes and edges, and more to do with *how demonstrations of disruption are enacted in organisational and social settings.*

[12] I further discuss digital methods in comparison to other methods such as ethnography and breaching experiments in Chapter Three.

More specifically, my concern is with how these methods of enrolling others in disruptions are shifting over time with the iteration of the entities that allow actors to demonstrate disruption. Conceptualising the digital with networks that render human actors as nodes greatly reduces the ability to examine their demonstrations and the in-situ work done that is not captured through natively digital data.

However, not all critical approaches to the digital are focused on networks and visualisations.

I am more concerned with how for-profit companies and public organisations build their own infrastructure and processes with their own specificities and expectations of use and how organisations and consumers choose to use these specificities to demonstrate and respond to mundane disruptions. Further, my interest lies in how these specificities iterate or morph over time and how institutions and consumers adapt and use these specificities for purposes that were not explicitly intended by the company. I mobilise this interest by examining demonstrations of mundane disruptions on digital and social media.

Kelty (2012) proposes an approach to the digital that supports this focus on enactments of demonstrations of disruption in organisational or social settings. His comparative work on 20th Century civil rights activism to social media activism describes an imperative to focus not only on the networks of what he describes as “Organised Publics”[13] participating in an issue, but, crucially, on the hierarchies of “Formal Social Enterprises”[14] being addressed. By doing so,

[13] Kelty (2012) describes Organized Publics as having membership that “is informal, temporary, and constituted primarily through attention.” Examples of what this could look like in the empirical work of demonstrations of disruption include London commuters, people concerned about or working in cyber security or, people who are disrupted by selfie sticks.

[14] In comparison to Organized Publics, a ‘Formal Social Enterprise’ is described as “any organization with a formal, especially a state-sanctioned legal and/or

Kelty conceptualises the digital as being more than networks that can be visualised using natively digital data. Rather, he asks us to pay attention to how Organised Publics and Formal Social Enterprises each use digital platforms such as Twitter or YouTube as a participatory resource. In Chapter Four, I describe how TfL as a Formal Social Enterprise goes one step further than using Twitter (the platform) as a digital resource and, works alongside Twitter (the company) to attempt more efficient means of demonstrating disruption to commuters. The approach put forward by Kelty (2012) goes some of the way towards countering the dissatisfaction of Venturini and Latour's (2010) focus on the topology of an issue, rather than *how actors understand their place within the situation*.

So why choose a multiple ontology approach (Marres 2017) to the digital if there are many other critical standpoints available? I argue that when observing digital demonstrations of disruption, there is an imperative to keep Kelty's conceptualisation in mind to consider that the digital manifests in many ways, sometimes concurrently and in ways that are not necessarily visible to all involved. In some instances this is quite simple; the Transport for London example in Chapter Four shows how the digital is both understood as a setting (Twitter) for demonstrating disruption, but that these demonstrations contain digital objects (tweets, favourites, retweets, etc.). Because the focus of the research question is on the situated human (and sometimes non-human) demonstrations of disruption, it is simply unrealistic to expect a network

regulated existence: such as a for-profit or non-profit organization, a foundation, a university research center. Members of the organization are contractually obligated to it" (Kelty 2012). In this empirical work, this could look like organisations such as Transport for London, the National Cyber Security Centre or, venues such as the National Gallery.

visualisation to contribute to the analytic work of understanding how different actors understand and react to digital objects. Similarly, in Chapter Five I describe digital demonstrations of digital assemblages being disrupted in cyber attacks. Digital disruptions are described in digital settings, it helps to delineate by specific which digitals are being dealt with. And, in Chapter Six the ontology of the digital is called into question with the examination of the selfie stick. Can a material object such as a selfie stick be considered digital if its primary intended purpose is to facilitate participation in digital social life? Again, this is a question that may not be helped by a singular understanding of the digital. By taking up an approach of multiple digital ontologies, I am more able to account for moments where the digital manifests itself in many ways within one instance. Crucially, this approach also allows me to observe how each of these notions of the digital influence an overarching understanding of the digital.

Digital as setting

In order to understand how particular settings and scriptings of demonstrations have emerged in a digital context, we must delve into the history of the web, and consider how it has been configured over time and how in turn communications have been reconfigured throughout these changes. In the early 21st century we saw a shift in the architecture of the web from Web 1.0 - that is, a World Wide Web with the limited capabilities to publish information online - towards Web 2.0 which frames the web as software rather than a digital facsimile of print or broadcast publishing. In this move towards the 'web as a platform' (Helmond 2015), the original intention as stated by Tim O'Reilly in 2005 was that the web would become more of a software or computational platform, but the reality was quite different. The practical application of Web 2.0 was ‘the participatory web’ whereby web users were encouraged to produce and consume web content and, interact with one another in more complex ways than were available in Web 1.0.

We are now in the midst of Web 3.0, which incorporates developments such as the Internet of Things (IoT) and chat bots; nonhuman actors that can respond to human generated data as well as generate their own. Within Web 3.0, we see the Internet of Things as an environment where Richard Rogers’ (2009) notion of ‘natively digital’ data comes to fruition in internet-enabled objects such as smart cars or fitness trackers, which generate and communicate their own data. I will describe the Internet of Things in further detail in Chapter 5. Chat bots will be discussed in further detail in the Transport for London chapter as my field research coincided with the public transport authority’s introduction of chat bots as part of their social media customer service offerings.

It is important to note that each iteration of the web does not replace the one that has gone before it. Rather, Web 2.0 builds on Web 1.0 and introduces a number of new entities and architectures, which in turn bring new configurations for users, data and communication. For example, Web 1.0 entities such as websites and message boards co-exist with Web 2.0 social media platforms such as Facebook or Twitter, which in turn can integrate data from Web 3.0 Internet of Things objects such as fitness trackers. But, how is this the genealogy of the web specifically relevant to understanding demonstrations of disruption?

If the aim is to compare the technical architecture of the digital to the settings in which demonstrations discussed earlier in this chapter occurred, the difference that Web 1.0 makes is rather simple. Teams, in the sense that I defined them above, are difficult to assemble to overcome disruption, as an actor is only allowed to leave a review or a comment on a website such as Amazon and expect no follow up. Similarly, on a Web 1.0 website, the web author could only receive comments for the entire website via the guestbook, rather than have a comments section on each and every page within their website. This meant that there was an added level of asynchronicity and unidirectionality to a demonstration. This leaves us with both the demonstration being distanced along with the response due to both physical geography and digital architecture. The end result is that within a Web 1.0 only setting, demonstrations of mundane disruptions still occur in private, via email or, are taken offline via telephone or face-to-face conversations.

With the introduction of Web 2.0, we have personal websites co-existing alongside personal blogs or social media profiles. The capabilities of blogs and social media meant that actors were able to interact with the demonstration in the digital location it had been placed. Additionally, as Anne Helmond (2015) discusses, Web 2.0 brings about the ‘platformisation of the web’ where social media ‘like’ or ‘share’ buttons embedded within web content such as news articles mean that Facebook, Twitter and the like can occur outside of their own ‘walled gardens’ (2015, p.7). This also means that the public and the addressee are now made more visible to an audience and the audience can grow as the demonstration becomes ‘viral’. Additionally, Web 2.0 has seen the introduction of the API (the Application Programming Interface), a software that allows those with enough technical expertise to create a program that can request and gather data from a social media platform and allow it to be repurposed in other digital spaces. For example, journalists from a news website could use the Twitter API to gather tweets about a particularly disruptive event such as a strike or natural disaster to embed within a news story about the event by using a programme such as Storify.[15] The Twitter user who has had their content appropriated and sometimes recontextualised or decontextualised is often unaware that this has occurred. Not only has the setting of the demonstration of disruption become multiplied (to include both Twitter and the news website) but it has greatly expanded the anonymous audience beyond the audience intended by the original poster. How might an understanding of some of the structural specificities of Web 2.0 challenge some of the non-digital ideas of scripting in demonstrations?

At first glance, Goffman's work around performance and presentation of self (1959) seems to dovetail with social media. It becomes all too easy to compare a social media platform to a stage where all users are actors and all actors are one another's audience. We don't see one another's backstage as we perform our best self on the digital stage. One could spend their entire digital life on the stage or, they could choose to spend it in the audience as a lurker. Or a more likely scenario would be that they could seamlessly move between audience and stage without much reflexivity at all. But as described in the demonstration portion of this chapter, the scripting of the performance becomes lost in

[15] This is also seen in Buzzfeed (and similar) articles where the journalist embeds a series of Instagram images around a theme that usually forms a numbered list. However, unlike using an API to pull across the data from its original source, the journalist uses piece of HTML embed code to display the image when the article loads.

translation when we start talking about setting and the digital. When referring to a non-digital environment, Goffman's talk of setting is relatively straightforward:

> "…There is the 'setting', involving furniture, decor, physical layout, and other background items which supply the scenery and stage props for the spate of human action played out before, within, or upon it. A setting tends to stay put, geographically speaking, so that those who would use a particular setting as part of their performance cannot begin their act until they have brought themselves to the appropriate place and must terminate their performance when they leave it." (Goffman, 1959: 33)

However, Goffman's notion of setting is similar and yet incongruous to the digital setting in that the 'furniture' - that is the graphical layout of the digital - is uniform within a platform. To use Facebook as an example - the news feed is the physical layout and the articles, posts and photos are the furniture, decor and props for the human action to be enacted through. The setting stays put, yet not in a geographic sense - at least not in a physical geography. An actor still has to go to the 'Facebook setting' to take part in discussion with other users there, however, one doesn't go to a Facebook setting to take part in a particular activity. The setting is far more general than other settings that allow a variety of actions to take place. Facebook (and other social media platforms), resemble more public places such as cafes and parks, where the purpose is multivalent and partly dependent on the configuration of people and objects available to hand.

Adding a Web 3.0 layer allows non-human actors the opportunity to demonstrate disruption. Dodge and Kitchin (2009) allude to this in their discussion around 'codejects' and 'logjects' as non-human mundane actors such as kitchen and laundry whitegoods that can communicate disruption or their need for human attention through a series of audio or visual cues. This is not too dissimilar to Suchman's (1987/2007) work with photocopiers, where the machines demonstrate their disruption to printing by way of displaying error messages, which the human then has to decipher in order to rectify the problem. These object-based demonstrations are helpful to keep in mind, as they often form the initial demonstration that makes the human actor involve a ‘core-set’ such as the manufacturer in a form of repair activity. However, in the case of Suchman’s example, we see problems arise where the humans struggle to understand and act upon the error messages being displayed.

This literature foreshadows discussions around the Internet of Things especially around smart household goods such as lighting, heating or security that can now be controlled via smartphone apps. Similarly, these objects can communicate to householders via a smartphone app to communicate their current status or any disruptions. In the Transport for London research we will see the use of chatbots on Twitter as non-human actors that can respond to and demonstrate tube network disruptions in a rudimentary way.

Although there is much discussion about the Internet of Things and Web 3.0 reconfiguring our digital practices, how then could we account for a rudimentary object such as the selfie stick, reconfiguring situated practices of creating digital images? Could the digital extend to objects implicated in digital practices?

Although this thesis explores how disruptions are demonstrated in each of these iterations of the digital as a setting, it is important to note, that this is not an exhaustive description, especially in regard to Web 3.0, which is still being stabilised. Rather than considering this as a hindrance to researching digital demonstrations of disruption, I have welcomed the opportunity to describe these new entities in the digital setting as they are being introduced and reconfiguring demonstrations. It also allows space for others to pick up on the work this thesis has produced to seek new knowledge about how the digital might reconfigure public demonstrations.

Others actors in digital demonstrations of disruption and complications for settings

Upon examination of the technical architecture of Web 2.0 and Web 3.0 entities, it becomes apparent that there is a silent audience of the demonstration. Every demonstration happens on a digital piece of real estate. And that real estate is owned by a company that imposes its own specificities in that space. There is the architecture that enables the public and the addressee to interact with one another, form a team and engage in rectifying the disruption. The architecture also allows the audience to see the demonstration, and participate by commenting, sharing or liking. But propping up the architecture is an infrastructure laid out by the owners that facilitate the demonstrations, the comments and, the collaboration. In doing so, corporations such as Facebook and Twitter have access to the data created by their users and can use this in recursive ways (Kelty 2005), primarily for advertising opportunities, but also to highlight trending topics or behavioural trends to a broader audience. While the public and the addressee demonstrate and reconcile disruption, those that provide the digital setting for this to happen also have one eye on the demonstration in order to derive commercial value from the data it generates. This gives the social media platform itself an added level of power and agency although they are silent in the demonstration.

This additional technical setting and audience gives another dimension to digital demonstrations in comparison to their non-digital counterparts. This is reminiscent of Ezrahi's (1990: 41-43) example of NASA's construction of the Saturn 5 spacecraft, which although it was owned by the publicly funded NASA, it was comprised of many components, made by many private companies. In using this example, Ezrahi highlights the fact that public actions are rarely completely public, they rely upon private enterprise to achieve the outcome. In a sense, this is similar to what occurs when we demonstrate disruption in public digital environments. Rather than demonstrating our disruption to an institution or organization's own private hotline or business address, we outsource the setting of a demonstration to a private firm operating in the public sphere hosted by another private company[16]. On the other side of that demonstration, organisations such as Transport for London choose to outsource the collation and 'dashboardisation' of these demonstrations to a private company, which we will read more about in the coming research chapters. Ezrahi speaks specifically to the liberal-democratic polity and public/private partnerships in order to have 'discrete actions fit into coherent programs of collective action,' (1990: 44). However, we can transpose this on to how we utilize the private companies' setting and infrastructure to carry out our demonstrations due to an assumption of convenience (a view that practically every company or institution has a presence on social media and is responsive). This utilisation of a private companies' setting produces an assumption that accountability can be achieved due to the fact that the demonstration is being staged in a digital location that has a high level of publicity attached to it. The public selects the social media

[16] But do we really have a choice? Is there an option for a digital setting to demonstrate a disruption that *isn't* owned by a private firm, and that has a critical mass to constitute an audience? While Sir Tim Berners-Lee invented the World Wide Web with the intention of including everyone without corporate ownership, this is not the reality of the digital settings we exist within.

platform as the setting because they wish to demonstrate their disruption in the setting where there is the highest likelihood of repair, problem solving or, a large audience. The addressees choose to have a presence on a social media platform because in addition to being seen by a large audience, they also wish to be seen to be accountable, responsive and attentive to that large audience.

But in some situations, there are additional corporate actors within the digital setting. As will be discussed further in the Transport for London chapter, there are companies that deal in social media management or ‘customer care’ by creating a digital setting that collates social media data and re-presents it in a format that makes it easier for respondents to see outstanding demonstrations that require a response. This means that we have a situation where a commuter could demonstrate their disruption in one setting via the Twitter app on their smartphone, while the respondent will see that demonstration via a dashboard-style interface within their social media management system. What are the implications for the dramaturgy of demonstrations now that the demonstrator and the respondent are in differently configured settings?

Trolls and spammers: unintended actors in digital demonstrations

In discussing digital reconfigurations of demonstrations, I have focussed on the actors who earnestly take part in the demonstration - those being disrupted and those responding to the disruption - but much like corporate actors that do not immediately come to mind, there are other actors who may also participate. These may take the form of trolls, spammers or spam bots. To be sure, such actors have been in digital settings in some way, shape or form in each of the web’s iterations. In Web 1.0, there was recorded activity of trolls in forums or boards (Donath 1999, Bartlett 2015), derailing conversations or creating havoc among users. In Web 2.0 we see various rogue audience members such as spammers in the comment sections of blog posts, trolls in the comment sections of news articles and spam bots on Twitter feeds. This is due to the specificities of the platforms offering more opportunities for these kinds of interventions, along with codes that allow spam bots to be created. As I will discuss in the selfie stick chapter, spam bots cause interesting interference when attempting to use the digital as a research instrument. This is because social media platforms that make use of hashtags as a form of indexing or indication of a trending topic attract the attention of spam bots. As a result, when using digital research tools such as TCAT[17] to collect or scrape social media data, a percentage of the data returned from the query will consist of Tweets unrelated to the research question.

Foucauldian approach - the digital as a device

Digital technologies have the potential to control, precisely by its very nature of being a space designed by others. Franklin (2004: 53-55) describes how Foucault (1979) asserts the distortion of discipline into control in 17th and 18th Century France through the imposition of hierarchies, ranks, drills and record keeping.

The devices that Foucault describes to impose discipline and control can similarly be seen in digital technologies such as social media platforms - the fields necessary to fill in to create a complete profile, the metadata collected in

[17] TCAT stands for Twitter Capture and Analysis Tool. It is a tool developed by the digital methods initiative that allows researchers to scrape Twitter for tweets including a certain hashtag and conduct different forms of analysis and visualization.

the process of demonstrating a disruption - compile an archive of data about the individual. The ways in which that archive is used is of interest when considering the Foucauldian aspects of the digital and control.

Sociology scholars apply Foucault's definition and description of devices in research of digital settings and assemblages. Beer and Burrows (2013) describe digital data as a form of record keeping that can be used as a form of control. Similarly, Gerlitz and Lury's (2014) work with numbers, orderings and values to explore further the potential for control and influence that actions such as 'likes', 'favourites' and Klout score carry within the digital setting.

Franklin (2004: 10) describes the use of technology as being either *holistic* or *prescriptive*. In referring to holistic technology, she refers to activities that resemble craft that do not require a uniform mode of production; she uses artisans such as potters and weavers who make decisions about the shape and composition of their creation as the activity progresses. In comparison, *prescriptive technology* is reminiscent of production lines whereby the process is controlled in order that each item produced is identical to the others. Franklin does not limit this idea of prescriptive technology to mass production; rather she notes its impact on bureaucracy:

> "Prescriptive technologies are not restricted to materials production. They are used in administrative and economic activities and in many aspects of governance… While we should not forget that these prescriptive technologies are often exceedingly effective and efficient, they come with an enormous social mortgage. The mortgage means that we live in a culture of compliance, that we are ever more conditioned to accept orthodoxy as normal, and to accept that there is only one way of doing 'it.'" (Franklin, 2004: 17)

The digital technologies we encounter in these demonstrations of disruption straddle both the holistic and the prescriptive. It is prescriptive in that social media platforms and the ways of interacting through them are bound in code - there are fields to fill out in order to demonstrate the disruption. But within those fields there is the ability to be creative, there is no prescription for the content of the text (apart from a character limit imposed by the underlying code base) nor is there a prescription for what is contained within an image. This allows the person demonstrating disruption a degree of freedom within the form and function of the platform. This places the analyst in a position where the constraints and uniformity of the specificities of the digital must be taken into account. But conversely the analyst must understand the practice within these platforms and how users work within and subvert the prescriptive nature of the digital setting they find themselves within.

Within STS there are similar discussions around prescriptive technology. Woolgar (1990) describes this concept as ‘configuring the user’, whereby the technology itself trains the human actor to use the object or device in a certain way. Woolgar describes this in regard to people learning how to use a certain piece of software while other scholars such as Grimes (2015) describe how children subvert prescribed modes of use on commercial online game worlds often linked with toys or television programmes. How might we see the digital as framing the demonstrations encountered in the research chapters? Similarly, might we witness instances where actors subvert these prescriptions?

The digital, inscription devices and social data

As discussed earlier in the chapter, Beer and Burrows’ (2013) work on the social life of data, social media provides a setting for us to enact social life in a public, digital place. However, one of the effects of this activity is that every keystroke, every like, and interaction with another user is placed in an archive. Similarly, Ruppert, Law and Savage (2013) describe the digital - and social media in particular - as an apparatus that organises and produces data on social networks and generates records on user activities and movements. Based on this description, might we understand social media as a form of inscription device (Latour and Woolgar 1986, Michael 2016, Akrich 1992)? This can take the form of surveillance on a large scale such as that done by the US NSA; or it could take the form of targeted advertising on websites or social media based on what we may have 'liked' or 'searched for'[18]. In the case of our demonstrations of disruption, selected personal details of the person making the demonstration of disruption is easily accessible to the addressee, depending on how the user's privacy settings have been configured. This allows the addressee to use that data to understand how best to placate the disruption at hand.

As Beer and Burrows have said:

> "Indeed, it could be argued that participatory web cultures are defined by the consumption of the mundane. On the one hand, we have people willing to communicate (selected) aspects of their private lives in the public domain; on the other, we also find that these mundane details are being consumed by other users." (Beer and Burrows, 2010)

These other users tend to be the addressees themselves who utilize the social media platforms in order to better understand their public. However, social media platforms such as Facebook, Twitter and Google use these data archives produced by their users in order to help businesses better understand their

[18] Anne Helmond (2015) describes this in further detail when discussing the 'platformisation of web', where social interactions such as the 'like button' from Facebook are embedded within an online news article, thus extending the reach of Facebook beyond its website or its smartphone application.

customers, place more effective advertisements and find similar users to their existing customers to promote their goods and services (Facebook, 2016)

Beer and Burrows (2013) discuss this in further detail with regard to the recursive use of relationship status data changes on Facebook at certain times of the year. In recent years, there have also been concerns about the socio-political ramifications of this arrangement, especially with discussions around filter bubbles in political campaigns.[19]

This use of data allows personal data to be commoditised, so that institutions may control individuals based on their attributes. To take this further, I refer to Gerlitz and Lury's critique of social media ranking services such as Klout, which utilize algorithms to give a person a score out of 100 that represents the amount and value of activity on their various social media accounts in addition to how much attention and feedback they have received in return. This process of ranking and enumerating users insinuates that not all digital demonstrations are equal in persuasion because users do not carry the same amount of agency or 'influence'. Gerlitz and Lury touch on this,

> '…While Klout provides the individual user with the basis for a sense of ownership of a Score and even if incentives to connect with others, thus *including* the individual in its participative metric, it does not do so on the basis of identification or belonging. Rather, it re-presents the inclusion in social media (the presentation of data-points) to individual users in terms that are highly compatible with the market as represented by third parties.' (Gerlitz and Lury, 2014: 184)

Although Gerlitz and Lury reflect on Klout as a 'measure of performance', and how it encourages reflexive social media practices for users, they have not

[19] This sentence could open up an entire thesis in and of itself, looking at filter bubbles, echo chambers and impact of digital settings on political campaigns in recent years within the US and UK. Thankfully, that task is not mine, but its relevance is worth mentioning as another example of an aspect of everyday social life reconfigured by the digital.

reflected so much on how it changes the way addressees respond to demonstrations of disruption. Klout has a sister company called Lithium which provides a ’social media listening and response tool’ to companies as a form of customer service management tool (Lithium, 2016). This tool incorporates Klout scores and other social media data about the user in order that the customer service representative might be able to triage responses to customers according to their Klout score, that is, their perceived digital agency.

It is problematic because the algorithm that calculates a Klout score is black boxed due to its commercial nature. If a user wants to improve their Klout score to gain an improved response to their digital demonstration of disruption, they must then participate more on social media platforms, thus relinquishing more data to corporate entities.

But do Klout scores and other similar ranking and user valuation schemes have any clout with respondents when it comes to mundane demonstrations of disruption? I will explore this question in more detail in the Transport for London research when we meet staff tasked with responding to commuter demonstration of disruption.

In the final section of this chapter, I will examine literature around disruption in order to get a better understanding of what is being demonstrated.

Mundane disruption as a catalyst for problematisation and enrolment.

How might focusing on mundane disruptions help us understand the increase in digital demonstrations? The answer to this lies in the subject matter of each of these reconfigured demonstrations occurring in the digital. Both Science and Technology Studies and ethnomethodology contribute to explorations of disruption in everyday life. In particular, I will focus on Susan Leigh Star (1999) and her ethnography of infrastructure to show what disruptions tell us about breakdown or failure and what we might expect to see demonstrated.

How can infrastructure help us observe disruption?

Infrastructure studies is an area of Science and Technology Studies that can help to better understand disruption in a practical context. Within this thesis we encounter non-human actors such as public transport and online security systems that are infrastructural to human actors and their situated practices. Star (1999) describes disruption of infrastructure as one of the ways in which we can better understand our relationship to it. Further, infrastructure tends to be ‘invisible’ or unnoticed until it no longer works the way we expect it to. It is in its failure that we better understand our expectations of and reliance on the network of non-human objects that support our mundane, everyday practices. And crucially, when these disruptions are demonstrated, we gain an insight into how an object or device is expected to work. As Star explains,

> ’The normally invisible quality of working infrastructure becomes visible when it breaks: the server is down, the bridge washes out, there is a power blackout. Even when there are back-up mechanisms or procedures, their existence further highlights the now-visible infrastructure.” (Star, 1999: 382)

Star’s description of infrastructure becoming visible upon breakdown sits alongside Graham and Thrift’s use of Heidegger’s ‘notion of the world as ready-to-hand,’ whereby ‘human beings do not focus on a tool or a piece of equipment but on the work in which they have become engaged.’ (Graham and Thrift, 2007: 2-3). When we find ourselves unable to carry out the task, ‘the tool suddenly forces itself upon us' (Verbeek, 2004: 79) and we must overcome its inadequacies or its broken state in order to carry on. Heidegger (1996) speaks of objects being 'objectively present' when they are the cause of disruption because they can no longer be used but they still demand our attention until we return to a situation of stasis. Graham and Thrift (2007) use the example of a frozen computer screen impeding the writer's ability to write until the problem has been rectified to clarify this definition.

In each of my empirical studies, we will see 'the tool suddenly forc[ing] itself upon us', albeit in different circumstances, to varying effects. In the chapter about TfL, we will see the tube network forcing itself upon commuters through breakdown, maintenance and strike action. In the cyber security chapter we will see tools such as passwords and security practices force themselves upon us so that we pay attention to what is at stake for those who do not adhere to best practice. And we will also observe how the selfie stick is a positive disruption for mobile photographers as a handy innovation to their image creation practices or how it is forced upon bystanders as an annoyance. We will also observe how the demonstrations of the respective disruptions act as a form of problematisation. The case studies give insight into how disruptions are responded to through being demonstrated and negotiated in digital settings.

But Star's description of disruption doesn't just lie with the concept that infrastructure is revealed upon breakdown. Many of Star's descriptions of the properties of infrastructure (1999: 380-382) help us understand what else is revealed as a result of disruption. Of particular interest are the properties of "*embeddedness, transparency, learned as part of membership, built on an* *installed base and, fixed in modular increments*". But how do these properties directly relate to the question of how infrastructural disruptions are demonstrated in the digital? This becomes clearer by examining each of Star's properties mentioned above with reference to the case studies we will encounter in the following chapters.

Star refers to infrastructure's *embeddedness*, the fact that infrastructure never stands alone, rather it makes up part of systems and social arrangements. Taking Transport for London's network as an example, the infrastructure - the trains, the tracks, the stations - are all part of the socio-technical arrangement of commuting. As we will see within the case studies, the disruption of the London Underground network makes visible the other infrastructure elements available to commuters. Digital demonstrations of disruption that originate from TfL staff, often encourage commuters to use less utilised infrastructure such as buses, boat services, suburban trains and pedestrian routes also embedded within the social arrangement in lieu of disrupted underground services. Comparing this to Verbeek's idea of the tool forcing itself upon us, we see these less known commuter tools forcing themselves upon us, to help us find and make a route around the disruption. How might we understand and see social media as becoming embedded in that commuting arrangement as more actors use it to seek service information and updates?

When referring to *transparency*, Star talks of infrastructure not needing to be rebuilt each time it needs to be used. An example of transparency could be Wi-Fi networks in that they are always on, ready for use when we connect, we do not need to set up the router each time we want to go online (Perriam 2013). As Star, Bowker and Neumann explain,

> “Transparency for one user means that he or she does not have to be bothered with the underlying machinery or software. In this sense, an automobile is transparent when a driver sits down, turns the key, and drives off, all without the foggiest notion of how internal combustion works. “ (2003: 242)

Transparency also relies on a certain level of expertise, depending on how often we encounter the infrastructure. Star (1999) uses the example of the .ftp download process being bewildering to the biologists who rarely encounter the system[20] and yet, simple to computer scientists who use the process often and have a working understanding of it. But how might this concept of the ‘theatre of failure’ challenge Star’s ideas around transparency? What if, in instances of infrastructure failing, audiences want to see proof even if they don’t understand it? We will encounter an example of this in the Transport for London research around proof of maintenance works, where the audience is shown an image of repairs but doesn’t have the required professional vision (Goodwin 1994) to understand the work going on within the image itself.

Star also tells us that infrastructure is *learned as part of membership* within a community of practice where ‘[s]trangers and outsiders encounter infrastructure as a target object to be learned about.’ (1999: 381) A commonplace example of this is in public places such as cafes, where access to the Wi-Fi is learned as part of membership because someone must ask cafe staff or regular customers for the password. This gives them both membership to the Wi-Fi network and to an added level of membership within the cafe from someone who is there to drink coffee to someone who is there to use the Wi-Fi (Perriam, 2013). When

[20] And indeed, as users of downloading and uploading technology in the 21st Century, we rarely have to encounter the .ftp process that Star describes. While we may have previously had to use .ftp processes to share or receive files online, it is now as easy as selecting a file or clicking on a link.

infrastructure is disrupted it forces itself upon the community of practice available to try to rectify the situation. In the cyber security research, we will see this exemplified as the ethical hacking community demonstrates easily avoidable security flaws to the public in the hopes that people adopt better practices to avoid having their digital devices being hacked.

Finally, infrastructure has the property of being *fixed in modular increments, not all at once.* As Star elaborates, ‘Because infrastructure is big, layered and complex, and because it means different things locally, it is never changed from above. Changes take time and negotiation, and adjustment with other aspects of the system are involved.’ (Star 1999: 382) Spatially, if we were to look at disruption as something that is enacted online, we also see modular increments - from the tool forcing itself upon us either in the analogue (offline) or the digital (online) and we then choose a digital method of demonstrating that disruption (email a help desk, start a Twitter conversation with a customer service account or, post an image depicting an example of social disruption on Instagram). This distribution of the disruption, the demonstration and the solution means that we find ourselves caught in modular increments because of the specificities of the digital enactment. A disruption may happen in one environment (either online or offline), the demonstration will occur in another and troubleshooting a solution in yet another.

But what to do with disruption once it has been diagnosed? How might disruption be beneficial? I assert that based on Star’s account of infrastructure along with Graham and Thrift’s discussion of breakdown, we can see disruption as being an effective first step on the way to repair.

Disruption, retrospective testing and repair

So why demonstrate a disruption? What is the desired outcome compared to demonstrations within the ‘theatre of proof’ or the ’theatre of use’? Disruption occurs as an unforeseen outcome for the entity, or a break in an infrastructure or object’s reliability. It is an outcome that wasn’t encountered during the testing phase of an entity’s creation. The literature that deals with tests and experiments is helpful in our exploration of disruption and failure precisely because it deals with all of the work of avoiding disruption or attaining standards or best practices for governing bodies.

I return to Pinch (1993) who describes three types of tests which each have an impact on how an addressee might respond to disruption. The first type of test is *prospective tests* that aim to establish the feasibility of a product or process. This is typical of any product development process. I return to Downer’s (2007) example of testing jet engines to determine whether they can stand up to bird strikes during take-off or landing. These tests attempt to recreate potential disruptive events to show that the engines meet the safety standards so there is relative certainty the plane will not falter during flight due to a bird strike. However, as Downer explains, these tests cannot replicate every possible bird strike by each species that may be near airports, indeed the tests often involve frozen chickens rather than birds commonly found near airports. This test with only one or a few species of birds leaves the engines susceptible to real world disruption, particularly by those bird species that were not included in testing.

Secondly, *current testing* is done in order to establish whether the entity is maintaining a good working order. Pinch (1993) gives the example of the regular testing of automobiles - such as annual MOT testing in the UK - to establish whether they are still considered roadworthy according to government regulations. We will encounter similar parallels in the case studies in the form of planned engineering work in the Transport for London chapter and penetration testing amongst the ethical hacking community in the cyber security chapter.

And thirdly, *retrospective testing*. This is testing that is done after a disruption in order to determine the root cause of the incident. Pinch cites the testing done after the 1986 Challenger space shuttle explosion as an example, but we need not look towards such catastrophe to understand retrospective testing. We need only look at forms of troubleshooting and iteration as a form of retrospective testing. When cars, appliances or any other manner of entities breakdown we go through a process of examining the object, keeping in mind the specificities surrounding the disruption and attempt to determine the cause of the disruption and how it could be repaired.

Could we understand some of these demonstrations we encounter in the case studies as moments of problematisation that result in a series of current or retrospective testing?

Understanding disruption among the human, non-human and more-than human

Disruption reveals the relationship between humans, non-humans and more-than humans such as animals and nature. I refer specifically to Michael's examples of hiking boots (2000) and interview equipment (2006). In his example of walking boots, Michael describes how the boots aid humans in accessing the ‘sublime’ within nature. However, while aiding the humans to access nature, the boots also provide a barrier between humans and the elements by protecting bare feet from sharp rocks or from muddy puddles. However, these non-human boots disrupt humans by causing blisters and irritation and they disrupt the wider more-than human environment by causing damage to flora and fauna on the trails.

Within interview scenarios, Michael asserts that non-human objects such as recording equipment can disrupt the conversation and highlight the differences between the interviewer and the interviewee. He uses the example of an interview he was conducting in someone’s home where his recording equipment was sat on by the interviewee’s cat, which then led to him being distracted by the non-human pets of the interviewee, thereby giving the non-humans more agency.

In each of these examples, we note two points about disruption. Firstly, we witness how relationships between human, non-humans and more-than humans can be simultaneously productive for some actors in one sense, while being disruptive to some or all actors in another. We will encounter this in the selfie stick research, where some human actors consider the selfie stick to be productive while other human and non-human actors (such as artefacts or works of art) may find the selfie stick to be disruptive or destructive. Secondly, we often witness disruption occurring as a combination of actions between humans and non-humans or more-than human actors. We see other examples of this in STS literature such as Latour's description of the 'gun-in-hand' (1999), where Latour asserts that the non-human gun is not in and of itself problematic, rather the gun in combination with a human operator becomes problematic. We could view the selfie stick in a similar light, that it is not disruptive in isolation, but it becomes disruptive when combined with certain human actors in certain public settings.

Conclusion

This chapter has examined the key concepts contributing to the research question: demonstrations, the digital and, disruption. By reviewing historical and sociological studies of science and technology demonstrations, I have shown how they have brought into view a theatre of proof focused on a consolidation of new knowledge, and in later work, a theatre of use focused on selling products in the information technology sector. I have introduced the concept of the theatre of failure as a useful way of understanding the role of demonstrations of disruption in convincing responsible and accountable actors of the gravity of a disruptive event or object. Additionally, I have focused on the setting and scripting of demonstrations, comparing public lecture-style demonstrations to those we see within the specificities of digital and social media. I have also described how digital settings reconfigure scripts to allow for opportunities to respond to or act upon a demonstration.

I have discussed how we encounter the digital in at least three forms: setting, object and, research instrument. This involved describing the entities and specificities of each iteration of the Web 1.0 through to Web 3.0, with specific reference to how they reconfigure demonstrations. I also described how these specificities introduce new audience members to demonstrations such as collateral audience brought in by digital and social media algorithms and, the social media platforms themselves using the data created by these demonstrations to further their commercial interests. I also touched on how the digital can be a research instrument in its own right and I will touch more on this in the next chapter dealing with methods.

And finally I examined disruption and what we might stand to gain from examining disruptions from an STS. From an STS perspective, we stand to gain an understanding of how these demonstrations of disruption can be a catalyst for current or retrospective testing.

Chapter Three: Researching Digital Demonstrations of Disruption

Introduction

In the previous chapter, I described the key concepts of demonstrations, the digital and disruption. In this chapter, I will explore the methodological approaches available for studying demonstrations of disruption empirically and how they inform the methods I have used to gather empirical data and materials on digital demonstrations of disruption and ‘theatres of failure'. While the digital is a topic of research of this thesis, there are pressing methodological questions concerning the digital that are investigated further in this chapter. How do you research the digital when it can be conceptualised in multiple ways: as a setting, as an actor and as a research instrument?

I will start by discussing the methodological standpoints necessary to research the empirical topics of my thesis: demonstrations, disruption and, the digital. I start with a ‘classical ANT' approach to demonstrations, which highlights the formation of networks that involve non-human actors. ANT also directs attention to the ways in which actors problematise, enrol and stabilise other actors through these demonstrations. From there I discuss the use of a post-ANT approaches to account for the multiple ontologies of the digital as a setting, actor or research instrument, especially within the growing area of digital sociology. Taking this methodological approach will allow me to combine different research methods in generating knowledge about the digital. I will then discuss how ethnomethodology can be used as an inspiration for researching disruption and accounting for what might make an event or an object disruptive.

Ethnomethodological methods such as breaching experiments (Garfinkel 1969/1991) are useful to gather explanations of disruption from actors in a digital context. Finally, I describe some of my ethical considerations in conducting digital ethnography, breaching experiments and, using the digital as a research instrument.

Approaches to studying digital demonstrations of disruption

As my research focuses on digital demonstrations of disruption, I would like to consider some different methodologies that have been put forward to research these three components. It strikes me that each component suggests a different methodological imperative. To study demonstrations, a ‘classical ANT' approach (Michael 2016) seems well suited, as it allows us to examine how knowledge is produced by an expert and shown to others to enrol the audience in that new knowledge. In comparison, studying the multiple ontologies of the digital requires more of a post-ANT approach (Michael 2016) to better understand how we might approach it as a setting, an actor and/or a research instrument (Marres 2017). And finally, in studying disruption, I believe it is necessary to consider ethnomethodology as it is a crucial means of ascertaining what the event of a disruption can tell us about the social processes being disrupted. I will not try to resolve the differences between these methodologies, but clarify why I think it is possible to combine them.

Studying demonstrations with Actor-Network Theory

By taking up Actor-Network Theory, I have chosen to study a broader group of actors than the humans caught up in and responding to disruption, choosing to incorporate non-human actors that are part of the network relations being made. The ramifications for the thesis is that an equal amount of time is spent examining three fields with three non-human actors at the forefront: the selfie stick as an actor with disruptive agency, the attributes of public transport infrastructure or, the persuasive work done by a cartoon explaining the Internet of Things. An Actor-Network Theory approach allows the ability to observe and record how human and non-human actors come together in particular combinations that culminate in a demonstration of disruption within the ‘theatre of failure' that arises from the disruption. In this sense, it follows a history of ethnography drawing on Science and Technology Studies such as the particular combinations of scientists, lab equipment and processes in the production of scientific knowledge (Latour and Woolgar 1986).

The research presented in this thesis has taken up one of two Actor-Network Theory approaches. The chapter on cyber security takes what Michael (2017) describes as a ‘classical’ ANT approach, while the Transport for London and selfie stick chapters follow more of a Post-ANT path. Michael (2017) states that, “drawing a line around ‘classical’ ANT is perhaps more difficult that might at first appear” (p 28). And I’m not attempting to draw an easy line around it either. For my focus on demonstrations, disruption and, the digital in this thesis, I am interested in the ‘classical’ ANT frameworks on non-humans and attributed agency and, the constructedness of knowledge for the purposes of problematisation and enrolling actors in these problems. In comparison, Post-ANT encompasses the iterations and “the complex unfolding of a nexus of practices, concerns, accounts that can be loosely brought under the umbrella term ‘post-ANT.’” (Michael 2017, 115) For the purposes of developing a framework for studying the digital, I focus on an iteration of post-ANT, which concentrates on the ontological turn. It is important to note that often post-ANT is informed by ‘classical’ ANT and builds upon it. The chapter on cyber security takes a classical ANT approach in order to further investigate the work that demonstrations within the ‘theatre of failure' do in articulating and enrolling citizen-consumers in a disruption or the potential for disruption. Further, it allows us to trace how these demonstrations do (or don’t) enrol actors in the disruption. The literature on demonstrations within STS takes a similar approach, when Simon and Schaffer (1985) describe historical experimental science demonstrations in the Scientific Revolution, they pay as much attention to the agency of the air-pumps being demonstrated as they do to the scientists demonstrating the new knowledge. By taking a classical ANT approach to researching demonstrations, we can examine and focus on the work that non-human, digital actors such as social media platforms or software do in enrolling us in demonstrative practices. However, enrolling audiences in demonstrative practices is only one way we might consider a classical ANT approach appropriate to explore the research question. In the discussion above, classical ANT has been described as a way to understand demonstrations within the ‘theatre of proof'. But how might a classical ANT standpoint be useful in thinking about the 'theatre of failure' as a heuristic to observe how actors persuade and enrol others into a disruption or the potential for disruption?

A classical ANT standpoint is useful to examine the ‘theatre of failure' because of terminology around problematisation (Callon 1986a, Callon 1986b, Michael 2016). This term describes how one actor may identify a problem within a practice or identity of another actor. In comparison to demonstrating failure, this identification of a problem is used to modify the practices of that actor and de-stabilise the network. This concept is relevant to the ‘theatre of failure' because demonstrations are often an act of problematisation, especially when it comes to getting actors to agree on the existence of a disruption. Demonstrations are an act of problematisation because they are the means by which one actor identifies a problem with another. We encounter this in each of the research chapters to come, but problematisation is particularly noticeable in the chapter about cyber security practices. Each of the demonstrations we encounter involves cyber security experts problematizing the cyber security practices of non-expert members of the public, especially around password practices. Demonstrations such as these and the others we will encounter act to problematise the practices or identity of one actor to enrol them in practices -

such as good password security - to stabilise (and in this case, secure) the network. But how might ANT also contribute to understanding other modes of disruption, such as deliberate acts of disruption from hackers who exploit vulnerabilities in the network?

Classical ANT is also useful as a methodological approach for examining the difficulties in demonstrating both the promise and problems of black-boxed (Callon and Latour 1981), as well as abstract concepts such as the Internet of Things. The Internet of Things as a material infrastructure is not exciting and nor is it easily demonstrated to those without computing knowledge: it is hardware, software and protocols. This is rarely demonstrated because it is not engaging or persuasive. Rather, what *is* demonstrated, are the actions that are made possible through The Internet of Things, the promise of connectedness and convenience or, the possibility of everyday IoT objects and their data being hacked with dire consequences for the consumer or the broader global community of Internet users.

This difficulty in demonstrating the Internet of Things in a tangible, non-abstract manner creates problems when it comes to the attempts to enrol actors in materially participating in the Internet of Things by consuming these products. Due to the black-boxed nature of the Internet of Things, it is similarly, if not more difficult to demonstrate disruption to the cyber security aspects of the Internet of Things to successfully problematizing and enrolling publics in this. If the Internet of Things is made up of a largely invisible, taken for granted network of infrastructure and code - apart from the input of information and instructions and an output of domestic convenience (to take the example of IoT connected objects for the home) – then how might we observe disruptions that occur to the taken for granted, infrastructural part of the IoT network? Similarly, how might we observe demonstrations of these disruptions and analyse their capacity to enrol those accountable for the disruption? In this research chapter, I have adopted a classical ANT sensibility, as it allows me to focus on questioning how the digital and social media are used to craft representations of the Internet of Things or safe cyber security practices with the aim of enrolling consumers into IoT products. A classical ANT approach also allows me to examine how human and non-human actors interact with black-boxed entities or assemblages such as the Internet of Things.

However, there is only so far that a classical ANT approach can take a researcher. For instance, concepts such as the digital could be understood to be somewhat black boxed from a classical ANT approach. But developments in ANT towards a Post-ANT sensibility can give a methodological standpoint from which to examine the digital for this research question. In particular, a post-ANT approach is more attentive to multiplicity in comparison to earlier ANT approaches.

Studying the digital with Post ANT and digital sociology approaches

In comparison to the Classical ANT approach described by Michael (2016), one distinctive feature of Post ANT is its concern with multiple ontologies. Perhaps the best-known and often-quoted description of this is from Mol (2002) in her ethnography of the multiple diagnoses of the cardio-vascular disease atherosclerosis in a Dutch hospital. Mol's ethnography demonstrates that an actor - in this case, a disease - can manifest and be problematised in multiple ways, that resist being summed up into one definition of the object or situation. Equally, it can also be treated or stabilised in multiple ways. As I will discuss below, the move towards Post ANT is not limited to the ontological turn within STS, it has had implications for how ANT is understood and used.

This has meant rather than working with the framework of Actor-Network Theory, I am working with many Actor-Network Theories, or as Mike Michael (2016) explains, 'a multitude of post-ANTs that are spinning off in different, though more or less loosely inter-related, directions.' (p151). Taking into account this 'multitude of post-ANTs' each of the research chapters utilises Actor-Network Theory in slightly different ways.

In comparison to more 'classical ANT' studies that are bound to certain settings such as laboratories, the research done in this thesis takes place in multiple digital and in situ settings. I observe disruptions through demonstrations on social media platforms such as Twitter or YouTube, as well as in situ settings such as London Underground stations, art galleries and, workplaces to account for *where* the disruption occurs and *how* they are then demonstrated and received. These multiple settings send the analyst into a mess (Law 2004) of settings, actors and demonstrations, none of which are contained or observed in such a straightforward way as observing scientific work in a laboratory (Latour and Woolgar 1986) or conversing with photocopy machine in an office (Suchman 1987). Rather, post-ANT approaches such as those explored by Mol in her examination of atherosclerosis account for not only multiple ontologies of the condition, but also the different settings in which it is articulated. This multiplicity is helpful to keep in mind when considering the varying ways we might observe the digital as setting, actor or assemblage. Law argues that the methods we use do not merely describe or show the realities of what is happening in the field sites, but that methods also participate in the realities depicted:

> "…It is that they [methods] participate in the *enactment* of those realities. It is also that method is not just a more or less complicated set of procedures or rules, but rather a bundled hinterland." (Law 2004: 45, emphasis original)

Law uses Annemarie Mol's *The Body Multiple* (2002) as a case to describe the methodological imperatives in taking a post-ANT approach. He frames Mol's approach within the term 'out-thereness' to describe the world encountered outside of controlled spaces such as the laboratory. Law's analysis of Mol's work offers a potential methodological approach to researching digital demonstrations of disruption. Take, for example, the enactments of atherosclerosis that Mol observes in Hospital Z. Law states "Intermittent claudication, calls for both a patient and a doctor. If it is to be enacted, it needs to be crafted out of a story by the former and the embedded knowledge of the latter." (2004: 46). How might we understand disruption in a similar way in the research chapters? Transport disruption calls for both a commuter experiencing disruption and the customer service agent with the embedded knowledge of the public transport network and information to respond. A hacking disruption calls for both an actor who has been hacked and a cyber security expert with embedded knowledge of how these types of disruptions occur and could be remedied or prevented. And a selfie stick disruption requires a disrupted party and someone who knows the rules and regulations of a certain public space. But much like the discussion in Chapter Two around the reconfiguration of the scriptings of demonstrations of disruption due to the digital, how might the digital reconfigure these enactments? Returning to the overarching question around the different forms the digital takes, Mol's study of the *many ways* that atherosclerosis is enacted can help consider the different settings and conditions under which the digital can be enacted and observed. The emphasis in my study is on the many ways digital demonstrations of disruption are enacted in mundane and everyday life in all its complications, contradictions and mess. In the chapter about TfL, we observe more of the complications and the mess. But the chapters about cyber security and, selfie sticks offer contradictory examples where demonstrations don't necessarily match up with enacted realities. In Chapter Six, I describe a situation where the online enacted reality of selfie sticks as a focus for disruption does not match the in situ enacted reality of selfie stick use, which seems to be not very disruptive. What to do with this contradiction?

Law advises us to look past the contradiction and see each disruption as a separate object:

> "We are not dealing with different and possibly flawed perspectives on the same object. Rather we are dealing with different objects produced in different method assemblages. Those objects overlap, yes. Indeed, that is what all the trouble is about: trying to make sure they overlap in productive ways." (Law 2004: 55)

In Chapter Six, I will describe the different ‘selfie sticks' each produced by the breaching experiment and the social media analysis as method assemblages. These methods will be discussed in further detail later in this chapter, but in this description of these different selfie sticks, I will describe how they overlap and how they don't overlap.

The Post-ANT notion of multiple ontologies has influenced the methodological imperatives of digital sociology. Marres outlines three ways a researcher might encounter the digital: as a phenomenon, as a method or, as a platform (2017, p 24-32). This informs the terminology I use in this thesis, which approaches the digital as an object or phenomenon to be demonstrated, as research instrument with which to examine a demonstration and/or, as a setting in which these demonstrations take place. Approaching the digital as multiple in this way allows me to choose appropriate methods for analysing the digital in its different incarnations.

The research of Transport for London and the selfie stick take a distinctly Post-ANT approach. Although I treat the digital as a setting in the Transport for London research, this setting is highly dependent on the specificities of each of the entities that help constitute it. Taking a Post-ANT approach in this research means observing each of the entities that are involved in demonstrating and responding to a disruption and paying attention to how they configure the setting, the actors and, their demonstrations. Further, I pay attention to how infrastructure, TfL staff, commuters and social media work as *demonstrative hybrids,* that is, how they come together into assemblages to produce a demonstration of disruption. A disruption certainly cannot be such without TfL infrastructure or commuters being disrupted, and its demonstration cannot take place without the addition of TfL customer service agents or social media and its management software to collate demonstrations and respond to them. As I will discuss later in this chapter, I attend to the entities participating in the enactment of disruption through workplace observations, semi-structured interviews and participant observation.

In addition to focusing on the digital as a research instrument, the selfie stick research reported in Chapter Six also takes on Post-ANT approaches, such as observing the multiple ontologies of the object. This is due to framing the digital (in this case, the selfie stick) as an actor in this research. At first glance, the proposition that the selfie stick - a rudimentary object that may be Bluetooth enabled at its most advanced - is a digital object, let alone a digital actor is quite strange. The selfie stick is implicated in situated digital photographic practices to create digital images; we can only understand it within the context of the digital. Outside of these practices for and within digital settings, the selfie stick could be considered a superfluous object. My question therefore is whether the selfie stick is disruptive and how it is disruptive. How is the selfie stick demonstrated as disruptive negatively? Similarly, are there ways in which the selfie stick is demonstrated as a positive disruption? How does a digital device become different objects enacted through demonstrated situated practices or encounters? Do these differing ontologies of the disruptive attributes of the selfie stick ever get discussed online? How might we observe the ways that the selfie stick is used as an auxiliary non-human object between a human actor and their non-human phone? By considering this, we can see how post-ANT can draw upon classic ANT concepts such as assemblages and human-non-human chains. To take some cues from Michael again, this research involves having to ‘cultivate a sensitivity toward the different realities you come across and the patterns of their interactions. Sometimes such realities will conflict, sometimes sit in parallel, sometimes merge, sometimes depend on one another's absence.' (Michael 2016 p.152)

But there are some aspects of digital demonstrations of disruption that are difficult to investigate from an ANT or Post-ANT standpoint. While these standpoints aid our research by following traces and actors involved in a disruption, it can be difficult to use this approach to get at the expected social order or stability of a given situation. What methodological sensibility might be useful to better understand what makes an event or object disruptive? I suggest that ethnomethodology can be used alongside ANT and Post-ANT approaches to guide the methods used to examine a disruption's disruptiveness. Further, in this chapter, I describe how I use ethnomethodology to explore these questions.

Studying disruption through ethnomethodology

When it comes to studying disruption in a broader, non-infrastructural, mundane sense, what methodology can help us understand and observe mundane disruption?

The other methodological sensibility I utilise in this research is ethnomethodology (Garfinkel 1967/1991). In comparison to ANT (and post-ANT)[21], which allows the researcher to describe the disruption on the level of what is being disrupted and how that is being demonstrated, we are still left with questions about the expected social order. What is the social order being disrupted that means that an event or an actor can be considered disruptive rather than the status quo? Breaching experiments – one of the methods used in an ethnomethodological approach - are described by Garfinkel as 'aids for the sluggish imagination,' (1967/1991, p.38). He hypothesises that by conducting interviews and experiments that challenge the social order, we are

[21] To be clear, ANT and Post-ANT draw on ethnomethodology in that the focus is on 'local interaction as a way of grasping the production of social order.' (Michael 2017)

then able to inquire into the expected, stabilised situation and how it came to be. He goes on to describe this far more poetically, saying that by utilising ethnomethodology, ‘they produce reflections through which the strangeness of an obstinately familiar world can be detected.' (Garfinkel, ibid) For this thesis, ethnomethodology is used in an attempt to answer the question: how is the disruption considered to be disruptive?

In particular, an ethnomethodological approach is particularly useful to investigate a phenomenon such as the introduction of the selfie stick because it allows a researcher to observe situations where the social order is challenged. As is further explained in the empirical chapters, ethnomethodology is applicable and used in both in-situ and digital forms. Breaching experiments are a method of carrying out a deliberate provocation to generate ethnomethodological data that inquires into the underlying social processes of everyday behaviour (Garfinkel 1967/1991). This method involves deliberately creating situations where everyday, taken for granted practices are ignored or modified to provoke a reaction or an explanation of stabilised practices. These reactions or attempts from those involved in the breach to return the interaction to the expected format generate knowledge about everyday practices and expectancies.

This is the method used in the selfie stick research to attempt to articulate some of the stabilised practices in public spaces such as art galleries. I shaped my breaching experiment in a similar vein to those conducted by Woolgar and Neyland (2013) when they investigated the social processes of airport liquid restrictions. In their breaching experiment, they took containers with more than

100 millilitres of water through airport security screening areas to inquire further as to why this volume of liquid was banned. This showed how 'Ordinary objects could acquire an insecure ontology. A water bottle was transformed into a potential object of terror.' (Woolgar and Neyland 2013. p223) Similarly, I wanted to use a breaching experiment to observe how the selfie stick could acquire an insecure ontology and become transformed into a potential object of disruption and damage. To do this, I conducted a breaching experiment in the National Gallery in London. This consisted of using a selfie stick in a place where it had been banned to further interrogate the reasons for the ban if someone approached me to ask not to use the selfie stick in that space. However, this breaching experiment did not provide the intended results of a reprimand from other actors in the gallery. Does this mean that the breaching experiment failed? Although conducting an auto-breaching experiment can be problematic (Perriam, 2017) I argue that the experiment wasn't a failure, rather it had unexpected results which still equally speak to both the social order within the gallery and the ontology of the selfie stick.

But is it necessary for a researcher to create a breach to gather data about the expected social order in a public place such as an art gallery? I approached the comments section of online articles discussing bans of the selfie stick with an ethnomethodologically inspired analysis of the comments with attention to how commenters discussed how they saw the selfie stick to breach the expected social order in public spaces such as galleries or museums. In this way, the ethnomethodologically inspired online analysis filled the gap of producing ‘reflection through which the strangeness of an obstinately familiar world could be detected' (Garfinkel 1967/1991: 37-8).

We also see ethnomethodology feature briefly[22] in the analysis of the Transport for London research. This takes the form of a small portion of Garfinkel's writing about ‘problem-solution relationships', which has been further developed and explored by Neyland and Milyaeva (2016). They describe how the description of a problem sets off a process, whereby seeking and implementing a solution to a problem allows time and attention to be paid to new problems and the development of further solutions. In the Transport for London chapter, I will be looking specifically at how the introduction of automated social media notification services allow the TfL agents to focus on addressing more complex customer disruptions.

As discussed earlier in the chapter, there are portions of this thesis that investigate digital demonstrations of disruption that can be easily explored using an Actor-Network Theory sensibility, focusing on describing these demonstrations and the human and non-human actors involved in them. We can use Actor-Network theory to guide our observations of how human and non-human actors are arranged in networks during disruptions and their subsequent demonstrations. We can also use Actor-Network Theory to allow us to consider how digital non-human actors are agential with demonstrations and the digital settings they are demonstrated within. However, Actor-Network Theory doesn't help us when trying to discuss the epistemology of a disruption; what an event, object or practice must be to be considered disruptive. This is

[22] I say briefly because the portion I refer to is a short paragraph in *Studies in Ethnomethodology* that Garfinkel writes about problem-solution relationships, but does not develop it further.

where ethnomethodology has analytic utility.[23] In this sense, the overarching research question about digital demonstrations of disruption demands a mixed-methods approach is there scope in this Post-ANT world for ethnomethodology to lend a methodological hand.

Digital Ethnography: an STS approach

In this section I examine some of the claims made about digital ethnography, which is a label used both in Science and Technology Studies and Sociology that best describes my research approach. Digital ethnography is still very much in a state of flux; much like the concept of the digital as discussed in the previous chapter; it is difficult to define and, pulled in varying disciplinary directions. Many researchers have defined digital ethnography in ways that suit disciplines such as cultural studies, media studies and, anthropology. However, my aim is to discuss digital ethnography from an STS standpoint as this may offer a way to attune my research to the multiple ontologies of the digital.

The version of digital ethnography that aligns best with the methodology outlined so far is what Hine (2015) describes as 'ethnography *for* the Internet'.[24] Hine argues that her ethnography is for the Internet rather than *of* the Internet 'because you cannot grasp the Internet as a complete entity.' (2015, p5) In saying this, she acknowledges the reconfigurations of digital ethnography from a Web 1.0 era - where academic researchers saw the Internet as a discrete

[23] But can ethnomethodology and Actor-Network Theory necessarily be good bedfellows? There has been debate about this (Latour, 1986, Lynch 1985,1993) which demonstrates the tension between the two methodologies. But I want to err on the side of saying yes, the two methodologies can work alongside one another, or at least they can in the context of this research question. And I want to do so not as an attempt to resolve the debate but rather to look at how this methodological tension can be useful in engaging with different portions of the research question.

[24] Although Hine describes ethnography for 'the Internet', her definition and methodology are similar to that which I use for 'the digital' within the context of the research question. Therefore, when referring to Hine's work, I consider the two phrases as interchangeable.

field where actors could carve out discrete identities to those offline - to a distributed field where the Internet is embedded in our everyday practices and our offline identity is no longer separate from our online one.[25] By comparison, in the first era of digital ethnography (Hine 2000, 2015), a field could consist of a forum website, centred around a particular topic (Baym 2000, Markham 1998, Nardi 2010) where the setting and the participants did not mingle in everyday life. In the era that we are now in, we have embodied practices, such as catching public transport interspersed with the digital as information about the service is placed in this setting. How might an ethnographer approach practices occurring in many fields? Hine emphasises that the digital is understood differently each time it is encountered and configured. In this respect, ethnography is ideal to study the digital because it is ‘an adaptive approach that is different for each circumstance in which it finds itself.' (Hine 2015, p13). However, while there are advantages for analysing the digital to the adaptive approach whereby ethnography can take the form of different activities like observation, participation, interviews and field notes, the practicalities are less straightforward. This becomes particularly clear when researching mundane, everyday activities such as those involving commuting or selfie-stick use.

So how to ethnographically research the digital – which is distinct from the Internet that Hine describes? Hine argues that:

> 'the Internet and the digital are not available in any transcendent sense but emergent in practice as they are realised through particular combinations of devices, people and circumstances (Ruppert et al. 2013). If the Internet is emergent in practice, it is then also potentially multiple (DeLaet and Mol 2000,

[25] As far as possible, I try not to use the offline/online binary as a way to describe the setting of situated practice, simply because it is often not that easy to distinguish where one begins and ends. However, in this comparison to early Internet ethnography where it was easier to make this distinction, I have done so. I prefer to use ‘online' and ‘in situ' to make the distinction between settings because in situ allows the researcher to acknowledge that often (and especially in the everyday, mundane) situated practices are entangled with online practices.

> Mol 2002) and not resolvable to a singular set of implications. Ethnography for the Internet need not assume that there is a single knowable Internet out there.' (Hine 2015, p 29)

To work with the argument that there is not a 'single knowable Internet out there,' the ethnographer needs to visit the instances or combinations of the digital as they emerge through the practice of devices, people and circumstances. But because there is not a 'single knowable Internet' to observe, the ethnographer also must accept that they are unable to observe each and every emergent practice of the phenomena they wish to study. Rather, they are contributing *an* ethnography to a broader, incomplete ethnography of the digital.

Other approaches to digital ethnography do not account for the digital in such a way that is helpful for the question of investigating digital demonstrations of disruption. While Murthy (2008) discusses the need to be attentive to events in both the digital and physical settings, he does take a platform-specific view. This approach tends to be too limited when observing demonstrations of disruption that occur concurrently across many platforms. Murthy's approach tends to suggest an ethnography of a platform rather than an ethnography of a phenomenon that occurs within digital settings.

At the other end of the spectrum, Pink et al. (2016) describe digital ethnography more broadly as ethnography done with digital devices or focusing on practices that incorporate the digital. While this is a helpful way of incorporating the digital as a research instrument through using their suggestion of incorporating social media or mobile phones as devices to create ethnographic accounts, it doesn't answer crucial questions about conducting ethnography in digital settings or around phenomena that have a strong digital component. Instead, Pink et al.

(2016) encourage ethnographers to take a ‘non-digital-centric' approach, by shifting the focus away from the digital and refocusing on the practices around it. However, this is simultaneously obvious and problematic within STS. It is obvious because STS' Actor-Network Theory standpoint lends itself to a flatter ontology and presumes that non-human actors such as digital devices or social media platforms are just as much a part of a network to be studied. To preference the digital as an actor above other actors within a network go against this idea of ‘flatness'. But a ‘non-digital-centric' approach becomes problematic when you're faced with conducting an ethnography with a multiplicity of digitals. How can you be non-digital-centric when observing a phenomenon, which involves actors in a digital setting interacting with digital objects? We will see an example of this in the cyber security chapter when human actors are involved with disruptions around hacking, arguably a phenomenon that happens in a digital space, involving digital objects such as passwords and databases, but also having disruptive ramifications within a physical setting depending on the outcome of a hacking event.

Taking an approach to digital ethnography that allows for multiple ontologies of the digital requires the ethnographer to steer clear of an overly prescriptive approach that Pink et al. or Murthy advocate. Instead, to achieve this, an ‘adaptive approach' that Hine (2015) describes allows us to observe and to account for each encounter and configuration of digital fields as they occur.

But how did we get to this point of observing the non-human specificities or the digital alongside human practices? Perhaps the best way to exemplify this is to take a brief tour of ethnography in various stages of the web. In the early web or ‘Web 1.0’ era, the academic community referred to digital ethnography as ‘virtual ethnography’ (Hine 2000, 2005, 2009) and ‘netnography’ (Kozinets 2009) as they observed online communities gathering on forums and bulletin board services. Digital ethnography in this setting was accounting for specificities of asynchronicity and heavily text-based sociality.

In Web 2.0, we see a shift towards sociality occurring on newly created social media platforms and blogs. The specificities of Web 2.0 allow ethnographers to observe not only text-based sociality but also social data that are made up of photographs, videos, memes and user actions such as ‘liking' and adding hashtags. This allows the ethnographer a broader range of observations to work with. This enables a broader group of ethnographers to conduct research. Where in Web 1.0, researchers were studying sociality in discrete, self-selected groups, in Web 2.0 researchers are able to study objects (such as the selfie stick) and the different ways in which digital settings encourage human actors to participate in sociality in different ways (as will be shown in the Transport for London chapter). However, Web 2.0 is highly metricised and data-driven -does that detract from ethnography's qualitative outputs? Or does it call for a mixed methods approach?

It is important to note that although we have encountered many iterations of the web, one does not replace the other. Rather they sit in parallel or build on one another. There are still situations where it may be entirely appropriate to do a virtual ethnography of a group within a forum or Facebook group. But similarly, Web 2.0 offers up opportunities to conduct research otherwise not possible in Web 1.0. An example of this can be seen in the selfie stick chapter, where I conducted a visual digital ethnography of the selfie stick on Instagram. In this research, I examined Instagram posts with the hashtag #selfiestick to observe how the selfie stick was an actor in the digital image creation and publication process. This would not have been possible in a text-based forum such as those within Web 1.0. However, I ended up gaining the most analytic value in researching the selfie stick from a Web 1.0 style analysis of the comments section of[26] a news article, thus showing that Web 1.0 and its methods are far from obsolete.

As mentioned in Chapter Two, we are currently situated in the developing stages of Web 3.0 or the 'semantic web', with innovations such as the Internet of Things, chatbots and virtual personal assistants such as Siri forming part of that iteration. Web 3.0 focuses more on the growing agential attributes of the digital as non-human actors. In this sense, Web 3.0 turns out to be very fruitful for STS ethnographers due to the ability to observe and interrogate the agency of non-human objects. In the cyber security research, I will use digital ethnography to observe how humans describe and enrol others into the Internet of Things and, issues around cyber security. Additionally, in the Transport for London chapter, I will observe the introduction of chat bots and automated subscription direct message updates as forms of non-human digital actors interacting with commuters about disruption and delays.

The practicalities of creating knowledge about digital phenomena through ethnography can be challenging. Where some ethnographic tactics remain the

[26] The comments sections of articles or videos have incorporated Web 2.0 specificities to allow people to comment using their Google account (on a YouTube video, for example) or using their Facebook account on websites that use third-party commenting plugin such as Disqus. However, the article I analysed, did not have these specificities that allowed the comments to be 'platformised' (Helmond 2015).

same, some are augmented and, new possibilities emerge due to the specificities of 'the combinations of devices, people and circumstances.' For example, field notes remain a vital part of the ethnographer's work as they record their observations as they occur. However, interviews and participatory activities may be reconfigured as the wheres and whats of the field move. And the specificities of the digital allow for traces or inscriptions of events to be logged and referred back to at a later date (Bowker 2005, Marres and Welrevrede 2013). And indeed, as discussed in the previous chapter, these traces are occurring more frequently as we encounter digital devices that create their data independent of the actions of human actors (Rogers 2009). Rogers describes this data as 'natively digital' as it has been created without human intervention or inscription. But how might ethnographers engage with these traces in a way that is both fruitful and critical?[27] Although these traces are available to draw upon to contribute to an ethnography, we should make no mistake that they do not replace field notes, rather they act as a supplement. And as Marres and Welrevrede (2013) and Hine (2015) point out, while these traces are often available to study, the technology with which to gather them can often be black boxed leaving the ethnographer without the crucial social, economic and political context with which to critically analyse them.

But does ethnography work for all aspects of the research question? I argue that it mostly does along with the intervention of one or two other methods. In particular, I argue that while ethnography is a fine method for examining and

[27] Rogers would choose to answer this question by stating that digital research would best be served by going beyond ethnography. Rogers (2013) advocates discussing 'the difference it would make to research if one were to follow the medium – by learning from and reapplying how digital objects (such as hyperlinks) are treated by devices.' This approach takes a step away from conducting ethnography to understand how people use the internet (and the digital by extension) and moving towards research 'to consider the Internet as a source of data, method, and technique.'

describing demonstrations and the digital, adding digital methods can bring out the distributed quality of the enactment of disruption. The unpredictable nature of disruption makes it difficult to plan to encounter a disruption as an ethnographer. Some disruptions happen often such as with public transport, so that is not too difficult to observe in due course. But with other disruptions, such as those we will encounter with the selfie stick, the problem is less about witnessing and observing the disruption and more about grasping precisely *how* other actors define it as disruptive.

I argue that it is not the sociality that makes digital ethnography any different to ethnography, but rather it is the specificities and the technologies that act as the setting for the sociality that make it different. This standpoint has been pioneered by those working in the area of digital methods (Rogers 2009). In particular, researchers such as Anne Helmond (2015) look at the specificities of social media platforms being integrated into other websites as a form of ‘platformisation of the web'. Similarly, Gerlitz and Helmond (2013) examine the specificities of social media infrastructures such as the ‘like button' and similar entities, which encourage users to interact with content. However, they highlight that while users see such specificities as enabling sociality or approval amongst their network, platform owners see them as valuation devices, creating economic value in areas such as advertising and marketing insights. These specificities are what cause the ethnographer to amend their method. There is a growing corpus of scholarly work that demonstrates not only these specificities, but also how (digital) ethnography has been configured alongside these new specificities.

Conducting empirical research with a focus on both Actor-Network Theory and Ethnomethodology requires the use of qualitative research methods. For the remainder of this chapter, I will briefly discuss how I practice digital ethnography within the broader frame of ANT and post-ANT.

Mixed methods ethnography

The research conducted in the three empirical chapters focuses on objects, infrastructure, platforms, settings, people and practices involved in mediating and demonstrating disruption. Following in the STS tradition of ethnography involving objects (Latour 1992, Michael 2000), infrastructure (Star 1999), and situated practices (Suchman 1987/2007, 1997), it is almost second nature to follow in the footsteps of the methods effectively used by others. And indeed, in some respects, that's all that is asked of the researcher: observe and describe. Interview, if you must but primarily, observe and describe the interaction between human and non-human actors in relation to the research question at hand. In some respects, that is precisely what I have done to describe how the use of digital and social media demonstrates and mediates disruption. But as has been discussed by many social scientists in recent years (Lupton 2012, Marres 2017, Ruppert et al. 2013, Rogers 2009), the emergence of social data being created, stored and analysed by digital means has had implications for how methods are conceptualised and implemented. And indeed, some of these discussions of digital social research - digital ethnography in particular - have happened earlier in this chapter. But what about those research activities that still help investigate aspects of the research question that do not involve digital methods? The methods I have chosen to support an Actor-Network Theory approach include observation - both in-situ and online - and semi-structured interviews. I have chosen breaching experiments, collection of online article comments and, structured interviews with elicitation devices to support an ethnomethodological sensibility. I will describe each method and discuss its application in the following sections.

The empirical chapters deal with the different forms the digital takes to *mediate* disruption and in particular, how it mediates between different entities or interested parties - such as a public and a respondent. This can be seen most clearly in the chapters that describe how Transport for London (TfL) uses social media platforms[28] along with social media customer care software. One way of researching this mediation could be to observe the conversations happening between TfL and commuters on Twitter or Facebook. While that approach would give rich textual data about the disruption and how it was resolved, it does not satisfy the question about how TfL's customer service agents use the digital to demonstrate disruption. To my mind as an STS scholar, this question is a far more interesting question, one that generates data that forces the analyst to describe the situated action and have a better understanding of the non-human agents at play in the demonstrations of disruption.

Interviews and observation

As a result, I took my cues from the likes of Lucy Suchman (1987/2007)[29] and Bruno Latour (1999) and went to observe how TfL staff worked within a digital

[28] Here I use the term 'platform' loosely to denote TfL's use of Twitter, and to a lesser extent, Facebook and Instagram to communicate with users rather than to enter into the waters of platform studies. Suffice it to say that TfL engages with commuters or followers on each platform according to their respective specificities and practices.

[29] Suchman's work with can be considered useful in both Actor-Network Theory and ethnomethodological sensibilities. Suchman uses conversation analysis (informed by ethnomethodology) to better understand how human actors respond to instructions from non-human actors (an STS-informed question). Is Suchman's work with the photocopiers technically a breaching experiment? She is intervening in something, but it's less to understand the social

setting to demonstrate and respond to disruption. Specifically, I wanted to observe the ‘theatre of failure’ consisting of commuters and TfL customer service agents demonstrating disruption to one another in the digital setting of Twitter. In addition to this, I also wanted to observe the ways in which social media data generated from these disruptions had a life that spanned long after the momentary disruption demonstrated in the ‘theatre of failure’.

In a practical sense, this meant gaining access to Transport for London's social media customer service team, to spend time with them, observe their work, and ask questions based on what I had observed both online and offline. Gaining access proved not to be too difficult, but having a part-time job as a researcher in the UK's public sector digital industry, meant that I had a head start in identifying and contacting relevant informants.

While in the field at TfL, I spent two half-days in August and October 2016 with the social media customer service team. I followed a loose semi-structured interview based on questions I had prepared ahead of time. These interviews were conducted in-situ, which allowed my informants the opportunity to use their computers or other objects or software in the office to further explain their processes. My informants comprised of middle management and front-line staff. I chose to interview both of these levels of informants because middle management had the institutional memory to be able to tell me the background story of how TfL's social media practices came to be stabilised in this way, while

order of working with a photocopier and more to prove a point about the communication difficulties between humans and the photocopier. In this thesis, I rely on Suchman's work more from an STS perspective to inform my approach to observing situated practices, rather than from an ethnomethodological, conversation analysis perspective. However, other scholars such as Dourish and Button (1998) have examined and applied Suchman's work in an ethnomethodological way that applies to Human-Computer Interaction (HCI) and Computer Supported Cooperative Work (CSCW).

front-line staff were able to describe and demonstrate the situated action of these practices. These interviews were audio-recorded, with corresponding field notes written to account for my observations of what they were demonstrating and describing.

I also had informal conversations, email contact and brief interviews with other TfL staff in charge of TfL's online strategy. Although they made decisions about the software used, the tone of voice and reporting back to the wider organisation about the performance of TfL on social media, they sat outside of the social media customer service team and didn't have very much to do with the day-to-day situated practices of demonstrating public transport disruption.

The observation portion of my field visits comprised of sitting with a social media agent and shadowing them as they worked for part of their shift. This was reminiscent of Suchman's work at both XeroxPARC and the air traffic control setting (1987/2012, 1997). In particular, I was asking my informant to explain the different technologies used to demonstrate disruption to customers but also to discuss and coordinate work amongst the team of social media agents, some of whom were distributed in different locations across London.

In the chapter about Internet of Things (IoT) and cyber security disruptions, the use of semi-structured interviews with experts and actors in the area allowed for descriptions of the 'theatres of failure' that occur through demonstrations on YouTube, blogs and Twitter. These interviews also allowed participants to describe entities and scenes being performed in the 'theatres of failure'. In particular, these interviews from core-set experts can help in describing black-boxed networks of actors such as the Internet of Things. Counter to the semi-structured interviews with TfL employees that focused on how they used particular software to mediate disruption; these interviews had more of a purpose to *clarify* technical details around cyber security and *describe* the actors involved in these demonstrations. These were more straightforward interviews, which tended not to deviate from the informant showing me something; they were more on the structured end of semi-structured interviews. When interviewing a cyber security expert from the ethical hacking community, I had a list of questions about the Internet of Things, botnets, DDoS attacks and, cyber security practices that built upon one another in a structured way. My informant saw through the step-by-step structure of the interview, and as a result, the interview became less structured. However, it was important to retain the interview structure to ensure he clarified technical details about cyber security and the actors within this setting.

Elicitation Devices

Elicitation devices feature in the research around IoT and cyber security and to a lesser extent in the TfL chapter. In an attempt to uncover the hacker community's understanding of the impact of IoT on everyday life, I played a corporate explainer video to my hacker informant to provoke a response around what was missing, neglected or misinformed from the video. The informant responded to the video with a dramatic reaction, which allowed me to ask follow-up questions about the portions of the video that caused that reaction.

In a small way, I also used social media posts as elicitation devices (Lezaun and Soneryd 2007), either by showing the informant some content or by referring to it when asking a question. This is similar to when Back and Sinha (2012)'s research on immigration issues was reported on digital and social media became a form of elicitation device for online conversations that furthered their research. The publication of their research findings on Home Office tactics to encourage immigrants to return to their country of origin provoked responses on social media that could then be used as qualitative data in further research in this area. Outside of a digital setting, Laurier (2004) gives an example of an elicitation device in his research into sales representatives who conduct some of their work while driving between meetings. Rather than interview informants in formal settings such as an office or a public space, Laurier chose to interview them in situ, as they went about their work. Laurier uses the motorway and the objects around the car as elicitation devices to generate knowledge about how the informants manage to conduct office work and drive to and from meetings at the same time.

How might elicitation devices be used when investigating digital demonstrations of disruption? I suggest using elicitations devices to ask those in the 'theatre of failure' - either the demonstrator or the audience - about the use of visual objects such as images or videos to understand how they might be effective in enrolling an audience in a disruption. One instance of using elicitation devices in interviews involved describing a tweet sent by TfL that included a picture of weekend engineering works as part of a question around the efficacy of including pictures when demonstrating disruption. By doing this, I was able to gather a description from TfL staff about how they enrolled the commuting public in a planned disruption.

But does the use of elicitation devices in an interview setting constitute part of an ANT or ethnomethodological sensibility? This is where the productive tension between the two methodologies reappears. In both of these situations, the elicitation devices were used as heuristic devices to direct the interview questions around the demonstrations, rather than the epistemology of the disruption. As a result, elicitation devices were used to answer part of the overarching research question being investigated through an ANT or Post-ANT imperative. In particular, the elicitation devices of maintenance images shared by TfL customer service staff helped further interrogate the reasoning and efficacy of demonstrating disruption via Twitter. I was able to further analyse how these images and videos such as Internet of Things explainer videos encountered in the cyber security chapter are non-human actors within a network that do the work of enrolling people on behalf of human actors. From an ethnomethodological standpoint, the Internet of Things explainer videos used as an elicitation device produce descriptions from cyber security professionals about the desired social order of citizen-consumers and their online practices.

Participant Observation

One of the unexpected places that my fieldwork with TfL took me was to a conference for the social media management software that they had recently procured. I went at the suggestion of one of my informants who was speaking at the conference and thought it might be helpful to my research. I'm indebted to that suggestion because it provided an angle to the research that would have otherwise been left out. The conference was not an academic conference; rather it was a corporate conference that focused on selling a product or retaining those customers who had already purchased the product. This was reminiscent of the work of Catelijne Coopmans (2011) with medical imaging software and the conferences held with the intention of selling the software to hospitals and health organisations. As part of this conference, there was a workshop afternoon that described the social media management products in more detail, with the intention of demystifying the software for those who may want to purchase it, as well as providing support and advanced tips for those who were already working with it.

As will be described further in Chapter Four I went into the workshop with the intention of observing the participants in the workshop. However, it soon became clear that the word 'workshop' was not a synonym for 'software demonstration', rather it was a hands-on experience with group activities around tables with flip charts and trial versions of accounts. During the workshop, I was outed as a researcher - as opposed to a potential client[30] - when the first workshop activity involved a scenario that included analysing social media data from the rail companies serving London and the South East of England. Thankfully, this was a source of humour rather than a source of trouble.

As will be discussed further in the Transport for London chapter, this participant observation experience provided the angle of how software companies configure their clients to use their products in certain ways by the design and capabilities of the product, and how this is reinforced in a workshop setting. It also provided me with knowledge of the product outside of TfL to inquire about

[30] Although other workshop participants hadn't known I was a researcher up until that point, the workshop organisers knew, as I had to approach them to gain access to the conference.

some of the features that the company was particularly proud of, such as sentiment analysis provided by the natural language processing (NLP) capabilities in the software.

But how do these non-digital research methods work alongside the digital methods discussed earlier in the chapter to help investigate digital demonstrations of disruption? In the next section, I will discuss in more detail the benefits of adopting a digital mixed methods approach in each of the chapters.

Digital Mixed Methods

Mixed methods are also described as multi-modal or online/offline methods by Christine Hine (2015). The use of mixed methods in digital research also tends to be unplanned, as Hine explains: "Many Internet researchers were able to identify themselves with the practice of mixing methods even if they had not overtly set out to do a mixed methods study,"(Hine 2015, p.504) This reflects my own experience of researching the selfie stick in particular, as I mixed methods of a breaching experiment and a digital ethnography of online comments on articles blog posts.

As mentioned earlier in the chapter, I conducted a breaching experiment to further enquire into the social order of galleries in light of a ban on selfie sticks in the National Gallery. However, this breaching experiment had an unexpected result when, despite the ban, there was no reprimand for using the selfie stick. This meant that the breaching experiment, while valuable in showing that the selfie stick wasn't considered disruptive enough for a reprimand in a gallery, didn't provide much further understanding of the selfie stick's ontology as a disruptive object. There were accounts of this in digital settings such as blog posts and online news articles that could shed light on the differing ontologies of the selfie stick.

As a result, I modified my methods to a mixed methods approach that took into account some of the online comments of news articles, in particular, an article on the feminist website *Jezebel* titled ‘The Smithsonian Says: F*** Your Selfie Stick’[31] (2015). In this instance, the article acted as a breach, with the commenters explaining the social order - or at least their explanation - from different standpoints such as people who worked at galleries or museums, people who had been annoyed by the use of selfie sticks in their vicinity and, people who had used the selfie stick in the gallery. By researching digital and in-situ fields I was able to understand the social order of the gallery from multiple vantage points. Much like Hine asserts, my intention was not to triangulate data but rather to incorporate differing views on the same research question.

Further to combining the data from the breaching experiment and the online comments, I also conducted a visual analysis of more than 10,000 Instagram posts containing the hashtag #selfiestick to observe how the object was demonstrated to be both negatively and positively disruptive.[32] This visual analysis allowed me to incorporate another vantage point on the research

[31] The choice of articles observed has little to do with the standpoint and political leaning of the publication and more to do with the commenting practices of their reader, where they have gone into depth explaining their choices for using or not using a selfie stick.

[32] I also coded these Instagram posts based on how the image was composed, who or what was in the image, and whether the selfie stick was included within the image. Although this part of the analysis was useful in understanding the situated practices of selfie stick use and image publication, there were few images that described or demonstrated disruption in relation to the selfie stick. Those few images are discussed in the selfie stick chapter.

question about how the selfie stick was demonstrated as a disruptive, faddish object.

Ethics

The ethical questions raised by my empirical work were in many ways similar to those encountered in other ethnographic work with most of them revolving around informed consent and anonymity. However, as I used a digital and mixed methods approach in some parts of the research, additional ethical issues have to be taken into consideration. I will therefore briefly outline the ethical aspects of my data gathering and analysis practice. My engagement with them is informed by literature and case studies (AOIR 2012, BSA 2002, Zimmer 2010) around ethical decision-making and the digital. In particular, I will discuss the literature around ethical practice in digital ethnography and social media scraping, both of which are ethical areas that continue to be discussed, debated and stabilised.

Although my empirical research discusses digital devices and demonstrations of disruption, much of my data has been generated from ethnographic approaches that include interviews and observation. To conduct this ethically, I produced a research overview sheet for interview participants to read and an informed consent form for them to sign. In my attempts to give the research participants agency, I also allowed the participants the right to choose whether they wanted to be named or made anonymous. And indeed, some participants did choose to be named when it came to signing the consent form, as they didn't foresee any problems with being named, as they were speaking in their official capacity as a representative of an organisation. However, for the sake of consistency and care, I have chosen to anonymise participants in the empirical chapters.

Ethics and social media data

When it came to analysing social media data, it became more difficult to make ethical decisions. At this junction, it is important to note that my empirical research concluded before the release of the British Sociological Association's *Ethics Guidelines and Collated Resources for Digital Research* in April 2017. This declaration is not intended to be an excuse for my ethical considerations, rather it is to situate my ethical decision making in a space where there was little information on digital research ethics that was truly applicable to research in Web 2.0 and 3.0 settings. This has meant that I have relied on a situated ethics approach. Stating that I have relied on situated ethics in a situation of perceived lack of other guidance does not mean that such an approach is superseded by the newly published guidelines. Indeed, the BSA guidelines and resources take into account situated ethics and ethics of care as an approach.

I gathered social media data from Instagram to conduct some visual analysis of selfie stick use and for some introductory research on Transport for London. This involved gathering data such as the image and the caption along with metadata from Instagram in early to mid-2015 by searching the hashtags #selfiestick and #tubestrike. I used a tool called IfThisThenThat (IFTTT)[33] that collected a random sample of Instagram posts containing the previously

[33] The process that I used to collect and analyse Instagram data is no longer available due to a change in Instagram's API policy in 2016. Bernhard Reider has a good summary of this problem and the implications for social research on his blog, *The Politics of Systems.* http://thepoliticsofsystems.net/2016/05/closing-apis-and-the-public-scrutiny-of-very-large-online-platforms/

mentioned hashtag. This data was then compiled into a series of .csv files that could be manually analysed and coded in a spreadsheet.

Gathering social media data invoked questions around privacy, consent and data protection. This was also complicated by the fact that I was collecting data not to analyse the humans responsible for creating the data, but rather, I was analysing the placement of a selfie stick in an image and, the public transport infrastructure used *instead* of the tube when there was strike action on the London Underground. Do you need to gain informed consent if the actor you are analysing isn't a consenting human? I argue not, but this becomes complicated when you seek to publish social media data as an example of a phenomenon. Issues around attribution and copyright become apparent, where informed consent may not be necessary; permission to use and publish social media data becomes necessary. Where I have analysed and referred to social media data, I have attributed the creator much like any other publication.

Due to the nature and attributes of IFTTT as a social media data-scraping tool, I was not able to scrape social media data from Instagram accounts that were set to private. This is not an attempt to paint a picture of opposed settings of public and private. As much literature on digital research ethics (Zimmer 2010) has outlined, it is difficult to justify this position of the public/private binary when approaching social media as a setting for research. Rather, we should accept that there are grey areas whereby some users may still make their account public, but with only certain publics in mind and similarly, by making their account private, they are making their data available to a *certain public* within their control. We must be attentive to this and try not to assume the level of publicity of social media data just like we should never assume that an academic paper is an intended public for a stranger's social media data. Where possible, I have asked for permission to publish social media data, and where I have considered the data from a situated ethics and ethics of care standpoint and considered it a low risk, I have published and attributed the data with an academic citation. This leads into ethical discussions around situated ethics and ethics of care.

Situated Ethics

As mentioned earlier in this section, the BSA's ethical guidelines annexe (2017) for digital research has a section discussing situated ethics and ethics of care in relation to digital and social media research. The annexe acknowledges that no two digital research fields are identical; therefore it is unlikely that a uniform approach to ethics would be suitable. This approach fits well with the STS orientation of this thesis in that it asks the researcher to consider the broader setting of the participants, and their interaction with non-human actors and, how the research may adversely impact their safety or perceived reputation. Suffice it to say; I received ethics approval from the Sociology Department to take a situated ethics approach in my research activities.

As an example of a situated ethics approach to my work, there have been circumstances where I have chosen to produce a written description of an image rather than publish social media data as an example, for reasons of privacy and consent. In particular, there is one example in the selfie stick chapter, of an image of someone using a selfie stick which appears to be a ‘creepshot' - or a picture that was taken without the subject's consent - of a person using a selfie stick in a gallery. In this situation, I could not guarantee the subject's consent and could not give appropriate ethical care to them. This has also been considered by visual social media researchers such as Anne Burns (2015) in greater detail, especially concerning the analysis and publication of visual social media data.

My research of the disruptive attributes of the selfie stick involved conducting a breaching experiment at the National Gallery in an attempt to further understand how people in-situ considered the selfie stick to be disruptive. I also took a situated ethics approach to this research activity, with particular considerations paid to the covert nature of this research to ensure that those I carried out the breaching experiment with along with those in the vicinity were not harm by the activity.

Conclusion

This chapter has described methodological approaches and challenges relevant to researching digital demonstrations of disruption In particular, I have discussed the multiple approaches to Actor-Network Theory - Post ANT(s) and Classical ANT - that I deploy in the empirical chapters. In regard to the digital aspect of demonstrations of disruption, I highlighted the challenges facing researchers in studying the digital as something that is multiple and fluid. I address this by using the heuristics of the digital as a setting, actor/assemblage and research instrument (Marres 2017). In order to conduct a digital ethnography that works with these heuristics, an approach such as Hine's (2015) that accounts for the multiple, unpredictable nature of the digital is required over more prescriptive digital ethnographic methods such as Pink et al (2016) and Murthy (2008).

The methods implemented in the empirical chapters contribute towards gathering evidence and examples of digital demonstrations of disruption. Further, the methodological standpoints described in this chapter, contribute to the ANT, post-ANT and ethnomethodological analytical frameworks such as problem solution relationships (Garfinkel 1967/1991, Neyland and Milyaeva 2016) and, problem amplification (Latour 1999) utilised in developing insights about chains of accountability and digital demonstrations of disruption.

Chapter 4: The digital as a setting for demonstrating disruption: Transport for London

Introduction

In recent years, rail services in the UK have been beleaguered by delays, and commuters feel they are losing time, rather than gaining it. One commuter, Matt Steel, who travels from Horsham, West Sussex to London for work decided to keep track of the delays to his two-hour journey from January to April 2016. By doing this, Steel discovered that only 37 per cent of his trains ran on time during this period, contrary to the rail company's claims of an on-time performance record of more than 80 per cent. "Between the beginning of January and mid-April I had lost more than 24 hours due to delayed or cancelled trains. And as I write in early May, that figure is now more than 29 hours, which doesn't include two days where I couldn't travel because of a strike," writes Steel in The Guardian

How can this be? As Steel has described, the train network that was once lauded for saving people time is now accused of taking time due to disruptions caused by strikes, infrastructure breakdown or, staffing issues. When the network of human and non-human actors supporting the train is stable, passengers are able to get to their destination without disruption. When the network breaks down, passengers face delays and are unable to travel from A to B as quickly as they would like to. In other places in the South-East of England commuters are also making their anger known at delays and overcrowding. To the east of London, commuters from Essex regularly use

Twitter to publish images demonstrating the overcrowding of their return trains from Fenchurch Street Station (@c2c_customers, Twitter 2016). And in Brighton to the south, commuters stage protests at the regular last-minute cancellations of their train services to London (Evening Standard 2016). In an extreme case of demonstrating disruption, a Brighton based animation studio used their talent and lost time on delayed trains by creating a viral video game, *Southern Rail Tycoon* (RamJam 2016, BBC 2016) which challenges players to cancel as many trains as possible by clicking on Southern Rail guards to prevent them boarding trains awaiting departure. Players are scored on how much money Southern Rail makes as a result of cancelled trains at the expense of commuters who have purchased season tickets.

These demonstrations of disruption occurring in Southeast England are worthy of investigation. These commuters demonstrate the pervasive, mundane disruption that occurs when a train is overcrowded, delayed or cancelled. They are extraordinary displays of rail services raising the ire of those who try to make use of them. In this empirical chapter, the focus will be turned towards the public transport communication infrastructure that many of these commuters may use as they continue their journey within London. In particular, this chapter describes and analyses the use of social media by Transport for London (TfL)[34], and how they proactively demonstrate disruption and conversely, how they respond to demonstrations from the commuting public. This chapter will follow the TfL staff that deal with customer inquiries and, the editorial staff that are making decisions on how social media ought to be used to notify the commuting

[34] Commuters may use both Southern Rail and TfL as they commute into and around London. The difference between the organisations is that Southern Rail is privately owned and Transport for London is a public organization governed by the Mayor of London’s office. The choice to focus on TfL was due to their maturity in using social media and their status as a public organization to gain access to their staff.

public about relevant events and issues. It will also introduce other actors such as third-party companies providing software that enables TfL to respond to social media and gather metrics on staff performance, commuter behaviour and trends.

What might demonstrations of transport disruption tell us about the ‘theatre of failure’?

As discussed in Chapter Two, the concept of the ‘theatre of failure’ takes forward some of the Science and Technology Studies concepts around public demonstrations (Schaffer and Shapin 1985) and the theatre of proof (Latour 1988, Collins 1988, Downer 2007) that exist to enrol a public in new knowledge or the safety of an existing practice. Similar to the ‘theatre of proof', the ‘theatre of use' refers to software demonstrations used to convince potential customers of the product's efficacy. The ‘theatre of failure' exists as a counterbalance to the ‘theatre of proof' and the ‘theatre of use' to explore how people demonstrate to others that a situation or an object does not work.   To do this, I touch upon three major concepts that occur within this research. These concepts have been observed to occur in the ‘theatre of failure’ for Transport for London when a new digital method for demonstrating or responding to disruption is introduced either by the commuter or by Transport for London. It demonstrates that the digital as a setting is rarely stable; it is continually being reconfigured as social media themselves are reconfigured. This usually sets off a loop of events that begins with configuring the user (Woolgar 1990, Grimes 2015) to adopt and use the reconfigured technology in a specified way, then using transactional data to measure the success of the reconfigured setting as a form of problem amplification (Latour 1999). This translation of transactional data to indicate the success of a reconfigured technology results in a form of problem/solution relationship (Garfinkel 1967/1991, Neyland and Milyaeva 2016) whereby the solved problems highlight other problems that may need to be dealt with by reconfiguring the ‘theatre of failure’ once more. This leads Transport for London staff and commuters into this loop once more. This loop is iterative, the ‘theatre of failure’ still remains within the digital setting, but some of its specificities and scripts change over time to suit the actors.

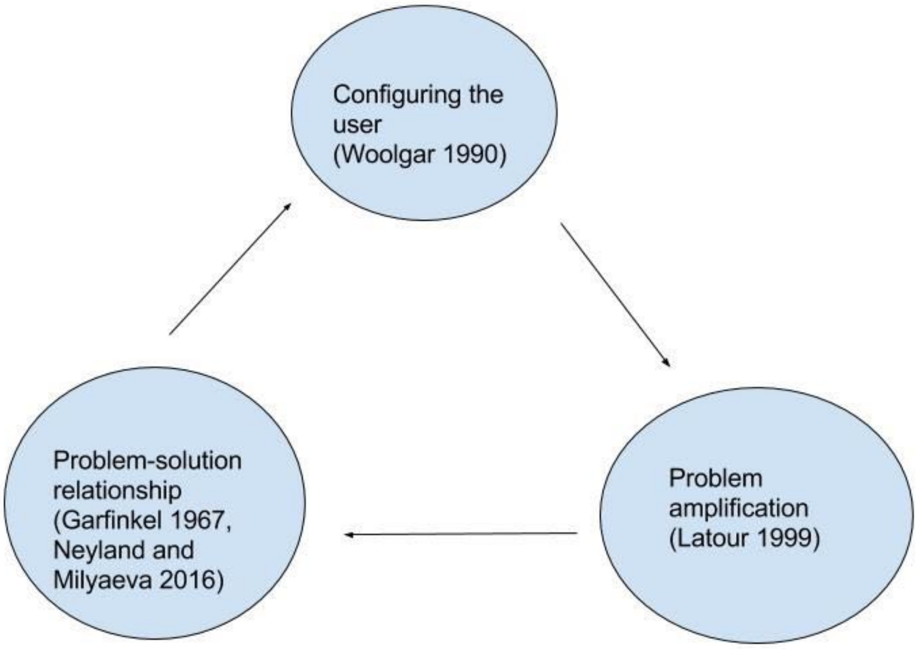

Configuring the user (Woolgar 1990)
Problem amplification (Latour 1999)
Problem-solution relationship (Garfinkel 1967, Neyland and Milyaeva 2016)

Figure 1: Diagram of the recursive loop of configuring users to a method of demonstrating disruption, which allows for problem amplification, which then leads to a problem-solution relationship.

Figure 1 describes how TfL’s social media staff and commuters are configured (Woolgar 1990, Grimes 2015) in the ‘theatre of failure’ by Twitter and social media management software companies. Commuters encounter the ‘theatre of failure’ through the configuration of Twitter, while social media customer service agents do so through social media management software. These different digital configurations of the ‘theatre of failure’, especially TfL’s use of social media management software allow for iterative actions to happen with the volume of qualitative and quantitative data gathered (Beer and Burrows 2013)

By describing TfL's use of Twitter and social media management software as a ‘theatre of failure', I will show how demonstrative tweets from commuters and their responses are metricised by TfL for performance review and auditing, workforce planning and, editorial decisions. I will discuss how this acts as a form of problem amplification (Latour 1999) that enables previous demonstrations of transport disruption to be performative in editorial decisions about how to create or respond to future demonstrations.

Finally, I describe how TfL has recursively reconfigured their customer service as a form of problem solution relationship (Garfinkel 1967/1991, Neyland and Milyaeva 2016, MacKenzie 2003) to make iterations to how they make demonstrations to enrol and stabilise commuters in the disruption as quickly as possible. I also describe how their problem amplification leads to a problem-solution relationship, whereby commuters are configured to use Twitter as a digital setting in new ways. I use the examples of TfL's introduction of a direct message subscription service and a customer service bot to describe how this works in a practical setting and how they hope these reconfigurations will improve their customer service.

But before launching into observation and discussion, I will briefly describe the field sites of TfL and Twitter.

Transport for London and Twitter as a field site

Transport for London is a worldwide icon. It is a prominent part of the visual landscape - it is the red double-decker bus, it is the London Underground and the tube map. It could be the most famous public transport infrastructure in the world.

Transport for London (TfL) is the non-profit, governing body of London's public transport services, which encompasses the underground (or ‘the Tube'), the overground, buses, riverboat services, trams, suburban rail services and even a rarely patronised cable car service. Additionally, they are responsible for monitoring traffic on London's roads. Approximately 28,000 people are working at TfL (pers. comm. 2017) in various ways to keep London's transport infrastructure running. Transport for London handles 24 million customer journeys daily and fields 130,000 customer interactions on social media each month (Gutierrez 2016). If this were a quantitative study, TfL would be considered to have a sample size large enough to make a substantial study. This is, however, a qualitative study with the volume of data mattering slightly less. But similarly, the volume of customer interactions that TfL deals with points to a high level of expertise in dealing with commuter demonstrations of disruption.

The TfL Online team is one of the few parts of the organisation that has an overarching view of the services and helps each portion of the business use social media in the most effective and appropriate way possible. TfL Online is not partial to any of the services - that is, they don't favour the tube over bus services in their decision-making. They have the role of determining policy and the overall strategy for social media channels for the different transport areas, as well as for public relations, marketing and the press office (Gutierrez 2016). When I first spoke to the Digital and Social Media Content Editor for TfL Online, he explained his role had the benefit of not being aligned with a particular transport service or role, which avoided politics amongst the different parts of the organisation. He said, quite often the different services do not need to communicate to one another, which leads to misunderstandings between the teams when they need to discuss those rare services in common. He also said his role was rare because it allowed time and space to reflect on the organisation's use of social media and develop best practice and social media strategy. Often those working day to day with social media for TfL, do not have the time or space to reflect on ways to improve their social media use.

One of these teams that TfL Online liaises with - the ones working day-to-day on TfL’s social media accounts - is the First Contact team. As the name would suggest, they are the first point of contact for tube, overground, Docklands Light Railway (DLR) and TfL rail commuters[35] getting in touch by email, telephone or social media. The team is based in TfL offices at North Greenwich in southeast London, and they deal with the many and varied queries and complaints customers have about TfL's services.

Customer service agents deal with queries ranging from train delays to stuck elevators, Oyster payment card suggestions to finding where to collect Tupperware left behind on the train. The customer service agents need an encyclopaedic knowledge of TfL or at least a comprehensive knowledge of where to find the right information. The team manager of the First Contact's

[35]. There is another team in TfL called CentreComm. They deal with communicating about roads and bus services - what TfL call ‘surface transport’.

social media team explained the expertise that customer service agents need to build up to work on social media. Customer service agents are not hired because they have social media experience; they are hired because they have customer service experience. When a new customer service agent starts with TfL's First Contact team, they must attend two weeks of classroom training and then be paired with an experienced customer service agent to listen in on telephone calls before starting to receive customer calls on their own. It is only once they have built up sufficient knowledge and expertise in taking customer calls and emails that they can apply to become part of the social media team.

But how did TfL start doing social media? Both the editor of TfL Online and the manager from the First Contact team - on separate occasions - told the almost folkloric story of how TfL started using social media in the early 2010's. Since the early days of Twitter, TfL had a twitter account that was active in communicating basic disruption information. As the manager of the First Contact team explains:

> "I guess it probably helps to go back in time a little bit to a year or two before the London 2012 games. They're quite pivotal to this. We first started exploring, first had a twitter account as a kind of experiment basis… called @LUTFLtravelalerts. So it was one twitter feed, and it was basically a supplement to broadcasting disruption… so very basic, you could sign in and get information on LU services."
>
> - Interview transcript with TfL customer service manager, 30 August 2016

However, TfL was acutely aware that the 2012 London Olympic Games was going to cause disruption, crowding and delays to commuters and visitors to the city. They needed a clear way of communicating real-time status updates to customers, especially to avoid overcrowding at certain times or locations throughout the Games. Additionally, they needed to accommodate the challenge of so many visitors, many of whom would be unfamiliar with the underground system. TfL then created Twitter accounts for each tube line and rail service, for buses and roads so to ‘empower customers to make better informed travel choices' (Gutierrez, 2016)

This social media effort for the 2012 Olympics was considered a success; so much so that the service continued and expanded. As of April 2016, there was 27 staff in the First Contact social media team. Of these 27 staff, four work on any given shift on a weekday, reduced to three staff per shift on weekends. There are three shifts across a 24 hour period: a day shift which runs from 6.45am through to 2:45 pm, an evening shift which runs from 2:45 pm to 10:45 pm and an overnight shift.

The number of customer service agents working with social media is likely to increase as more commuters and visitors to the city utilise Twitter and Facebook as means of contact. According to an Ofcom study from 2015, 72% of people in the UK have at least one social media profile. Another study commissioned by TfL reports that 11% of commuters get public transport service information from social media, in comparison to 70% of commuters who report finding service information from a website, and 63% who say their receive information from staff announcements at stations (Transport for London 2016b). Additionally, changes in the technology used to demonstrate disruption and respond to it are likely to increase the volume and complexity of enquiries received by the team.

As mentioned earlier, TfL does not directly use the Twitter or Facebook interfaces to collate, display and respond to customer interactions. It uses a third party 'social care'[36] software to work through customer complaints and enquiries. Later in this chapter, I will explain this software and its role in how disruption is demonstrated and responded to at TfL. The software as a device plays a large role in configuring customer service agents and their use of Twitter and social media (Woolgar 1990, Grimes 2015) when discussing transport disruption.

TfL is also indirectly configuring how their customers use Twitter. In 2016, Twitter changed its feed from a chronological list of tweets to an algorithmic feed, with tweets displayed in order of relevance. (Kantrowitz 2016) This led to TfL and Twitter collaborating on new ways to keep Londoners and visitors up to date on tube services with real-time updates from automated direct messages and bots. Further in the chapter, I will describe how this collaboration worked and how TfL uses Twitter to configure the customer towards automated and self-service information.

An introduction to Twitter as a setting for the 'theatre of failure'

Twitter is the main social media platform used to demonstrate disruption on the TfL network, whether that is instigated by the commuting public or by TfL staff[37]. Twitter allows for communication in multiple forms. This includes public tweets that are relevant to anyone who receives them and are similar to broadcasting information. It also includes interpersonal communication between one or more people, this is usually seen by conversations where recipients or participants

[36] 'Social care' is a poor term to describe what is essentially customer service, especially when 'social care' is also a term used to describe services on the boundaries of health and social work. However, 'social care' is the term companies marketing these social media customer service platforms use so from time to time, I will refer to them in this way.

[37] TfL also use Facebook for customer service to a lesser extent. They also use Instagram for marketing and public relations purposes and, LinkedIn for recruitment activities.

are incorporated into the conversation by mentioning their Twitter handle; this type of interpersonal communication can also take place via Direct Message, which is a conversation taking place only between named parties. Twitter also allows for communication that could involve a more social form of communication that is neither broadcasting information, nor is it merely a conversation between named people. These conversations where any user could join in or contribute are usually centred around a hashtag for an event or a subject area.

But these tweets can be analysed and used in many ways beyond its intended form of discourse. Consider the following composite of field notes and observations of online interactions between a commuter and TfL staff as an example of how a tweet might be read, understood, analysed or mobilised over the course of a few weeks.

It's the morning rush hour on a Friday morning in November and commuters are trying to catch a tube service on the Northern Line. The Northern Line is one of the services that form the backbone of travelling North or South across London. In the central portion of the Northern Line, it splits into two branches. The Charing Cross branch takes commuters through the West End to tourist hotspots near Soho, Oxford Street and Trafalgar Square. The Bank branch passes through the eastern side of central London, depositing office workers to London Bridge, The City and the Old Street ‘Silicon Roundabout' area. On any given weekday morning it becomes difficult for commuters to catch the tube, often waiting for two or three services to pass before they find a carriage which has space for them to embark. A commuter at Clapham Common has been trying to get into a carriage and has had three services pass by, all without space for her to get on board. The platform is getting increasingly crowded as more commuters attempt to catch these overflowing services. She wants to know why this is happening, so she gets out her smartphone, takes a picture of the overcrowding on the platform, opens the Twitter app and sends a tweet to @northernline to try to get answers.

At the First Contact centre in North Greenwich, a TfL customer service agent is on the day shift with three other colleagues, responding to social media messages from commuters on the morning rush. He has two screens open in front of him; the right one is taken up with an Internet browser with a programme that looks like an email inbox with many folders. This programme is a social media 'customer care'[38] programme that collates all of the social media messages sent to TfL's many Twitter, Facebook and Instagram accounts in reverse chronological order. This programme is also the interface from which customer service agents can write and post tweets. They do not use the Twitter website or app to write tweets. On the left-hand screen, he has the TfL website open on the tube line status page (which is also called 'the rainbow screen' - due to the resemblance of the different coloured tube lines to a rainbow). On this screen, he also has his Outlook email account open along with an instant messaging programme.

The customer service agent has been working his way through the inbox of tweets and Facebook messages since 6.45am. This inbox of tweets and posts

[38] Much like the phrase 'social care' mentioned earlier in this chapter, 'customer care ' is also marketing jargon to describe how social media management software that has a customer service focus. The phrase 'customer care' was commonly used by the company responsible for the software rather than TfL.

from other social media platforms is a third party ‘social media customer care' programme that looks much like an email inbox, they are displayed in chronological order, from most recent to least recent. Unlike an email inbox, these tweets and Facebook messages are not sorted by TfL service. Our customer service agent might bounce between queries about District Line delays, Oyster card questions and complaints about advertising on the tube. He marks the last tweet he responded to as resolved and the programme automatically displays the next tweet in the queue from the woman stuck at Clapham Common. He sees the picture of the overcrowded platform. Before writing a response, he consults the tube status on the TfL website on the adjacent screen and sees that the Northern Line appears to be running a good service. He then opens the instant messenger to get in touch with one of his customer service colleagues working from the London Underground Control Centre (LUCC) in Southwark. He asks them if there is any information that might shed light on what is happening. The agent embedded within LUCC has access to real-time information such as CCTV and tube line displays that may give more context to why the overcrowding is going on at Clapham Common.

The customer service agent embedded within LUCC responds a minute or two later, saying that the overcrowding is happening due to the knock-on effect of an earlier delay coupled with the fact that it is rush hour. They also tell him that tube services will soon be running more frequently so the problem will soon be resolved.

With this information to hand, our original customer service agent returns to the enquiry and starts typing a response to the commuter with the information he has received from LUCC, condensed in such a way that it makes sense but still conforms to Twitter’s 140 character limit. He sends the tweet and marks the demonstration as resolved.

TfL's response time correlates with the volume of enquiries received. During busy times such as the morning or evening peak, this may mean that it takes up to an hour to respond to a customer. By this stage, our commuter at Clapham Common may or may not have made it onto a tube service, at which point the response is not much use to her. However, the commuter's question and TfL's response is not useless to those considering travelling by tube from Clapham Common, who may choose to travel using an alternative route as a result of seeing the Twitter exchange. In any case, when the commuter sees the response she may consider that the end of the matter.

The performative work of Twitter demonstrations

However, the tweet lives on and it will live on for quite some time. It is at this point, and within the setting of Transport for London, that a tweet is not merely a tweet. The tweet will form one portion of a metric; it may be used for a performance review of the customer service agent's work within the ‘theatre of failure’. It could be copied and pasted into a PowerPoint presentation that describes the positive aspects of embedding customer service agents within LUCC. It could also be shown to Northern Line managers to highlight the shortcomings of the Northern Line service and the dangers of overcrowding during rush hours. And for our commuter, it's not merely a tweet either. It is a public way for them to keep TfL accountable to a standard of service and safety. In these ways, a tweet is a demonstration that lives on and morphs in many other ways.

Similarly, Twitter is not just Twitter. When considered in relation to TfL, it acquires functions specific to that setting. Take, for example, Twitter's shift from a chronological to algorithmic feed. It would have made little difference to a Twitter user who posts about topics relevant to their field of work or study. But in the setting of TfL, chronology and timeliness are essential functions of their deployment of Twitter for travel updates and information for commuters. How can the commuter be informed to ‘make better travel choices' if the information is presented hours after the fact? As we will see later, Twitter takes on two forms in relation to TfL: one as a setting for demonstrating and responding to disruption and, another as a business that they must work with to ensure a suitable digital setting for demonstrations.

Configuring the TfL customer service agent

Earlier in this section, I mentioned that Twitter configures how a commuter might see TfL tweets, in terms of being displayed algorithmically, rather than in chronological order. But conversely, TfL is configured by the customer care software as to how they see and interact with commuters on social media. When observing the customer service agent's use of the software in the Contact Centre, he mentioned that he did not see the tweets as belonging to Twitter. "It's more of an email inbox," he remarked. This is telling of how Twitter (the platform) is reconfigured in a social care setting comparative to other, individualised settings. As described earlier, the software is set up in such a way that tweets from all of TfL's First Contact owned accounts go into one big inbox; Twitter accounts are not separated or classified by tube line. One agent works from the top of the queue (most recent) down, another agent works from the bottom of the queue (oldest) up, another agent works in the LUCC, and another takes on the complex, more detailed enquiries such as those about payment. The aim is to get to ‘inbox zero' and resolve all of the enquiries within a set amount of time. This ‘inbox zero’ aim shows that for TfL, the ‘theatre of failure’ for public transport disruption involves addressing every customer query. By instigating an aim to meet ‘inbox zero’, it demonstrates that the TfL First Contact team considers themselves to be responsible for addressing these commuter demonstrations.

The social media management software company encourages this inbox zero configuration. At a workshop, the CEO described how it worked - while vehemently saying he wasn't prescriptive about the tool – and said the point was to try to get to inbox zero. "The more important thing is that you *try* to work to inbox zero," he said, so that organisations don't contradict the response times listed on their social media profile. TfL's First Contact’s Twitter accounts are listed as being ‘Responsive 24/7' while on Facebook, the Transport for London page is listed as typically replying 'within an hour'. This expectation that organisations will commit to their estimated response time is the foundation for the software being configured to facilitate the inbox setup. The fact that when one query is resolved, another one takes its place without requiring the agent to select another question further demonstrated how the software configures the agent (Woolgar 1990) to work towards inbox zero as quickly as possible.

The software was also set up to configure agents to work as accurately as possible. It had an inbuilt spell-check, along with the option for managers to blacklist phrases that contain profanities or other indicators of a lack of professionalism. In so far as the spell check was concerned, this configuration helped the agent out immensely as he was often right clicking on red underlined words to correct them. However, this configuration didn't assist him in an audit when his manager picked up that one of his tweets contained an error that involved a word that wasn't caught by the spell check because it was a homonym.

Configured metrication - software company ideals of how organisations would quantify qualitative data

As mentioned earlier in this chapter, Transport for London uses a programme to triage, respond to and, analyse the more than 130,000 social media posts they receive each month (Gutierrez 2016). TfL is a relatively recent, high profile customer of this programme. They made the switch in early 2016 after realising that their previous social media management service, wasn't able to handle the high volume of Twitter accounts, tweets and messages from other social media platforms. As a result of this switch, two of TfL Online's editorial staff were asked to give a presentation at the software company's annual European conference in London in September 2016. They were among airlines, utility companies and telecommunication companies invited to present case studies of how the company's products contributed to their organisation's success. One of the TfL Online editors suggested I attend the conference to understand a bit more about the company and to see how others used the programme. The day before the conference was an afternoon of workshops which consisted of demonstrations of the company's two main products.

I went to both demonstrations because at that stage I had only briefly seen the social media customer care software used at TfL during interviews. It was also an opportunity to see a software demonstration much like the medical imaging software demonstrations described by Coopmans (2011) in a similar setting. In comparison to Coopmans' experience, the workshops contained what seemed to be fewer smoke and mirrors, in that there was no selective obfuscation of the software's features and capabilities that participants were aware of. However, there was a large amount of prescription as to how users were thought to want to use both of the products as a setting for dealing with customer enquiries or conducting further analysis on data from their social media platforms.

The first workshop I attended focused on the company's social media data analysis programme - which is more complex than the software used by TfL to respond to demonstrations of disruption. The workshop did not follow a software demonstration route that has been encountered in ‘theatre of use' demonstrations described by Smith (2009) and Coopmans (2011), where someone might stand at the front and show how the software worked so that the audience might be able to imagine integrating it into their practices. Instead, this workshop went a step further than demonstrating and involved a role-playing group activity, where attendees sat around each table had to pretend that they were in the role of senior manager at one of London's suburban rail companies.[39] In the scenario, these senior managers wanted to use social media demonstrations from commuters to inform their decision-making on improvements to the rail company and its service. This example from the

[39] I didn't know that this exercise would be quite so close to my research question, so it came as quite a surprise to have this unfold. It also made for a few laughs when I introduced myself to the facilitator and other workshop participants.

demonstration shows how the software company uses workshops such as these to prescribe their use case for the software, which involves this problem amplification activity.

In framing this workshop activity, the facilitator introduced the participants to the two personas we were to take on: one was Simon, a senior marketing manager and the other was Anya, the head of performance[40]. The facilitator then asked participants to consider what kept these two personas up at night. For Simon, the senior marketing manager, he was kept up at night by a list of acronyms representing certain metrics: CSAT (Customer Satisfaction), NPS (Net Promoter Score) and CPA (Cost Per Acquisition). He was also concerned with the overall reputation of the rail company. In Anya's performance role, she was more concerned with the operations of the service and whether there were any incidents and how to adhere to rail company regulations.

The participants were given the task of considering how to use the software to make Simon and Anya's role easier; or at least answer the questions that kept them up at night. The participants had to come up with business questions - or research questions - to bring to the software. The company had already pre-filled the software with social media data – or what could be considered as ‘demonstrations of disruption’ collected over time.

But what to do with these demonstrations of disruption collected by the software company? How were we as participants expected to use them within the context of these personas that we were asked to adopt? What was interesting

[40] In this rail company setting, the head of performance is the person who is concerned with the performance of trains and railway infrastructure. Essentially, their main concern is ensuring that train services run safely and on time.

was how Simon (the senior marketing manager) was configured as a persona that cared strongly about metrics. This meant that in order for his job to make sense, he had to quantify qualitative social media data to fit into the marketing metrics that measured the train company and his role.[41] When the workshop participants decided on the questions they would use to interrogate the database on behalf of Simon (or Anya), they were then instructed to open up a demonstration session of the software on their laptops. From there they were to follow some instructions set out for them in their workshop pack to gain insights relevant to Simon and Anya.

When the participants opened the software, it was clear that Simon and Anya or those of their ilk would not be using the software to gain insight on their own. The programme is based on complex Natural Language Processing (NLP) software[42]. It is a complex system, which has pre-formatted and categorised Twitter data through NLP algorithms, but it requires a lot of expertise to be able to query the data. Someone using it has to have a clear idea of what they do and do not want to include in a search. Most of the participants muddled their way through using the product with a lot of pointers from staff who were hovering over people as they were attempting the task.

The facilitator then directed the participants to open another programme, which looked to be an easy to read, palatable version of the complex NLP output. It contained a dashboard with key metrics. It contained line graphs of the topics

[41] Our task was to determine how we could use the data and the software to help these personas ‘sleep at night’ and feel like they were doing their job well.

[42] Software company representatives told me they had recently acquired the social media management software to sidestep some of the complexity of their staple NLP products. The acquisition was intended to boost the social media management software's capabilities with NLP while putting on a user-friendly side to the NLP products.

contained within social media data to help the likes of Simon and Anya see at a glance what customers were tweeting. It allowed users to create data visualisations that could be emailed or dropped into a presentation. Part of this process allowed users to pull out examples of tweets to illustrate the point the visualisation is attempting to make. In a way, it is as though the problem amplification (Latour 1999) has rapidly gone full circle with the software. Tweets are gathered en masse and categorised by way of algorithm to produce a recognisable problem or theme. That problem or theme is then demonstrated through a chart but then also de-aggregated with one or two individual examples of the problem or theme pulled out for others to examine.

This example from the social media management software company shows how demonstrations of disruption made in digital settings are used and analysed beyond the initial instance. It shows how commuter demonstrations are able to form part of metrics for measuring the success or failure of a train company's customer service or performance. Indeed, the premise of the software is to help companies better articulate their problems to address them.

But how does this work in the settings that the software is deployed in? This can be explored further by returning to TfL's First Contact centre.

Metrics of demonstrations of disruption and problem amplification

The earlier claim that 'a tweet is not just a tweet' assumes that a tweet is used and understood in many different ways by many actors with differing motivations. The next obvious question to ask is: how is this so? What are empirical examples of this? To discuss how a tweet is not just a tweet, I will refer to two ways in which TfL compiles Twitter data into some key metrics as a form of problem amplification to enrol decision makers in finding and implementing solutions.

The first empirical example describes how metrics are used by the TfL Online team to set editorial direction for the team and also make decisions about the future direction for the tools and software used by the TfL First Contact team.

The second empirical instance places metrics right in the heart of TfL's First Contact team. This example shows how the team manager uses the analytics side of the customer care software to look at how the team and individuals have performed over periods of time. It will also describe and examine how this data is used for performance review purposes. Of particular interest here is how the first part of the example is an automated quantification of qualitative data, while the second part looks at how individuals do a qualitative assessment of qualitative data which still results in a quantitative, binary assessment.

These empirical examples will be viewed through the lens of problem amplification (Latour 1999) as a part of a problem-solution relationship. This shifts the focus on the concept of quantifying qualitative data to amplify and produce a recognisable problem. Once the problem is solved, it allows other problems to emerge and come to the attention of those responsible.

Coordinating the ‘theatre of failure’

Over in the TfL Online offices, the editor is using the data from the social media customer care software to find insight to understand more about the issues and subjects that commuters are discussing. By taking each tweet and categorising it thematically, he can see what commuters are talking about at certain times of the day and modify how customer service agents work accordingly. For example, at peak times, he might see a pattern of commuters discussing delays or overcrowding on services, so he will instruct customer service agents to be across the rainbow board or in contact with the agent in the control centre. Later in the day or after peak travel periods, he might see that commuters are asking more questions about payment problems, or more niche questions, which may not necessarily be so urgent. In doing so, the editor is aggregating many individual tweets to amplify and exemplify the existence of a recognisable pattern or problem to remedy it and move on to problems that develop or emerge. This quantification of qualitative data is an example of problem amplification (Latour 1999) as it gathers the data in such a way that it brings attention to a problem to generate (often) a qualitative solution.

In 2015, the large volume of tweets received by TfL's First Contact services cause a problem: its (now previous) social media management software was not able to handle or present the increasing volume of tweets for customer service agents to respond to them adequately. The specificities of the software also meant that it was difficult to work with multiple Twitter accounts at the same time within the same browser window. Statistics reflecting the increase in social media traffic along with the difficulty of using the software were amplified and led the TfL Online team to put together a case to procure the new social media management platform that they currently use.

Performative uses of data from the ‘theatre of failure: performance review and workforce planning

It is a Wednesday morning at Transport for London's First Contact centre, and I have come to shadow social media customer service agents go about their work and also ask more questions about how management use the social media customer service programme's reporting functionality. This is in comparison to the programme's inbox functionality which customer service agents use to receive and respond to commuter enquiries.

The customer service agent I'm shadowing has taken his lunch break, so it was time to ask the team manager more about how TfL used the reporting side of the software. Initially, the team manager said that he primarily uses the reporting side for performance review. He showed me how the landing screen for the reporting side is essentially a dashboard that reports on how many ‘actions' were taken by staff over a set period, with these statistics being represented in bar charts and pie charts. In the programme, an ‘action' is anything done to a social media post received in the inbox. It could be marking a tweet as resolved, it could be responding to a tweet or message, or it could also be tagging a tweet or post for someone else to action or look into further. The manager had the dashboard set up with a bar chart to show actions taken over a six-month period. Below that, there was a pie chart that broke down these actions by type to show what kinds of actions were performed most often.

The dashboard could be switched to show this performance by the entire team or by customer service agent. To show how this worked, the team manager brought up the dashboard profile of a customer service agent who was not working at that time. It showed that she had spent 700+ hours working on actions in the last six months, along with a breakdown of those actions within a pie chart.

The manager could also glance at a bar chart, look at the peaks and troughs and correlate a customer service agent’s performance to events that occurred where their volume of actions may have been higher due to a large-scale incident. Similarly, he would be able to tell when they worked an overnight or weekend shift based on a smaller volume of actions depicted on the bar chart. In this way, he was able to qualitatively or contextually read a quantitative rendering of social media data.

He then went on to describe how he uses the reporting section of the software to audit staff as part of his duties as their line manager. He did this by opening an Excel file, which powered a line management-reporting tool. This line management tool had a set of criteria against which a manager could score a social media customer service agent's response to a commuter's tweet. These criteria were: friendly tone, educating the customer, correct information, and good spelling and grammar (which was, incidentally, spelt ‘grammer'). Each of these criteria required the manager to give the customer service agent a mark out of five. Based on the mark given for each section, the Excel spread sheet in the background would calculate whether or not the customer service agent was passing the audit. If the customer service agent had passed the audit, the line manager was also offered the opportunity to discuss how the customer service agent displayed a ‘wow factor' in their response to the customer.

This line management audit activity is curious because it asks the line manager to manually score and quantify a single tweet, in comparison to other activities where an algorithm will quantify many tweets for a single insight or outcome. Similarly, in this line management setting, we see yet another way in which a tweet is not just a tweet. It is an example of someone’s work, a way of reviewing their performance against a pre-configured set of qualitative metrics, ending in a quantitative score.

This metrication of tweets also served a purpose for workforce planning. In comparison to the first field visit to the TfL First Contact Centre, I noticed on my second visit that there were more social media agents present - almost double. I initially put that down to the assumption that the first interview and observation session was held at the end of summer, a time where rotas and shifts had less staff due to holiday breaks. But the manager clarified that during the intervening time, TfL had hired more staff in the First Contact social media team because there had been an increase in the volume of social media engagement from commuters. He put this increased demand in staff down to the ways TfL encouraged commuters to get in touch via social media channels. This corroborated one customer service agent's insight that actions had increased since these contact channels were advertised on the tube. The contact page on the TfL website was also configured to open up directly to a Twitter or Facebook direct message conversation if the commuters were also logged into their social media account. By taking this increase in volume into account, the manager was able to take these factors and changes into account to make decisions about staffing. He was able to look at the volume of actions taken as a team and individually to determine that adding to the team could spread the load. In this way, the quantitative metrication of tweets can be used in a problem-solution relationship to counter any issues with having sufficient staff to respond to social media inquiries. Additionally, we can see within this workplace setting that a tweet is not just a tweet because each tweet equates to a task that a customer service agent must spend time working on to resolve. In this sense, a tweet equates to the time and money spent on agent resources.

This exemplifies work done by Garfinkel (1967/1991) regarding problems and solutions becoming a cycle of uncovering problems which in turn surface more problems. Or as Garfinkel writes, "The sense of the problem was progressively accommodated to each present answer, while the answer motivated fresh aspects of the underlying problem." (1967: 90)[43]. The editor of TfL Online identified the volume of tweets as a problem for the social media response process but had the context of the (now replaced) programme as a solution that worked for a time, but no longer solved the current problem. This allowed him to go on the recursive process (Kelty 2005) of identifying a new solution to a reconfigured problem. This solution then allowed him to address the problem in different ways, but with potential for more problems to emerge, such as the problem they soon encountered with a reconfigured Twitter timeline.

But how to grapple with this tangle of problems and solutions, with configurations and reconfigurations? This will be further explored in the following section on how TfL, Twitter and the social media management software configure their respective users in the 'theatre of failure'.

[43] It should be noted though, that the context of this citation from Garfinkel is describing an experiment with his undergraduate students where one student was asked to take on the role of a counsellor while another student sought personal advice from them. While Garfinkel's experiment is somewhat ethically dubious due to its deceptive nature, it yields fruitful insights that can be applied to the setting of TfL and social media use.

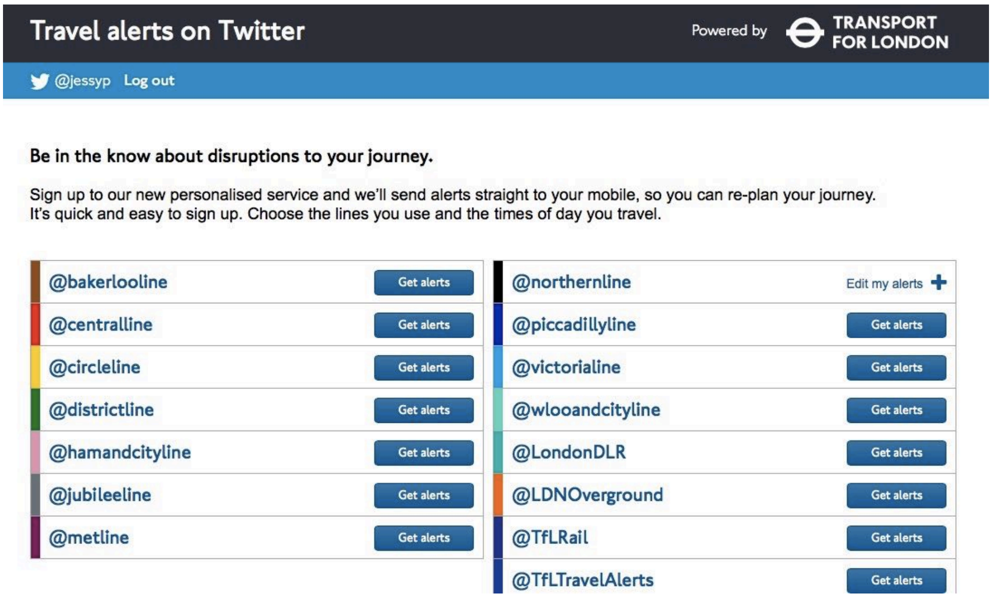
Twitter configuring users, TfL reconfigures workflow

In the time spent with TfL’s First Contact team, it was clear that changes were happening rapidly and often in their line of work. In each of my field visits, TfL staff were discussing features or tools they were in the process of rolling out to commuters using Twitter. During each site visit to TfL’s North Greenwich office, staff described the impact of Twitter’s feed changes on their ability to effectively do their work. The chronological order of tweets in a user’s feed configured commuters and TfL to expect timely travel updates to appear close to the top of the feed. When Twitter changed this by replacing the chronological feed with an algorithmic feed, both TfL and commuters had their ‘theatre of failure’ rendered unusable with travel alerts appearing at unpredictable places in the feed. It had caused minor chaos in a previously stable digital setting.

The ‘theatre of failure' faced a problem because TfL had configured commuters to use Twitter in one way to receive transport updates, while Twitter had reconfigured itself and its users to expect Tweets out of order. This, in turn, threatened to undermine TfL's ability to provide timely travel alerts to commuters. The situation posed a problem for TfL: how to continue using Twitter - because their customers were still using it - yet use it in a way that still allowed the public to access the information at the most relevant time?

At first glance, the reconfigured algorithmic Twitter feed seems to be a large problem for TfL's customer service provision. However, that was not quite the case. According to the TfL Online Editor, TfL's standing as a large, non-profit organisation with some Twitter advertising spend and some available technical staff allowed them to come up with an inventive solution: collaborate with Twitter (as a business) to reconfigure Twitter (as a platform) to allow commuters to receive timely updates on services.

I saw this solution when I went for my first field visit to TfL's North Greenwich offices. This reconfigurative solution of Twitter for TfL's benefit involved creating a direct message alerts service. Where previously, commuters would have to scroll through their feed for travel updates, they were able to subscribe to receive direct messages from the Twitter account of tube lines they regularly took when there were delays. As an example, a commuter who regularly travels on the Victoria line to get to and from work could subscribe to receive direct message notifications of delays from @VictoriaLine on weekday mornings and evenings.

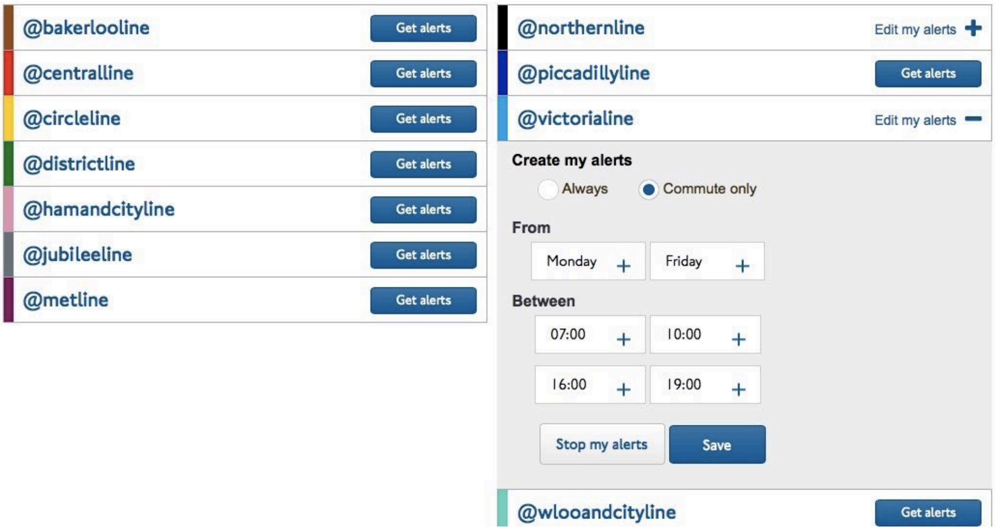


Be in the know about disruptions to your journey.

Sign up to our new personalised service and we'll send alerts straight to your mobile, so you can re-plan your journey.
It's quick and easy to sign up. Choose the lines you use and the times of day you travel.

@bakerlooline	Get alerts	@northernline	Edit my alerts +
@centralline	Get alerts	@piccadillyline	Get alerts
@circleline	Get alerts	@victorialine	Get alerts
@districtline	Get alerts	@wlooandcityline	Get alerts
@hamandcityline	Get alerts	@LondonDLR	Get alerts
@jubileeline	Get alerts	@LDNOverground	Get alerts
@metline	Get alerts	@TfLRail	Get alerts
		@TfLTravelAlerts	Get alerts

Figure 2: Screen capture of the Twitter travel alerts sign up page on the TfL website. This page allows you to select a tube line to subscribe to disruption alerts. (tfl.gov.uk 2016)



Create my alerts

○ Always ● Commute only

From

Monday + Friday +

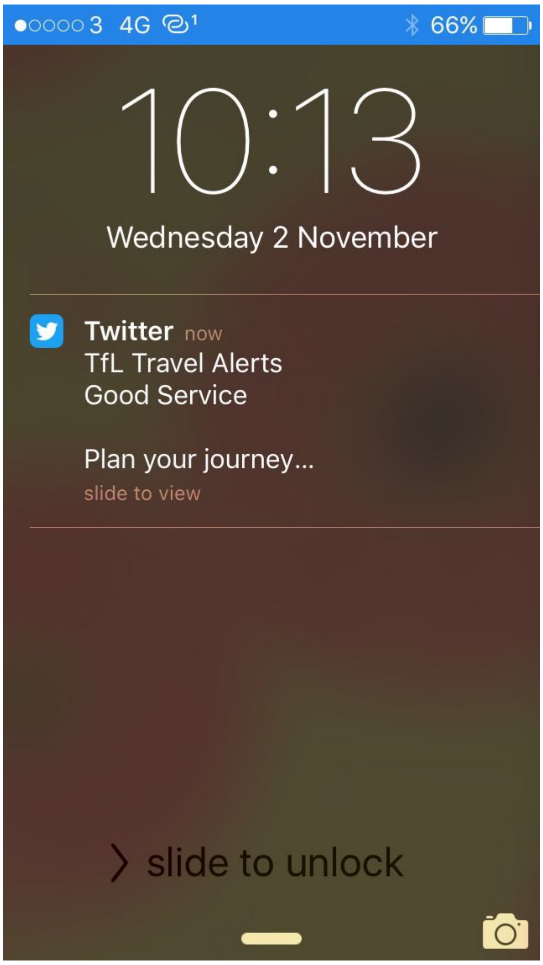
Between

07:00 + 10:00 +

16:00 + 19:00 +

Figure 3: Screen capture of the next step in the TfL travel alert sign up process. This step asks a commuter to refine their alerts to certain days and times of the week, if they wish. (tfl.gov.uk 2016)

The commuter would then receive direct message alerts anytime there were delays, including the severity and location of these delays. These direct messages would be sent out when the LUCC changed line status on the rainbow board. The direct message would continue to be updated until a good service resumed on the line.



Twitter
TfL Travel Alerts
Good Service

Plan your journey...

Figure 4: Screen capture of a push notification of a TfL travel alert on Twitter.

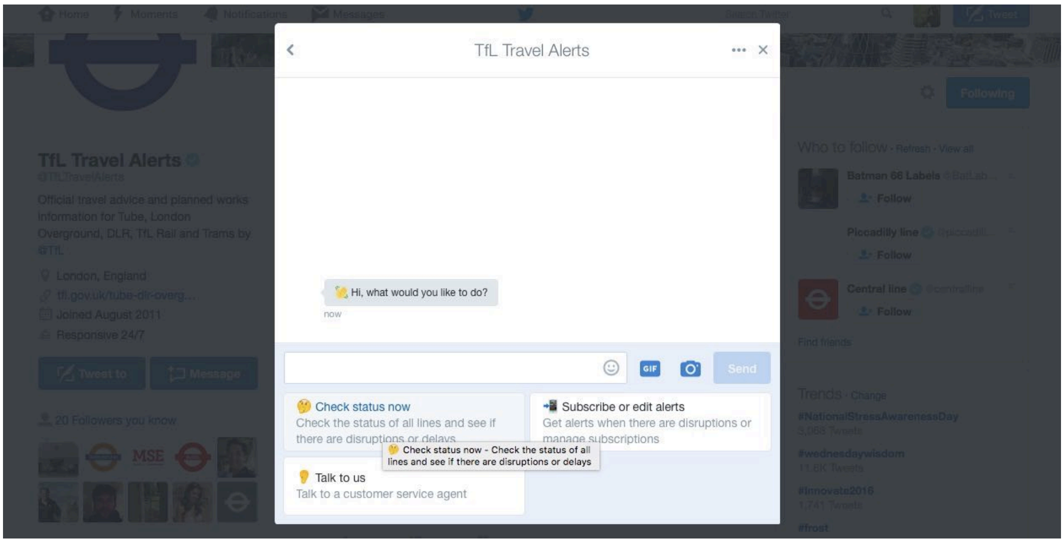
In this way, we see how TfL and commuters were configured in sending and receiving information on disruptions. Additionally, we see how TfL recognised this as a problem and worked with Twitter to come up with a solution by reconfiguring travel alerts into Twitter's direct message entity.

TfL configures users to take up new features.

TfL's collaboration with Twitter made space for reimagining and reconsidering how the transport organisation could reconfigure Twitter in more ways. The example of the reconfiguration of Twitter through direct message alerts was only the first example of TfL's reconfiguration of Twitter. In the second field visit to TfL's First Contact centre, there were more to be shown, only this time it was TfL that was reconfiguring the user, rather than Twitter.

I was just getting settled into a session shadowing a customer service agent when the manager came over to mention that the new bot service had been launched that day. The conversation turned to a description of how the bot service worked. The customer service agent explained that TfL and Twitter had developed a bot function that worked alongside the existing tweeting and direct messaging services.

The bot function could be accessed through the direct message function on the @TfLTravelAlerts Twitter account. Let's take the Northern Line as an example of how the bot would work. To begin, the Twitter user would click to send @TfLTravelAlerts a direct message, and in addition to the expected text box, a few other options would appear.


TfL Travel Alerts

Hi, what would you like to do?
now

Check status now
Check the status of all lines and see if there are disruptions or delays

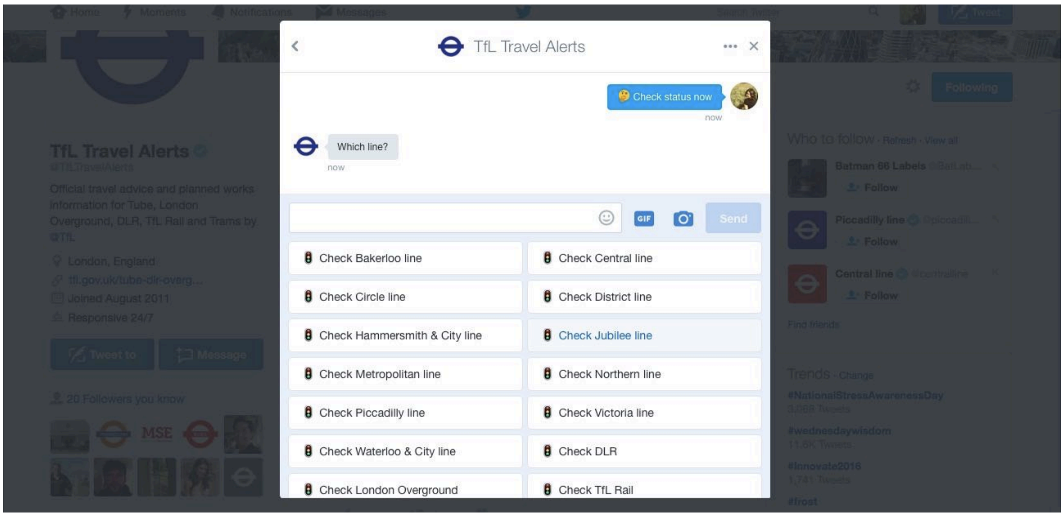
Subscribe or edit alerts
Get alerts when there are disruptions or manage subscriptions

Check status now - Check the status of all lines and see if there are disruptions or delays

Talk to us
Talk to a customer service agent

Figure 5: Screen capture of the beginning of a conversation with the TfL chat bot. At this stage, the chat bot is asking the commuter what they would like to enquire about. (@TfLTravelAlerts 2016)

Commuters could choose to inquire about the Northern Line by clicking the ‘Talk to Us' button to start a direct message conversation with an agent. Or they could click on ‘Check status now' to start a ‘conversation' with the Twitter bot about the Northern Line's current status. This would then present the commuter with a list of transport services to check. The commuter would then click on ‘Check Northern Line'.



TfL Travel Alerts

Check status now

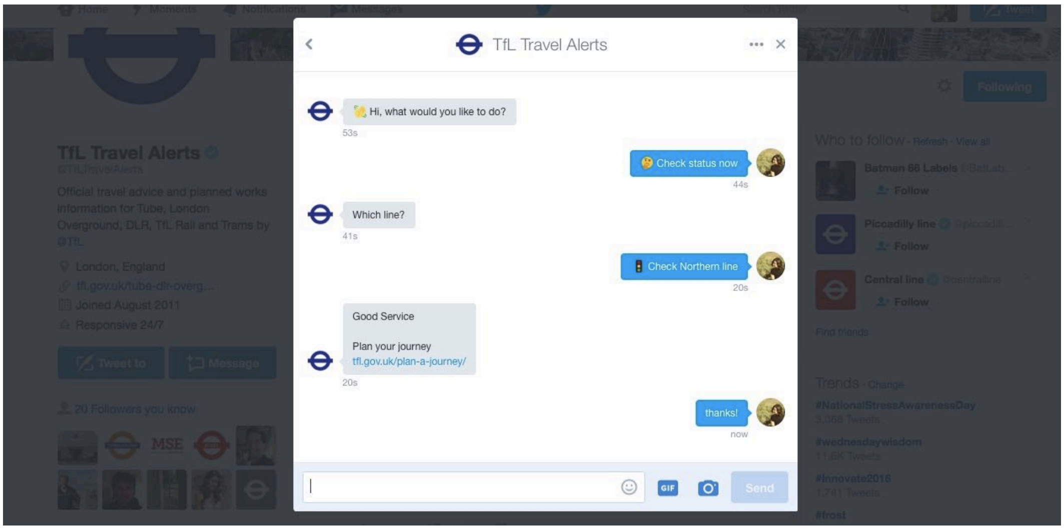
now

Which line?

now

Figure 6: Screen capture of the next step of the conversation with the TfL chat bot. In this step, the commuter has asked to check the status of the line and the chat bot is asking them, which tube line they would like further information about. (@TfLTravelAlerts 2016)

The bot will then check in with the rainbow board (or at least the data source that feeds the rainbow board) to see whether the Northern Line has a good service or whether it was experiencing any difficulties. Within a matter of seconds it responds with a status update on the service, as seen below:



TfL Travel Alerts

Hi, what would you like to do?
53s

Check status now
44s

Which line?
41s

Check Northern line
20s

Good Service

Plan your journey
tfl.gov.uk/plan-a-journey/
20s

thanks!
now

Figure 7: Screen capture of the remainder of the commuter - chat bot conversation. The commuter has asked about the status of the Northern Line. The chat bot has responded by saying there is a good service. The commuter has thanked the chat bot. (@TfLTravelAlerts 2016)

This introduction of a bot service to check status update - alongside offering the direct message alert subscriptions - was a choice made by TfL Online's team to encourage commuters to self-serve information that is easily accessible in the first instance. But how did this need for a move towards self-service become apparent? Referring to earlier discussion in the chapter about metrics and problem amplification, the TfL Online team reviewed the statistics of volume and types of enquiries received and hypothesised that a volume of them could be resolved through self-service. This would then free up time for customer service agents to attend to more time-intensive, individualised demonstrations of disruption, such as emergency scenarios, Oyster enquiries or lost Tupperware. This reconfiguration of Twitter is of interest because it shifts Twitter's use in different directions. Most importantly, it shifts the work done by both commuters and TfL staff. Where previously, commuters had to search through a tube line’s Twitter feed to see whether there’s already mention of the disruption, demonstrate a disruption and wait for a response, they are able to reduce that work to a brief conversation with a chat bot. And where TfL Staff were previously responding to many commuter enquiries about the same disruption, they now need to ensure that the information that the chat bot is using is correct. The introduction of the chat bot as an actor in the ‘theatre of failure’ reduces the work done by both commuters and TfL staff in demonstrating basic disruptions to tube lines, and frees them to demonstrate and respond to more of the edge case disruptions.

Bots and scripting

The bot service also reconfigured the notion of what a bot is on Twitter. Previously bots on Twitter were conceived as a nuisance entity that sent spam content. However, this new, tightly configured bot contains attentive, helpful attributes that aren't considered to be disruptive or worthy of elimination.

What is interesting to note here is how disruptive or fallible the Twitter bot became in the agents' workflow. The screen captures above were taken from a trial run done during the site visit while the customer service agent and the manager were explaining how the bot worked. Looking carefully at the last portion of the ‘conversation' with the bot, I thought I would be courteous to the bot and say thanks. This courtesy backfired because it did not stick to the bot's script. It was soon explained to me that if you go off-piste in the bot conversation, you get transferred through to social media customer care programme, and your message of thanks was flagged for the customer service agent to respond to.

There were a few other commuters being courteous to the bot, and this was starting to cause some low-level chaos for agents working in the programme.

There was nothing for them to respond to but they had to read and resolve them anyway, costing them time. This bot-related disruption was an example of how a demonstration needed to be made to identify and amplify a problem to come up with a solution to it. In this case, TfL First Contact was demonstrating the bot-related problems to TfL Online staff to devise a solution. [44]

This problem is reminiscent of Suchman's observations of the situated practices of humans trying to work a photocopier. Suchman (1987/2007) describes scenarios where people are trying carry out a task by following step by step instructions given by the photocopier's display. In some instances, the instructions were difficult to follow or they did not fit what the human was encountering. In this situation with the Twitter bot and the commuting public, we see a reversal of this, whereby the human is communicating something unexpected to the bot and it finds itself defaulting to unnecessarily referring the courteous end of the conversation to the social media customer care software. This example shows how human actors within the 'theatre of failure' are able to create disruption to non-human actors when the scripts are not stabilised or known. It also shows how non-human actors such as chat bots demonstrate disruption to TfL staff - who are responsible for maintaining the script that they run to - which in turn caused temporary mundane disruption to TfL staff.

Conclusion

In this chapter, we have seen empirical examples of how Transport for London has used social media as a setting for a 'theatre of failure'. By using the

[44] A few months after my field visits, I checked in with TfL First Contact Centre staff to see whether this problem of commuters going off-script had been resolved. They responded, "This has been fixed although there can be times where these may appear intermittently although it is quickly rectified" (pers. comm 2017)

heuristic of ‘digital as a setting’ we have been able to see how the specificities of the setting matter in understanding how commuters and TfL staff go about demonstrating disruption. The empirical examples have shown how demonstrations and scripts are modified when the specificities of the setting are modified. And through these examples, we have learned that this digital setting for ‘theatre of failure' is not a stable or static entity. It is not stable or static because Twitter is not a stable setting, as evidenced through their shift from a chronological to algorithmic feed. This meant that TfL had to adapt their ‘theatre of failure’ with the help of Twitter in order to continue demonstrating disruption. But it is not solely Twitter that changes. TfL or commuters could choose to leave Twitter as a ‘theatre of failure’ in favour of many other digital settings.

The example of TfL's 'theatre of failure' shows that it goes through an iterative loop from configuring the user to current arrangement to using the data generated in the demonstrations to amplify any problems (and indeed any successes) that may be happening. This process of problem amplification is used to enrol people into creating solutions that iterate and improve demonstrations and responses within the ‘theatre of failure'. Users are then configured in this modified ‘theatre of failure', and the loop continues.

We saw this process enacted in how TfL modified the ‘theatre of failure' for their staff by replacing the social media customer care software so that a higher volume of demonstrations could be dealt with. We also saw it enacted with commuters when TfL and Twitter set up a direct message subscription service and a customer service bot so that self-service information about the current public transport status was available, allowing customer service agents to attend to other enquiries.

What might this loop mean for the reconfiguration of demonstrations? For TfL, this has meant that their demonstrations of commuter disruption have gone from being private to public to personalised. In the private, pre-social media phase, TfL staff describe a process where commuters could telephone, write or email the organisation to discuss a disruption or ask for a refund. In the public phase, we see this process replicated in a digital setting, where onlookers are able to be part of the audience being demonstrated to. This reconfigures the demonstrations to be something that informs all audiences of a disruption, but holds TfL to account for it. The publicity of these demonstrations means that TfL must be attentive to them. Lastly, in the personalisation phase, we see commuters either choosing the disruptions they wish to have demonstrated to them by direct message notification or by interacting with a chat bot. Commuters need not interact with a human actor about public transport disruptions.

But what is helpful to note about these reconfigurations of demonstrations of disruption is that much like the history of the web, each iteration does not replace another. Rather, they sit alongside one another. Just as Web 1.0 static web pages sit comfortably alongside Web 3.0 Internet of Things objects; so too can a commuter equally call TfL to demonstrate a transport-related disruption as readily as they can refer to a Twitter chat bot. How might the observations and empirical examples from observing demonstrations of disruption through TfL’s ‘theatre of failure’ on Twitter help us observe and understand other instances of demonstrations of disruption? This chapter helps describe how we might recognise other instances of digital settings being used in configuring users to demonstrate disruption or respond to disruption through problem amplification. The next chapter will pick up on problem amplification and use the concept to critically evaluate how social media demonstrations effectively enrol citizen consumers in potential cyber security disruptions

Chapter 5: The role of demonstrations in performing cyber security in the UK

Introduction

On a rainy Tuesday evening in late January, I entered the basement room of a pub near London's Oxford Circus. I wasn't certain what I was getting myself into when I was told about this monthly hacking meet up via a Slack[45] message from a colleague of mine who we will meet in this chapter[46]. My colleague suggested that this meet up would be of interest to me based on my interest in demonstrations of cyber security and disruptions.

The room was full of people there for the monthly DC4420 meet up. The DC4420 meetup is a local event spawned from the DefCon hacker conference. The numbers are a nod to phone phreaks and describe the location of the meetup using the local telephone code. When I arrived, the hackers were taking it in turns introducing themselves, their interests and explaining why they were there. The majority of them said who they were, where they worked (although some were more forthcoming than others about this) and what they did within the information security or cyber security sectors. Two men standing on a

[45] Slack is a form of social media for teams or work groups. It allows people to send messages to others on 'channels' based on a pre-determined theme.

[46] While completing this PhD thesis, I worked as a researcher at a digital agency that specialized in the public sector digital transformation. My colleague does contract work for the same agency, conducting 'penetration testing' for clients to ensure that the services are built and used to ensure cyber security. After performing the testing, he also spends time analyzing and communicating security flaws to clients (particularly IT staff and management level staff) in order to prevent behavior (such as insecure password practices) that could increase the chance of a cyber attack occurring. He had been working in the IT sector for 20 years and started specializing in cyber security 10 years into his career. He also does cyber security training for workplaces and some public speaking at cyber security events. While we work in the same company, our projects do not overlap. Throughout this chapter, I am referring to him as 'my colleague' to retain anonymity, and for the sake of brevity. The conversations with him that I refer to all happened within an interview setting, rather than a participant observation setting.

slightly raised platform in the corner of the room were compering the evening. This group of predominantly men meet in this basement room once a month to see a talk from someone in the hacker or information security (or commonly abbreviated to 'InfoSec') community.

At this month's meet up, there was a talk from a researcher about the Internet of Things regarding security and safety. He was talking about the different ways to hack an Internet of Things enabled car. He referred to the car components that could be hacked as 'attack surfaces'. In this male-dominated environment, I stuck out as there were only one or two other women in the room, one of whom was also a PhD researcher with a focus on the social psychology of hackers.

It didn't strike me until a few days later that this event - held just blocks away from the Royal Institution - was reminiscent of the public scientific demonstrations held there by gentlemen scholars in the 17th and 18th centuries (Shapin and Schaffer, 1985), right down to the ratio of men to women. This group came together because they wanted to see the latest advances in hacking and InfoSec. They presented in this space because they wanted to show their work to peers. They also wanted to enrol others in the new knowledge they had discovered. In short: they demonstrate potential disruption and spend time debating and discussing these disruptions and broader issues in the cyber security profession, such as corporate responsibility for maintaining cyber security. One example of this was the presentation about the possible 'attack surfaces' on an Internet of Things enabled car. The question and answer portion of the presentation soon turned towards how manufacturers could be held responsible for releasing products with attack surfaces and other vulnerabilities.

But what is the point? In this setting, the intentions behind this hacking are not sinister, and it is not strictly activism in the sense of how hackers are typically portrayed with allusions to Anonymous or Wikileaks. These hackers rarely hack to make a political point - or at least, not a partisan political point. They wish to demonstrate flaws in networks, objects and websites, so the personal details of consumers don't get hacked, a mundane disruption if ever there was one. But is this seemingly simple rationale the only one driving hackers and the cyber security profession?

This chapter digs deeper into demonstrations around cyber security and the actors demonstrating the potential for disruption by way of data breaches or DDoS attacks. We will visit a Twitter account using humour to demonstrate the potential disruption of IoT-enabled everyday products. In contrast, we will then look at an explainer video from a large technology company that attempts to demonstrate and define the IoT as convenient or simple. By examining this, I want to compare corporate, cyberbolic (Woolgar 1999) definitions of the IoT to the demonstrations of potential disruption from the cyber security profession.

We'll visit the blog of a cyber security professional that demonstrates the disruption of a database storing personal data from an Internet of Things toy. And lastly, we'll find out more about the blogging work that the recently formed

UK Government’s National Cyber Security Centre is doing to demonstrate the ways that citizens and businesses can prevent disruptions.

These demonstrations are performances and are performative and informative. This chapter looks at who they are seeking to inform - that is, who they are audiencing in their ‘theatre of failure' - and how their demonstrative performances are understood and acted upon. Crucially, this chapter will focus on the ways they demonstrate these disruptions in a digital setting via Twitter and blogging. In particular, it will show how Twitter is used to signpost people to demonstrations of cyber security disruption occurring on blogs, YouTube and online news websites, where demonstrators have more time or word count available to carry out these demonstrations. This chapter will focus on the work done by demonstrating cyber security disruption on blogs.

In this chapter, I explore how the Internet of Things (or IoT as I will often refer to it) is a group of digital actors that are demonstrated in the digital setting. I focus on two narratives at play around the Internet of Things. The first is promoted by corporations and entrepreneurs and fashions a story that a world or lifestyle incorporating IoT devices leads to extreme convenience (Shove 2004). The second narrative is advanced by the cyber security profession and describes IoT as a security risk often referred to on social media as ‘the internet of shit'[47], which describes the range of products that are IoT enabled for no discernible reason. These demonstrations also highlight the lack of care that has been taken to ensure these IoT objects are secure. It is this second narrative around

[47] This is a common term used by people who are critical of the Internet of Things. There have been many times when I've been discussing this research with people, and they've said, "Jess, you do know people call IoT the ‘internet of shit'?" So while it is a colloquial way to describe this, I will refer to this only when specifically talking about the Twitter account of that name (@InternetofShit) or in a verbatim quote.

IoT products - that they are insecure actors - that threaten the material and social arrangement (Law and Ruppert 2013) of cyber security.

The empirical focus of this chapter is on Internet of Things related disruptions that take two forms: botnets and data breaches. In each of these cases, disruptions are demonstrated as events that are produced in order to prevent them from recurring or; they are demonstrated as events that are curated to raise awareness of measures that could be taken to avoid them. As will be discussed further in this chapter, these demonstrations occur as a means of mediating or enrolling actors (Michael 2017, Callon 1986) into the problem at hand. In particular, the demonstrations involving botnets are intended to enrol consumers to ensure the security of their IoT products so that they won't be co-opted into botnets. The demonstrations involving data breaches are deployed as a cautionary tale to enrol manufacturers and developers to take better care when designing the products and their supporting infrastructure to ensure the security of consumer data.

Not only is the term ‘Internet of Things' in itself vague and problematic, so is the network of actors who make up the hacking and cyber security profession. I will spend the first portion of this chapter defining terms surrounding the Internet of Things and hacking to develop working definitions for this research.

I then focus on how this compares to the ideas around testing and tinkering put forward by Pinch (1993) and Knorr (1979). I also look at the reasons given by the white hat[48] community for hacking and demonstrating security flaws in IoT

[48] In hacking circles; there are white hat, grey hat and black hat hackers. White hats are those who do non-criminal hacking while black hats are conducting illegal activity with their hacking.

objects, alongside the responses of manufacturers, government regulators and consumers. It will pose the question: do these demonstrations within a theatre of failure effectively highlight issues of cyber security? Additionally, it will ask if the issue public of the hacker community is the best public to demonstrate this disruption to encourage manufacturers to design more secure IoT products. Is there scope for industry organisations or regulatory bodies to more effectively demonstrate the potential for disruption and create a visible chain of accountability?

Describing the Internet of Things and cyber security

Before jumping headlong into these demonstrations, it is important first to define some of the cyber security jargon we will encounter in the course of this chapter. My guide in this world of hacking, InfoSec and, cyber security is a colleague of mine, who we met at the start of the chapter. He is a penetration tester - more commonly known as a pen-tester - a hacker who is paid by a company or organisation to proactively seek out internet security risks that a malicious hacker could exploit. Pen-testers are also known as ‘ethical hackers'. He then writes reports highlighting the security risks facing a company and highlighting how they could avoid them in the future. A lot of the time, this involves reiterating the need for employees to use strong passwords.

My colleague is frank, sarcastic, cynical and exasperated at the state of cyber security, as will become evident later in the chapter, but his experience in the hacking and cyber security community places him well to help define the terms and add much-needed insight from the standpoint of a hacker.

Grey hats inhabit the grey areas between legality and illegality with their actions. These varieties of hackers will be discussed in more detail further in the chapter.

‘So, Jess, how are you going to describe the Internet of Things in your PhD?' my colleague asked as we completed an interview about botnets co-opting IoT products for DDoS attacks. We had just been discussing the difficulty in defining the Internet of Things. The definition changes in emphasis and technicality depending on who is asked and how they view the Internet of Things. He also knew that the definition of Internet of Things that you go with ends up defining the scope of what ends up being discussed and investigated.

‘I think I’m going to go for the simple, non-marketing definition,’ I responded.

Technical definitions versus marketing definition

To go for the ‘non-marketing' definition is a bit of a misstep as the ‘Internet of Things' is commonly used as a marketing term to describe the network formed by an everyday object that could now connect to the Internet and other similarly enabled objects. However, that could mean anything from a kettle or a light switch to something more sophisticated such as fitness tracker, or a car. The Internet of Things is a catchall marketing term that could easily fall into the category of ‘cyberbole' [49](Woolgar 2002), around the internet and its utopian capabilities. But what about a non-cyberbole definition? According to Greengard (2015), the Internet of Things consists of devices or things that have:

> "… a unique identification number (UID) and an Internet Protocol (IP) address. These objects connect via cords, wires and wireless technology, including satellites, cellular networks, Wi-Fi, and Bluetooth. They use built-in electronic circuitry as well as radio frequency identification (RFID) or near-field communications (NFC) capabilities that are added later via chips and tags. Regardless of the exact approach, the IOT involves the movement of data to enable processes from across the room or somewhere on the other side of the world."

[49] Woolgar (2002) describes cyberbole as ‘the exaggerated depiction (hyperbole) of the capacities of cyber-technologies’

Dodge and Kitchin (2009) do similar work in defining objects implicated in the Internet of Things as ‘codejects’ and ‘logjects’. They define the Internet of Things as:

> “…using technologies of RFID tags and electronic product code (EPC) databases, makes objects uniquely identifiable, inherently trackable, and potentially communicative of their status across distributed networks. In much the same way that the location of a website can be `looked-up' through its unique domain name from anywhere on the Internet, it is envisaged that the `Internet of Things' will facilitate the same for any tagged object. It is essentially a universal indexing for anything and everything that matters and a mechanism by which objects can connect to, transfer, and process information with each other and people.”

Dodge and Kitchin's work (2009) conceptualises and explains how the Internet of Things may work in a retail supply chain or domestic setting (especially with the concept of smart kitchens). However, they do not touch upon some of the negative aspects that we will be encountering in this chapter such as ensuring the security of the codejects and logjects consumers are now finally placing in our homes and working environments, almost a decade after their initial work.

The Internet of Things is a marketing term intended as the first stage in a broader concept of the ‘internet of everything'. The networking technology company, Cisco puts forward a definition of the Internet of Everything that describes ‘a business opportunity’ comprising ‘the networked connection of people, process, data and things.'(Cisco 2013) Cisco also argues in their promotional materials[50] that 'The benefit of IoE is derived from the compound

[50] The definition of the ‘Internet of Everything’ that Cisco envisions will be built atop the ‘Internet of Things’ was also described in their Frequently Asked Questions website as “The Internet of Everything represents the business opportunity that the new brand campaign addresses.” However, the website also states that the Internet of Everything as an architecture or trademark “is not solely owned by Cisco”

impact of connecting people, process, data, and things, and the value this increased connectedness creates as “everything” comes online.” (Cisco 2013)

But how beneficial is it from the perspective of consumers to have everything come online? And how can everything within the Internet of Everything be secure? Most importantly, to whom is it helpful to connect people, process, data and things?

Object, devices or products? How to describe the ‘things’ of the Internet of Things?

It is tempting to call the ‘things' within the Internet of Things ‘object' or ‘devices'. However, to call it an ‘object' would be to walk into a discussion about object-subject relationships and agency, something that there isn't space within this research to enter into. Similarly, by calling the ‘thing' a ‘device', there is the danger of walking into an unhelpful discussion around terminology. Would I mean device regarding ‘assemblage' (Latour 2005), ‘dispositif' (Foucault, 1980), market device (Callon 2007, Muniesa, Millo and Callon 2007) or ‘apparatus' (Ruppert et al. 2013). This discussion would detract from the research at hand. Within this research, I will be describing IoT ‘things' as ‘products'. By doing so, I will be emphasizing how IoT products do not appear from the ether; instead, they are actors[51] that are designed, produced and made by manufacturers for commercial purposes to be introduced to a pre-existing digital network by the consumer. By referring to them as products, I also want to highlight how their features and capacities are negotiated in this production process. Similarly, these products are produced with an ideal user and use cases in the designer’s

[51] I use the term ‘actors’ here in the Actor-Network Theory approach to granting agency to things. As produced and designed as IoT objects are, they are agential when considered in relation to humans and other non-humans.

mind, but have real users who may encounter and use the product in completely different ways (Akrich 1992).

What is a hacker?

In this research, there are two types of hackers discussed. Hackers go by a lot of descriptors, but rarely are these titles self-assigned, rather they are designated by others, unless it is a professional designation, much like a job title. Kelty (2008) echoes this in a description from one of his fieldwork participants who said, "You are a hacker when another hacker calls you a hacker." This situation where hackers are reluctant to define themselves but dependent on their audience to recognise and identify them is similar to Goffman's (1959) observations on maintenance and expressing control or misrepresentation:

> "Sometimes when we ask whether a fostered impression is true or false we really mean to ask whether or not the performer is authorized to give the performance in question, and are not primarily concerned with the actual performance itself. When we discover that someone with whom we have dealings with is an impostor and out-and-out fraud, we are discovering that he did not have the right to play the part he played, that he was not an accredited incumbent of the relevant status." (Goffman 1959, p.66)

Curiously though, Goffman writes about these descriptors concerning people who are deliberately deceptive, such as someone impersonating a trusted professional such as a doctor, whereas hackers are reluctant to classify themselves due to the fact they may be identifying as engaging in (potentially) criminal activities.

There are a number of ways to classify hackers. *Script kiddies* are novice hackers who tend to run pre-written scripts of code to create botnets and DDOS attacks (Mead, Hough and Stehney 2005, Arbaugh, Fithen and McHugh 2000).

Script kiddies tend not to be able to understand how these scripts of code work, and are looked down on by more experienced hackers. Kelty (2008) describes script kiddies as ‘teenagers who perform the hacking equivalent of spray painting’. Unsurprisingly, the term ‘script kiddie' is not one that someone would happily self-assign as it denotes novice status in the community.

Black hat is term perhaps more familiar to the non-hacking community to describe someone who hacks for malicious reasons (TechTarget 2017). Similarly, *grey hat* refers to someone who errs on the side of illegality when carrying out their hacking. It is also a term that is usually designated by someone other than that hacker. *White hat* refers to someone who hacks within the bounds of the law. This name is commonly self-assigned.

A *pen-tester* is short for ‘penetration tester', a white hat hacker who is paid by a company or organisation to proactively seek out internet security risk that malicious hackers could exploit. They are also known as ethical hackers. Technically, they are breaking the law; save for the fact that they have signed waivers outlining the permission their clients have given them to carry out this kind of work.

Professional organisations or certification bodies such as CREST accredit ethical hackers by running a certification scheme, which requires pen-testers to pass an examination and have spent a minimum amount of time working within the industry. For example, someone who is certified (as opposed to lower levels of ‘practitioner’ and ‘registered’) usually has a minimum five years of experience and can lead a team of less experienced pen-testers (CREST 2017).

The bulk of this chapter will describe how white hat hackers and pen-testers demonstrate the disruption or the potential for disruption caused by script kiddies, black hats and grey hats.[52]

Demonstrations of hacking disruptions

Although, I have described the cyber security field, along with InfoSec or ethical hacking professionals, and some of the ways they demonstrate disruption in face-to-face situations, my focus is on how they demonstrate cyber security disruptions in digital settings. Many of these demonstrations occur when a cyber attack such as WannaCry in 2017 which targeted vulnerabilities in computers running older, unsupported versions of Windows operating systems, or Dyn cyber attack in 2016, a botnet made up of insecure Internet of Things products that then carried out a DDOS attack[53] on major websites such as Twitter and Netflix. The potential for these cyber attacks to occur are often demonstrated by cyber security experts ahead of time. In the case of the Dyn DDOS attack, cyber security professionals and press (Motherboard 2016) along with the US Government (US-CERT 2016) were already aware and publishing warnings that a script for creating the botnet had been made publicly available and there was a likelihood of IoT products being involved in cyber attacks.

[52] A quick word on women in the hacking community: Women make up 10% of the cyber security workforce (Dallaway, 2016). I asked my colleague about the lack of women in the hacking community, and he said it is a problem. He cites the common reasons given for there being fewer women in the tech industry - lack of encouragement for women to enter and remain in STEM subjects, hostile working environments for women - with these factors being ‘on steroids' in the cyber security profession. While he freely acknowledged these problems, he indicated that he did not have any solutions to this. As a feminist STS scholar, I cannot help but wonder how diversity in this sector - not just regarding employing or including more women - could help to demystify it to the general public and organisations that could consider using their services.

[53] DDOS is a form of Denial of Service attack. Denial of Service means any activity that disrupts or prevents someone from using a telecommunications service. These attacks could be as rudimentary as repeatedly calling a telephone number to prevent people from using it. A DDOS - or distributed denial of service - attack is a denial of service attack carried out by many devices across many locations. Dyn, is a domain name server company that owns and sells IP addresses for websites. Dyn’s clients were targeted in this attack.

But if experts knew that cyber attacks involving IoT products were imminent, then why weren't owners of IoT products demonstrated the potential for their products to cause disruption so that they might take necessary preventative steps in ensuring their products weren't co-opted into a botnet? In this chapter, I explore the argument that demonstrations of cyber security disruptions do not meet and enrol audiences of internet users and IoT product owners who could play a role in minimising cyber security disruptions. I also explore the argument that consumers form audiences that receive demonstrations of IoT-related convenience and utility, far more often than demonstrations that highlight potential cyber security risks related to the Internet of Things. The first stop on this exploration of cyber security demonstrations of potential disruption is a Twitter account that makes fun of the proliferation of Internet of Things products.

The @InternetofShit: a digital demonstrative catalogue of IoT disruption

One of the main 'theatres of failure' where IoT disruption - both the malicious and the tinkering kinds - is demonstrated is on a Twitter account called @InternetofShit. This account acts as an unofficial newsfeed for all things related to IoT.

The twitter account has a large following (245,000 followers in October 2017) and often prompts responses, both serious and humorous. From my analysis and following of this account, I have found that this Twitter account is a focal point of IoT critique for the non-hacking tech community, or those with interest in technology but none of the technical expertise to engage with the technology through hacking.

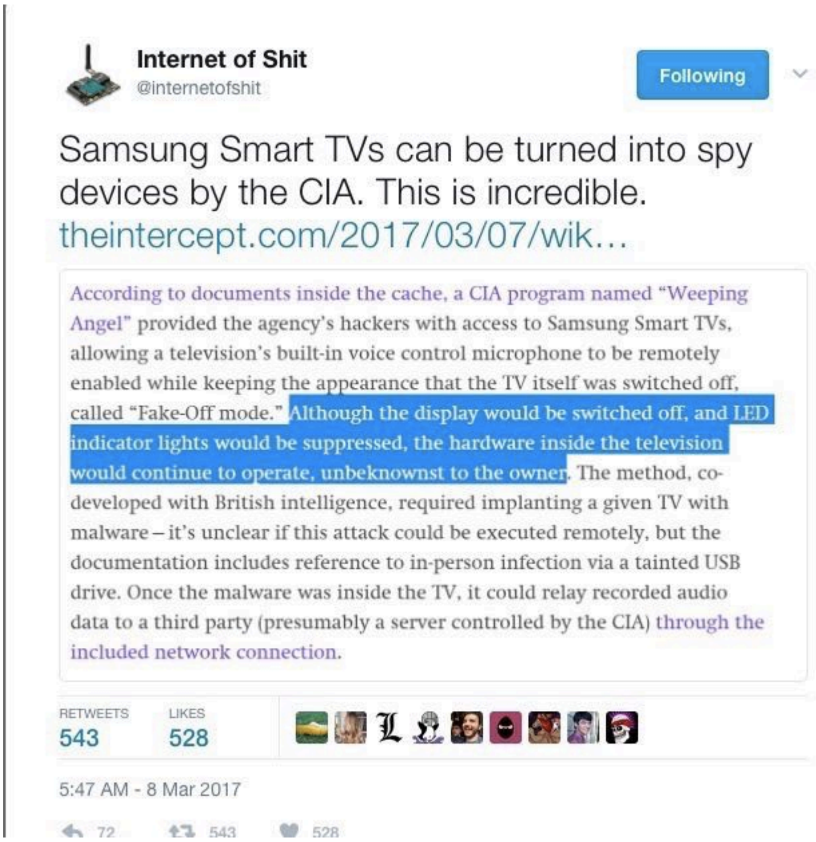
This ‘theatre of failure' is one example of demonstrating a counter-narrative to the tech utopian vision to a consumer public that could become part of the issue public.

The @InternetofShit account makes a few posts a day dedicated to areas such as:

- Malicious IoT attacks such as DDoS attacks or hacks on insecure databases linked to IoT products.
- IoT products that serve no apparent purpose by being internet enabled
- Examples of tinkering hacks
- Memes that are critical of IoT

Each of these types of posts does slightly different work in creating an awareness of the counter-narrative to the technological utopia, in a format accessible to the consumer public.

Posts which link to news and explainer articles about DDoS attacks and similar hacking events are written in layman’s terms, rather than the highly technical language that is only understood to those with technical expertise.



Internet of Shit
@internetofshit

Samsung Smart TVs can be turned into spy devices by the CIA. This is incredible. theintercept.com/2017/03/07/wik…

According to documents inside the cache, a CIA program named "Weeping Angel" provided the agency's hackers with access to Samsung Smart TVs, allowing a television's built-in voice control microphone to be remotely enabled while keeping the appearance that the TV itself was switched off, called "Fake-Off mode." Although the display would be switched off, and LED indicator lights would be suppressed, the hardware inside the television would continue to operate, unbeknownst to the owner. The method, co-developed with British intelligence, required implanting a given TV with malware – it's unclear if this attack could be executed remotely, but the documentation includes reference to in-person infection via a tainted USB drive. Once the malware was inside the TV, it could relay recorded audio data to a third party (presumably a server controlled by the CIA) through the included network connection.

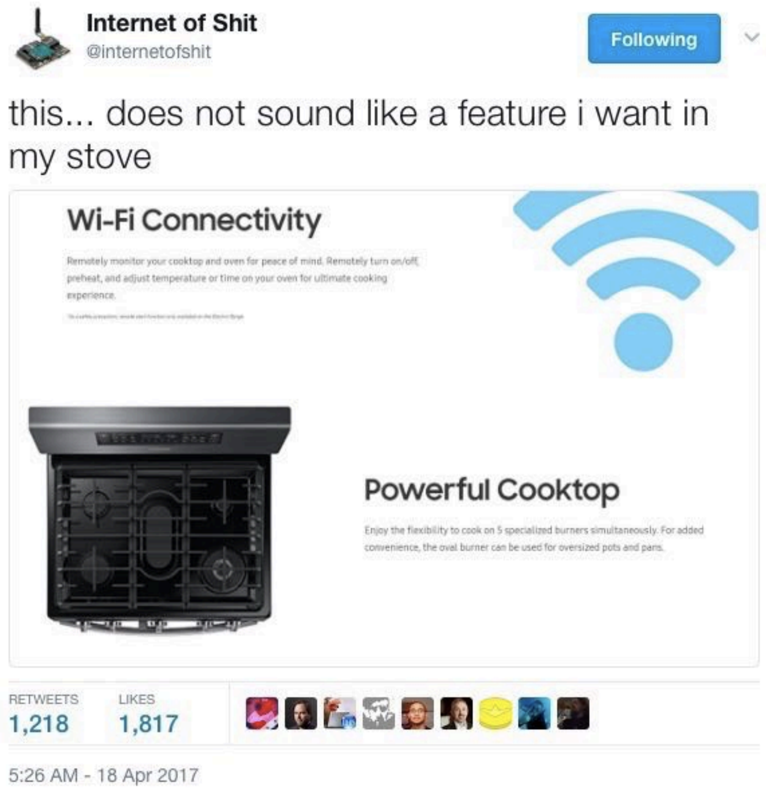
RETWEETS 543 LIKES 528

5:47 AM - 8 Mar 2017

72 543 528

Figure 8: Screen capture of tweet from @InternetofShit which describes how an IoT-enabled television could be hacked. (@InternetofShit, Twitter 2017)

The @InternetofShit twitter account is also a place for critiquing the choices of companies to make products internet-enabled. This ranges from Internet of Things connected kitchen ovens, to light bulbs and even door locks.



Internet of Shit
@internetofshit

this... does not sound like a feature i want in my stove

Wi-Fi Connectivity

Remotely monitor your cooktop and oven for peace of mind. Remotely turn on/off, preheat, and adjust temperature or time on your oven for ultimate cooking experience.

Powerful Cooktop

Enjoy the flexibility to cook on 5 specialized burners simultaneously. For added convenience, the oval burner can be used for oversized pots and pans.

RETWEETS 1,218 LIKES 1,817

5:26 AM - 18 Apr 2017

Figure 9: Screen capture of a tweet from @InternetofShit, discussing the drawbacks of an IoT-enabled oven. (@InternetofShit, Twitter 2017)

The purpose of this twitter account is one part mockery of how anything and everything is being commoditised and quantified by being connected to the Internet. However, this mockery has reflexive consequences: by presenting these hyperbolic advertisements in a humorous way, we are forced to consider them differently and reconsider our enrolment in the Internet of Things.

As mentioned in the list above, the @InternetofShit account often links to other sources within the white hat community, the most prominent of these being videos, blogs and articles from technology journalists.

The twitter account was also where I found one of the demonstrations to be discussed in this chapter, a blog post detailing an insecure Internet of Things connected toy.

The @internetofshit Twitter account demonstrates the potential for disruption by using humour to enrol consumers to be sceptical of IoT-enabled products, as presented by the companies producing them. But how do companies demonstrate the convenience and ease of IoT-enabled products?

Demonstrations of utopia and risk

When you think of the Internet of Things as a consumer, you may think one of a few thoughts. The first impression may well be, ‘what actually is the Internet of Things?' And it's relatively easy to see why that may still be where public thinking is at; the Internet of Things is quite an abstract concept. We're familiar with the Internet, we're familiar with things, but just precisely what the Internet of Things is, and how it works is often confusing to people who are not from a technical background. The next thought after getting some basic understanding could feasibly be, ‘that's great, but how what does that look like in my everyday life?'

Large IT companies respond to this curiosity by producing short explainer videos as a form of ‘theatre of use' (Smith 2009) style demonstration that shows how IoT products could be incorporated into someone's everyday life and surroundings. These explainer videos are produced by technology companies such as IBM (2015) and Intel (2014) and have titles such as: *How it works: The Internet of Things* and *Intel IoT – What does the Internet of Things Mean?* The videos are relatively popular, with the IBM explainer video receiving more than 870,000 views in just over two years. The videos are almost always produced as animations, maintaining a sense of intangibility to the IoT, as though if it were done as live action, it would appear incredibly mundane.

These videos contain the corporate vision of IoT that involves smart cities, intuitive healthcare and insurance rewards. The corporate vision of IoT manifests itself in YouTube videos with an upbeat guitar soundtrack, showing a cartoon narrative of someone driving an IoT-enabled car that monitors the status of the brakes and not only notifies them of the brakes failing but also of the nearest garage to get them repaired. The videos depict simplicity and convenience. Why go to the bother of remembering to take your car for regular maintenance if your car can remind you?

When I interviewed my colleague about botnets and the Internet of Things, I also showed him a YouTube video produced by IBM about IoT and its use in IoT-enabled cars. I chose this video because it presented complex concepts about how the Internet of Things worked in simple language, using examples. This video was an example of problem amplification (Latour 1999) in simplifying how the Internet of Things works and yet I wanted to see whether the accuracy of how the Internet of Things worked was lost in the demonstration. The use of the video within the interview was a form of elicitation device (Knoblauch et al. 2008, Graham et al. 2009, Laurier 2004) to generate some rebuttals, examples or, confirmation from him about the Internet of Things and its security levels.

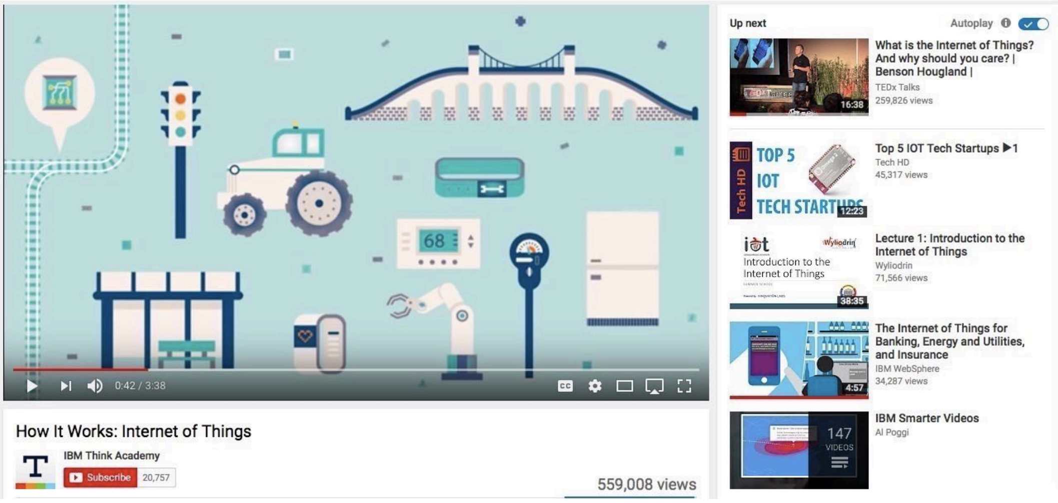

0:42 / 3:38
How It Works: Internet of Things
IBM Think Academy
Subscribe 20,757
559,008 views
Up next
Autoplay
What is the Internet of Things? And why should you care? | Benson Hougland |
TEDx Talks
259,826 views
16:38
Top 5 IOT Tech Startups ▶1
Tech HD
45,317 views
12:23
Lecture 1: Introduction to the Internet of Things
Wyliodrin
71,566 views
38:35
The Internet of Things for Banking, Energy and Utilities, and Insurance
IBM WebSphere
34,287 views
4:57
IBM Smarter Videos
Al Poggi
147 VIDEOS

Figure 10: Screen capture of an explainer animated video that describes the Internet of Things (IBM Think Academy, YouTube 2015)

The first screenshot from this video shows the myriad objects that could feasibly be part of the Internet of Things. It includes traffic lights, tractors, thermostats and fridges, among other products.

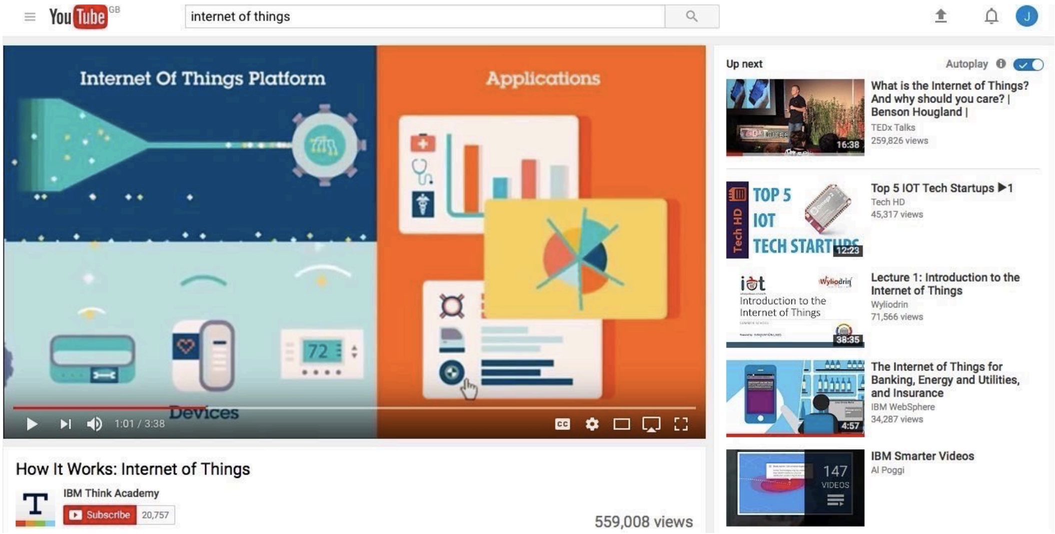

YouTube GB
internet of things
Internet Of Things Platform
Applications
Devices
72
1:01 / 3:38
How It Works: Internet of Things
IBM Think Academy
Subscribe 20,757
559,008 views
Up next
Autoplay
What is the Internet of Things? And why should you care? | Benson Hougland |
TEDx Talks
259,826 views
16:38
Top 5 IOT Tech Startups ▶1
Tech HD
45,317 views
12:23
Lecture 1: Introduction to the Internet of Things
Wyliodrin
71,566 views
38:35
The Internet of Things for Banking, Energy and Utilities, and Insurance
IBM WebSphere
34,287 views
4:57
IBM Smarter Videos
Al Poggi
147 VIDEOS

Figure 11: Screen capture of a video describing the components making up the IoT. (IBM Think Academy, YouTube 2015)

The second image demonstrates how IoT products act alongside the nondescript 'Internet of Things platform' and applications.

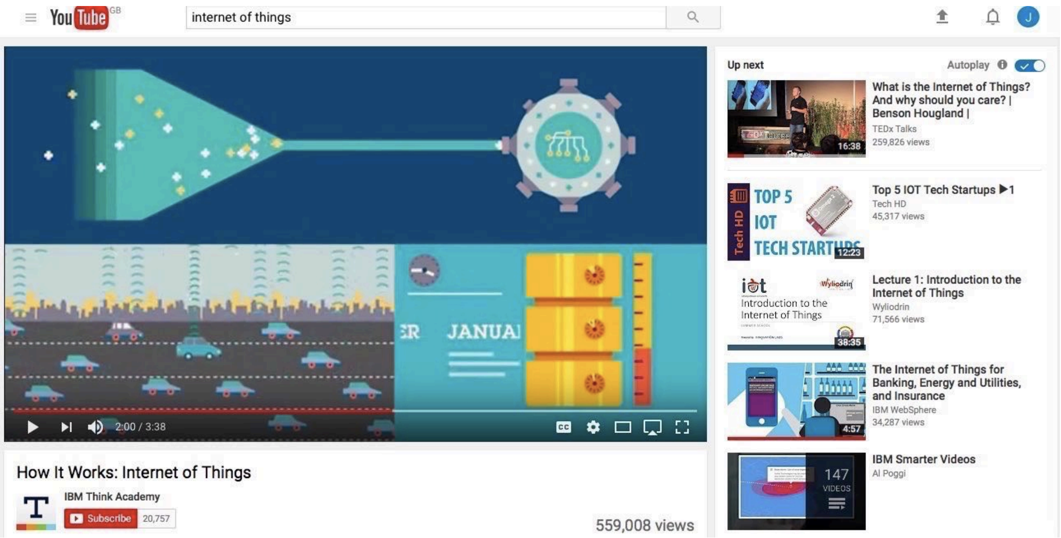


Figure 12: Screen capture of video describing how the IoT components work together to diagnose a car fault and book the car into a mechanic. (IBM Think Academy, YouTube 2015)

Lastly, the video describes and shows how an Internet of Things product such as a car sends data to the Internet of Things platform, which then passes to applications that record the data and send notifications to those using the Internet of Things product so that the consumer can then take action on those notifications. It effectively answers those conceptual ‘what is the Internet of Things?' and ‘how does it work?' questions in a swift three and a half minutes.

My colleague's response to the video included a series of sarcastic retorts and melodramatic head holding. When asked why he responded to the video this way, he said:

Colleague: They said other things in this thing [the video] - ‘it will securely communicate!' - Oh, that'd be nice, some of them do. The odds are at the moment, most of them don't, they talk unencrypted. The fact that it's telling the car company your exact location, it's said as a feature, but that depends on your privacy. And so on and so forth… In theory, lots of good things could be done for it. In practice, the customers don't know what they're getting, and therefore unsurprisingly they're not getting what they'd hope.

JP: Yep… so I think tying this all together, and I'm guessing you can see this coming, but using IoT devices to form a botnet.

Colleague: Yes, has already happened. And was used massively… Was used for the largest denial of service that we've yet seen on the internet and is really entertaining because it was done off what seems to be one vulnerability that was built most of the botnet and used IoT off the back of it. I think it was something as stupid as default credentials or something. So like I said, vulnerability might be over-stretching this you know cos you can login in with the same username and password on a large number of devices.

JP: So it was like 'admin', '1234' kind of credentials?

Colleague: That kind of stuff.

- Transcript, interview, 24 January 2017.

From this conversation, we gain a description of how the simplified, amplified (Latour 1999) corporate depiction of the Internet of Things and its possible application in everyday life, could be at odds with the reality that cyber security professionals see in threat reports (such as those issued by US-CERT or by the UK's National Cyber Security Centre). Or rather, the corporate, three-minute 'theatre of use' depiction of the Internet of Things misses the measures that consumers must take to ensure that their use of this network of products does not inadvertently contribute to a cyber security disruption similar to those described above.

But rarely do we see these 'theatre of failure' demonstrations, outlining the potential for disruption from core-set experts in the cyber security industry that simplify the problem to the extent that non-cyber security professionals could understand.

Not all cartoons and upbeat music: the cyber security industry’s response

In response to this utopian ideal of the Internet of Things presented by corporations, IoT critics use examples of IoT devices co-opted into attacks or IoT objects with obvious security flaws to highlight the failings of these objects. Alongside examples of work done by malicious hackers, there are white hat and possibly grey hat hackers tinkering (Grommé 2015), and breaking IoT objects. Hackers do this to demonstrate the potential uses for these objects outside their intended purpose, for the data that they collect to be gathered and used by black hat hackers. Examples of this include hackers who take part in the DefCon conferences or local meetups such DC4420, or by cyber security bloggers such as those we will meet later in the chapter.

Aside from educating the public on the security flaws of the Internet of Things, the white hat community carrying out these demonstrations also seek to hold the manufacturer accountable (Marres 2012) for their poor quality concerning security.

At this point, it may be valid to critique these demonstrations as just a way for pen-testers and red teams to drum up business. Isn't it akin to a locksmith, breaking into a lock to demonstrate the need for tighter security that only he or she can provide, thus providing a business opportunity?

While it is a good analogy, the answer, according to my colleague, is ‘not really'. The analogy fits in crudely describing the situation; there are digital ‘locks' (to borrow from the analogy) in desperate need of fixing. However, according to my colleague, it doesn't accurately describe the fact that these kinds of demonstrations are illegal; companies and institutions would be more irritated and angry rather than thankful that this happened without their consent. Pen-testers, in particular, bank on the fact that they have accreditation from industry bodies such as CREST and are therefore trustworthy. Hacking as a stunt is a sure-fire way to demonstrate to companies and organisations that you are not trustworthy enough to poke around in their networks.

What pen-testers and white hat hackers *do* demonstrate online are situations where black or grey hat hackers have exploited a security flaw, with or without the responsible organisation's knowledge. These demonstrations through blogs from cyber security professionals such as Troy Hunt (whose blog post will be analysed shortly) alert peers, manufacturers and consumers that there may be a security breach relevant to them and the safety of their sensitive personal data.

While the intention is to demonstrate flaws that may have been leaked to them, there is no career value in s*eeking out flaws* and poking holes in them. However, there may be value through a formalised process where a company specifically asks for it via bug bounty websites[54] or similar requests. That results in a lack of trust from the very people who could hire you. However, there is an active white hat community demonstrating and discussing e*xisting flaws* that

[54] Bug bounty websites are places where companies explicitly invite hackers to find vulnerabilities on their websites or services in return for a reward.

could directly impact consumers who are unaware of them. These discussions happen to build trust in cyber security experts. At this point, it is helpful to describe hackers and vulnerabilities forming a hybrid of sorts. In paraphrasing Latour (1993, 1994), Michael (2017) states: "Strip a person - a doctor, a teacher, a factory worker, a politician, a scientist - of their technologies and they cannot operate as such," (p.42) This concept applies to the hacking end of the cybercrime and cyber security communities: Strip a hacker of their technological vulnerabilities and they cannot operate as such. Indeed, strip hackers of vulnerabilities and they become everyday technology users or programmers.

When describing the reasoning for the white hat community's hacking, my colleague argues that a combination of cost and convenience prevents consumers being enrolled in the security risks of IoT products. While there are cheaper, less secure products in the market, consumers will continue to gravitate towards them. Security remains invisible as a selling point or disincentive from purchase. In other words, how would a consumer know to make sure the IoT product they are purchasing is secure if security is not a selling point?

Additionally, the promise of convenience - not only in the use of the product but in its set up - means that consumers are blinded by the promise of ease of use. This perceived ease of use then becomes negated if the manufacturer adds additional set up steps - such as changing the username and password - to ensure the security of the products. This is especially the case if these optional steps have not been designed similarly, leaving the consumer with a complicated process to endure to ensure the security of the product. The expectation of consumers with IoT products - especially those related to the home - is that they become part of the infrastructure of the home, with thought only given to them when something (such as temperature or timing) needs adjustment for comfort or convenience purposes. If an IoT product becomes part of the infrastructure of the home, there is an expectation that it is transparent, it doesn't have to be ‘reinvented each time' much like Star (1999) describes, even when it comes to security. But how can that be if vulnerabilities shift, change and, emerge over time? Although IoT products when placed within the infrastructure of the home, such as smart lighting or heating, are convenient, they come with the expectation and cognitive load of maintaining them (Shove 2004). Rather than maintaining the lighting or heating manually within a home with a switch, consumers now have the task of maintaining the products and apps that do this for them.

Furthering the difficulty of enrolling the consumer is the fact that IoT security related problems - such as botnets and DDOS attacks - are an unintended consequence of owning an IoT-enabled product. This presents a challenge for a cyber security professional wanting to demonstrate the potential disruption from IoT products. The consumer may be aware that their internet-enabled kettle or toaster may be co-opted into a botnet, but the outcome of this - a botnet attack on a series of high profile websites - will not directly impact them; or if it does it is not obvious how a consumer’s printer or kettle contributed towards their Netflix or Twitter account being momentarily unavailable to them. If the result may not affect them, then what motivation do they have to fix the problem or ensure that their product is secure? How then could the cyber security profession demonstrate this potential for disruption in ways that enrol consumers in the necessary security work to prevent their IoT enabled household goods being co-opted into disruptive botnets?

The security risk posed by IoT products forms a problem worth addressing, according to cyber security professionals and academics (Roman, Najera and Lopez 2011). What forms do these demonstrations take? And how do they demonstrate both their expertise *and* the risk of disruption in ways that the consumer public can understand? Is that group of experts the best public to call for accountability from manufacturers and the government? It would appear that consumers would be the best public to form around this problem and yet they remain mostly silent. What are the factors that cause them to stay silent on this issue?

The white hat hacking community goes about demonstrating the potential for disruption to consumers caused by security breaches through a number of online means. There is the use of Twitter to catalogue, joke about and distribute items of IoT-related problems and failures through accounts such as @InternetofShit. YouTube is used to show some of the techniques pen-testers and red teams use to breach a network. And blogging is used to tell a more in-depth narrative of high profile breaches, such as the Dyn DDoS attack caused by a botnet of IoT products.

Bloggers

This section will examine how IoT disruptions are demonstrated by cyber security professionals via blogs. In particular, I will analyse the ways InfoSec bloggers demonstrate the technical aspects of a breach to show where manufacturers have failed to ensure the security of an IoT product. I will be focussing on InfoSec blogger Troy Hunt's post ‘Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages' (2017) and the entities incorporated such as videos, screenshots of code and emails to demonstrate how data from an IoT children’s toy had been compromised. Hunt addresses many audiences within this blog post, each with varying levels of enrolment, due to the technical nature of the demonstrations. Through analysing this blog post, I will show how Hunt demonstrates this disruption of personal data security to fellow cyber security professionals, the manufacturer responsible for the product and the database of messages and, people who may have purchased or own the product.

The IoT product in question is a range of soft toys called CloudPets. And the unique selling point of these toys is that adults can:

> “record and send messages using the CloudPets App from anywhere in the world. A parent or loved one at home gets the message on their CloudPets App and then approves it and delivers it wirelessly to the CloudPet. When the CloudPet has a message, its heart blinks. When your child squeezes its paw, the message plays.”(CloudPets 2017)

If you are an adult family member who is often away from a child, this product might be a nice way to stay in touch with them. But the technology that is running CloudPets can and was hacked, as Hunt demonstrates in his blog. This meant that sensitive personal data about the adults and children using CloudPets were publicly available, along with the audio messages.

The blog post - posted on the @internetofshit Twitter account – is not brief by any stretch of the imagination; it clocks in at over 5,000 words. But Hunt’s use of embedded videos and screenshots of databases, file structures, and emails demonstrate the neglect on behalf of the manufacturer to ensure the security of the CloudPets audio recordings. To use Goffman's dramaturgical analogy, there are a lot of props for Hunt to use in his 'theatre of failure' to demonstrate how the disruption occurred and how it was also ignored.

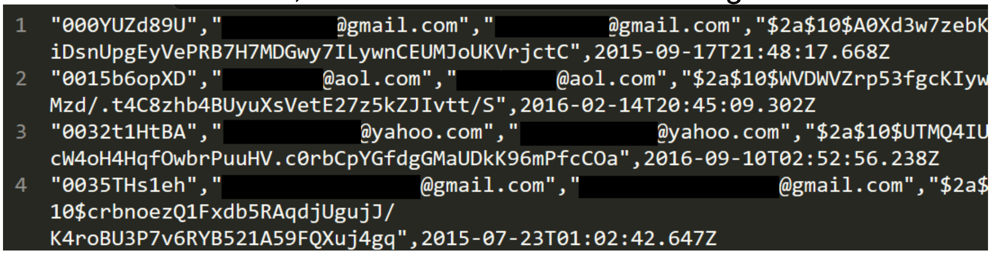
As Hunt demonstrates, the weak link in this IoT product is not the toy itself, nor is it the smartphone the parent uses to send or receive voicemail messages. Instead, it is the space in between - the database that the voice messages are held in, or 'the Internet of Things platform' if we are working with the IBM explainer video description - that poses the security risk. Hunt uses the bulk of the blog post to demonstrate through screenshots just how vulnerable the databases of usernames, passwords and voice messages held in the cloud is.

He describes how:

> "every one of those recordings – those intimate, heartfelt, extremely personal recordings – between a parent and their child is stored as an audio file on the web. They certainly wouldn't realise that in CloudPets' case, that data was stored in a MongoDB that was in a publicly facing network segment without *any* authentication required and had been indexed by Shodan (a popular search engine for finding connected things)."
>
> - Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages troyhunt.com, 28 February 2017.

The database of voice messages being indexed on Shodan meant that people were alerted to the fact that this database could be accessed. Hunt describes how he was leaked some data by 'someone who travels in data breach trading circles' and how he went through a verification process to try to determine whether this was from the CloudPets database:

“I started going through my usual verification process to ensure it was legitimate and by pure coincidence, I was in the US running a private security workshop at the time and one of the guys in my class had a CloudPets account. Sure enough, his email address was in the breach and it was time-stamped Christmas day, the day his daughter had been given the toy. His record looked somewhat like these, the first few in the data I was given:



```
"000YUZd89U","[redacted]@gmail.com","[redacted]@gmail.com","$2a$10$A0Xd3w7zebK
iDsnUpgEyVePRB7H7MDGwy7ILywnCEUMJoUKVrjctC",2015-09-17T21:48:17.668Z
"0015b6opXD","[redacted]@aol.com","[redacted]@aol.com","$2a$10$WVDWVZrp53fgcKIyw
Mzd/.t4C8zhb4BUyuXsVetE27z5kZJIvtt/S",2016-02-14T20:45:09.302Z
"0032t1HtBA","[redacted]@yahoo.com","[redacted]@yahoo.com","$2a$10$UTMQ4IU
cW4oH4HqfOwbrPuuHV.c0rbCpYGfdgGMaUDkK96mPfcCOa",2016-09-10T02:52:56.238Z
"0035THs1eh","[redacted]@gmail.com","[redacted]@gmail.com","$2a$
10$crbnoezQ1Fxdb5RAqdjUgujJ/
K4roBU3P7v6RYB521A59FQXuj4gq",2015-07-23T01:02:42.647Z
```

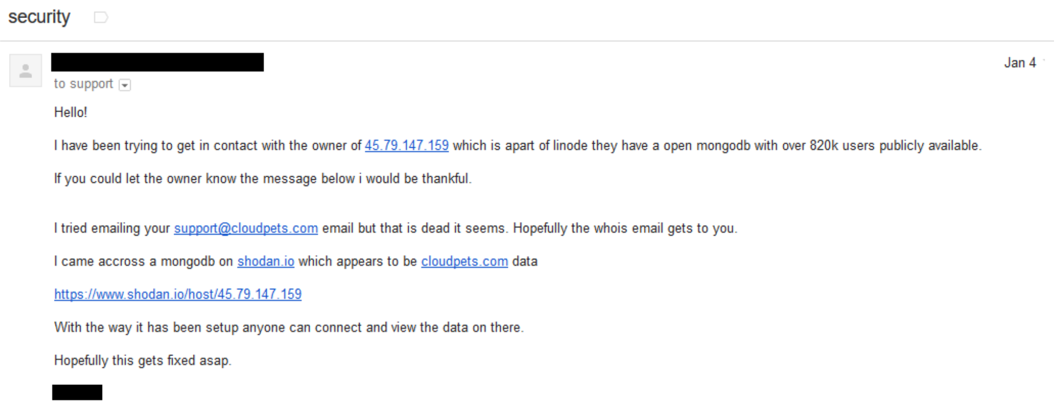
Figure 13: screen capture of a database of email address logins and timestamps from the breached CloudPets database (Troy Hunt, 2017)

The password was stored as a bcrypt hash and to verify it was legitimate, he gave me his original password (I asked him to change it on CloudPets first) and I successfully validated that the hash against his record was the correct one (I'd previously validated the Dropbox data breach by doing the same thing with my wife's account). The data was real.

CloudPets left their database exposed publicly to the web without so much as a password to protect it.”

- Excerpt from ‘Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages’, Troy Hunt, 28 February 2017. (emphasis original)

This excerpt demonstrates both the data breach and the process he went through to test that the tip-off was legitimate. And at this point, the audience could rightly be wondering why the person who leaked the database to Hunt had not tried to notify the company beforehand as a form of goodwill and fair warning. It turns out he or she had. Hunt then describes how the leaker emailed the company repeatedly to warn them of the insecure database, what was at stake and how to attempt to fix the problem; all with no response from CloudPets, its marketing company or its hosting company.



security

[redacted]

Jan 4

to support

Hello!

I have been trying to get in contact with the owner of 45.79.147.159 which is apart of linode they have a open mongodb with over 820k users publicly available.

If you could let the owner know the message below i would be thankful.

I tried emailing your support@cloudpets.com email but that is dead it seems. Hopefully the whois email gets to you.

I came accross a mongodb on shodan.io which appears to be cloudpets.com data

https://www.shodan.io/host/45.79.147.159

With the way it has been setup anyone can connect and view the data on there.

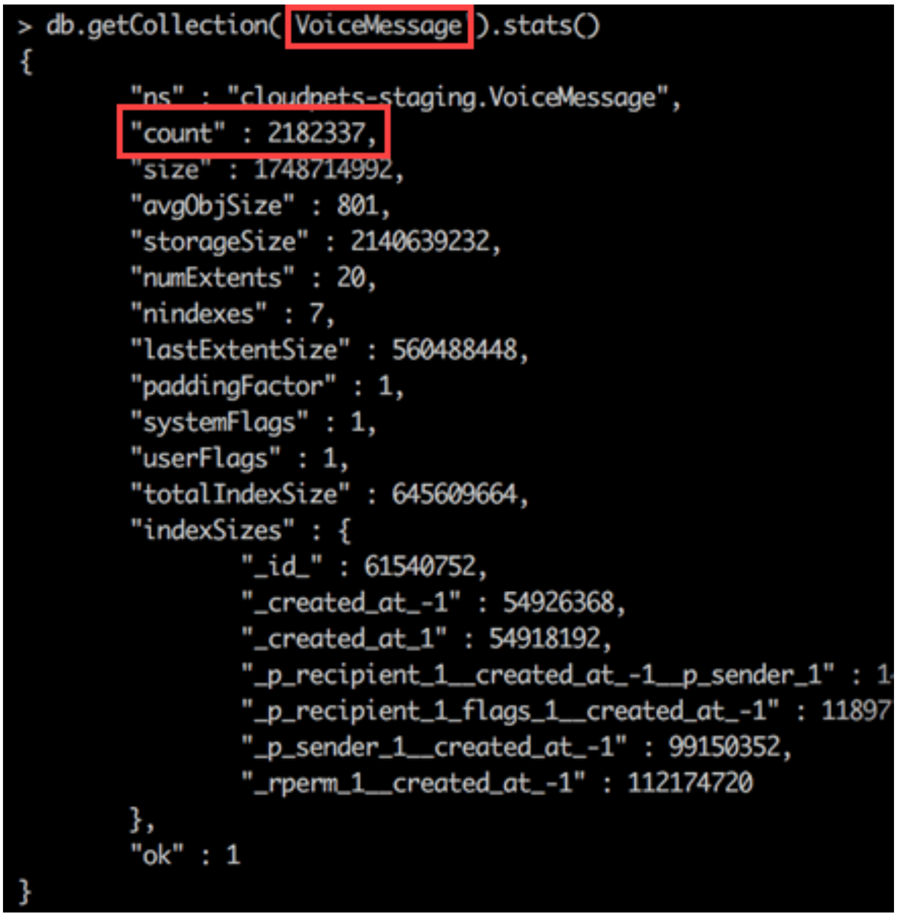
Hopefully this gets fixed asap.

[redacted]

Figure 14: Screen Capture of email used to demonstrate attempts to contact CloudPets to alert them of the vulnerabilities in their databases [redactions original] (Troy Hunt 2017)

Hunt uses his blog as a theatre of proof, with the screenshots as the props to demonstrate how the data breach occurred along with the attempts made to rectify the problem. These screenshots are important as they show Hunt's professional vision of ‘producing and articulating material [or digital, in this case] representations’ (Goodwin 1994) of the database breach not only to the consumer public but also to the cyber security profession who reads his blogs. In particular, Hunt acts as the senior archaeologist described in *Professional Vision* (Goodwin 1994), with these databases serving as an archive of activity where he must point out to us - his readers as the junior archaeologists - how to read these screenshots of databases, file structures and excerpts of code. In particular, as he continues with his discussions of CloudPets' failure to protect consumer data, he shows database excerpts demonstrating exposed voice recordings and insecure and easily guessed passwords.

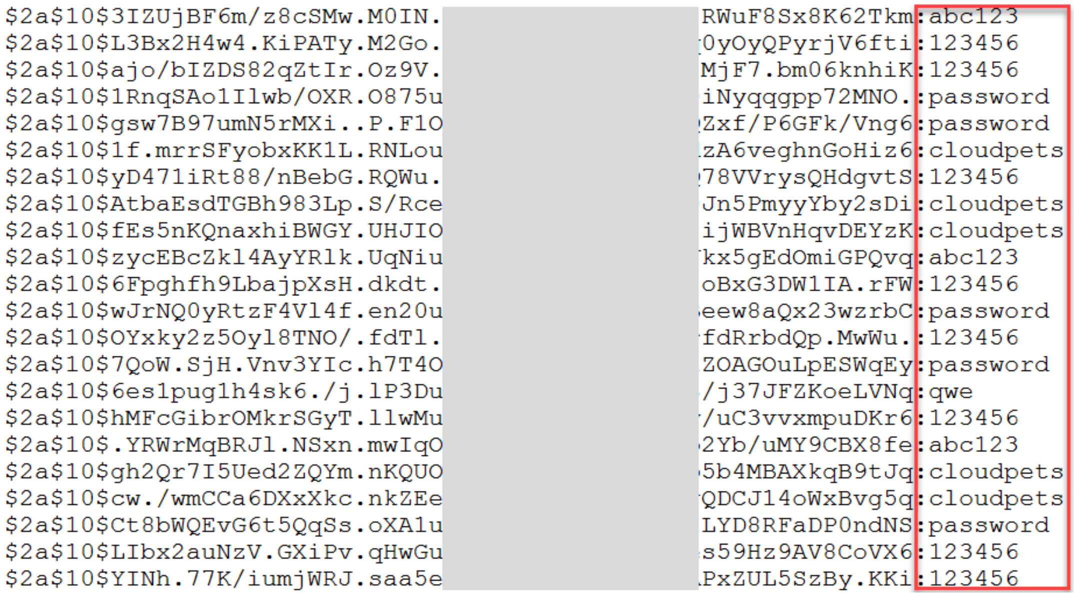
)



```
> db.getCollection( VoiceMessage ).stats()
{
        "ns" : "cloudpets-staging.VoiceMessage",
        "count" : 2182337,
        "size" : 1748714992,
        "avgObjSize" : 801,
        "storageSize" : 2140639232,
        "numExtents" : 20,
        "nindexes" : 7,
        "lastExtentSize" : 560488448,
        "paddingFactor" : 1,
        "systemFlags" : 1,
        "userFlags" : 1,
        "totalIndexSize" : 645609664,
        "indexSizes" : {
                "_id_" : 61540752,
                "_created_at_-1" : 54926368,
                "_created_at_1" : 54918192,
                "_p_recipient_1__created_at_-1__p_sender_1" : 1
                "_p_recipient_1_flags_1__created_at_-1" : 11897
                "_p_sender_1__created_at_-1" : 99150352,
                "_rperm_1__created_at_-1" : 112174720
        },
        "ok" : 1
}
```

Figure 15: Screen capture of database containing voice messages from CloudPets accounts. [highlights original] (Troy Hunt 2017)

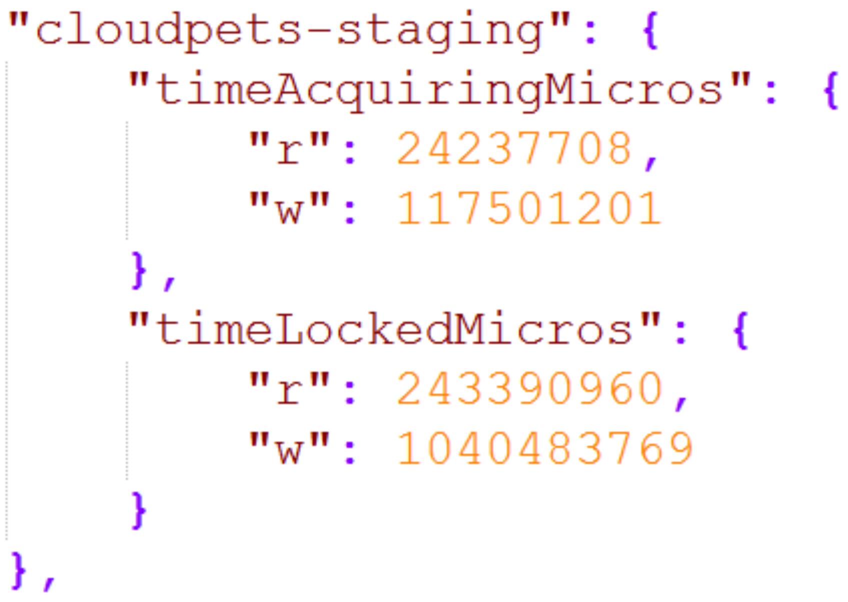
In this screenshot, Hunt uses these boxes to draw our attention to the fact that the database containing CloudPets voice messages includes more than two million messages. And in the screenshot below, he shows some of the easily crackable passwords created by consumers. The passwords were easily cracked because the CloudPets development team chose not to set a rule regarding password strength. In fact, Hunt even goes so far as to explain that in an instructional set-up video produced by CloudPets, they use the very short ‘qwe' as an example of a password.



```
$2a$10$3IZUjBF6m/z8cSMw.M0IN.[redacted]RWuF8Sx8K62Tkm:abc123
$2a$10$L3Bx2H4w4.KiPATy.M2Go.[redacted]0yOyQPyrjV6fti:123456
$2a$10$ajo/bIZDS82qZtIr.Oz9V.[redacted]MjF7.bm06knhiK:123456
$2a$10$1RnqSAo1Ilwb/OXR.O875u[redacted]iNyqqgpp72MNO.:password
$2a$10$gsw7B97umN5rMXi..P.F1O[redacted]Zxf/P6GFk/Vng6:password
$2a$10$1f.mrrSFyobxKK1L.RNLou[redacted]zA6veghnGoHiz6:cloudpets
$2a$10$yD471iRt88/nBebG.RQWu.[redacted]78VVrysQHdgvtS:123456
$2a$10$AtbaEsdTGBh983Lp.S/Rce[redacted]Jn5PmyyYby2sDi:cloudpets
$2a$10$fEs5nKQnaxhiBWGY.UHJIO[redacted]ijWBVnHqvDEYzK:cloudpets
$2a$10$zycEBcZkl4AyYRlk.UqNiu[redacted]kx5gEdOmiGPQvq:abc123
$2a$10$6Fpghfh9LbajpXsH.dkdt.[redacted]oBxG3DW1IA.rFW:123456
$2a$10$wJrNQ0yRtzF4Vl4f.en20u[redacted]eew8aQx23wzrbC:password
$2a$10$OYxky2z5Oyl8TNO/.fdTl.[redacted]fdRrbdQp.MwWu.:123456
$2a$10$7QoW.SjH.Vnv3YIc.h7T4O[redacted]ZOAGOuLpESWqEy:password
$2a$10$6es1pug1h4sk6./j.lP3Du[redacted]/j37JFZKoeLVNq:qwe
$2a$10$hMFcGibrOMkrSGyT.llwMu[redacted]/uC3vvxmpuDKr6:123456
$2a$10$.YRWrMqBRJl.NSxn.mwIqO[redacted]2Yb/uMY9CBX8fe:abc123
$2a$10$gh2Qr7I5Ued2ZQYm.nKQUO[redacted]5b4MBAXkqB9tJq:cloudpets
$2a$10$cw./wmCCa6DXxXkc.nkZEe[redacted]QDCJ14oWxBvg5q:cloudpets
$2a$10$Ct8bWQEvG6t5QqSs.oXA1u[redacted]LYD8RFaDP0ndNS:password
$2a$10$LIbx2auNzV.GXiPv.qHwGu[redacted]s59Hz9AV8CoVX6:123456
$2a$10$YINh.77K/iumjWRJ.saa5e[redacted]PxZUL5SzBy.KKi:123456
```

Figure 16: Screen capture of leaked passwords from CloudPets accounts. [highlights original] (Troy Hunt 2017)

One of the reasons why Hunt's theatre of proof-style post of the CloudPets data breach is so hefty is because the story doesn't stop at the database being publicly available and consumers using easily guessed passwords. The demonstration includes numerous attempts from cyber security professionals aware of the breach to notify the company involved. The story continues with the databases being hacked and held to ransom by parties demanding payment in the cryptocurrency BitCoin to release the databases:

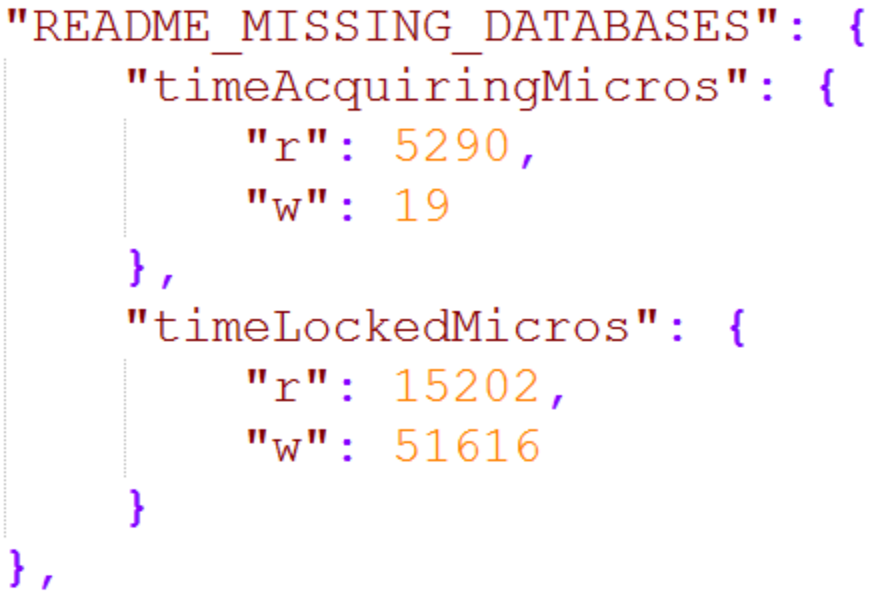


```
"cloudpets-staging": {
    "timeAcquiringMicros": {
        "r": 24237708,
        "w": 117501201
    },
    "timeLockedMicros": {
        "r": 243390960,
        "w": 1040483769
    }
},
```

Figure 17: Screen capture of exposed CloudPets database listed on Shodan. (Troy Hunt 2017)

This screenshot is the result of a Shodan search which shows that the CloudPets staging database[55] - also known as the production or live database - was exposed. In the screenshot below, Hunt shows how in a week or so after the database was shown to be revealed, malicious parties had made a copy of the production database, deleted the original database. They then labelled these copied databases with names including variations on ‘README' to denote that there was a ransom on the database.

[55] There was also a testing database that was exposed, but testing databases tend to exist for developers to make edits and changes to website and test them out before pushing them to the live version of the website or service.



```
"README_MISSING_DATABASES": {
    "timeAcquiringMicros": {
        "r": 5290,
        "w": 19
    },
    "timeLockedMicros": {
        "r": 15202,
        "w": 51616
    }
},
```

Figure 18: The altered CloudPets database listed on Shodan, after malicious hackers held it to ransom. (Troy Hunt 2017)

In addition to using screenshots to demonstrate disruption, Hunt also demonstrates frustration about the lack of response to instances where he has demonstrated the disruption to those responsible, in this case, the manufacturer:

"…one of the greatest difficulties I have in dealing with data breaches is getting a response from the organisation involved. Time and time again, there are extensive delays or no response at all from the very people that should be the most interested in incidents like this. If you run any sort of online service whatsoever, think about what's involved in ensuring someone can report this sort of thing to you because this whole story could have had a very different outcome otherwise."
- Excerpt from 'Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages', Troy Hunt, 28 February 2017.

But Hunt isn't solely mediating between the cyber security profession and the manufacturers in this demonstration. He identifies parents or guardians as an audience when he demonstrates this particular type of disruption - a hack of *children's* data:

“Circling back to the parents' position for a moment, you *must* assume data like this will end up in other peoples' hands. Whether it's the Cayla doll, the Barbie, the VTech tablets or the CloudPets, *assume breach*. It only takes *one little mistake* on behalf of the data custodian – such as misconfiguring the database security – and every single piece of data they hold on you and your family can be in the public domain in mere minutes. If you're fine with your kids' recordings ending up in unexpected places then sobeit [sic], but that's the assumption you have to work on because there's a very real chance it'll happen. There's no doubt whatsoever in my mind that there are many other connected toys out there with serious security vulnerabilities in the services that sit behind them. Inevitably, some would already have been compromised and the data taken without the knowledge of the manufacturer *or* parents.”
- Excerpt from ‘Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages’, Troy Hunt, 28 February 2017. (emphasis original)

Hunt ends his demonstration of the CloudPets hacking disruption by advising people who think they may have been hacked to check their email address against the Have I Been Pwned website.

Blogging as an in-depth demonstration

Through this blog, Hunt is demonstrating to his peers in the cyber security or IT profession. He could be demonstrating to the online, cyber security version of the Royal Institution. The highly technical nature of the screenshots requires knowledge to read and understand databases, tables and code. This points to an audience that has a similar level of expertise in the architecture and configuration of IoT products and the internet infrastructure that supports it. However, this description would be telling part of the story because while these screenshots act as evidence that CloudPets' databases were exposed and vulnerable, the narrative structure of Hunt's account of the breach can be read and understood by others who have a less technical background. These ‘others' could include people who purchased the product and wish to know more about the breach. Hunt shapes his narrative in a linear structure that takes the reader from an introduction of the product and how it worked to how it was vulnerable and eventually breached. Crucially, he includes a timeline of what happened and who was proactive or inactive at specific points in time.

Another audience could be the manufacturer. This lengthy blog post acts as a demonstration of the company’s inaction and a rebuttal of sorts to the company’s narrative that the database was secure and the accounts and voice messages were safe. In terms of the rebuttal, Hunt’s digital paper trail of emails unanswered and voicemails easily downloaded act as damning evidence of neglect and cover-up.

But this blog post is addressed to a few more audiences who will be discussed in more detail in the next section of this chapter: developers and consumers. Hunt's blog post acts as a ‘how not to' tale to would-be developers and those already in the field. In particular, back-end developers - who deal with coding the processes for data to be passed to, stored in and, retrieved in databases - are warned to ensure their work secures consumer data. For consumers, we see a cautionary tale around ensuring a high standard of passwords. What is the implicit message of this cautionary tale? Do all you can to ensure security of your data as a consumer because it is difficult to know whether the manufacturer will do that for you. Hunt takes this argument one step further by citing the example of the German government banning the sale of Internet of Things products aimed at children, on the grounds of potential hacking events and breaches of privacy.

Is it reasonable to expect these demonstrations as cautionary tales to be the last line of defence when it comes to ensuring consumer safety when using IoT products? Can a demonstration such as this, with so much expert-level detail be reasonably expected to enrol consumers into safer cyber security practices? Could these types of demonstrations enrol government organisations[56] in attempts to regulate IoT enabled products and avoid the self-responsibilisation of consumers? In the next portion of this chapter, I examine a form of demonstration in the theatre of failure that seeks to enrol consumers into better cyber security practices through encouraging reflexivity.

Demonstrations of disruption as a blame game

So far this chapter has focused on describing the demonstrations of potential or actual disruptions caused by malicious hackers. But the reasoning for these demonstrations is based on a dangerous yet prevalent assumption from the hacking community: users are lax with security and manufacturers care solely about profit margins. While there is some truth to these assumptions, they don't present the full picture of the setting that consumers and manufacturers find themselves in.

Similarly, the argument could be made that these demonstrations made by the cyber security profession are insular and unhelpful (in that they rarely give practical advice). The demonstrations are pitched at such a high expertise level

[56] Some governments – such as the German government - are proactive in regulating IoT products, especially those that are aimed at children. The German Bundesnetzagentur (equivalent to OfCom, the telecommunications regulator) banned the sale of an IoT-enabled doll (The Telegraph 2017)

However, levels of regulation vary between countries. In the US, the Federal Trade Commission suggests manufacturers abide by "a voluntary set of standards suggested by an industry trade association called the broadband internet technology advisory group (Bitag)." (The Guardian 2017) In the UK, a 2014 report from the Government's Chief Scientific Officer suggested that: "Data and devices must have proportionate "security by default". Standards must protect against cybercrime and national security threats, and help to ensure that the system is trustworthy and trusted." (Government Office for Science 2014) that people who use IoT products for everyday tasks find themselves unable to understand the demonstration, let alone act upon it.

In comparison to cyber security professionals, the National Cyber Security Centre (NCSC) appears to be pragmatic and far less cynical. As a public-facing part of the Government Communication Headquarters (GCHQ),[57] they exist to: "…help protect our critical services from cyber attacks, manage major incidents, and improve the underlying security of the UK Internet through technological improvement and advice to citizens and organisations." (NCSC 2017)

In comparison, to cyber security professionals who are hired to consult or test with businesses or organisations, the NCSC says that it "understands cyber security, and distils this knowledge into practical guidance that we make available to all" (NCSC 2017)

They actively demonstrate a willingness to investigate the causes of vulnerabilities from many angles, rather than resorting to existing tropes around an ignorant consumer public and slapdash developers and manufacturers up against sneaky, malicious hackers who only they can overcome and defeat.

[57] The National Cyber Security Centre has been in existence for a relatively short amount of time, since being founded from a merger of six GCHQ departments in 2016 in response to the 2015 National Security Strategy which highlighted 'cyber threat as one of the most significant risks to the UK'. (NCSC 2017) The purpose of the NCSC lies in four areas including understanding cyber security through links with industry, academia and, international partners; reducing cyber security risks to the UK through helping public and private sector organisations secure their networks; responding to cyber security incidents and; growing and educating cyber security professionals.
Counter to how GCHQ-related organisations have previously run under high security and secrecy; the NCSC strives to be open and collaborative. According to the interview participant from the NCSC, this was in part to ensure that the NCSC becomes a trusted source for people to turn to if they wanted to know more about how to be cyber secure or if they wanted to know what to do if they had their security compromised.

The NCSC Technical Director Ian Levy summarises this problem by critiquing the narrative put forward by the cyber security industry.

> “We are allowing massively incentivised companies to define the public perception of the problem,” he said.
> “If you call it an advanced persistent threat, you end up with a narrative that basically says ‘you lot are too stupid to understand this and only I can possibly help you – buy my magic amulet and you’ll be fine.’ It’s medieval witchcraft, it’s genuinely medieval witchcraft.”
> - *GCHQ cyber-chief slams security outfits peddling 'medieval witchcraft’,* The Register, 3 February 2017

But what does a practical and less cynical demonstration of potential cyber security disruption look like? And how can it genuinely mediate and highlight the risks for consumers, business and government?

Demonstrating trust to avoid disruption

The National Cyber Security Centre has a multidisciplinary Sociotechnical Security Group (StSG) that looks at the different actors implicated in cyber security. The StSG offers a counterpoint to the hackers' assertion that consumers are lazy or stupid and that manufacturers (or at least those coding the software) aren't taking security flaws seriously. In line with the NCSC's vision to be ‘open and accountable' (NCSC 2017) they demonstrate their work and known hacking disruptions online. I interviewed a member of the StSG about their rationale for demonstrating disruption through digital channels.

The StSG is a research group within the NCSC that focuses on how people, processes and organisations interact with and impact on cyber security. They roughly break their research into three areas: people (or users), developers and engineers and, risk management. By dividing their research into these three areas, they have identified three main types of actors who may be enrolled in cyber security practices in differing levels of responsibility. They then examine the situated practices (Suchman 1987/2007, 1997) of each of these groups to determine recommendations on how to better support each of these groups in achieving cyber security. The group is multidisciplinary, consisting of scientists, philosophers, psychologists and engineers. They also collaborate with industry and academia to ensure that these groups remain involved in the discourse around cyber security as the area grows, matures and stabilises.

Although they have only been functioning as a research group for since 2016, the StSG's research is performative in that it is published in publicly accessible and understandable ways.

Reflexive, performative digital demonstrations

The StSG demonstrate (or contribute to demonstrations) in a few ways. They write regular blog posts from each of their three focus areas with analysis and suggestions of best practice for all actors involved in ensuring cyber security. They hold Twitter Q&A sessions and make explainer videos that are on YouTube. Their research also contributes to NCSC guidance, which often takes the form of infographics. These methods differ from those in the hacking community because they have considered the publics that will be encountering these demonstrations and their education and expertise levels. My StSG interviewee explained that they want citizens (as they call users or consumers as the group exists to encourage cyber security for all UK citizens or residents) to be able to access 'risk-based information' to help them make better decisions when it comes to cyber security. This means that Cyber Aware (the part of the NCSC that gathers and synthesises cyber security research to communicate to citizens) need to write their public output aimed at citizens that meets the average reading age of 11.

> "…we have a focus on understanding their behaviour and then trying to influence those people who are developing the platforms, application and things like that to take account of the user, to think about the user. But regarding informing the citizen about potential risks, CyberAware are the organisation that is designated to do that. So CyberAware is who we inform in order for them to inform the citizen. So we are doing some work in our risk-based research, with a chap called Professor David Spiegelhalter. And he's had a lot of success in the healthcare industry to communicate risk in a way that people understand. So historically they've had this paradox of the average reading age in the UK is 11 years old and so when you're producing risk-based information on medical matters to someone who you equate to an 11-year-old, you can't actually put much useful information in there. And then people that actually read the leaflets probably have a reading age of much higher than that, so there's all sorts of conflicts. More recently, the healthcare industry has brought out these sort of decision trees that you might see if you get a smear test invitation or something. Now you get a decision tree about 'if I do this, this provides me with this chance of finding this but this risk of that.' So we like the way that David Spiegelhalter has approached this way of communicating statistics to the citizen, to the user. And it's something that we're pursuing to understand how can we use that kind of thinking to communicate cyber risk to a citizen, to the user."
>
> - Interview with Sociotechnical Security Group researcher, 20 April 2017

One of the ways this is demonstrated is through an explainer video they produced to describe the concept of 'people-centred security': the idea that understanding the hurdles that people face in being cyber secure and the workarounds they do to be able to use their workplace IT infrastructure in the most expedient way.

Like the tech-utopian Internet of Things explainers produced by large tech companies, these videos also take the form of short animations. But rather than demonstrating how the technology will make lives easier, the video presents the opposite. It demonstrates a worker deluged with so many logins and passwords that they need to write them down on a piece of paper, thus making a security risk for the organisation they work for.

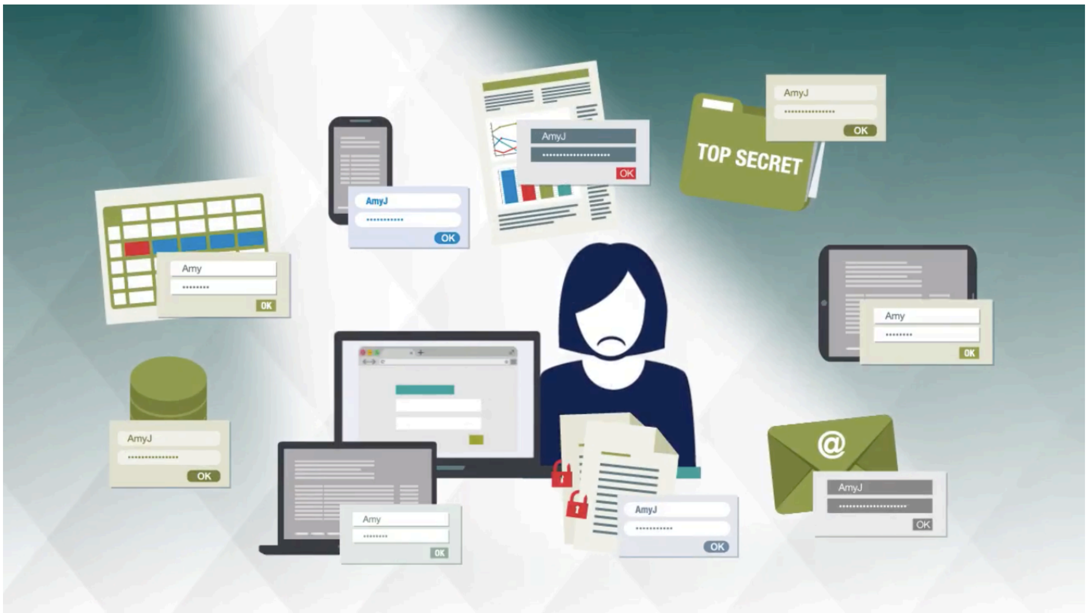


Figure 19: Screen capture of explainer video from the National Cyber Security Centre, depicting the amount of cyber security measures people have to remember across a day (NCSC_HMG, YouTube 2017)

But rather than exhorting people to remember their passwords, change them often and not to write them down, the StSG uses the video to encourage workplaces to examine the cyber security practices of their staff. This helps them understand what is causing them to resort to insecure practices and consider other ways of ensuring cyber security without such a heavy cognitive load on their workers.

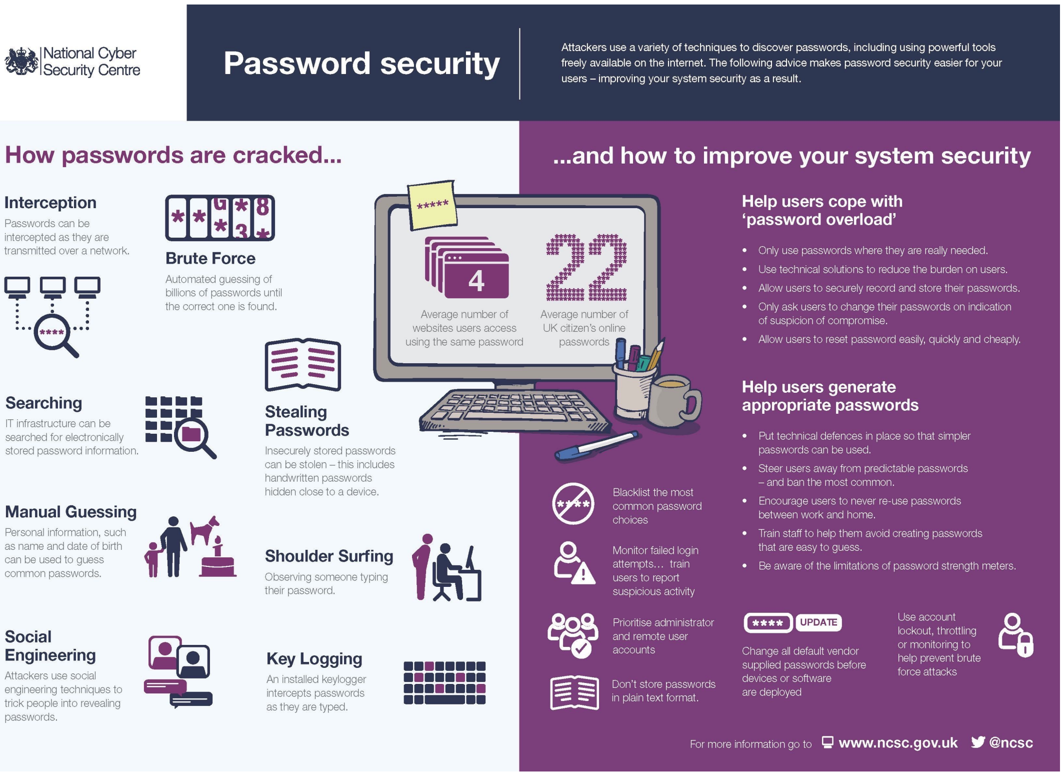
Using another method, the StSG make the same point but with a slightly more academic grounding. In one blog post, the StSG addresses the barriers facing consumers in ensuring cyber security. In particular, they mention the concept of a *compliance budget* (Beautement, Sasse & Wonham, 2008), which asserts that users only have a limited amount of mental capacity (or budget) to spare on security. As a result:

"Pouring user effort into managing and memorising difficult passwords is a common use of the compliance budget, and it's (mostly) a huge waste of this precious resource. Users generally find such policies impossible to comply with; they provide no particular defence against many common password attacks, and there is a real limit on how much protection user passwords can give to a system. Because most times, if your user passwords *can* be directly attacked, then you've got bigger problems."

- *Spending our users' security budgets wisely,* Sociotechnical Security Group blog, 13 October 2016

They then go on to note that organisations with the most stringent password policies for their staff see little increase in cyber security (Florencio & Herley, 2010). With this in mind, they note: 'User passwords are only one of many ways in which we defend our systems. They can't compensate for all vulnerabilities elsewhere, so we shouldn't rely on them further than is justified.' (StSG blog, 2016). To extrapolate on the StSG's remarks, it could be asserted that the secure management of IoT product also falls under a consumer's compliance budget; product security is equivalent to yet another password to remember.

The StSG use blogs to demonstrate the potential for disruption due to weak passwords. They explain that weak passwords allow an easy way for hackers to gain a foothold into the system and install a backdoor to gain 'sustained and undetected access even after the password is changed.' They suggest that manufacturers find different ways to ensure secure access in and out of systems, freeing up a user or consumer's compliance budget to focus on the systems that rely on passwords. Additionally, they suggest ways for manufacturers or employers who build, purchase or administrate systems to help ensure users avoid some of the most common cyber security risks. In keeping with the NCSC's aims of communicating as openly and simply as possible, this information has been synthesised into an infographic aimed at employers and systems administrators.



National Cyber Security Centre

Password security

Attackers use a variety of techniques to discover passwords, including using powerful tools freely available on the internet. The following advice makes password security easier for your users – improving your system security as a result.

How passwords are cracked...

Interception
Passwords can be intercepted as they are transmitted over a network.

Brute Force
Automated guessing of billions of passwords until the correct one is found.

Searching
IT infrastructure can be searched for electronically stored password information.

Stealing Passwords
Insecurely stored passwords can be stolen – this includes handwritten passwords hidden close to a device.

Manual Guessing
Personal information, such as name and date of birth can be used to guess common passwords.

Shoulder Surfing
Observing someone typing their password.

Social Engineering
Attackers use social engineering techniques to trick people into revealing passwords.

Key Logging
An installed keylogger intercepts passwords as they are typed.

4
Average number of websites users access using the same password

22
Average number of UK citizen's online passwords

...and how to improve your system security

Help users cope with 'password overload'

- Only use passwords where they are really needed.
- Use technical solutions to reduce the burden on users.
- Allow users to securely record and store their passwords.
- Only ask users to change their passwords on indication of suspicion of compromise.
- Allow users to reset password easily, quickly and cheaply.

Help users generate appropriate passwords

- Put technical defences in place so that simpler passwords can be used.
- Steer users away from predictable passwords – and ban the most common.
- Encourage users to never re-use passwords between work and home.
- Train staff to help them avoid creating passwords that are easy to guess.
- Be aware of the limitations of password strength meters.

Blacklist the most common password choices

Monitor failed login attempts… train users to report suspicious activity

Prioritise administrator and remote user accounts

Don't store passwords in plain text format.

Change all default vendor supplied passwords before devices or software are deployed

Use account lockout, throttling or monitoring to help prevent brute force attacks

For more information go to www.ncsc.gov.uk @ncsc

Figure 20: Infographic demonstrating the different ways passwords can be stolen along with the security measures that can be taken to protect them (National Cyber Security Centre 2016)

The difference between these demonstrations from the StSG and the demonstration from Troy Hunt's blog about the CloudPets breach is the focus on demonstrating ways that cyber security breaches commonly occur, alongside preventative measures that citizens could take. StSG researchers don't assume that their audience has prior knowledge of cyber security architecture and terminology (as Hunt's blog does), but they do assume a familiarity with the everyday practices that citizens are faced with in ensuring their own cyber security in the workplace.

In defence of the developer

In another blog post, the StSG also describe the factors impacting on manufacturers - more specifically, the developers writing the code for these products - in creating a secure product. They describe competing interests and time pressures, insufficient experience in coding for security and a lack of coding for usability as reasons why IoT products are open to being hacked.

They firstly acknowledge the competing pressures from all sides of developing a product. When coding a product or a service, they often have to account for the views of stakeholders such as CEOs, legal advisors, visual designers and accountants, not to mention the end consumer. In short: the security concerns of building a product are only one consideration on a laundry list of people and elements that need to be balanced and placated when developing a product.

The StSG also argues that developers don't necessarily have the cyber security or cryptography experience to successfully ensure that they are correctly coding and building a product that is as secure as possible. Developers often rely on code libraries - or pre-existing code written by others - to code in security features, rather than writing their own code based on the situated security needs of the product at hand:

"Consider a developer - with no domain expertise in cryptography - using a cryptographic library API. These are potentially powerful tools to protect data, but used incorrectly they can create a false sense of security. Choosing the most appropriate algorithm and mode of operation is vital. Then selecting a sensible approach to key generation and secure key storage all require fairly detailed crypto knowledge. But, they are prone to misuse, which can lead to vulnerabilities such as a failure to validate certificate chains correctly, insecure encryption modes and inadequate random number generators."

- *Developers need help too*, Sociotechnical security blog, 6 December 2016

And returning to the argument for security features that are people-centred, the StSG argue that the usability of security features of an IoT product are rarely considered in the design process:

"Usability. It is rarely seen as a fundamental requirement for design - let alone for security. We don't think it's reasonable to promote a 'secure' product, but state that the security depends on how it is used. How does a developer ensure that their product is going to be *secure enough, no matter how* it is used, bearing in mind there's no such thing as perfect security?"

- *Developers need help too*, Sociotechnical security blog, 6 December 2016

In this blog post, the StSG are demonstrating that in amongst these competing demands for developers' focus, there is rarely a thought given to the differing ways that end users may enact security through their different situated uses of the product. However, rather than blaming the developer community for these shortcomings, they want to research how developers gain the skills and mindset needed to create the most secure products possible.

In comparison to speaking with people from the cyber security profession where a narrative of fear and cynicism reigns, talking with representatives from the StSG about cyber security was a different experience. The StSG readily admits that the cyber security community, accreditation, and public understanding and confidence are yet to stabilise. They accept it in a rather neutral way. There is no malice towards the cyber security profession, nor are they withering of the public or the business community. There is an acknowledgement that the UK is not as cyber secure as they'd like it to be, but that has to come through conversations with the main actors currently responsible for cyber security and, consumers who may need more information on how to be cyber secure. They choose calm, open acknowledgement over calamity; and this shows in their demonstrations.

Demonstrations and performativity

In this chapter, we have met some of the actors who demonstrate the potential for disruption to cyber security. We have met professional, ethical hackers who demonstrate the ways that IoT products could be insecure, leading to ways they could be co-opted into botnets. And we have met an InfoSec blogger who demonstrates how insecure consumer IoT products and their supporting infrastructure are captured and ransomed by hackers. To be sure, these are demonstrations of disruption as they use screenshots, videos, infographics and humour (in the case of the @InternetofShit Twitter account) to enrol audiences into the disruptive potential that comes with introducing IoT products into a home or workplace. But what is frustrating is that these demonstrations are made from a core-set expert to an audience of peers, being too complex for many consumers to understand. It could be argued that it is not the role of experts to communicate this to consumers; rather it is the role of others such as educators, the media or those in the public or third sectors to educate. But there seems to be a vacuum of demonstrations of cyber security disruption for consumers and citizens, outside of the recent efforts from the NCSC.

But how are these demonstrations performative? Do they just problematise, generating fear among consumers? These demonstrations show that there are possible disruptions for consumers lurking around every corner. Are they also performative in generating business from those consumers who are now fearful? If this is the case, then my critique is that these types of demonstration leave little agency for consumers and organisations to be confidently cyber secure - without paying lots of money to test and retest for vulnerabilities. Perhaps they are performative in solidifying their expertise and professional vision (Goodwin 1994) amongst their own community.

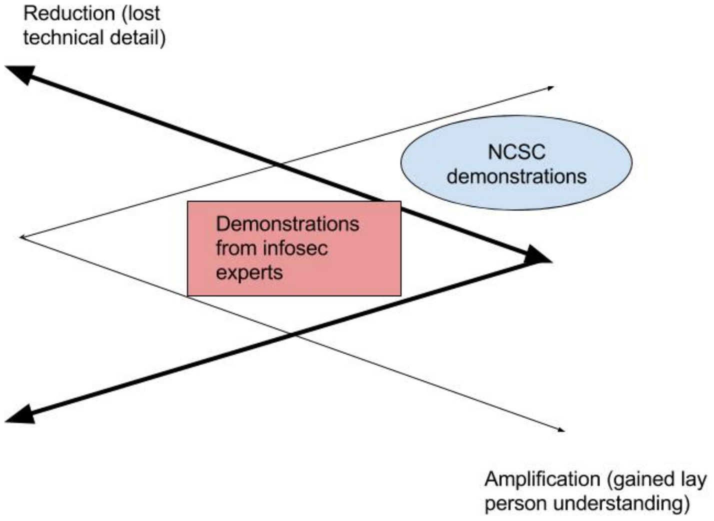

Reduction (lost technical detail)
NCSC demonstrations
Demonstrations from infosec experts
Amplification (gained lay person understanding)

Figure 21: Amended problem amplification (Latour 1999) diagram. This diagram plots cyber security demonstrations on the diagram of lost technical detail versus increased layperson understanding.

I also argue that if we were to use Latour's diagram of problem amplification (see amended version in Figure 21), we can see that the demonstrations of cyber security disruption from core-set experts sit within in an unhappy middle ground where there is too much technical detail to still be amplified. We can also see in Figure 16 that the NCSC demonstrations are amplified, but they are greatly reduced, containing very little technical detail.

Counter to demonstrations from cyber security professionals, the NCSC's demonstrations of disruption are performative in an entirely different manner. The NCSC - and the StSG in particular – have a tough task: to discuss and exemplify best practice in cyber security for a broad range of audiences. Contrary to cyber security professionals, they must demonstrate in a way that is performative and practical. In essence: their demonstrations must *give agency* rather than reduce it; they must empower citizens to make good cyber security choices rather than employ experts out of fear generated by a lack of agency.

The day after I interviewed the researcher from the StSG, I read a report about cybercrime in young people (National Cyber Crime Prevent Team 2017) which stated that the average age of cybercriminals upon arrest was 19, in comparison to the average age of those convicted of drug crimes at 37. This reminded me of the conversation I had with my InfoSec colleague about ensuring devices were secure. He suggested something akin to a kite-mark to denote products that meet a recommended level of security or the ability for consumers to modify or update security settings. According to him, that kite-mark would signify that ‘a 12-year-old can't break into this system having spent 10 seconds looking at this.' However, this level of regulation comes at a cost that manufacturers and consumers may not want to pay. Again, he explains, ‘that is one of these normally regulatory trade-offs is the ‘how much do you want to add to the cost of these things?' Because normally a lot Internet of Things stuff is just pennies or pounds and if you add a regulatory burden to this that adds an extra 50p to a pound's worth of device, that's not very popular.'

He proposes a different solution, one that doesn’t involve consumers having to take care of ensuring their devices weren’t left vulnerable:

> “If the… piece of software ships in an insecure state and you’re required to secure it afterwards, most people [consumers] won’t. But that even goes for Fortune 500 companies and where there’s millions of pounds on the other end of the system partly because they just assume it must be secure. So it should ideally ship in a secure or relatively secure state and equally important it should automatically patch itself. Because people make mistakes, people discover mistakes, it’s nice to be able to fix the mistakes.”

As a cyber security professional, my colleague's ideal solution to preventing young people from engaging in cybercrime is to mandate through regulation that products be made secure to reduce the likelihood of the crime happening.

However, the StSG takes a different view - and this is where the socio-technical comes to the fore - they suggest that legislation and regulation isn't the answer. Much like their demonstration of people-centred security, they support an approach where research is done to identify why people engage with vulnerabilities in technology - in this case, IoT products. While the StSG researcher I interviewed spoke of legislation such as the Data Protection Act, there was more of a focus on solidifying 'a partnership to tackle responsible disclosure of vulnerabilities,' Or in other words, responsible demonstrations of disruptions that could be further exploited. This involved formally accrediting cyber security undergraduate and postgraduate programmes so that the cyber security profession might mature, and that would-be malicious hackers could see cyber security as a legitimate career path. This also aligns with the findings of the National Crime Agency report (2017), which suggested that 'targeted interventions at an early stage can steer potential offenders towards positive outcomes.'

The future for cyber security demonstrations of disruption

As the StSG suggests in their interview, the cyber security profession in the UK (including the NCSC) hasn't yet stabilised. We still see actors such as citizen-consumers implicated in cyber security incidents, who may not be entirely enrolled or literate in cyber security. Part of the immediate challenge for the NCSC is to enrol these citizen-consumers through demonstrations to solidify their status as a trusted entity in the cyber security area. But as these initial demonstrations do the performative work of stabilising citizen-consumers to such a place where they can make informed choices about their own cyber security, they will be able to approach the more complex problems with cyber security. But this is only one piece of the puzzle necessary to avoid cyber security disruption. More broadly, there must be an organisation willing to regulate the manufacturers of vulnerable products that cause disruption. It mustn't be solely down to the self-responsibilised citizen to ensure cyber security.

The NCSC are in the relatively early stages of demonstrating disruption to the public, in comparison to the strides that Transport for London has made in demonstrating commuter disruption. When asked about the nature of the NCSC's demonstrations on social media, my interviewee from the StSG said that it's mostly one-way, with very little response from the public. Could there be a possibility for the NCSC's social and digital media use to become similar to that of TfL's, with citizens being able to demonstrate and discuss their own disruption, thus starting a problem-solution relationship (Garfinkel 1967), enabling the StSG to find further lines of enquiry about people-centred security?

The cases discussed in this chapter have shown that it is not enough to problematise when demonstrating a cyber security disruption, much like the cyber security profession has done for years. Demonstrations aimed at citizen-consumers need to have performative, reflexive aspects, allowing the audience to have agency and act according to the knowledge they gained. We see the beginnings of this happen through the work and demonstrations of the StSG.

However it will be interesting to see how their demonstrations change in nature over time, according to the further enrolment of citizens and stabilisation of cyber security.

But there is one elephant left in the room. Cyber security is dependent on technology and verification processes that help certain people access data and yet prevent others from doing so. And yet cyber security is a process of ever-shifting goalposts with the expectation that human actors are willing and able to keep up. Rather than being enrolled into cyber security, human actors are conscripted into various processes to keep themselves and their data safe and chastised when they cannot keep up or cannot quite act according to the correct process. In a similar manner to the activities of TfL, the technology of cyber security changes over time and so to do the processes that support it. Could cyber security-related demonstrations of disruption look different if the emphasis was flipped and placed on what human actors were feasibly able to do, with those responsible for designing and producing non-human actors being enrolled to meet those needs and requirements?

Conclusion

This chapter has examined how demonstrations of disruption *could* be used to educate and enrol citizen consumers in adopting better cyber security practices. I say ‘could’ because this chapter has highlighted problems with existing demonstrations of cyber security related disruption that can be shown through the analytic framework of problem amplification (Latour 1999). The existing demonstrations analysed in this chapter show that citizen consumers encounter detailed demonstrations of disruption that require a high level of technical expertise to understand and apply to everyday life. On the other end, demonstrations of how the Internet of Things works in everyday life are simplified to the point where complex security considerations are omitted.

However, this chapter has also highlighted and examined how government organisations such as the NCSC attempt to demonstrate disruption and enrol citizen consumers by explaining common practices that lead to cyber security disruption. This approach is not only a form of problem amplification, but it also produces reflexivity amongst their audience with, in turn, enrols them in improving their cyber security practices.

In the next chapter, I step aside from examining the demonstrations of disruption from the standpoints of the digital as a setting or the digital as an actor or assemblage to be disrupted. Instead, I use the digital as a research instrument to attempt to locate demonstrations of disruption about the selfie stick.

Chapter 6: Using the digital to detect the disruptive selfie stick

Introduction

In previous chapters, I examined the roles of the digital as a setting and the digital as an actor in demonstrations of disruption. In Chapter 4, I examined how the digital might be understood as a setting for demonstrations of disruption through the fieldwork with Transport for London. In Chapter 5, I looked at how the digital could be considered as an actor or to be disrupted through the research of digital demonstrations of cyber security issues and best practices. In this chapter, I will discuss the introduction of the selfie stick as a disruptive object in public settings and describe how digital methods can be used to detect disruption. As we will see, part of the difficulty here is how and where to locate demonstrations of the selfie stick's disruptiveness. Even though disruptions were reported in the news, it proved difficult to detect them elsewhere. As such, this chapter shows the difficulty in locating and researching the 'theatre of failure' for the selfie stick amongst other demonstrations of the selfie stick that do not address its disruptiveness. I will describe how myself and colleagues from CISP[58] attempted to locate selfie stick related disruption using digital methods involving social media platforms such as Twitter and Instagram. Then, I will describe a change in course to try to detect the disruption through the ethnomethodological method of the breaching experiment (Garfinkel 1967). I describe how I then used a hybrid of the two methods to find explanations of the selfie stick's disruptive attributes in the comments section of blog posts and online news articles.

[58] CISP is the Centre for Invention and Social Process at Goldsmiths, University of London. It is a multidisciplinary centre that gathers around Science and Technology Studies.

Why examine the selfie stick as a disruptive object?

On first glance it seems trivial to devote an entire chapter to the selfie stick. The mainstream media discusses faddish objects such as the selfie stick, hover boards or fidget spinners through opinion pieces (that often critique the object and its users), or articles about venue managers seeking to ban them in public spaces. The use of opinion pieces acknowledges the existence of these objects; it also dissuades a critical examination of how their introduction and spread throughout everyday life impacts the social order. Meanwhile, the specialist technology press loves a good biomedicine story, or a report on the latest corporate hacking scandal, or news about developments in the self-driving car industry. But the selfie stick? For all intents and purposes, it is just a telescopic pole with a clamp at the end. If you are lucky, it will come with a remote or be Bluetooth enabled to allow you to take photographs without having to fiddle about with a self-timer. How can the selfie stick be examined from a Science and Technology Studies standpoint? Similarly, how has this rudimentary object provoked so many opinion pieces and become an object that has been banned in venues around the world?

While science and technology studies in both theory and research to date has devoted some time to everyday and mundane objects - such as Velcro (Michael, 2006), seatbelts, automatic doors (Latour, 1992), rubbish bags (Woolgar and Neyland, 2013), teapots (Marres, 2011) and, washing machines (Shove, 2004), it has not devoted much time or word count to objects that appear on the ‘Most popular Christmas gift of 2014’ list. But the faddish nature of the selfie stick is precisely the uncharted waters to wade in to in order to discover why mundane objects help us better understand disruptions and how they are described, how people convince others of an object's disruptiveness. These faddish objects arrive seemingly out of nowhere but demand that we pay attention to them and the activities to which they seem so essential. This reasoning is similar to the reasoning for studying the pervasiveness of the mundane (Woolgar and Neyland 2013), being that trivial and small matters take up a lot of our everyday, and reveal volumes of how we approach the world and others.

In comparison to the disruptions that have been described in previous chapters - which deal with disruptions to public transport internet or cyber security infrastructures - this chapter deals with how the selfie stick object could be considered disruptive to other actors in public spaces. But the selfie stick is not necessarily just a negative disruption. It is also a disruption of how people consider the process of creating images in public places to be disrupted. Rather than being asked by strangers to take their portrait in public places, the selfie stick is a 'tool forced upon' (Verbeek, 2004) us that asks us to reconsider how we create photographic images in public.

The possibility of many types of disruption related to the selfie stick prompts some questions. How do we know that the selfie stick is disruptive? And how might we study it? One way the disruptiveness of the selfie stick could be examined is through breaching experiments similar to those carried out by Garfinkel (1967/1991) whereby he recruited his students to temporarily adopt strange mannerisms among - for example - family members in order to understand the expected social behaviours in those settings. Rather than deliberately fabricating breaching experiments, the unprompted digital demonstrations of selfie sticks on social media allow us to examine how the object is used to expose expectations about social behaviour in these settings.

For some this disruption of the selfie stick is a welcome, positive disruption, in that it is a device that enhances someone's photographic capabilities. It is self-portraiture made easy. On Instagram, people who have recently purchased a selfie stick post self-portraits with friends, family, pets, or landmarks to demonstrate how this positive disruption to their photographic practices. Yet to others, it is a negative disruption. It is dangerous, unwelcome, mockable and - somewhat bizarrely - a spark of further tech-related moral fear, worry, and lament.[59] It is narcissism made easier. The selfie stick is disruptive, but is its disruption provocative enough to be an issue? To find out more, it is necessary to find the demonstrations of selfie stick disruption to determine where and how people understand the social disruption they attribute to selfie sticks.

What precisely does the selfie stick disrupt? At the base level, it is a seemingly mundane disruption or innovation and, in most circumstances, a welcome or benign one. Let's take Latour's example (1992, 225-258) of innovation to the entry to the Ecole des Mines, where an automatic door took over the function of a doorman that would have once stood at the door to ensure the elements, unwanted strangers, and creatures were kept separate from the building. It is

[59] I do not want to go so far as to label this a 'moral panic' which is indicative of something more akin to Cohen (2002), Young (2009) or Hall et al's (1978) work around social, political or economic crisis. To be sure, the dis-ease and criticism towards digital technologies and social media seems to originate from a moral standpoint around how people should view and present themselves to others, as we will read in this chapter. However, these criticisms and fears do not amount to a moral panic, at least not yet. Some do use texts from scholars such as Turkle (2011, 2015) and McLuhan (1960) to justify their fears.

easy to draw comparison to this account and say that the selfie stick has taken over the function of the person co-opted to take the photograph. But this base level disruption, while technically accurate, doesn't ring true to the discourse surrounding this disruption.

Looking past the base level, literal description of the disruption caused by the selfie stick, we see a surprising and varying number of objections to the selfie stick that are removed from the replacement of a photographer with a stick.

The selfie stick was introduced for sale in mid-2014 (BBC Trending 2014). I first started noticing their use in public places soon after returning to London to commence this PhD. While taking walks along the Southbank past vantage points for landmarks such as St Paul's cathedral and the London Eye, I noticed that more tourists were using selfie sticks when posing with landmarks, rather than asking passers-by for assistance. Towards the end of 2014 there were news articles and opinion pieces written that described the increase in selfie stick use in public places, along with some critique of people using the object. These news articles described locations in the UK that were starting to ban the object, and reports from South Korea that stores selling unregistered selfie sticks[60] could face a fine of more than £17,000 (BBC 2014)

The field in this case, takes up multiple locations and multiple methods, as I am particularly keen to see how the disruption differs across these different fields. These fields include two social media platforms (Twitter and Instagram), along with a selection of online news articles and, a field visits to major tourist

[60] In South Korea, selfie sticks that are Bluetooth enabled must be registered with the radio management agency because they may use frequencies that interrupt other devices (BBC 2014)

locations around London. Each part of this chapter will look at a different form of disruption and helpfully, each of these locations of demonstrations are revealed with a different field.

Through looking at these different ways of examining the selfie stick, I examine how it could be considered an issue from an Actor-Network Theory (ANT) standpoint. And while I will not be referring specifically to Goffman's work on performance (1959) or behaviour in public places (1963), as explained in the literature review, it is important to consider how the digital has impacted the setting and scriptings of demonstrations of disruption while reading this empirical chapter.

Observing the selfie stick through a breaching experiment

The selfie stick is a part of everyday moments because it is an object that is used to capture everyday moments. However, the use of the selfie stick in these everyday settings disrupts the space and the expectations of how people and objects are 'supposed' to interact in public places. One example from Instagram involves a 'creepshot' image (a covert image taken without the consent of the subject) of a woman in an art gallery. This both a demonstration of disruption and also an ethnomethodological breach as the selfie stick upsets the expectations of how people are expected to interact with art. Demonstrations such as these show how the selfie stick and those using them can disrupt gallery spaces and gallery visitors as they stand beside and close to the object or artwork, holding a stick away from them and the object in order to create an artefact of the visitor-art encounter, physically closing off other people from seeing the art until they have completed their interaction. These

Instagram based demonstrations of disruption involving the selfie stick (such as the one described) show how the selfie stick is considered by demonstrators to be an obstructive object in a public space. Demonstrations such as these also include captions that include further critique about the object and its disruptiveness. In the particular demonstrations I refer to, the caption includes the phrase “LOOK AT THE ART!” which describes the behaviour that the demonstrator desires others to have. As we will see in the next section, this breach was seen to be so problematic that the selfie stick was banned in some venues.

This new act of creating images with the art causes a disruption of a different form, which cause us to question why it is so important that people want to include themselves in images of art. This form of questioning the necessity of a person including him or herself in the frame has led to the selfie stick gaining the attribute of being ‘narcissistic’, as it is an object that enables people to take self-portraits. However, as Latour (1999) would remind us in his example of gun-related violence, the selfie stick in and of itself is not narcissistic, because they are being published for others to see[61]. But when teamed up with a person who is very keen to take and publish self-portraits, it is plausible to see how it acquires this attribute

Finding the ‘theatre of failure’ for selfie stick disruptions

In this chapter, I describe how selfie sticks are disruptive in two ways: both positive and negative. But how do we know this? How can we find evidence to back up this assumption? The challenge in this chapter is in locating the

[61] Rather than as an image that someone has for their own admiration, to take the mythology of Narcissus literally.

demonstrations so that we might be able to observe how selfie stick related disruption occurs and who demonstrates this and to what audience.

In the first instance, there was an attempt to locate the ‘theatre of failure’ through a collaborative social media data-scraping project.[62] This is the first account looks at using a digital methods (Rogers 2009, Marres 2015) approach to locate the ’theatre of failure’.

As discussed earlier in Chapter Three, a digital methods approach is the practical application of conceptualising the digital as a research instrument (Marres 2017). For the purposes of this thesis it involves using digital tools to gather data and produce a corpus (or a ‘data scrape’) of tweets or instagram posts in order to conduct analysis to detect the emergence of an issue. From a practical perspective, this involved using digital research tools such as TCAT[63] to gather tweets and, IFTTT[64] to gather Instagram posts containing the #selfiestick. In framing the digital as a research instrument, the hashtag itself is also considered as part of the digital, but as an object of research.

In analysing the tweets and posts we had scraped, we were attempting to determine whether the selfie stick was an issue. This involved using TCAT and the associational profiler tool to conduct issue mapping of the selfie stick. Marres (2017) describes issue mapping as work that ‘relies on online

[62] This social media data scraping was done as part of the CISP Salon in March 2015, which attempted to locate the selfie stick as an issue on Twitter, Instagram and, in situ. Many thanks to Noortje Marres, David Moats and Ana-Maria Herman for their collaboration.

[63] TCAT stands for Twitter Capture and Analysis Tool. It was created by the Digital Methods Initiative at the University of Amsterdam. It connects to the Twitter API to collect a sample of tweets from any given query.

[64] IFTTT stands for IFThisThenThat. It is a web based tool that allows you to create an automated process by outlining a set of instructions (or as they describe as ‘creating a recipe’). For the purpose of this piece of research, the instructions were: IF someone creates a public instagram post containing #selfiestick, THEN add that post to a line in a spreadsheet.
This is just one way that IFTTT could be used. There are other ‘recipes’ for very different things. For instance people can create ‘recipes’ that work with their smart meter or thermostat data.

techniques like hyperlink and hashtag analysis to locate, analyse and visualise so-called ‘issue networks’ on the Web – networks of organizations, individuals and other agents assembling around a common topic or concern’ (p. 85). This proved difficult particularly with examining tweets because the analysis hinged on co-word analysis [65](Callon et al 1983, Marres 2012) in order to determine what else was being written about or occurring frequently alongside mentions of the selfie stick. The problem with the corpus of tweets was that it contained a bulk of tweets from people who did not follow formal conventions for tweets. Rather than using hashtags to join a conversation about an event or subject, the hashtags co-occurring alongside the #selfiestick tended to be nondescript or nonspecific to the selfie stick such as #love, #happy, #NYE, #2015 (we conducted the data scrape in the Christmas / New Year period in 2014/15). This confused us because in comparison to other projects that used co-word analysis done with Twitter data (Marres 2017) the words used along the main query help to describe an event or a subject or some of the issues around it. The problem with the words brought up alongside #selfiestick was that #love and #happy tend not to do similar work. They describe how people were feeling when they took the picture (with the selfie stick) but it does not describe how the selfie stick may have been disruptive in either a positive or a negative way. But more crucially, the hashtags used alongside #selfiestick were not used to co-ordinate a discussion with a group of Twitter users about its disruptiveness (or lack of disruptiveness). In this circumstance, the lack of social media literacy of Twitter users has methodological implications for using issue mapping to detect

[65] Co-word analysis (Callon et al. 1983) started life as a method ‘to detect the emergence of happening problems and topics *at the intersection of categories* and fields.’(Marres 2017). This method has been tested as an ‘interface method’ by Marres and Gerlitz (2016), who investigate how co-word analysis could be modified and conducted with social media data such as hashtags to identify the emergence and relevance of hashtags over time, as well as how hashtags relate and appear alongside one another over time.

ongoing demonstrations of the selfie stick and disruption. Because of this lack of hashtag literacy from Twitter users discussing the selfie stick, other digital methods needed to be explored to detect selfie stick related demonstrations.

In comparison to Twitter, I collected more than 10,000 Instagram posts that included #selfiestick in the caption. Rather than conducting a co-word analysis on these posts[66], I conducted a visual analysis of the scraped images and coded them according to the caption and composition of the picture. Conducting a visual analysis allowed me to see the situated practices (Suchman 1987/2012) of people using the selfie stick; the settings they were using the selfie stick in, who they were including in the picture and, how the caption corresponded to the image.

In this sense, the analysis done with Instagram posts located the ‘theatre of use’ for the selfie stick. I learned that people created Instagram posts incorporating #selfiestick showed how for the most part it made a positive disruption to their selfie-taking practices. I was able to see that people were able to incorporate more actors (be they human, non-human or more-than human) into their photographs. There were also images taken with a selfie stick that managed to include the object within the frame. It’s unclear whether in that situation the selfie stick was considered to be disruptive to the image or whether the person posting the image was happy to share the frame with the object. But in conducting this visual analysis, there were moments where the ‘theatre of failure’ emerged.

[66] When using TCAT, there are additional tools that allow you to conduct co-word analysis, along with other forms of analysis. However, due to the way I collected Instagram data, there was no easy way of conducting a co-word analysis.

The selfie stick as a banned object

While the CISP group was conducting the pilot study attempting to detect an issue related to the selfie stick, there were reports of selfie stick bans coming into place at public venues in the US and the UK. One of the highest profile selfie stick bans was at all of the Disneyland theme parks. The company announced in late June 2015 that ‘Visitors will now be asked to leave their selfie sticks in lockers at the parks' entrances to collect later.’(BBC, 2015) The park-wide ban was reported to be an extension of an existing ban on all of the rides due to the potential for the selfie stick to interfere with and damage the mechanism of the rides. This ban makes the assertion that the network of human and the non-human entities comprising the theme park ride were stabilised prior to the introduction of the selfie stick. But upon the selfie stick’s addition to the network, this equilibrium was effectively destroyed with potentially deadly consequences.

Although on one hand, banning the selfie stick from ‘the happiest place on earth’ seems like a killjoy manoeuvre (as some selfie stick enthusiasts on Twitter have mentioned), on the other hand it would seem to come from a place of genuine concern and pragmatism in safeguarding against selfie-related injuries. Similarly, while the same BBC article that reported the selfie stick ban also mentioned that ‘A spokesperson for St John Ambulance said the first aid charity had not noticed a surge in selfie stick-related injuries’ (BBC); in Russia there has been a campaign for safe selfie taking practices. Authorities in Russia instigated the campaign after an increase in selfie-related deaths or serious injuries involving people who were taking selfies in extreme locations or situations. Among the road sign styled symbols is a depiction of a person using a selfie stick in front of an oncoming train. These bans and reports around them suggest that there is potential disruption to be had to both humans and non-humans. But when it comes to finding reports of actual disruption happening, evidence is hard to find, as shown in the BBC's quote from St John Ambulance.

Figure 22 Image from a Russian safe selfie-taking campaign from 2015. It depicts the various situations that citizens are not advised to take selfies in (Russian Interior Ministry 2015). [redacted for copyright purposes]

The examples of both the Disneyland bans and the Russian selfie safety campaign shows an important point with regard to how we can understand the selfie stick from an STS perspective. If we take an Actor-Network Theory perspective of considering whether the selfie stick is disruptive, we could come to the conclusion that it is not; at least not when it is thought of as a non-human actor in isolation. Comparing the selfie stick to the situation we see described in *Pandora's Hope* (Latour, 1999) where Latour discusses the situated danger of guns, we see that the selfie stick only presents a danger when it is coupled with a human actor. The danger of the selfie stick is mitigated when the non-human object is decoupled from its human operator and is in the safety of a locker on the outskirts of Disneyland's premises, away from other people and other machinery that could injure and cause harm.

But did the selfie stick carry the disruptive attributes reported online? How might people in public places explain or demonstrate the potential for selfie stick related disruption, especially in light of the growing list of bans? In order to explore this question, I carried out some in-situ research. The National Gallery in London was one of the venues reported to have banned the selfie stick (BBC 2015). In comparison to searching and scraping for digital demonstrations of selfie stick related disruption on social media, the National Gallery's ban presented an opportunity to understand the selfie stick from a different vantage point.

Instagram as a 'theatre of failure'

In particular, there was a category of selfie stick images involving the Instagram user taking a picture (sometimes covertly) of other people using selfie sticks in front of artworks in a gallery or elsewhere. This type of image serves to make the selfie stick visible by highlighting the fact that it is in a setting where it can cause damage to other human actors or non-human actors that are deemed valuable, such as artworks or artefacts. These images resemble creep shots: a form of image where someone takes a photograph of someone else without their knowledge or consent and posts it online (Burns 2015).

In one image[67] (mentioned earlier in the chapter) there was a picture of a woman using a selfie stick to take a selfie in front of a piece of art. The image was blurry, indicating that it was likely a creep shot, taken hurriedly without the subject's consent. The caption complains about the person in the image and asks them to "LOOK AT THE ART" (emphasis from the caption). It also includes hashtags such as #ego and #art alongside #selfiestick. This post is an example of a demonstration of selfie stick related disruption because it is attempting to convince the viewer of the disruptive attributes of the person-selfie stick hybrid in the art gallery setting. This image depicts a setting where the selfie stick is disruptive both because it is physically blocking people from moving within the

[67] I've chosen not to include the image within this thesis on ethical grounds because it is unclear and unlikely that the subject of the image has given their consent to be photographed.

space, but also because its use is drawing the attention of other gallery visitors away from the art.

Further, this type of image and the accompanying caption polices selfie stick use by describing the behaviour the demonstrator expects people to adopt in galleries – looking at the art as opposed to standing with it. The demonstrator also uses the hashtag #ego to describe what they consider egotistical or narcissistic behaviour. This demonstration aims to do the opposite of enrolling people actors into certain practices and instead, acts as a deterrent to those who consider taking their selfie stick into an art gallery. One may speculate that these types of demonstrations involving creep shots are essentially acts of surveillance of people and their practices within a public space. On a more subjective level, these demonstrations place assumptions on a person's cultural capital. In the eyes of this demonstrator, someone carrying and utilising a selfie stick in a public cultural space is presumed to have less cultural capital in comparison to someone who stands silently and thoughtfully in a museum. Through the eyes of some Instagram users, a selfie stick is seen to be a cardinal gallery sin, similar to running or shouting in the space. Thus, the demonstration is performative and the object gains disruptive, uncultured attributes and portrays the selfie stick user as someone who cares only about art in order to be seen with it, not to contemplate it, admire it or, intellectualise it.

Although there have been partial encounters with demonstrations through using digital methods, there were few empirical examples of demonstrations - apart of news media reports - explaining how the selfie stick could be considered disruptive. There was an absence of Twitter or Instagram users demonstrating disruptions that they had encountered. During the digital methods exercise and for a while after, there were news articles describing how the selfie stick had been banned in public venues across the UK.

From the analysis of the Instagram dataset, the group collaborating with digital methods were able to see demonstrations of the settings within which the selfie stick was disrupting the expected interactions between people and objects. The CISP group was able to see how Instagram was used to report these 'breaching moments' that demonstrate disruption in public places. However, for the purposes of the pilot study to detect an issue - or for the purpose of detecting demonstrations of selfie stick related disruption - we were still no clearer to finding a well-coordinated disagreement or discussion between opposing parties that could chart the problematisation of the selfie stick.

Comparing digital attributes to in-situ observations

In March 2015, I purchased a selfie stick and conducted a breaching experiment in a public place where it had been banned. The breaching experiment followed Garfinkel's approach (1967/1991) to a certain extent in that I deliberately broke an established rule in order to enquire about the reasoning for the rule. I diverged from Garfinkel's approach in that he usually devised the breaching experiment, but asked others (often students) to carry out the activity so that he could analyse the results afterwards. I devised and carried out the breaching experiment and so it took on an auto-ethnographic element. From a reflexive standpoint this confronted me as I didn't particularly want to purchase a selfie stick and I'm not a rule-breaker by nature. This made the breaching experiment difficult because I was balancing the need to conduct the experiment to provoke a discussion about the selfie stick and its disruptiveness with my own discomfort about being caught breaking a rule in public. At times it felt as though I had to have a conversation with myself and attempt to understand the reason for my reluctance to break a rule. But as far as rule breaking was concerned, the stakes were rather low. And in terms of adding another offline perspective and some tacit knowledge to the multi-modal research (Hine 2015) around selfie sticks, it would prove invaluable. I would become a selfie stick owner, a selfie stick user, and perhaps not a compulsive selfie or 'groupfie' taker but I could at least have a chance of understanding the object better by getting my hands on one.

I brought along a friend to join the breaching experiment. This was so that I could experiment with the practices of using the selfie stick to take a picture with more than one person in the frame – as being able to include more people within a selfie (or groupfie as they become with more than one person) is one of the selling points of the selfie stick. It was also so that I could reflect on the breaching experiment with someone else.

We went to the National Gallery on a Saturday afternoon. We had a few practice runs with the selfie stick outside the entrance in Trafalgar Square before venturing in. As we entered, we noticed a sign saying that the some rooms of the National Gallery would be closed due to strike action. I immediately wondered how this would change the setting and impact on the attentiveness of the gallery docents towards my rebellious behaviour.

My friend studied art at university and wanted to show me a Caravaggio painting but it was in one of the closed rooms, so we went to another gallery with an optical illusion painting that both of us were familiar with. As we angled ourselves to see the skull appear in the painting, we decided it was time for the first breaching experiment attempt. For our first selfie stick picture we deliberately placed ourselves slightly out of sight of a docent. We felt quite silly taking a picture but we did it, knowing we would have to do it again. We took eight photographs with the selfie stick, each time within line of sight of docents or security guards and at least twice we timed it so a guard would be walking directly past as we were taking a picture. Each time we thought we would be tapped on the shoulder and politely told to stop. We were never told to stop. If the docents noticed, they didn’t care. In a final act of desperation, we stood on the steps in the foyer area and deliberately tried to take a photograph with a docent in the frame. In the end, my hair ended up blocking the docent in the image but as we were taking the picture, a National Gallery employee walked past; and said nothing.

In discussing it with my friend, we had two observations. The first rather obvious conclusion was that using a selfie stick in a gallery makes you stand out and look rather foolish. This can be shown by the Instagram posts - such as those discussed earlier - by people who have noticed those using selfie sticks in public places. A person using a selfie stick to take a picture with a work of art is still an unusual event, more unusual than similar activities such as people taking art equipment into a gallery and sketching the work. The second, more surprising conclusion came from my friend. She admitted that the visit to the National Gallery was *more* enjoyable than usual because of the breaching experiment and the fun of breaking a rule and not getting caught. She explained further that the breaching experiment involved an 'element of uncertainty, curiosity and you got to see art.' For her that enhanced the gallery experience because sometimes she felt that when she is in a gallery she has to see it all. But because we were there primarily to break rules with the selfie stick, we walked into a room, saw the artwork that caught our attention, attempted to create an image with the selfie stick and then quickly moved on to the next interesting piece. For her, the selfie stick disrupted the way she interacted with the gallery. She paid less attention to the layout of the space and the ways the space was designed to encourage a prescribed pathway through the space. Instead, the breaching experiment with the selfie stick in the gallery made her focus on the pieces of art she wanted to see and be seen with.

Disruptive, but not too disruptive?

How do we understand these observations in comparison to the attributes acquired by the selfie stick via digital media? To unpack this question further: How might we compare reports and observations of selfie stick disruption occurring both in a digital setting and in situ? And how might we compare conflicting reports that are mediated differently due to the settings they take place within? In this circumstance, the selfie stick did not physically disrupt the gallery in terms of harming other gallery visitors or valuable objects. Despite there being a selfie stick ban in place at the National Gallery, our use of the selfie stick when conducting the breaching experiment did not result in a reprimand or provide an opportunity to seek an explanation for the ban from those responsible for administering the ban. What does it say about the selfie stick's supposed disruptiveness if some places have seen fit to impose and publicise a ban, but not implement it? In these respects, the digitally demonstrated attributes of the selfie stick do not match up to the offline experience of using the selfie stick in public.

However, while the selfie stick was not disruptive in accordance with the attributes it had acquired, it was disruptive in other ways. It disrupted the interaction of the selfie stick using gallery visitor within the space because the ban meant that the selfie stick had taken on the attribute of being an unwelcome object in that setting. The disruptive attributes to the selfie stick in the digital and had transferred across to the offline setting and had an impact on the way I encountered the space. But what to make of this transferral of attributes from the digital setting to the in-situ setting, especially when these attributes were not founded in the expected response?

Additionally, the selfie stick caused disruption in the way it made us interact with the space; this is something that had not been demonstrated online. The addition of the selfie stick to our gallery visit shifted the possibilities of how we could interact with the art and the space. Because we were able to create images and artefacts rather than merely look at them, we did not navigate the gallery in the linear, recommended way encouraged through the layout of the space.

But was the breaching experiment a success? After having two and a half years to reflect on it, I think it was and it wasn’t. While I didn’t get reprimanded for using a selfie stick in the space and therefore not receiving an opportunity to ask someone in authority about the ban, my friend and I didn’t leave the setting empty handed in terms of observation and insight. If I were to compare the breaching experiment to those written up by Garfinkel (1967/1991) in *Studies in Ethnomethodology* then perhaps it was a failure because I didn’t get that moment to ask for an explanation. In an ideal situation, the whole point of a breaching experiment is to reproduce a situation where a rule or expected behaviour occurs to enquire further into the reasoning for it. The breaching experiment helps us gain an explanation for the phenomenon that may otherwise have been left unspoken and taken for granted. But what is a researcher to do when those moments of provocation and explanation do not arrive? What are you to do when you are the actor on the stage in the ’theatre of failure’ but your fellow actors do not say their lines or do not even enter scene? On one hand the breaching experiment was a failure. I did not get to have the much anticipated conversation and explanation. But on the other hand, it was not a *complete failure*. It forced me to reflect on what was not said. It also allowed me to think about other ways I might seek out the ‘theatre of failure’ and those breaching experiment style explanations of the selfie stick’s disruptive attributes. It also allowed me to consider how I might return to the digital as a research instrument to seek out ethnomethodological explanations of selfie stick disruption online.

Disruption offline, discussed in the comments section

The process of trying to locate a ‘theatre of failure’ for the selfie stick felt frustrating at times. When discussing the research with friends or acquaintances (many of whom had never wielded a selfie stick), there were so many reactions and rich descriptions of why they objected to the object. It was difficult because those conversations do not make for good, ethical, empirical data[68]; nor are they located in the digital. But these conversations made me certain that they were also there in some digital format, in a digital setting. But by doing another scrape of #selfiestick on Twitter after a rush of bans had come into place, mostly in the US, I was able to see that some of the tweets linked to news articles reporting on the ban. Perhaps these news articles and the comments below them would provide me with a 'theatre of disruption' to observe.

As a contrast to Twitter and Instagram, I found the comments section of online news or opinion pieces to be a rich ground for discussing the selfie stick as a problematic, disruptive object. In particular, I examined a news article from the feminist online news website Jezebel which describes the selfie stick ban at the Smithsonian Museums. This article was chosen for analysis because it described the selfie stick ban and allowed a comment section for people to discuss and respond to the article and to other commenters. This article is very critical of selfie stick use with the headline "The Smithsonian Says: F*** Your Selfie Stick" (Jezebel, 2015), and has a bias against the selfie stick. However, the comments section contained some interaction among commenters with people discussing, explicating and debating the pros and cons of the selfie stick and its use in public spaces.

For example, as one commenter describes their understanding of the selfie stick:

[68] I chose not to write up these conversations as fieldnotes because they were conversations that happened in the pub, or in cafes with friends when I was describing my work. Most of these conversations were with people who had not used a selfie stick or knew anyone who used a selfie stick. It was hard to determine whether they objected to the selfie stick based on first-hand experience or based on news media that they may have encountered. On one hand, the decision not to write up any of this as fieldnotes was an ethical decision, they hadn't given consent and although they would have been anonymised, these conversations were happening in a setting where I was not clearly a researcher.

> “I don't have one (nor will I), but I work at a place that people take lots (and lots and lots) of pictures at, particularly selfies. It's a thing that once rang, but can't ring anymore. You get the idea. SO MANY DAMN SELFIE STICKS. And they do exactly what this article says: endanger the resource (they get soooo close to the damn thing with them, trying to take picture around, under, what have you) and I've seen more than one visitor whapped upside the head with them. And like most technology, it never really works properly the first time, so people try again and again and again, taking up lots of space, almost hitting lots of people and making the wait to see said object much longer. We've started to have to put the kibosh on them during busy hours.”
> - Comment on article “The Smithsonian Says F*** Your
> Selfie Stick”, *Jezebel* 3 April 2015.

This was an example of an explanation we were looking for within the pilot study to locate the selfie stick as an issue and, it was also a demonstration of disruption.

The highly critical tone of the article acted as a breach of sorts and provoked a response from the readership, some of whom supported the author’s standpoint and others who did not.

The comment section of the article included anecdotes of people who had witnessed selfie sticks being used in public places and their reaction to them. Interestingly, the comments from the Jezebel article contained more anecdotes from people who worked in places where the selfie stick was often used. They were the very actors my friend and I tried to provoke a response from through doing an in-situ activity.

There is a great deal being said in this comment, more than could be expressed within 140 characters on Twitter or within an Instagram post. It could even be more than what that actor could be willing to describe in-situ while identifying as someone who works for that institution. Could this finally be the digital form of an ethnomethodological provocation for an explanation of the selfie stick's disruptive attributes?

As discussed earlier in the chapter, the comments on online article describe these disruptions happening when a hybrid of a person, selfie stick and camera occurs within a public space such as a gallery or museum with precious objects that are expected to be the focus of attention. They never occur when one actor is missing from the combination - take away the selfie stick and the visitor no longer has the capacity to create an image in the way that the selfie stick allows. This is similar to the situation in the previous chapter with InfoSec professionals and cyber security vulnerabilities. Much like a hacker being stripped of the technological vulnerabilities would prevent them from carrying out a job; so too would stripping a museum patron of a selfie stick would prevent them from taking a picture with *and* potentially harming a valuable object.

Remove the people from the setting and the selfie stick loses the actor and actions responsible for its disruptive attributes. Remove the gallery setting and the objects within it and you no longer have a reason and object to create an image with. However, this commenter blames the technology (in this case, the selfie stick) because 'it never really works properly the first time' and thus makes others wait longer to see the object of interest. It is this portion of the comment that I find particularly interesting, as the commenter describes the fallibility of the selfie stick rather than the disruptive actions of the person using it. What is also curious to note is that this comment highlights the fact that the selfie stick is not only spatially disruptive but it is also temporally disruptive. The selfie stick's inclusion in settings where there are more people attempting to see a popular object results in its exclusion 'during busy hours'.

Further in the comment section of this article, we see demonstrators sticking up for the selfie stick, but their reasoning differs from the detractors:

> "Okay, so I know admitting this means I'm telling y'all that I'm a huge dork, but whatever. Here's the thing... I absolutely love museums, but I like going to them alone so I can visit at my own pace. And I like to take pictures of the items at museums. Every once and a while there is something on display that prompts me to take a selfie with it in commemoration. (My dad once told me that a beautiful picture without me in it is just a postcard, not special to my trip.) And simply holding the camera up with my arms does not do the job. Plus, I'm pretty shy with strangers and do not like asking people to take my picture. So, selfie-stick. But rarely! And I'll wait until no one is around to avoid becoming a nuisance. So, yes, I use a selfie-stick. (Or did use one. I doubt I will anymore after this.)"
>
> -Comment, "The Smithsonian Says: F*** Your Selfie Stick", *Jezebel* 3 April 2015

This comment highlights some of the reasons for wanting to use a selfie stick. This commenter acknowledges their shyness and their preferences for visiting museums on her own. Through explaining why she uses the selfie stick in places such as these, she demonstrates that the object helps her overcome a problem without having to navigate the social anxiety of approaching a stranger for help. In this situation, the selfie stick acts as the stranger she is too nervous to approach for help. This echoes Latour's discussion on the introduction of automatic doors as a non-human replacement for doormen (Latour 1992). However, she describes her awareness of the strong negative perception of the selfie stick that has been demonstrated through digital and social media, as well as the possibility that she may have encountered that perception in-situ. She also describes how she avoids situations where others are not in the vicinity so that she will 'avoid becoming a nuisance.' From this comment, she is acknowledging herself and her selfie-stick as having the potential to be disruptive. Later she says, ‘I doubt I will [use a selfie stick] anymore after this,’ which tends to indicate that she is self-conscious to the point of refraining entirely from taking selfies in museums rather than feel the judgment of her fellow commenters. This shows that the selfie stick has the ability to take on agency that has been ascribed to it by another person (i.e. The detractor). This in turn has changed the relationship between the person and the selfie stick where once the object was an aid in an uncomfortable situation, it is now the cause of uncomfortable situations as the person realises the scorn others have for it and, by association, her.

However, this commenter’s demonstration of her own selfie-stick related disruption, has caused others within this ‘theatre of failure’ to be reflexive about their standpoint. In a response to the above comment, another commenter said, “You seem to have legit selfie stick reasons. I'm apportioning you a nerd pass. Get on with your bad self and your nerd-stick.” (Jezebel article, 2015) this response shows that counter demonstrations of the usefulness of the selfie stick are able to enrol detractors in some of the positive disruptions of the selfie stick.

Conclusion

In this chapter, I explored how the digital could be considered as a research instrument to find and examine ‘theatres of failure’. In many ways, this raises more questions than it answers, as detecting disruption with digital methods was not as straightforward as we initially imagined. To locate the positive and negative disruptions attributed to the selfie stick, I had to take a roundabout path. It took a level of persistence that challenged popular narratives that the digital makes research easy, more traceable or more analysable.

Digital methods have been said to enable 'real-time research' (Back, 2012): these can be used a research instrument *while* the phenomenon is emerging. This is because many online research tools gather and analyse social media data *as it is produced and published*, rather than being used retrospectively. This has many implications for research design and analysis. The researcher must detect *the potential* for there to be a phenomenon worth studying and then very rapidly deploy the digital as a research instrument. This has been discussed by Marres (2017) and Back (2012) in terms of live methods and my exploration in this chapter fit this definition insofar as we attempted to locate demonstrations of selfiestick disruption online and in situ as they were happening. As shown in this chapter, the use of the digital as a research instrument is often one of many steps used to elucidate a phenomenon or - in this specific case - to detect a ‘theatre of failure’.

Could we use the digital as a research instrument to detect a ‘theatre of failure’ for similar mundane novelties that have appeared in the years since? Or does this approach need to be modified to observe objects such as fidget spinners (banned in schools) or hover boards (regulated in the UK)? These objects have had a similar trajectory to the selfie stick in appearing seemingly from nowhere, becoming popular (especially with young people), being noticed in public places, observing divergent opinions and witnessing reports of disruption in digital spaces[69]. After participating in the selfie stick pilot study and

[69] In the case of something such as the hoverboard, this could consist of reports of some catching on fire due to faulty batteries. When thinking about the fidget spinner as a possible

independently continuing the research, I can see an opportunity to use social media not only to gather *some* initial demonstrations of the ’theatre of failure’, but to locate ‘theatres of failure’ in other places such as blogs and news articles that have the space for people to demonstrate and explicate how they perceive these mundane novelty items to be disruptive.

In comparison to the research reported in the previous chapters, the selfie stick is different because it is difficult to locate both the ‘theatre of failure’ and its audience. Who is being demonstrated to? In this research it is unclear who are the experts determining a disruption. To be sure, in this researching the selfie stick, we are able to locate actors who have the authority in certain settings to determine that the selfie stick is disruptive enough to ban. For example, in the National Gallery, it is the gallery staff that have the authority to ban the selfie stick. Their staff also have the authority to choose to enforce that ban. But perhaps this lack of institutional frame helps us understand the ontology of disruption in comparison to an annoyance. In the ‘theatres of failure’ we encountered in the case of TfL and the cyber security community, we were able to easily observe that phenomena - public transport or a previous secure data - had been disrupted because there were experts who determined this. But the disruption is less clear with the selfie stick precisely because of this vacuum of core-set experts who could exert accountability or regulation to prevent the selfie stick disrupting other actors in public spaces. We were then able to observe many instances in which the selfie stick was demonstrated as being annoying or *potentially* disruptive within certain public spaces. The selfie stick research provides a limit case for observing similar demonstrations and

example, this could involve reports about the efficacy of the object such as whether it actually prevents fidgeting (or whether it’s merely another form of fidgeting) and whether one person’s figdet spinning is a distraction to those nearby.

disruptions that are not as obvious as those encountered in the previous chapters.

Chapter Seven: Conclusion

Introduction

Throughout this thesis, I have examined three digital demonstrations of disruption: public transport disruption, cyber security breaches and, selfie stick use in public. Each of these empirical examples has given insight into demonstrations and disruption that contribute knowledge to both of these areas of study. These examples have also shown a different aspect of demonstrations of disruption to help us understand the emerging role(s) of the digital in this space.

By why study demonstrations of mundane disruption? And how can studying them contribute more broadly to studies of demonstrations, everyday life or, the digital? When starting this research in late 2014, I was curious about the behaviour I was starting to observe on social media platforms such as Facebook and Twitter. In addition to the sociality of photos and updates appearing on my feed, I started noticing another genre of post: the complaint to businesses or public institutions. I wanted to know how this trend had started, what people were hoping to achieve and where it was heading.

From a theoretical perspective, these questions could be explored through the literature on demonstrations, where concepts such as the 'theatre of proof' (Latour 1988) went some of the way towards explaining the 'what people were hoping to achieve' question by showing a history of demonstrating events or objects in order to convince others of knowledge. But what about failure? The literature on the ‘theatre of proof’ and the ‘theatre of use’ has a bias towards success (Marres and McGoey 2012) where failure is frowned upon. How might the research in this thesis create knowledge around demonstrations of failure and disruption?

I use the concept of the ‘theatre of failure’ to frame social media as a place where people demonstrate disruptions in everyday life to convince others of a failure that is taking place or has taken place. The ‘theatre of failure’ takes place on social media because it is a public place where those demonstrating disruption can attempt to gain accountability from those responsible for the disruption.

Accountability is one of the key words in considering how people choose to demonstrate disruption, particularly in a setting with a potentially large audience. The development of social media platforms in recent years has provided a way for businesses and institutions to create a profile. It has also provided consumers and citizens with a method of contacting businesses and institutions with a shortened chain of accountability and a level of publicity that demands transparency and a swift response to demonstrations of disruption. Prior to social media use by institutions these chains of accountability could be lengthy and opaque. The underlying assumption is that the ‘theatre of failure’ emerges on digital and social media so that demonstrations of disruptions might be translated into accountability through action and response.

But how does that assumption work in practice? Each of the research chapters provides different insights into digital demonstrations of disruption and how they might – or might not – translate into accountability. The chapter about Transport for London's use of social media focuses not just on the demonstrations of disruption, but the *digital apparatus* and procedures that produce demonstrations and responses to disruptions. The cyber security chapter focuses on the *performative expectations* of digital demonstrations of disruption and what happens when these expectations are mismatched or miscalculated with the intended audience. And the selfie stick chapter is a limit case that depicts the *instability* of digital demonstrations of disruption. This instability and uncertainty of demonstrations makes it difficult to determine whether an object or event is actually a disruption.

The apparatus of digital demonstrations of disruption

In Chapter Four I visited Transport for London and saw how and where we demonstrate disruption in the digital setting. This chapter describes insights around the apparatus that supports demonstrations of disruption. We saw how TfL customer service agents have modified their demonstrations of public transport disruption over time since first adopting Twitter as a customer service channel to broadcast disruption information. From there, we have seen how demonstrations have shifted in response to large events such as the 2012 Olympics and new configurations of technology. These shifts in how TfL's customer service agents use social media to demonstrate disruption has shown to occur in a loop starting with configuring the user (Woolgar 1990) - or commuter - to demonstrate disruption using a new method or digital apparatus. The loop then continues through TfL collecting and reviewing (often quantitative) data from these demonstrations and responses as a form of problem amplification (Latour 1999) in order to highlight how TfL is managing commuter demonstrations of disruption and how they could be better improved. This problem amplification then leads to a problem-solution relationship (Garfinkel 1967/1991, Neyland and Milyaeva 2016), where TfL's online editors and customer service management make decisions and implement solutions to solve identified problems. This process of implementing solutions then returns TfL to a situation of configuring the user to the solutions and amendments to demonstrating disruption in this digital setting. By following this loop, TfL demonstrates continual accountability to its commuters.

Expectations of demonstration of disruption

In Chapter Five I described how the potential for cyber security disruption is demonstrated through digital media. This example shows the difficulty in demonstrations to be used to enrol citizen-consumers in disruptions related to lax cyber security practices related to Internet of Things products. The chapter highlights the difficulties in determining who holds responsibility for communicating cyber security disruptions to consumers; is it the manufacturers, cyber security expert and practitioners, or government organisations? Returning to the overarching theme of digital demonstrations of disruption forming part of a demand for accountability, this chapter highlights the expectations of what demonstrations should do, and *for whom*. After researching cyber security related demonstrations, it would appear the expectations of the everyday user of Internet of Things products is not taken seriously, resulting in demonstrations of potential cyber security related disruption that struggle to enrol everyday citizen consumers.

The chapter returned to the theoretical standpoint of problem amplification

(Latour 1999) to observe how these three groups of experts, manufacturers and government organisations attempt to demonstrate cyber security disruption. Analysing blog posts and videos discussing the promise of Internet of Things products or, the disruption caused by them through the framework of problem amplification showed a problem of too much or not enough demonstration. Explainer videos from technology companies such as IBM or Intel demonstrated a too simplified version of the Internet of Things that skips over the possible cyber security disruptions caused by insecure devices or devices that cannot easily be made secure. These videos demonstrated all of the promise of convenience and none of the risks. Conversely, demonstrations from cyber security practitioners about disruptions that have already occurred rely heavily on core-set expertise that a citizen-consumer might not be able to understand or act upon. Finally, government organisations such as the National Cyber Security Centre demonstrate the potential for cyber security related disruption through writing blog posts that are written with citizens or small businesses in mind. Crucially, prior to demonstrating the potential for disruption, they also describe and demonstrate the context, practices and, workarounds that people often engage in that can increase the chance of a cyber security disruption. In terms of problem amplification, the NCSC blog posts gather complex information about cyber security disruptions and amplifies it to the important, understandable information that allows citizen-consumers to understand the problem, the potential disruption and ways to act upon it.

However, this chapter highlights some unanswered questions around who *is* responsible for ensuring that IoT products cannot be easily disruptive in the first place. Although there have been suggestions for UK government regulation in to IoT products, at present this is not a reality. This lack of regulation is what makes it difficult for citizen-consumers to demonstrate any of their own cyber security disruptions. Who are they to demonstrate their disruption to if the chain of accountability is unclear or non-existent?

Instability of demonstrations of disruption

Chapter Six focused on locating emerging demonstrations of disruption. The demonstrations of the selfie stick serve as a limit case for disruption in comparison to the well-defined disruptions that occur in the TfL or cyber security chapters. Using the example of the introduction of the selfie stick and its eventual ban in many public locations, I attempt to locate demonstrations of selfie stick related disruption through digital methods. This proved difficult due to the liveness of the research and some difficulties of locating demonstrations or discussions of disruption with an audience that didn't have the expected digital literacy to track them via methods such as co-hashtag analysis or interface methods. This difficulty to locate demonstrations of disruption through Twitter and Instagram scraping lead to attempts at other methods such as the breaching experiment at the National Gallery. The experiment attempted to gather an explanation of the selfie stick ban (and the disruption that a ban might prevent) by using the selfie stick in a public place. However, this experiment did not provoke the expected outcome of being reprimanded for using the selfie stick in the place. This meant that an explanation of the selfie stick's supposed disruptiveness in public was still not described. Did this mean that the selfie stick was disruptive, or at least as disruptive as it was described and demonstrated in the news media?

This chapter describes the platform specificity of demonstrating disruption – in particular, how the selfie stick was demonstrated as disruptive in online news media, but this did not translate to demonstrations in the form of user-generated content on social media platforms.

A hybrid of both the breaching experiment and the digital methods proved resourceful in gathering examples, demonstrations and discussions of the disruptiveness of the selfie stick. These were found in the comments section of a news article describing the ban of the selfie stick at the Smithsonian Museum in the US. In these comments, museum staff and museum-goers described their positive and negative experiences of the selfie stick in disrupting the museum space. In this circumstance, we could understand that the news article was the breach or the provocation for these explanations from people as to why they considered the selfie stick to be disruptive (or not) in this space. This chapter has methodological implications for future attempts to locate demonstrations of emerging mundane disruptions in digital settings. This example of the selfie stick research advocates a mixed digital methods approach that acknowledges that sometimes our first attempts to locate the digital or situated field to study may not work. However, they do lead us to fields that can tell us more about a phenomenon or a disruption.

But how might we take what has been learned from these different pieces of research and consider the questions that they might provide for future inquiry into digital demonstrations of mundane disruption?

Private to public to personalised: will demonstrations of disruption ever stabilise?

One of the main observations of this thesis has come through charting the course of demonstrations of disruption from private to public to personalised formats. This has included the relatively private, pointed demonstrations between a disrupted person and someone in authority that take place via post, telephone or, email as described by our long-term Transport for London customer service manager. In recent years we have seen the transition of these demonstrations from telephone or email to Twitter and Facebook. These have become very public demonstrations of disruptions on social media that - due to the algorithmic nature of displaying social media content - incorporate a far broader audience than just the demonstrator and those responsible.

In the Transport for London chapter, we saw demonstrations go one step further - towards personalisation - with the introduction of chat bots and direct message alerts. This meant that those disrupted didn’t need to demonstrate disruption to TfL to find out simple information such as the status of their public transport service. Rather, they were able to self-serve that information about demonstrations from a non-human actor in the form of a chat bot or an automated message. This allowed TfL’s customer service agents to spend more time focusing on less common disruptions, or disruptions that require a private conversation. Pushing the common disruption information towards personalised and self-service methods also means that there is a reduction in the amount of public demonstrations made about TfL’s service disruptions and therefore, less of an algorithmic audience. This is positive for Transport for London, who would want to be seen as proactive - rather than an organisation that receives many queries and complaints. It is also positive for the algorithmic audience who may have no interest whatsoever in whether the Piccadilly Line is currently delayed.

But will digital demonstrations of disruption ever stabilise? And what might that look like? In comparison to the ant's eye view of TfL, we could gain a better understanding from the eagle's view (Latour 1993). In isolation, demonstrations of disruption between a demonstrator and a single addressee in a digital setting appear to be helpful and useful. But taking the eagle's view to having a social media user able to demonstrate disruption to multiple addressees in a digital setting could allow for corporate actors running the setting a corpus of data about that user that was previously unavailable. In short, digital demonstrations could stabilise behind walled gardens such as Facebook and become monetised.

At Web Summit 2017, Facebook's VP of Product for Facebook Messenger, Stan Chudnovsky, described a future where most customer service with a company would occur through a conversation with a chatbot (Chudnovsky and Segall 2017). Chudnovsky described that Facebook users don't like using the phone anymore, so it made sense to move customer service online to chatbots. He then showed a brief video of a customer enquiry on Facebook Messenger to demonstrate how this would work, ending in the user purchasing a product with one click. He said that chatbots would be able to do the easy work at the start of the customer enquiry (much like we saw with the TfL chatbot) but that the conversation would be able to be passed over to a human customer service agent if the conversation reached a level of complexity that required human intervention. Since completing fieldwork with Transport for London, their customer service team now includes a Facebook chatbot as an option to receive live travel information.

But why should Facebook care about this and want its infrastructure used for customer service? The answer lies in the opportunities to gather more data on its users. The more a user seeks customer service on Facebook, the more data it can gather. Depending on the type of customer service being sought, this data could include personal sensitive data or highly contextual data that will allow Facebook to serve the user more targeted ads. Due to the walled garden nature of Facebook, the opportunities to study and research the impacts of these demonstrations of disruption would be greatly reduced. While it is convenient for citizen-consumers to conduct all of their demonstrations of disruption to addressees in one digital setting, is this the future of demonstrating disruption that is necessarily useful, helpful and transparent for citizens?

But further research may be required into chatbots and the scripts of demonstrating disruption. In another session at Web Summit 2017, Mark Curtis, the founder of design and innovation consultancy Fjord described a future where chat bots could alter and tailor their scripts depending on the traits and preferences of the human making a demonstration of disruption:

> "Artificial intelligence is getting very good at understanding who we are… computers will begin to mirror us… no company on earth will be able to resist the charm of mirroring its customers, by knowing who they are, by understanding who they are by scraping their social media… If they can do that, then what happens when you talk to a company soon is that they'll be scraping your social media, they'll be looking at you, they'll be thinking about the way they interact and they will drive their chat bot through machine learning to mirror who you are. Now what's the consequence of that? Every brand becomes like you."
>
> - Mark Curtis. *The Past, Present and Future of Conversation*. Web Summit 2017

How might we study future demonstrations of disruption where responses are being rapidly configured and reconfigured based on who is making the demonstration and their attributes? Future research would need to focus on the process and the non-human actors involved in creating such a persuasive scripted response to a demonstration of disruption. Suffice it to say, there is still scope to study the ongoing personalisation of demonstrations of disruption and their responses in terms of how this might impact chains of accountability between citizen-consumers and addressees.

Demonstrations and convenience

The digital demonstrations of mundane disruption that we have encountered in this thesis have each had an aspect of convenience attached to them. In the Transport for London chapter, we are shown an example of how using Twitter chat bots to demonstrate public transport disruption is convenient for both the commuter and for customer service agents. Commuters can self-serve the information they need and customer service agents do not need to repeat themselves many times in a small space of time.

However, in the other empirical chapters, we see disruptions that occur through acts of convenience. For example in the cyber security chapter, convenience in setting up an IoT product or the convenience of adopting bad password practices has the potential to lead to disruption in the form of DDOS attacks or database hacking. In the selfie stick chapter, we see how the object is convenient in avoiding having to ask a stranger to take a portrait and yet it is disruptive to other human and non-human actors in some settings.

This correlation between convenience and disruption could be of interest for further study or applied research into potential solutions. For example, how might we demonstrate the potential disruption of the convenience of a reused password across one user's many digital accounts? Or how could we visually or materially demonstrate when someone's IoT device is insecure and could be vulnerable to hacking? Does a demonstration of potential disruption need to necessarily be writ large on social media or on blogs, or could it be something demonstrated to individuals over time as the practice is occurring?

Crucially, these questions demonstrate the trade-off human actors make everyday when negotiating convenience lead by non-human actors in their everyday lives. Where might the research done by the likes of Shove (2004) around domestic and everyday convenience intersect with the disruptive attributes of technological convenience described in this thesis?

Politics and inequalities in digital demonstrations of disruption

One general observation from all of the research projects is that many of them are male dominated areas. The most obvious of these is cyber security, with a workforce that is 90 percent male. But in Transport for London, I couldn't help but notice that all of my informants were men, and that while there were women working in the team, I wasn't introduced to them. What impact might a feminist approach to demonstrations of disruption have on cyber security and public transport related disruptions? Again, it is obvious to reach towards cyber security as a prime example of how a feminist approach to demonstrations of disruption may enrol more citizen-consumers into better cyber security practices. But what could a feminist approach to cyber security look like? My observations from the National Cyber Security Centre are a glimpse of what that could look like[70]. With an approach that involves more caring than scaring, the

[70] [1]The National Cyber Security Centre also boast of having a better ratio of women to men working there than in the cyber security industry: "half of our senior leadership are female, and

NCSC describes how the situation between the human and non-human actors in the cyber security agencement can be understood. The emphasis on the demands that non-human actors make in creating passwords and adhering to many complicated protocols demonstrates an understanding of the situated practices that arise from complicated security requirements. What might a feminist approach to cyber security look like in practice? How could a feminist approach to cyber security take into account the situated practices of humans in attempting to achieve cyber security in order to tailor security that doesn't set humans up to fail?

From the observations I have made, I believe there is a need for further interdisciplinary, practical research into how we create cyber security that works for everyone. Part of this involves a piece around digital literacy, another part would involve building cyber security measures that work for those with accessibility needs. A feminist approach to this would carry through an ethos of care, not scare. At the moment, there is an emphasis on berating the public for not knowing enough about cyber security and the consequences of poor cyber security habits, however this is being done without educating the public beforehand. How might we demonstrate the different types of vulnerabilities that citizen-consumers might face in a way that doesn't put them off using technology in their everyday life? Rather, how might we teach citizen-consumers about different types of vulnerabilities in such a way as to allow them a sense of agency if they encounter them in the course of their everyday digital life?

we are determined to improve the figure of one third of our staff being female." (NCSC blog post, 12 October 2017. https://www.ncsc.gov.uk/blog-post/your-best-and-wisest-refuge-all-troubles-your-science)

Similarly, accessibility is another piece of the cyber security puzzle that could greatly benefit from a feminist approach. Some cyber security measures are inaccessible for people with accessibility needs. For example, the CAPTCHA mechanism - the process where users need to type a series of letters and numbers displayed in an augmented way that is not machine readable to authenticate their identity - is not accessible for those with visual impairments or dyslexia (May, W3C 2005). How might people with these needs access services that use these mechanisms, let alone access them securely?

Another consideration for inequality and demonstrations of mundane disruptions relate to those we encountered at Transport for London. This raises questions about people and social media that are yet to be answered. If we consider social media to be a growing place for demonstrations of mundane disruption to occur -to the point of it being a preferred and expected way of demonstrations to be dealt with - then how do we account for people who for many reasons are not a part of social media? If demonstrations of disruption continue to be mediated through third party providers with commercial interests, what are the ramifications for this? Will citizen-consumers be strongly influenced to remain active on walled garden services such as Facebook in order to receive customer service? Will we see people having Twitter accounts just to access chatbot services such as those provided by Transport for London? Crucially, if we consider the increasing commodification and datafication of social media, we begin to question whether social media is really ‘social’ anymore or whether it is ‘commercial media’ or ‘consumer media’.

For what it’s worth, the descriptions of Web 1.0 through Web 3.0 layering on one another, along with the descriptions of the many contact methods TfL has on offer indicate that we will not likely see a situation where a social media platform is the single source of customer service. But it is still worth noting that ambitions to increase customer service activities on social media will have an impact on how we perceive and use these digital settings.

Practical applications for multiple ontologies of the digital

This thesis has considered the digital in many ways: as a setting, an actor/assemblage and, as a research instrument (Marres 2017). As each of the research chapters demonstrate this with varying levels of success. Considering the digital as a setting as shown in the Transport for London chapter was a relatively straightforward exercise, as that was where the demonstrations and the responses were occurring. However, observing and understanding the digital as an actor or assemblage in the cyber security chapter was a little more difficult. This difficulty sprung from disruption occurring with digital actors in what could be considered digital settings. How then to delineate between a non-human, digital actors and the setting they are disrupted within? In one part, focusing on the demonstration helps with that confusion.

And finally, considering the digital as a research instrument in the selfie stick chapter demonstrated the difficulty of using digital methods to detect demonstrations of disruption. This difficulty stems from some of the attributes of digital methods, such as the necessity to collect social media data as it is being published, rather than after the fact. Digital methods allow for a ‘liveness’ of research, and yet it can also send the researcher down a rabbit hole or a dead end if the data doesn't necessarily describe a phenomenon in such a way as to analyse the findings. Using the digital as a research instrument in the selfie stick chapter, I echo Hine (2015b) and her call for digital research to take a mixed methods approach to attempt to observe a phenomenon from many standpoints. Often one approach describes a portion of a phenomenon, whereas multiple methods can begin to account for more portions of a disruption.

Are there other ways we could conceptualise and deploy the digital in order to study phenomena such as demonstrations of disruption? I argue that there could be, due to the nature of the theatre of failure and its lack of stability. For example, if there were further research done into the role of chatbots in demonstrations of mundane disruption, the emphasis could be changed to observe and research the chatbot as a digital, non-human actor that is very much interacting with a human actor. In this research, chatbots have been considered through the heuristic of the digital as a setting, but how might that research change if the heuristic were different?

What difference does studying digital demonstrations of disruption make?

Through studying digital demonstrations of disruption, we are able to see that not all demonstrations have a bias towards success. In comparison to demonstrations of new knowledge in the 'theatre of proof' and demonstrations of how a new product or process could work in everyday life in the 'theatre of use', demonstrations of mundane disruption form a 'theatre of failure' that demands further action, responsibility or, accountability from its intended audience.

The ‘theatre of failure’ is by no means a new theatre to emerge; it is not something that has occurred due to the digital. Demonstrations of disruption have been occurring in non-digital formats for a long time, and this is evidenced by the accounts of the Transport for London customer service manager who has spent his career responding to public transport demonstrations in a range of formats. However, what the digital has done is configure demonstrations in such a way that afford more publicity and a broader audience to the disruption at hand. Observing digital demonstrations of disruption at this particular, fleeting moment in time has also allowed me to see how demonstrations of disruption are now beginning to be configured again towards personalisation through chatbots and direct messaging. While this shift towards personalisation requires more research as it unfolds, it raises questions about accountability and responsibility if the audience for these digital demonstrations of disruption are becoming non-human actors. Amongst many other potential applications, the research done in this thesis is applicable as a form of STS-informed history for those wanting to studying the emerging role of chatbots in everyday digital life.

Studying digital demonstrations of disruption also allows us to observe how they can enrol audiences. In the cyber security chapter, this took the form of analysing demonstrations of cyber security disruption from experts, corporations and government organisations to observe how citizens were (or weren’t) enrolled to make better cyber security practices. As mentioned earlier in this chapter, the research done in this thesis indicates that there is still work to be done in enrolling citizens (amongst many other actors) in adopting effective cyber security measures.

The first disruption I researched for this thesis was that of the selfie stick, and it was quite possibly the most difficult disruption to make sense of. Along with the research having implications for how we use the digital as a research instrument, it also raises questions about how we know something is a disruption and who decides whether an object or event is, in fact, disruptive. It also raised questions about the role of the digital in publicising or enrolling people in disruptions that involve faddish objects. While finding and observing digital demonstrations of selfie stick-related disruption from outside the news media was difficult, I believe the lessons learnt from attempting to locate explanations of selfie stick disruption on social media could be helpful for those attempting to locate demonstrations for similar faddish objects.

Having spent the past three years seeking out ‘theatres of failure’ through which digital demonstrations of mundane disruption occur, I have observed that these demonstrations are not stable. Digital demonstrations of disruption are shifting according to shifts in configurations and scriptings of human actors and increasingly, non-human actors. I look forward to seeing, reading and possibly participating in future research.

References

Agence France-Presse, 2015. “A selfie with a weapon kills”: Russia launches campaign urging photo safety. The Guardian.

Akrich, M., 1992. The De-scription of Technical Objects, in: Bijker, J., W. & Law (Ed.), Shaping Technology/Building Society. Studies in Sociotechnical Change. MIT Press, pp. 205–224.

Arbaugh, W.A., Fithen, W.L., McHugh, J., 2000. Windows of vulnerability: a case study analysis. Computer 33, 52–59. https://doi.org/10.1109/2.889093

Back, L., 2012. Live sociology: social research and its futures. Sociol Rev 60, 18–39. https://doi.org/10.1111/j.1467-954X.2012.02115.x

Back, L., Sinha, S., Bryan, with C., 2012. New hierarchies of belonging. European Journal of Cultural Studies 15, 139–154. https://doi.org/10.1177/1367549411432030

Bartlett, J., 2015. The Dark Net. Windmill Books, London.

Baym, N.K., 2000. Tune in, log on: soaps, fandom, and online community, New media cultures. Sage Publications, Thousand Oaks, Calif.

BBC News, 2016. “Train delay” game inspired by Southern. BBC News.

BBC News, n.d. National Gallery bans selfie sticks to protect artworks [WWW Document]. BBC News. URL http://www.bbc.co.uk/news/entertainment-arts-31844292 (accessed 10.6.15).

BBC Trending, n.d. Does this 90-year-old photo show the world’s first “selfie stick”? [WWW Document]. BBC News. URL http://www.bbc.co.uk/news/blogs-trending-30550998 (accessed 10.6.15).

Beautement, A., Sasse, M.A., Wonham, M., 2008. The Compliance Budget: Managing Security Behaviour in Organisations, in: Proceedings of the 2008 New Security Paradigms Workshop, NSPW ’08. ACM, New York, NY, USA, pp. 47–58. https://doi.org/10.1145/1595676.1595684

Beer, D., Burrows, R., 2013. Popular Culture, Digital Archives and the New Social Life of Data. Theory, Culture & Society 30, 47–71. https://doi.org/10.1177/0263276413476542

Beer, D., Burrows, R., 2010. Consumption, Prosumption and Participatory Web Cultures: An introduction. Journal of Consumer Culture 10, 3–12. https://doi.org/10.1177/1469540509354009

Bowker, G.C., 2005. Memory practices in the sciences, Inside technology. MIT Press, Cambridge, Mass.

boyd, danah, 2017. How “Demo-or-Die” Helped My Career [WWW Document]. LinkedIn Pulse. URL https://www.linkedin.com/pulse/how-demo-or-die-helped-my-career-danah-boyd (accessed 8.2.17).

British Sociological Association, 2017. Ethics Guidelines and Collated Resources for Digital Research: Statement of Ethical Practice Annexe. British Sociological Association.

Bullen, J., 2016. Southern commuters stage protest on eve of 24-hour walkout [WWW Document]. Evening Standard. URL http://www.standard.co.uk/news/transport/southern-rail-strike-commuters-stage-fresh-protest-at-brighton-station-on-eve-of-24hour-walkout-a3276636.html (accessed 10.21.17).

Burns, A., 2015. “Picturing the Social”: Questions of method, ethics and transparency in the analysis of social media photography. Impact of Social Sciences.

C2C Customers, 2016. 6.22 from Fenchurch street - arguing and shouting. 25 min later - no better @c2c_Railpic.twitter.com/yQEV3bLyfi. @c2c_customers.

Callon, M., 1986a. Some elements of a sociology of translation: domestication of the scallops and the fisherman of St Brieuc bay, in: Law, J. (Ed.), . Routledge, London, pp. 196–232.

Callon, M., 1986b. The Sociology of an Actor-Network: The Case of the Electric Vehicle, in: Mapping the Dynamics of Science and Technology. Palgrave Macmillan, London, pp. 19–34.

Callon, M., Courtial, J.-P., Turner, W.A., Bauin, S., 1983. From translations to problematic networks: An introduction to co-word analysis. Information (International Social Science Council) 22, 191–235. https://doi.org/10.1177/053901883022002003

Callon, M., Latour, B., 1981. Unscrewing the big Leviathan: how actors macro-structure reality and how sociologists help them to do so., in: Knorr-Cetina, K.D., Mulkay, M. (Eds.), Advances in Social Theory and Methodology: Toward an Integration of Micro-and Macro-Sociologies. London, pp. 275–303.

Castells, M., 1997. The power of identity, Information age. Blackwell, Malden, Mass.

Chudnovsky, S., Segall, L., 2017. The evolution of conversation: Facebook’s Stan Chudnovsky, Web Summit 2017. Facebook.

Chun, W.H.K., 2016. Updating to remain the same: habitual new media. The MIT Press, Cambridge, MA.

Chun, W.H.K., Fisher, A.W., Keenan, T. (Eds.), 2016. New media, old media: a history and theory reader, Second edition. ed. Routledge, New York, NY.

Cisco, 2013. Internet of Everything FAQ [WWW Document]. URL http://ioeassessment.cisco.com/learn/ioe-faq (accessed 4.5.17).

CloudPets, 2017. CloudPets, a message you can hug [WWW Document]. CloudPets, a message you can hug. URL http://cloudpets.com/how-it-works (accessed 11.25.17).

Cohen, S., 2002. Folk Devils and Moral Panics: The Creation of the Mods and Rockers. Psychology Press.

Collins, H.M., 1988. Public Experiments and Displays of Virtuosity: The Core-Set Revisited. Social Studies of Science 18, 725–748. https://doi.org/10.1177/030631288018004006

Coopmans, C., 2011. “Face value”: New medical imaging software in commercial view. Social Studies of Science 41, 155–176. https://doi.org/10.1177/0306312710389226

Cotton, E., 2016. Self-employment is precarious work. LSE Business Review.

CREST, 2017. CREST - Ethical Security Testers. http://www.crest-approved.org/

Curtis, M., 2017. The past, present and future of conversation, Web Summit 2017. Facebook.

Dallaway, E., 2016. Closing the Gender Gap in Cybersecurity. CREST. http://www.crest-approved.org/wp-content/uploads/CREST-Closing-the-Gender-Gap-in-Cyber-Security.pdf

De Laet, M., Mol, A., 2000. The Zimbabwe Bush Pump: Mechanics of a Fluid Technology. Soc Stud Sci 30, 225–263. https://doi.org/10.1177/030631200030002002

Dodge, M., Kitchin, R., 2009. Software, Objects, and Home Space. Environment and Planning A 41, 1344–1365. https://doi.org/10.1068/a4138

Donath, J., 1999. Identity and Deception in the Virtual Community, in: Communities in Cyberspace. Routledge, London.

Dourish, P., Button, G., 1998. On “Technomethodologyn”;: Foundational Relationships Between Ethnomethodology and System Design. Hum.-Comput. Interact. 13, 395–432. https://doi.org/10.1207/s15327051hci1304_2

Downer, J., 2007. When the Chick Hits the Fan: Representativeness and Reproducibility in Technological Tests. Social Studies of Science 37, 7–26. https://doi.org/10.1177/0306312706064235

Emma W, 2016. Spending our users’ security budgets wisely. Sociotechnical security blog.

Ezrahi, Y., 1990. The Descent of Icarus: Science and the Transformation of Contemporary Democracy. Harvard University Press, Cambridge, Mass.

Facebook, 2015. Facebook Adverts [WWW Document]. Facebook for Business. URL https://en-gb.facebook.com/business/products/ads (accessed 5.30.16).

Faircloth, K., 2015. The Smithsonian Says: Fuck Your Selfie Stick [WWW Document]. Jezebel. URL http://jezebel.com/the-smithsonian-says-fuck-your-selfie-stick-1689389959?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed: jezebel/full (Jezebel) (accessed 10.6.15).

Florêncio, D., Herley, C., 2010. Where Do Security Policies Come from?, in: Proceedings of the Sixth Symposium on Usable Privacy and Security, SOUPS ’10. ACM, New York, NY, USA, pp. 10:1–10:14. https://doi.org/10.1145/1837110.1837124

Foucault, M., Gordon, C., 1980. Power/knowledge: selected interviews and other writings, 1972-1977, 1st American ed. ed. Pantheon Books, New York.

Foxx, C., 2015. Disney confirms selfie stick ban at theme parks [WWW Document]. BBC News. URL http://www.bbc.co.uk/news/technology-33311071 (accessed 10.24.15).

Franceschi-Bicchierai, L., 2016. Blame the Internet of Things for Destroying the Internet Today [WWW Document]. Motherboard. URL https://motherboard.vice.com/en_us/article/vv7xg9/blame-the-internet-of-things-for-destroying-the-internet-today (accessed 10.28.17).

Franklin, U.M., 2004. The real world of technology, Rev. ed. ed, CBC Massey lectures series. House of Anansi Press ; Distributed in the United States by Publishers Group West, Toronto, Ont. : Berkeley, CA.

Galloway, A.R., 2004. Protocol: How Control Exists After Decentralization. MIT Press.

Galloway, A., R., 2016. Protocol vs. institutionalization, in: New Media, Old Media: A History and Theory Reader. Routledge, New York, NY, pp. 263–274.

Garfinkel, H., 1991. Studies in Ethnomethodology, 1 edition. ed. Polity, Cambridge, UK.

Gerlitz, C., Helmond, A., 2013. The like economy: Social buttons and the data-intensive web. New Media & Society 15, 1348–1365. https://doi.org/10.1177/1461444812472322

Gerlitz, C., Lury, C., 2014. Social media and self-evaluating assemblages: on numbers, orderings and values. Distinktion: Journal of Social Theory 15, 174–188. https://doi.org/10.1080/1600910X.2014.920267

Goffman, E., 1974. Frame analysis: an essay on the organization of experience. Harvard University Press, Cambridge, Mass.

Goffman, E., 1963. Behaviour in Public Places. Free Press.

Goffman, E., 1959. The Presentation of Self in Everyday Life, 1 edition. ed. Anchor, New York N.Y.

Goodwin, C., 1994. Professional Vision. American Anthropologist 96, 606–633. https://doi.org/10.1525/aa.1994.96.3.02a00100

Government Office for Science, 2014. The Internet of Things: making the most of the Second Digital Revolution A report by the UK Government Chief Scientific Adviser. Government Office for Science.

Graham, C., Laurier, E., O'Brien, V., Rouncefield, M., 2011. New visual technologies: shifting boundaries, shared moments. Visual Studies 26, 87–91. https://doi.org/10.1080/1472586X.2011.571883

Graham, S., Thrift, N., 2007. Out of Order: Understanding Repair and Maintenance. Theory, Culture & Society 24, 1–25. https://doi.org/10.1177/0263276407075954

Greengard, S., 2015. The internet of things, MIT press essential knowledge series. MIT Press, Cambridge, Massachusetts.

Grimes, S.M., 2015. Configuring the Child Player. Science, Technology, & Human Values 40, 126–148. https://doi.org/10.1177/0162243914550253

Grommé, F., 2015. Turning Aggression into an Object of Intervention: Tinkering in a Crime Control Pilot Study. Science as Culture 24, 227–247. https://doi.org/10.1080/09505431.2014.992331

Gutierrez, S., 2016. How Transport for London (TfL) meets the social CS demands of London's commuters.

Hall, S., Roberts, B., Clarke, J., Jefferson, T., Critcher, C., 1978. Policing the Crisis: Mugging, the State, and Law and Order, 1978 edition. ed. Macmillan, London.

Heidegger, M., 1996. Being and Time: A Translation of Sein und Zeit. SUNY Press.

Helen L, 2016. Developers need help too. Sociotechnical security blog.

Helmond, A., 2015. The Web as Platform. Data Flows in Social Media. Universiteit van Amsterdam, Amsterdam.

Hern, A., 2017. Five things that got broken at the oldest hacking event in the world. The Guardian.

Hine, C., 2015a. Ethnography for the Internet. Bloombury, London ; New York.

Hine, C., 2015b. Mixed Methods and Multimodal Research and Internet Technologies, in: The Oxford Handbook of Multimethods and Mixed Methods Research Inquiry. Oxford University Press, Oxford ; New York.

Hine, C., 2008. Virtual ethnography: Modes, varieties, affordances Nigel G Fielding, Raymond M Lee, Grant Blank, in: Fielding, N.G., Lee, R.M., Blank, G. (Eds.), The SAGE Handbook of Online Research Methods. pp. 257–270.

Hine, C., 2005. Virtual Methods. Bloomsbury Academic, Oxford ; New York.

Hine, C.M., 2000. Virtual Ethnography, 1 edition. ed. SAGE Publications Ltd, London ; Thousand Oaks, Calif.

Huggler, J., 2017. Germany bans internet-connected dolls over fears hackers could target children. The Telegraph.

Hunt, T., 2017. Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages [WWW Document]. Troy Hunt. URL https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/ (accessed 2.28.17).

IBM Think Academy, 2015. How It Works: Internet of Things. https://www.youtube.com/watch?v=QSIPNhOiMoE

Intel, 2014. Intel IoT -- What Does The Internet of Things Mean? https://www.youtube.com/watch?v=Q3ur8wzzhBU

Kantrowitz, A., 2016. Twitter To Introduce Algorithmic Timeline As Soon As Next Week [WWW Document]. BuzzFeed. URL https://www.buzzfeed.com/alexkantrowitz/twitter-to-introduce-algorithmic-timeline-as-soon-as-next-we (accessed 9.19.17).

Kelty, C., 2005. Geeks, Social Imaginaries, and Recursive Publics. Cultural Anthropology 20, 185–214. https://doi.org/10.1525/can.2005.20.2.185

Kelty, C.M., 2008. Two Bits: The Cultural Significance of Free Software and the Internet. Duke University Press, Durham.

Kelty, C., 2012. From Participation to Power, in: Delwiche, A., Henderson, J.J. (Eds.), The Participatory Cultures Handbook. Routledge, pp. 22–32.

Knoblauch, H., Baer, A., Laurier, E., Petschke, S., Schnettler, B., 2008. Visual Analysis. New Developments in the Interpretative Analysis of Video and Photography. Forum Qualitative Sozialforschung / Forum: Qualitative Social Research 9.

Knorr, K.D., 1979. Tinkering toward success: Theor Soc 8, 347–376. https://doi.org/10.1007/BF00167894

Kozinets, R.V., 2009. Netnography: Doing Ethnographic Research Online. SAGE Publications Ltd, Thousand Oaks, CA.

Latour, B., 2005. Reassembling the social: an introduction to actor-network-theory, Clarendon lectures in management studies. Oxford University Press, Oxford ; New York.

Latour, B., 1999. Pandora’s hope: essays on the reality of science studies. Harvard University Press, Cambridge, Mass.

Latour, B., 1994. Pragmatogonies: A Mythical Account of How Humans and Nonhumans Swap Properties. American Behavioral Scientist 37, 791–808. https://doi.org/10.1177/0002764294037006006

Latour, B., 1993. We Have Never Been Modern. Harvard University Press, Cambridge, Mass.

Latour, B., 1992. Where are the Missing Masses? The Sociology of a Few Mundane Artifacts, in: Wiebe E. Bijker, John Law (Eds.), Shaping Technology/Building Society: Studies in Sociotechnical Change. MIT Press, USA, pp. 225–258.

Latour, B., 1988. The pasteurization of France. Harvard University Press, Cambridge, Mass.

Latour, B., Woolgar, S., 1986. Laboratory life: the construction of scientific facts. Princeton University Press, Princeton, N.J.

Laurier, E., 2004. Doing Office Work on the Motorway. Theory, Culture & Society 21, 261–277. https://doi.org/10.1177/0263276404046070

Law, J., 2004. After Method: Mess in Social Science Research, 1 edition. ed. Routledge, London ; New York.

Law, J., Ruppert, E., 2013. THE SOCIAL LIFE OF METHODS: Devices. Journal of Cultural Economy 6, 229–240. https://doi.org/10.1080/17530350.2013.812042

Lee, D., 2014. Selfie-stick sales outlawed in S Korea. BBC News.

Lezaun, J., Soneryd, L., 2007. Consulting citizens: technologies of elicitation and the mobility of publics. Public Underst Sci 16, 279–297. https://doi.org/10.1177/0963662507079371

Lupton, D., 2012. Digital Sociology: An Introduction. University of Sydney, Sydney.

Markham, A.N., 1998. Life Online: Researching Real Experience in Virtual Space, 1St Edition edition. ed. AltaMira Press, Walnut Creek, CA.

Marres, N., 2017. Digital sociology: the reinvention of social research. Polity, Malden, MA.

Marres, N., 2015. Why Map Issues? On Controversy Analysis as a Digital Method. Science, Technology & Human Values. https://doi.org/10.1177/0162243915574602

Marres, N., 2012. Material participation: technology, the environment and everyday publics. Palgrave Macmillan, Houndmills, Basingstoke, Hampshire ; New York.

Marres, N., 2007. The Issues Deserve More Credit: Pragmatist Contributions to the Study of Public Involvement in Controversy. Social Studies of Science 37, 759–780. https://doi.org/10.1177/0306312706077367

Marres, N., Gerlitz, C., 2015. Interface methods: renegotiating relations between digital social research, STS and sociology: Interface methods: renegotiating relations between digital social research. The Sociological Review n/a–n/a. https://doi.org/10.1111/1467-954X.12314

Marres, N., Lezaun, J., 2011. Materials and devices of the public: an introduction. Economy and Society 40, 489–509. https://doi.org/10.1080/03085147.2011.602293

Marres, N., McGoey, L., 2012. Experimental failure: Notes on the limits of the performativity of markets. Presented at the After Markets: Researching Hybrid Arrangements.

Marres, N., Weltevrede, E., 2013. Scraping the Social? Journal of Cultural Economy 6, 313–335. https://doi.org/10.1080/17530350.2013.772070

May, M., 2005. Inaccessibility of CAPTCHA: Alternatives to Visual Turing Tests on the Web. https://www.w3.org/TR/turingtest/

McLuhan, M., Fiore, Q., 2008. The Medium is the Massage: An Inventory of Effects. Penguin Classics, London.

Michael, M., 2016. Actor network theory: trials, trails and translations, 1st edition. ed. SAGE Ltd, Thousand Oaks, CA.

Michael, M., 2006. Technoscience And Everyday Life: The Complex Simplicities of the Mundane, New. edizione. ed. Open Univ Pr, Maidenhead.

Michael, M., 2000. These Boots Are Made for Walking...: Mundane Technology, the Body and Human-Environment Relations. Body & Society 6, 107–126. https://doi.org/10.1177/1357034X00006003006

Miller, D., Slater, D., 2001. The Internet: An Ethnographic Approach, 1 edition. ed. Bloomsbury Academic, Oxford ; New York.

Mills, C.W., 1959. The Sociological Imagination. Oxford University Press, Harmondsworth.

Mol, A., 2003. The Body Multiple: Ontology in Medical Practice. Duke University Press, Durham.

Muniesa, F., Millo, Y., Callon, M., 2007. An introduction to market devices. The Sociological Review 55, 1–12. https://doi.org/10.1111/j.1467-954X.2007.00727.x

Murthy, D., 2008. Digital Ethnography: An Examination of the Use of New Technologies for Social Research. Sociology 42, 837–855. https://doi.org/doi: 10.1177/0038038508094565

Nardi, B.A., 2010. My life as a night elf priest: an anthropological account of World of warcraft, Technologies of the imagination. University of Michigan Press : University of Michigan Library, Ann Arbor.

National Cyber Crime Prevent Team, 2017. Pathways Into Cyber Crime (Intelligence Assessment). National Crime Agency. http://www.nationalcrimeagency.gov.uk/publications/791-pathways-into-cyber-crime/file

National Cyber Security Centre, 2017. Overview - National Cyber Security Centre. https://www.ncsc.gov.uk/document/ncsc-overview

National Cyber Security Centre, 2016. Password Guidance: Simplifying Your Approach. National Cyber Security Centre, London. https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

NCSC_HMG, 2017. NCSC CyberUK2017. https://www.youtube.com/watch?time_continue=160&v=QiCunzkr2CI

Neyland, D., Milyaeva, S., 2016. The Entangling of Problems, Solutions and Markets: On Building a Market for Privacy. Science as Culture 25, 305–326. https://doi.org/10.1080/09505431.2016.1151489

Oltermann, P., 2017. German parents told to destroy doll that can spy on children. The Guardian.

Perriam, J., 2017. Ethnography, Objects and Reflexivity: A Case Study of the Selfie Stick. Ethnographies of Objects in Science and Technology Studies 1, 19–25. https://doi.org/10.13154/eoo.1.2017.19-25

Perriam, J., 2013. Coffee and Wi-Fi: An ethnographic examination of the “sociability” of people, objects and infrastructure in independent cafes (Masters). Goldsmtihs, University of London, London.

Pinch, T., 1993. “Testing - One, Two, Three ... Testing!”: Toward a Sociology of Testing. Science, Technology & Human Values 18, 25–41. https://doi.org/10.1177/016224399301800103

Pink, S., Horst, H., Postill, J., Hjorth, L., Lewis, T., Tacchi, J., 2015. Digital Ethnography: Principles and Practice, 1 edition. ed. Sage Publications Ltd, Los Angeles.

RamJam, n.d. Southern Rail Tycoon [WWW Document]. RamJam. URL http://www.ramjam.co.uk/portfolio/southern-rail-tycoon (accessed 11.7.16).

Rieder, B., 2013. Studying Facebook via Data Extraction: The Netvizz Application, in: Proceedings of the 5th Annual ACM Web Science Conference, WebSci ’13. ACM, New York, NY, USA, pp. 346–355. https://doi.org/10.1145/2464464.2464475

Reider, B., 2016. Thoughts on Software, Power, and Digital Method. The Politics of Systems.Rogers, R., 2004. Information politics on the web. MIT Press, Cambridge, Mass

Rogers, R., 2013. Digital methods. The MIT Press, Cambridge, Massachusetts.

Rogers, R., 2009. The End of the Virtual: Digital Methods. Vossiuspers UvA, Amsterdam.

Roman, R., Najera, P., Lopez, J., 2011. Securing the Internet of Things. Computer 44, 51–58. https://doi.org/10.1109/MC.2011.291

Ruppert, E., Law, J., Savage, M., 2013. Reassembling Social Science Methods: The Challenge of Digital Devices. Theory, Culture & Society 30, 22–46. https://doi.org/10.1177/0263276413484941

Sarah L, 2017. “Your best and wisest refuge from all troubles is in your science.” National Cyber Security Centre.

Savage, M., Burrows, R., 2007. The Coming Crisis of Empirical Sociology. Sociology 41, 885–899. https://doi.org/10.1177/0038038507080443

Shapin, S., Schaffer, S., Hobbes, T., 1985. Leviathan and the air-pump: Hobbes, Boyle, and the experimental life: including a translation of Thomas Hobbes, Dialogus physicus de natura aeris by Simon Schaffer. Princeton University Press, Princeton, N.J.

Shove, E., 2004. Comfort, Cleanliness and Convenience: The Social Organization of Normality. Bloomsbury Academic, Oxford, England; New York.

Smith, A., 2015. Disney bans selfie sticks over safety fears [WWW Document]. CNNMoney. URL http://money.cnn.com/2015/06/26/news/companies/disney-selfie-stick/index.html (accessed 10.10.15).

Smith, W., 2009. Theatre of Use A Frame Analysis of Information Technology Demonstrations. Social Studies of Science 39, 449–480. https://doi.org/10.1177/0306312708101978

Star, S.L., 1999. The Ethnography of Infrastructure. American Behavioral Scientist 43, 377–391. https://doi.org/10.1177/00027649921955326

Star, S.L., Bowker, G.C., Neumann, L.J., 2003. Transparency beyond the individual level of scale: Convergence between information artifacts and communities of practice, in: Digital Library Use: Social Practice in Design and Evaluation,. pp. 241–269.

Steel, M., 2016. When rail companies claim their trains are "on time" – but you know they aren't [WWW Document]. the Guardian. URL http://www.theguardian.com/money/2016/may/13/rail-companies-trains-on-time-delays-cancellations-punctuality (accessed 5.13.16).

Suchman, L., 2006. Human-Machine Reconfigurations: Plans and Situated Actions, 2 edition. ed. Cambridge University Press, Cambridge ; New York.

Suchman, L., 1997. Centers of Coordination: A Case and Some Themes, in: Resnick, L.B., Säljö, R., Pontecorvo, C., Burge, B. (Eds.), Discourse, Tools and Reasoning. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 41–62.

TechTarget, 2017. What is black hat? - Definition from WhatIs.com [WWW Document]. SearchSecurity. URL http://searchsecurity.techtarget.com/definition/black-hat (accessed 10.28.17).

Thomson, I., 2017. GCHQ cyber-chief slams security outfits peddling "medieval witchcraft" [WWW Document]. URL https://www.theregister.co.uk/2017/02/03/security_threat_solutions/ (accessed 4.22.17).

Tkacz, N., 2014. Wikipedia and the Politics of Openness. University of Chicago Press, Chicago ; London.

Transport for London, 2016a. Review of Social Media team being based in LUCC. June – September 2016.

Transport for London, 2016b. Social Media Strategy.

Transport for London, 2016c. Travel alerts on Twitter [WWW Document]. Transport for London. URL https://www.tfl.gov.uk/travel-information/social-media-and-email-updates/travel-alerts-on-twitter (accessed 11.25.17).

Turkle, S., 2015. Reclaiming Conversation. Penguin Press, New York.

Turkle, S., 2011. Alone Together. Basic Books, New York.

Usborne, S., 2016. All aboard the Southern chaos train: the commuters caught in a war on rails. The Guardian.

US-CERT, 2016. Heightened DDoS Threat Posed by Mirai and Other Botnets (No. Alert (TA16-288A)). US Computer Emergency Readiness Team.

Verbeek, P.-P., 2005. What Things Do: Philosophical Reflections on Technology, Agency, and Design. Penn State Press.

Woolgar, S. (Ed.), 2002. Virtual society?: technology, cyberbole, reality. Oxford University Press, Oxford ; New York.

Woolgar, S., 1990. Configuring the user: the case of usability trials. The Sociological Review 38, 58–99. https://doi.org/10.1111/j.1467-954X.1990.tb03349.x

Woolgar, S., Neyland, D., 2013. Mundane governance: ontology and accountability, First Edition. ed. Oxford University Press, Oxford, United Kingdom.

Young, J., 2009. Moral Panic: Its Origins in Resistance, Ressentiment and the Translation of Fantasy into Reality. Br J Criminol 49, 4–16. https://doi.org/10.1093/bjc/azn074

Zimmer, M., 2010. "But the data is already public": on the ethics of research in Facebook. Ethics Inf Technol 12, 313–325. https://doi.org/10.1007/s10676-010-9227-5