Volume 9.1 (2022): pp. 9 – 23

Lasers, Mantraps And Alligators: Visualising Physical Security In Data Centre Tour Videos

Samuel Kininmonth - RMIT University

samuelkininmonth@gmail.com

Abstract

This article examines how video tours of data centres visually foreground physical security infrastructure. Despite the importance of cloud computing to many people's lives, data centres, a key piece of cloud computing infrastructure, are often hidden from public view — but not always. Many companies promote their services by making tour videos of their data centres. An emerging body of research in media and communication studies has examined how promotional material visualises data centres, but there is little research on how promotional videos represent physical security infrastructure. This paper consists of a qualitative content analysis of 66 data centre tour videos from data centres located around the world. It finds that data centre video tours often spend significant time visualising security features used to protect data centres from unauthorised physical access. The videos often feature various security measures, including 24-hour guards, boom gates, fences, radio-frequency identification (RFID) cards, guard stations, biometric scanners, man traps and underfloor lasers. I argue that the video tours are marketing materials that act as security theatre and foreground physical security features to perform a security discourse of control over territory, people and data. The videos also unexpectedly foreground human labour within the security apparatus. They demonstrate that security infrastructure governs the workers that maintain it.

Keywords

Data Centres, Security, Video Tours, Infrastructures

Introduction

Media researchers are paying greater attention to communication infrastructure and how infrastructure is mediated. Communication infrastructure such as data centres are often remote and difficult to access. Earlier research has shown that organisations that operate data centres produce media to promote some aspects of their infrastructure, such as its environmental efficiency or security; the infrastructural elements that organisations choose to promote help build their "corporate identity" (Holt and Vonderau, 2015, p.90). Many data centre operators have produced or participated in data centre tour videos to promote their brand and stake their infrastructural corporate identity.

For example, in one video, a tour guide, dressed in a jacket and jeans, guides the viewer through a Google data centre one location at a time – from the bright foyer to the racks of servers to the cooling systems on the roof (Google Cloud Tech, 2016). He is joined in every area by enthusiastic Google employees who excitedly explain the infrastructure they maintain and support many of Googles services. In this video, every location also contains a third person. A silent, motionless security guard is standing in the back of shot. The producers shot this data centre tour video using a 360-degree camera that stitches the footage together to create a virtual reality (VR) experience. While the guide speaks, viewers can use

their mouse to pan and tilt the camera in any direction. The guard is not immediately apparent; viewers need to pan away from the exuberant tour guide to find them, but they are there. Figure 1 illustrates examples of the guard in several locations: among the server racks; next to the auxiliary power supply; next to the cooling system, roaring as it works to cool the powerful computers. The production appears to have purposefully made the guard visible.

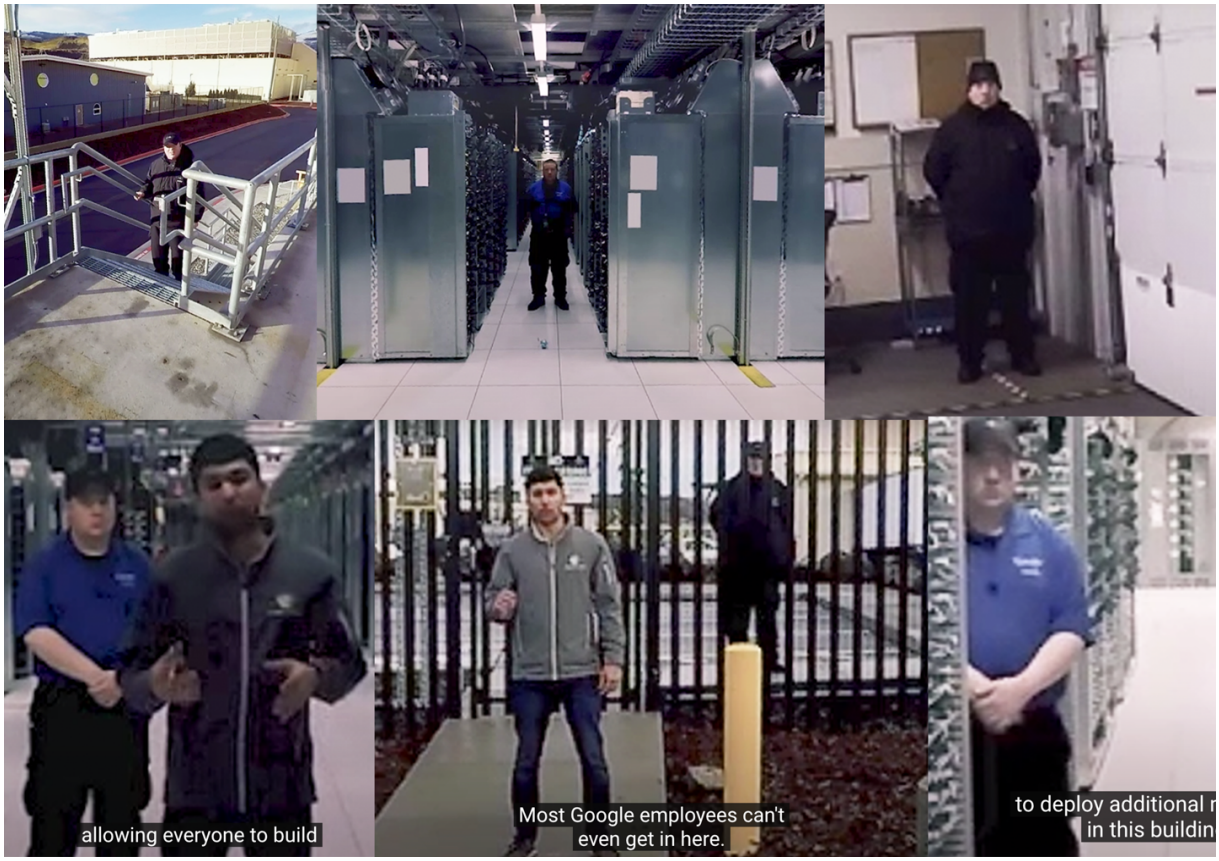

Figure 1. A glimpse from the 360 video tour of a Google data centre. A motionless security guard appears in the background of every location. Source: (Google Cloud Tech, 2016).

Like other kinds of telecommunications infrastructure, such as undersea cables (Starosielski, 2015), data centres are often located far away from the customers they serve. A host of factors can influence the location – land prices, access to fibre optic cables, access to electricity, air temperature, frequency of natural disasters, government policies – but certainly a significant reason is that operators often do not want them to be publicly accessible (Rossiter 2017; Hu 2015). Data centres are primarily designed to function invisibly in the background. But this is not always the case. Like the Google tour video described earlier, companies exhibit their business infrastructure to potential clients in data centre tour videos. The tour videos are designed to reassure potential clients that the data centres will continue to provide service in the face of external threats such as natural disasters or intruders and technical failures such as fires or power failure. Recent research has examined how data centres are put "on display" (Holt and Vonderau, 2015 p.89; see also Taylor, 2017; 2019). Because data centres are essential infrastructures that are often inaccessible to the public and researchers, the media made about them is crucial for understanding part of the infrastructure that underpins much of our digital communications.

This article reports on the representation of security from a content analysis of 66 data centre tour videos. In addition to highlighting power reliability and cooling efficiency, the video tours spend significant time presenting physical security infrastructure. I argue that data centre security videos foreground physical security to make certain features "hypervisible" (Holt and Vonderau 2015). By emphasising physical security features, the promotional videos cultivate an image of sovereign territory

Volume 9.1 (2022): pp. 9 – 23

guarded against external threats (Hu 2015). The tour videos perform a particular kind of security theatre that channels a discourse of control of territory and people. This security discourse of control extends to the people who maintain and guard the data centres. Workers require access to data centres to maintain and defend them, and the tour videos spend a significant portion of their time visualising the features that restrict or allow access to particular areas. The videos demonstrate that data centres are sociotechnical infrastructures and that the companies that run the centres believe that control of people within data centres is important to their clients.

I first outline previous research that interrogates why data centre operators choose to visualise certain aspects of their infrastructure and what role security features play in performing discourses of security. I then briefly detail how I conducted qualitative content analysis on a corpus of data centre marketing videos. The content analysis identifies several recurring security representations in the videos, including how visualising physical security infrastructures links to corporate identity, layers of access and security staff. Finally, I discuss how the tour videos perform the construction and control of territory to sell the data centre's services and smooth over perceived threats from workers within the data centre.

Current Debates

As media and cultural studies take an "infrastructural turn", scholars have focused on data centres as critical internet infrastructures. A growing number of scholars have examined the representation of data centres (Holt and Vonderau, 2015; Taylor 2017; 2019), their labour (Velkova, 2020), territoriality (Hu, 2015; Rossiter, 2017, for cables, see Starosielski, 2015), political economy (Mosco, 2015) and environmental costs and interactions (Cubitt et al., 2011; Peters, 2015; Hogan and Vonderau, 2019).

An issue in the emerging research concerns how data centres represent certain features over others in their promotional materials. Jennifer Holt and Patrick Vonderau (2015, p.90) argue that promotional materials, including videos, serve to "stak[e] corporate territory", locating the company and service in the material world. The companies that promote their data centres make certain features "hypervisible". Holt and Vonderau argue that promotional materials foreground some features while hiding others in "plain sight" (2015, 92). Hypervisibilised infrastructure cultivates an identity for the organisation that builds, maintains and uses it. A crucial recurring narrative in data centre promotional materials is their security features.

Although modern data centres are highly automated, they require people to maintain them (Greenburg et al., 2009). There is a tension between access to data centres and their security. As computer security expert Gene Spafford noted in 1989, "The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards — and even then I have my doubts" (Spafford via Schneier, 2018, 19). A server that has been powered off, cast in concrete and lined with lead is useless to store accessible information. In other words, a totally secure data centre is a useless data centre. As internet security expert Bruce Schneier (2018, p.19) notes, "[s]ecurity is always a trade-off". A data centre without labour to maintain it would be useless, but labour's presence is a perceived threat.

A common way out of this dilemma is to downplay workers' presence in data centre promotional materials. ARE Taylor found that data centre management actively cultivates an aesthetic of facilities that are futuristic, full of white space (2017) and "pure machine" (2019 p.4). A photographer who works for data centre clients recounts that "most data center [sic] briefs specify that they don't want their workers in the photographs" (Taylor, 2019 pp.13-14). A Chief Operating Officer of a data centre explains that they minimise human representation because it is perceived as the weakest security link (Taylor, 2019). Taylor (2019, p.14) notes that phrases such as "'humans are the easiest thing to hack' or 'people are the weakest link in data center security', are frequently encountered in industry discourse and reflect a specific brand of 'automation bias' (the trusting of machines over humans)". The invisible labour of data centres

is in tension with their security. However, this research illustrates that human workers are more foregrounded in data centre tour videos than might be expected, but primarily when functioning in a security role.

Data centres project their security through control of specific territory and the people within it. Scholars including Tung-Hui Hu (2015) and Ned Rossiter (2017) have considered the relationship between data centres' security discourses and their territoriality. Hu (2015, pp. 91-92) argues that security is a "widespread discourse" used by various, often antagonistic, actors who share the common value of "freedom". This liberal freedom functions as the reaffirmation of shared values to an external threat. For data centres, the danger stems from "external, unfree enemies" such as hackers or scammers (Hu, 2015, 92). Hu asks, "why are so many data centers [sic] housed inside militarized structures built to defend physical territory?" (Hu, 2015, 91). The answer for Hu lies in the staking of "sovereign power within the cloud, power as dependent on or coterminous with a specific territory" (Hu, 2015, 92). Territory is linked to sovereignty, creating ruled space. For Hu, data centres represent "the guarded camps of the Pony Express, in which messengers retreated for the night from the unsafe territory outside" (Hu, 2015, 81). As a worker at The Bunker data centre remarks to Hu, "Security is our way of thinking . . . We consider everything outside the client firewall as hostile" (Hu, 2015, 81). Security features are a political intervention that governs who can access infrastructure and how. Rossiter (2017) argues that studies of data centres need to account for "the apparently paradoxical" tension between data centres' differences and industry-wide security standards. He notes that data centres can prompt issues around "security, surrounding economies, labouring subjectivities and so forth" (Rossiter 2017, 6). Importantly, data centres are heavily securitised spaces that rely on on-site and offsite workers to maintain them. Data centres have a kind of sovereign territoriality but are inextricably, simultaneously linked to local labour markets, international standards, and data markets.

Julia Velkova (2020) conducted participant observation in the Yandex data centres in Finland and created a photo essay about the lives of the workers who maintain and guard it. Velkova describes how the workers persist in the often inhospitable workplace by growing plants, making art and cooking for each other. The activities reaffirm their humanity even as the work itself addresses them as "non-people' in a "not-for-humans space" (2020, p.49). Guarding is a significant task, even if it is often long and tedious. As one guard tells Velkova (2020, p.49), "Very little happens here. There is nothing. I kind of feel that I am guarding an empty space". Velkova notes how the guards are themselves surveilled by the data centre site manager. As the site manager tells her, "The security guard [booth] looks like an aquarium. [The guards] are the fishes inside" (Velkova, 2020, p.54). The security infrastructure applies to both potential intruders and workers within the data centre.

The previous studies demonstrate that data centre operators promote certain infrastructure features to market their services. Operators foreground physical security features to project secure, ruled space in contrast to perceived external threats. Some studies have observed that data centre operators prefer to minimise human labour in their promotional materials because they perceive people as unavoidable security threats. Foucault noted that security is not always a "binary division between the permitted and the prohibited" (Foucault, 2007, pp. 20-21). Security can mean governing somewhere between an optimal and acceptable bandwidth. Put another way, the videos convey the impression that the affordances of security infrastructure permit acceptable behaviour on-site (Davis 2020). This research aims to understand why, unlike the material studied by Taylor (2019), data centre tour videos visualise workers within the security apparatus and what that means for security discourses of sovereignty and territoriality.

Method

I constructed a corpus of videos from the video streaming service YouTube in late 2019 to explore the representations of physical security features and staff in data centre tour videos. I began by collecting videos from the curated YouTube playlists Data Center Tour and Data Center Knowledge. I then

Volume 9.1 (2022): pp. 9 – 23

expanded the collection by searching variants of "data center tour" using YouTube's internal search engine in the Firefox browser's "Private Browsing" mode. I collected over one hundred videos in total before removing videos of product demonstrations at trade shows and other videos not filmed at data centres. After removing those videos not filmed at data centres, the corpus contained 66 videos with a total of around thirteen million views [1]. The videos are diverse. They vary in a) views – the least with several hundred views, the highest with around five million, b) length – from a couple of minutes to half an hour, c) production site – they were produced by different companies and in different countries (although a large section are from the United States), and d) format – 11 of the videos in the corpus feature 360/VR footage.

I conducted a qualitative content analysis on the corpus of tour videos, deploying the common practice of coding information within a media sample into categories to establish patterns or trends (Mayring, 2004). I coded any security features explicitly mentioned by tour guides or in on-screen text and any security features shown on-screen. I then inductively collected the different security features together into recurring themes.

Promotional videos are useful for studying industry discourses. Previous research illustrates how news organisations (Bednarek and Caple, 2015) and Australian universities (Gottschall and Saltmarsh 2017) use promotional videos to distinguish their brand by foregrounding desirable attributes like trustworthiness or a "good life". The data centre tour videos are marketing materials used to promote their security, reassure clients and distinguish themselves from competitors. This isn't to say that the tour videos mislead the viewer with the security features they highlight. The texts blur the true and the political. Data centre operators produced the videos to foreground some elements over others to sell the data centre's services to potential clients. Bruce Schneier (2009) argues that much overt physical security infrastructure is "security theatre" that makes people feel more secure without actually improving their security. While many of the security elements of data centres are prescribed by international standards (Spring 2011; Rossiter 2017), numerous security features and scenarios discussed in the tour videos resemble the "movie-plot threats" that Schneier (2009) describes. However, this security theatre is productive, sustaining a particular sociotechnical imaginary of security (Hockenhull and Cohn 2021). The videos stake corporate territory and identity by performing the same security discourses described by Hu (2015), Rossiter (2017) and Taylor (2019).

Promoting Security in Data Centre Videos

The content analysis of the corpus showed that security is a significant focus in data centre tour videos. Most videos featured three key elements: security, cooling and power. While the systems that cool and power the servers are often an appreciable part of the tours, the security features such as cameras, gates, and radio-frequency identification (RFID) badges often feature heavily and feature first. Generally, tour videos devoted around one third of their total running time to security, although a few videos devoted at least half their time to security infrastructure. Three key themes emerged from the content analysis: first, that the videos tie security to data centres' identities; second, the videos emphasised that security is layered; and third, that the videos foreground security guards as working within layers of security.

Tying Security to Organisational Identity

The video centre tours visualise the security infrastructure to emphasise aspects of companies' identities. The caption to the OneNeck tour video, promoting one of their data centres based in the United States, reads: "Take a look inside a OneNeck state-of-the art data center and see first-hand the security and compliance measures taken to ensure your data is safe!" (OneNeck IT Solutions, 2017). LeaseWeb's (2016) video notes that it is a "Fort Knox for your data". Oracle's (2017) tour boasts that the physical

security is at the "Forefront of Oracle's first defence against threats and compromises" and that their "buildings are among the most secure in the world". A Visa DPS (2014) tour video states that,

> "In here, the Visa promise is rooted in metal, fibre optics, concrete and electricity … Infrastructure like this doesn't just happen. It comes from investment."

Another video notes, "Steel, granite, brick. … This place is a bunker" (Gestalt IT, 2017). The physical security infrastructure stands in for the organisations' commitment to protecting their customers' data.

While some physical security at data centres might be unsurprising, several data centres promote their ability to repel threats that could come straight from a Hollywood film. A tour guide at a data centre in Brazil notes that "[i]n the case of an invasion, all our doors are automatically locked" (TIVIT_Oficial, 2017). Another data centre claims to be safe from "biological attack" (Data Center Knowledge, 2008). Some data centres reference nothing less than the end of the world. As a tour guide notes in one video, "Yeah, this place is a fortress, great for a zombie apocalypse" (Gestalt IT, 2017). Tour videos also note the following: attacks via a vehicle, deploying gates and bollards; attacks by an intruder, deploying anti-climb technologies (such as barbed wire) and bulletproof glass; attacks by a visitor, who must be escorted at all times and navigate different layers of access; and attacks by an employee, many of whom are given the access to or the location of the data centre, or must be monitored at all times when on-site. The videos foreground physical security features to promote their resilience to a range of physical threats. By connecting the company's brand to impervious security structures, the data centre operators stake their corporate territory and render the identity corporeal (Holt and Vonderau 2015).

Security Layers

The tour video corpus promotes the idea that security features often operate as an assemblage of security *layers*. The tours frequently refer to security as "multi-layered", or "seven layers", or "six zones", or "two" or "three" "factor" authentication. According to the marketing materials, the layers act as both a redundancy measure and for structuring access. By layering independent security measures, an intruder would have to overcome each one in different ways. Even authorised workers and visitors operate within multiple layers of security. As the Chief Operating Officer of the Involta 360 Data Center explains, they use a "least privileged approach" where clients can only access certain areas in the data centre (Involta, 2018). The security functions to discipline action between the optimal and the acceptable, for an intruder, visitor, and employee alike.

The security of the data centres starts with their choice of location. Different videos boast that their data centre has no external signage to identify it, and many do not allow visitors. As one tour guide boasts, their centre is "so secure even some of our employees don't know where it is" (TradeCraft, 2016). To create these secure buildings (as well as cool and power them), some companies build data centres in existing buildings. A considerable number of data centre videos feature data centres built in repurposed buildings. Repurposed structures in the sample include an old mineshaft (Iron Mountain, 2017), retired silos (CLUMEQ, 2009), converted factories (Intel, 2009), including an old microchip factory (Intel, 2016), a cotton mill built in 1876 (Congruity360, 2017), a remodelled shopping centre (Data Center Knowledge, 2009) and an old nuclear bunker in Sweden (touted as a Bond lair) (Pionen Data Center, 2017).

Volume 9.1 (2022): pp. 9 – 23

A potential intruder who could identify and reach a data centre would then have to contend with entering the grounds. Many data centre operators use the tour video to promote how heavily they guard their premises. For example, numerous data centres in the tour videos featured extensive and high fencing. Operators augment the fencing with other features, including "anti-climbing devices" or charging the fence with "10,000 volts of electricity" — "the highest legal limit", one video boasts (Leaseweb, 2016). Other videos feature shots of what appears to be a moat, while another features a "beware of the alligators" sign (see Figure 2). Management may have placed the sign for the safety of employees, but the decision to feature it in a video tour of a data centre gives the impression that alligators are protecting clients' data. Visitors seeking to pass the various barriers might do so through any combination of gates, boom gates, licence plate recognition cameras, closed-circuit television (CCTV) cameras and well-lit spaces. An intruder might have to pass any of these features to reach a data centre's car park.

Figure 2. Beware of the Alligators sign outside a Google data centre. Source: (The Soul of Politics, 2017).

Once a visitor has reached a data centre's buildings, they might then walk past anti-ramming devices or retractable bollards to reach the door, measures to stop a vehicle from ramming into the building. Other videos boast about bulletproof windows or bulletproof film applied to the glass. The types of efforts seem to indicate that the intruders may be armed or dangerous.

Tour videos and their guides typically move into the entrance or foyer of the data centre, sometimes after announcing themselves to security guards through an intercom next to a remote access door. Once inside the threshold, data centres may have security staff checking each visitor against a pre-approved list of authorised entrants. Visitors may be identified by photo ID or biometric scanners. Once checked in, visitors may then be issued with a marked badge or lanyard, some with an RFID function to access certain areas in the centre.

In the videos, after the security check-in, visitors will generally move through the data centre using a combination of an RFID badge, passcodes or biometric scanners. The tour videos promote the use of a variety of biometric scanners, including fingerprint scanners, facial recognition cameras, iris scanners (that scan your eyeball) and vascular scanners (which use infrared light to recognise the patterns of veins in a finger). In the video tour of Congruity360 Data Center, the group jokes about which finger an intruder would need to cut off an employee to gain entry (Gestalt IT, 2017). The tour videos often mention that operators use multiple security features together. As a guide at the Involta 360 Data Center

tells the camera, "there's no getting beyond these doors without clearing both" a preapproval process to receive a proximity (RFID) badge and a "thirty-two point" iris scanner (Involta, 2018). The visitor still requires an escort.

The videos demonstrate how passcodes and scans allow visitors to pass through various portals and security cages. These portals might be reinforced steel doors, while others are more elaborate. Some centres feature turnstiles within the facility, ensuring that someone without authorisation cannot follow someone with clearance between rooms. "Mantraps" also feature in tour videos. Mantraps are devices with two doors that usually require the first door to be closed before the second can open. Mantraps function to stop an unauthorised person walking behind an authorised person or 'tailgating', but security can also trap intruders between doors. Some tour videos show centres with individually locked "cages" around the actual server racks. Technicians may need passcodes, RFID badges or metal keys to access the servers.

The videos promote the idea that visitors often move between other kinds of surveillance technology while walking around the centre. Many data centre tours explicitly showed and mentioned the high number of CCTV cameras spread across the facilities. In one video, the tour guide boasts that a centre in Cairo has over 130 cameras (GPX 2017). In another, a guide boasts about how ubiquitous the CCTV coverage is when he says, "You can't stand anywhere in this facility without a camera being able to view you" (IPC, 2016). Another guide echoes, "Everywhere we've been, there are two or three cameras" (Gestalt IT, 2017). One video notes that some Google data centres use sophisticated thermal imaging cameras to identify the heat signatures of intruders at their perimeter or within their grounds (Google Workspace 2013).

Some centres use algorithms in addition to guards to analyse the surveillance footage for suspicious behaviour. As a Google tour video explains, it uses "video analytics" that "automatically detect anomalies in the video and alert security staff to investigate further" (Google Workspace 2013). CCTV cameras are not the only sensors, though. Other areas might be protected by motion detectors, including lasers in the underfloor vents. "Lasers?!" a visitor excitedly exclaims in one video (Gestalt IT, 2017). The security measures featured in the corpus of tour videos illustrate how the security features do not simply prevent unauthorised access but structure that access. Security staff work for and within layers of security.

Guards: Watching and Watched

Figure 3. A guard checks cars at a checkpoint outside a Google data centre. Source: (Google Workspace, 2013).

Volume 9.1 (2022): pp. 9 – 23

Security staff feature heavily in data centre tour videos. The videos promote security guards as an essential security element in a data centre. Many of the videos boast of a "24/7" or "24/7/365" security presence. As the video tours work their way towards the racks of servers, they may feature a host of security guards at work. Some of these jobs might include guard posts stationed next to the gates and boom gates. In Figure 3, a security guard gazes vigilantly out from the perimeter of a Google data centre for intruders. The guard checks the identity documents of employees as they approach a boom gate to enter the grounds.

The video tours often show guards performing their work inside the data centre. In the videos guards perform their duties from behind counters and front desks, checking credentials and issuing passes. Beyond the front desks, visitors may then pass a metal detector test and x-ray machine. Guards are also featured in command centres, watching rows of monitors with CCTV footage or graphical representations of the centre. Figure 4 shows guards at a Google data centre watching and discussing video surveillance feeds in the command centre. The video explains that security guards are trained to immediately investigate anything out of the ordinary and that Google maintains "relationships with local law enforcement" alongside footage of a police cart arriving at the gate (Google Workspace, 2013). The videos also feature guards who aren't tied to a particular location. Tours show and boast of round the clock patrols of the buildings and grounds, with some mentioning audits of restricted space "every hour" (OneNeck IT Solutions, 2017). In some data centres, guards escort visitors at all times during their visit. One Google data centre equips patrolling security guards with a garage of cars and jeeps to secure the grounds (Google Workspace, 2013).

Figure 4. Guards staff a security command centre inside a Google data centre. Source: (Google Workspace, 2013).

The videos often promote features that allow technicians to work within the security layers of the data centre. Many data centre tour videos show features designed to make data centres habitable for their clients' technicians. Standard amenities appearing in the tour videos include meeting rooms, kitchenettes and hot desk spaces. Some data centres offer more comprehensive domestic features such as gyms, showers and sleeping quarters. These spaces enable people to inhabit and effectively work in the austere data centres. In some data centres, the security extends beyond protecting the capital of the server racks to the workers. One tour video boasts that workers can enjoy an outdoor break area "within the secure area" (RagingWire Data Centers, 2017). People secure and are secured within the data centre.

The corpus of video tours demonstrates the prominent role physical security features take in data centre promotion. The videos make specific security infrastructures hypervisible to perform particular

security discourses. The tour videos illustrate the tension noted by Taylor (2017) that data centre workers are perceived to be a weakness in the security, making their representation in the tour complex. As the videos demonstrate, security guards are often critical to data centre security. The security is represented in the videos in layers to account for potential weaknesses and reassure clients that those who work within the securitised space are themselves governed. As a tour from the Iron Mountain data centre tells the viewer, its officers are "vetted [and] background checked" (Iron Mountain, 2017). A guide at the IPC Data Center in the Philippines tells the viewer that "we have eyes on all visitors all the time" (IPC, 2016). The videos smooth the tension of perceived risk by layering security for the people who work within the data centres.

Discussion

The analysis of data centre tour videos highlights that physical security is vital to promoting data centres. The infrastructure needs to be secure and operational, even in the face of disaster (what is referred to as continuity-of-operations plan or COOP (see Spring, 2011)). Data is a crucial part of our lives, and many institutions and essential social processes rely on keeping personal information (Nissenbaum 2010) and health data (Lupton, 2018) secure. Data flows and storage are also crucial to structures of power (D'ignazio and Klein 2020). Infrastructure is supposed to be reliable and seamless. The physical security infrastructure is tied to the identity of the organisation that runs it and the clients who might use it. Choosing a data centre is both an operational decision but also a political one. Infrastructure is usually hidden, or *infra,* and operators choose to exhibit the infrastructure for political reasons.

Contrary to industry preferences expressed in previous research, the video tours foreground workers within the security apparatus of data centres. Unlike the material observed by Taylor (2019), where workers are hidden from the camera lens, the data centre video tours used the workers, and other security measures, to perform the discourse of guarded, ruled space described by Hu (2015). The promotional videos highlight physical security features as a security theatre, pre-empting and nullifying potential threats to underline the centre's brand or corporate identity.

Mark Andrejevic (2007) terms the increasing use of surveillance through a growing number of inputs as constructing the "digital enclosure". The dream of the digital enclosure, according to Andrejevic, is "the creation of an interactive realm wherein every action and transaction generates information about itself" (2007, p.2). Data centres and the cloud are foundational for enabling mass surveillance and calculation for the digital enclosure to function (Rossiter 2017), but it also appears that its logic has turned within. As the Google video tour at the beginning of this article illustrates, data centre tours communicate that even media crews working for Google are always accompanied by guards within the centre. Other videos echo this sentiment, and some state explicitly that visitors are escorted by guards at all times, while many display the enormous amount of surveillance equipment used within the data centres and their grounds. Andrejevic notes that the digital enclosure facilitates only two things: "commerce and policing" (2007, p.132). The staff in the data centre work towards the ends of commerce and policing, securing the data centre and ensuring it continues to provide uninterrupted service against "external, unfree enemies" (Hu 2015) even in the face of existential threats such as climate change (Cubitt et al., 2011; Peters, 2015; Jones, 2018; Hogan and Vonderau, 2019). The tour videos demonstrate the discourse used to sell the securitised future of the internet to corporate clients even in the face of potential social and environmental upheaval.

Conclusion

This article shows that the data centre tour videos foreground physical security infrastructure and security workers. The tour videos tie the physical security infrastructure to the corporate identity and communicate the durability and reliability of the service. The video tours perform a certain kind of

Volume 9.1 (2022): pp. 9 – 23

security theatre to promote their services and stake their corporate identity, guarding their sovereign territory against perceived external threats. They foreground security features such as 24-hour guards, boom gates, ID checks and CCTV to illustrate their control over the data centre territory. To underline their security, some also claim to be ready for movie-plot threats such as an "invasion", a "biological attack", or a "zombie apocalypse". Rather than considering this security theatre as a distraction, it might be more helpful to consider its role in performing security discourse, branding data centres, and putting infrastructure on display (Holt and Vonderau 2015).

The video tours also highlight ongoing tensions associated with working in data centres (Rossiter 2017). Previous research has noted a reticence to include people in promotional material for data centres because people present a possible security threat (Taylor 2019). However, tour videos often feature security guards and technicians at work. The tour videos smooth this tension by communicating that the security works in layers with comprehensive surveillance of visitors and workers. Rather than an authorised/unauthorised binary, the videos give the viewer the impression that the security structures access. Much of the security work featured in the videos occurs away from the towers of servers, communicating that workers are only allowed where necessary.

Data centres are central to many growing uses of digital technology, including cloud data storage, data processing, media streaming services and automation. The operators of data centres appear to consider it essential to communicate the physical security they use to guard their services. The tour videos foreground physical security to perform specific security discourse and establish governed corporate territory. The data centre tour videos give an insight into a vision of the future of computing and the internet that is much more closed and securitised than might have been previously imagined. Further research is required to critically examine how this promotional material is produced and how it relates to data centre workers' lives and working conditions. Cloud storage and computing seem likely to increase in importance, but workers will occupy changing roles as data centres are further automated. Following work such as Starosielski (2015) or Rossiter (2017), future research might study how the representation of data centre security changes in different political and cultural contexts across countries. So, even as you read this article you downloaded from a server somewhere, think of the alligators.

Acknowledgements.

I would like to thank the anonymous peer reviewers for their helpful and constructive comments. I also thank the special issue editors for persevering through a challenging time during intermittent Covid lockdowns. The research benefitted from valuable discussions with Mark Andrejevic, Libby Lester, Ramon Lobato and Julian Thomas. I completed the revisions while visiting the University of Tasmania as a university associate and I thank the UTas media school for their support.

Endnotes

1. Please contact the corresponding author for a full copy of the data centre tour video corpus.

Referenced Data Centre Tour Videos

Btirelandbusiness (2013, 20 November) BT Data Centre - Take a Virtual Tour. Retrieved from https://www.youtube.com/watch?v=Iyk2D8HVlUk

CLUMEQ (2009, 14 November) Sun Constellation System CLUMEQ. Retrieved from https://www.youtube.com/watch?v=1qyCH2G8epo

Congruity360 (2017, 20 November) Congruity360 Data Center Tour. Retrieved from https://www.youtube.com/watch?v=beH1SLMwBbE

Data Center Knowledge (2008, 12 August) Cooling the SuperNAP: WDMD. Retrieved from https://www.youtube.com/watch?v=mFywyGUKu7o

Data Center Knowledge (2009, 16 November) Inside Rackspace Headquarters. Retrieved from https://www.youtube.com/watch?v=5mZcuY0I_yQ

Gestalt IT (2017, 21 November) Congruity360 Data Center Tour. Retrieved from https://www.youtube.com/watch?v=beH1SLMwBbE

Google Cloud Tech (2016, 24 March). Google Data Center 360° Tour. Retrieved from https://www.youtube.com/watch?v=zDAYZU4A3w0

Google Workspace (2013, 19 September) Security and Data Protection in a Google Data Center. Retrieved from https://www.youtube.com/watch?v=cLory3qLoY8

GPX (2017, 18 October) GPX Cairo 2 TIER 4 Data Center Tour. Retrieved from https://www.youtube.com/watch?v=nNqzRrdwJ3Y

Intel (2009, 9 February) Intel Data Center Tour Featuring CPI Ducted Cabinets. Retrieved from https://www.youtube.com/watch?v=ELB3chJJe7w

Intel (2016, 19 July) World-Class Data Center Tour. Retrieved from https://www.youtube.com/watch?v=EYK0KeHG2lk

Involta (2018, 19 June) Involta 360 Data Center Tour. Retrieved from https://www.youtube.com/watch?v=OX0yCtXBafo

IPC (2016, 16 August) IPC Data Center Parañaque Tour. Retrieved from https://www.youtube.com/watch?v=4Bv0PkmqzB8

Iron Mountain (2017, 12 December) A virtual tour of Iron Mountain's Underground Data Center. Retrieved from https://www.youtube.com/watch?v=Bvf00GEiZFY

Leaseweb (2016, 29 June) Data center 360° VR tour – LeaseWeb. Retrieved from https://www.youtube.com/watch?v=sS7UxiCVqrg

OneNeck IT Solutions (2017, 23 January) OneNeck Data Center Tour. Retrieved from https://www.youtube.com/watch?v=Zm2cUXvNr8U

Oracle (2017, 12 January) Tour Oracle's State of the Art Data Centers. Retrieved from https://www.youtube.com/watch?v=f4RBs43G17g

Pionen Data Center (2017, 31 March) This Data Center Looks Like a Villain's Lair Out of James Bond. Retrieved from https://www.youtube.com/watch?v=lRffsXIASNQ

Volume 9.1 (2022): pp. 9 – 23

RagingWire Data Centers (2017, 2 March) RagingWire Dallas TX1 Data Center Virtual Tour. Retrieved from https://www.youtube.com/watch?v=s9W4vtg6CMQ

The Soul of Politics (2017, 8 May) Google Data Center Inside Tour in Google headquarters in Mountain View, CA. Retrieved from https://www.youtube.com/watch?v=evHVnkZBpW4

TIVIT_Oficial (2017, 14 September) Welcome to Data Center TIVIT - Tour 360º. Retrieved from https://www.youtube.com/watch?v=HtY-sCfjW7g

TradeCraft (2016, 26 April) Rackspace Virtual Tour of the Dallas/Fort Worth Data Center. Retrieved from https://www.youtube.com/watch?v=pHPybh0THDI

Visa DPS (2014, 18 March) Visa DPS Data Center Tour. Retrieved from https://www.youtube.com/watch?v=6x81jayoH0Y

References

Andrejevic, M. (2007). iSpy: Surveillance and power in the interactive era. University Press of Kansas Lawrence.

Bednarek, M., and Caple, H. (2015). Promotional Videos: What Do They Tell Us about the

Value of News? In R. Piazza, L. Haarman, & A. Caborn (Eds.), Values and Choices in Television Discourse. Palgrave Macmillan.

Burgess, J., and Green, J. (2018). YouTube: Online video and participatory culture. Polity Press.

Cubitt, S., Hassan, R. & Volkmer, I. (2011). Does cloud computing have a silver lining? Media, Culture & Society, 33, 149-158.

Davis, J. L. (2020). How artifacts afford: The power and politics of everyday things. MIT Press.

D'ignazio, C., and Klein, L. F. (2020). Data feminism. MIT press.

Foucault, M. (2007). Security, territory, population: lectures at the Collège de France, 1977-78. Springer.

Gottschall, K., and Saltmarsh, S. (2017). 'You're not just learning it, you're living it!' Constructing the 'good life' in Australian university online promotional videos. Discourse: Studies in the Cultural Politics of Education, 38(5), 768-781. https://www.tandfonline.com/doi/pdf/10.1080/01596306.2016.1158155

Greenburg, A. et al. (2009). The Cost of a Cloud: Research Problems in Data Center Networks. ACM SIGCOMM Computer Communication Review, 39, 68-73.

Hashizume, K. et al. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4, 5.

Hockenhull, M., and Cohn, M. L. (2021). Hot air and corporate sociotechnical imaginaries: Performing and translating digital futures in the Danish tech scene. New Media & Society, 23(2), 302-321.

Hogan, M. & Vonderau, A. (2019). The Nature of Data Centers. Culture Machine.

Holt, J. & Vonderau, P. (2015). 'Where the internet lives': Data centers as cloud infrastructure. In Signal Traffic: Critical Studies of Media Infrastructures, (Eds, Parks, L. & Starosielski, N.) University of Illinois Press Urbana, pp. 71-93.

Hu, T.-H. (2015). A Prehistory of the Cloud. MIT Press.

Jones, N. (2018). How to stop data centres from gobbling up the world's electricity. Nature, News Feature [12 September], https://www.nature.com/articles/d41586-018-06610-y

Lupton, D. (2018). Vital Materialism and the Thing-Power of Lively Digital Data. In D. Leahy, K. Fitzpatrick, & J. Wright (Eds.), Social Theory, Health and Education. Routledge

Mayring, P. (2004). Qualitative Content Analysis. A companion to qualitative research 1 (2): 159–76.

Mosco, V. (2015). To the cloud: Big data in a turbulent world. Routledge.

Nissenbaum, H. (2010). Privacy in context: technology, policy, and the integrity of social life. Stanford University Press.

Peters, J.D. (2015) The marvellous clouds: Toward a philosophy of elemental media. University of Chicago Press.

Schneier, B. (2009, November). Beyond Security Theatre – Schneier on Security. Retrieved 2021-08-23 Available at: https://www.schneier.com/essays/archives/2009/11/beyond_security_thea.html

Schneier, B. (2018). Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. WW Norton & Company.

Rossiter, N. (2017). Imperial Infrastructures and Asia beyond Asia: Data Centres, State Formation and the Territoriality of Logistical Media. The Fibreculture Journal, 220.

Spring, J. (2011). Monitoring Cloud Computing by Layer, Part 1. IEEE Internet Computing.

Starosielski, N. (2015). The Undersea Network. Duke University Press.

Subashini, S. & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34, 1-11.

Taylor, A.R.E. (2017). The Technoaesthetics, Temporalities and Transparencies of Data Centre White Space. Imaginations Journal of Cross-Cultural Image Studies/revue de études interculturelle de la image, 8.

Taylor, A.R.E. (2019). The Data Center as Technological Wilderness. Culture Machine, 18.

Volume 9.1 (2022): pp. 9 – 23

Velkova, J. (2020). The Art of Guarding the Russian Cloud: Infrastructural Labour in a Yandex Data Centre in Finland. Digital Icons: Studies in Russian, Eurasian and Central European New Media.

List of Figures

Samuel Kininmonth is a PhD Candidate at RMIT University and consumer advocate at the Australian Communications Consumer Action Network (ACCAN). Sam's research examines how automation is changing communications infrastructure. His PhD thesis explores the development of programmatic advertising and the automation of media buying in Australia.