xCoAx 2019 Conference on Computation, Communication, Aesthetics & X Milan, Italy

Craig Fahner
craig.fahner@gmail.com

Ryerson University

Matthew Waddell
matthew@matthewwaddell.me

Axis Z Media Arts

DEEP SOLUTIONS: Artistic interventions in platform capitalism

Keywords
social media
surveillance
media art
platforms
virtual reality
interactive art

The business model held by platforms like Facebook and Google is dependent on practices of user tracking and data collection. These practices place their users in a highly asymmetrical position in which platforms know significantly more about their users than users are able to know about the tracking strategies of platforms. This paper argues that media artworks are uniquely equipped to level these asymmetries by creating sites that reveal the inner workings of these processes. We present a virtual reality installation called DEEP SOLUTIONS that aims to interpret the data that is collected by Facebook, creating an environment wherein issues of platform surveillance are contended with and experimental alternatives are proposed.

Final Draft

1 INTRODUCTION

The project we are presenting is centred on themes of surveillance and commodification within the everyday spaces of the internet. Platforms like Google and Facebook have become primary access points to the internet, thriving on an economic model that has recently been referred to as surveillance capitalism (Zuboff 2018). These platforms rely on the collection of user data, rendering user activity as a commodity that is exchanged with marketers, advertisers, political campaigns and other actors.

Due to legislative pressure, Google and Facebook now provide limited means to view the data that is stored on their users (Böhmecke-Schwafert, Niebel, and Berlin 2018, 4). This information, however, tends to be sequestered deep in application settings, far from the viewing, "liking" and sharing behaviours these platforms primarily afford. Furthermore, this information tends to be of such a significant quantity and variety that any effort to access and comprehend it requires some extraneous means of contending with its sheer magnitude and complexity.

This fundamental asymmetry between the data stored through tracking systems and its limited accessibility to users presents a significant opportunity for artistic intervention, in which strategies of narrativization, data visualization and virtual worldbuilding might work towards elucidating these murky but ubiquitous systems. The artwork we are presenting in this paper, entitled DEEP SOLUTIONS, attempts to seize upon this opportunity through the creation of a personalized VR experience based on the data collected by Facebook's algorithms. This paper will outline the research, artistic process and audience interactions that resulted from the creation and exhibition of this work. Drawing from our experiences creating this work, we also present questions that consider the possibilities, challenges and contradictions that emerge through the process of visualizing the surveillance systems that are deliberately kept hidden by monopolistic media platforms.

2 CONTEXT

In the past decade, ubiquitous computing has become woven into the fabric of everyday life. Innovations in high-speed networking, high-resolution sensors, predictive algorithms, microelectronics and data collection, while creating myriad opportunities for the mediation of nearly all realms of social life, have also afforded a magnitude of new sites of increasingly pervasive forms of surveillance. As the networked technologies that characterize the "internet of things" expand into new spatial configurations, the scope of monitoring processes, too, creeps further into the physical spaces where encounters with interactive systems occur. Mark Andrejevic has used the term ubiquitous surveillance to describe a world in which "it becomes increasingly difficult to escape the proliferating technologies for data collection, storage and sorting" (2012, 92).

Final Draft

Ubiquitous surveillance is derived from a related term, ubiquitous computing, which has come to characterize the assemblage of embedded networked technologies that has proliferated into public space and into the home. While buzzwords such as "smart technology" and "cloud computing" have been used in the marketing of GPS-enabled mobile devices, home automation tools, transit systems and payment devices, these terms do little to elucidate the processes of data collection and commodification that passively occur through everyday interactions. "If the goal of ubiquitous computing," writes Andrejevic, quoting from MIT's Project Oxygen initiative, "is to 'bring abundant computation and communication, as pervasive and free as air, naturally into people's lives,' it does the same thing for surveillance" (2012, 92). With each innocuous, technologically-mediated gesture – tapping an RFID-embedded transit card at a turnstile, for instance – results the expansion of the data-fied ghosts that follow our movements through public spaces.

Inasmuch as online environments and social media platforms extend and mediate public space, we can also examine the data collection strategies of internet monopolies as components of a larger, ubiquitous surveillant assemblage. Data collection is built into the economic model of free online services like Facebook, whose profitability depends upon the unfettered collection of user data which is transformed into a saleable commodity. Coupled with the affordances of digital platforms, which actively encourage the sharing of personal information, the capacity of social platforms to collect and retain highly personalized information about their users is unparalleled. This informational body that reflects the material self has been referred to as the "data double": a mirrored, quantified version of the self whose engagement with interactive technology draws from – and, in many ways, determines – the behaviours and experiences of its human equivalent (Haggerty and Ericson 2000, 606).

Andrejevic indicates that the data collection practices of online platforms work to enact a digital enclosure: a space delineated by the range of sensors, data collection systems and storage technologies. Evoking the notion of enclosure, which conceives of prisons, hospitals, factories and families as institutions that impose control on subjects through the logic of interiority, (Deleuze 1992, 4) Andrejevic argues that digital enclosures separate "users from the product of their activity enabled by the capture of control over the productive resources they use" (2012, 93). The spatial connotation of the term "enclosure" is useful, as it provides a dynamic paradigm to describe the manner by which users pass through a variety of different spheres of electronic mediation, which are all characterized by an interoperability of protocols and services. Each moment that a user interacts with a digital enclosure is a moment in which metadata can be extracted and stored. While these processes of capture, storage and analysis are fundamental to the promise of convenience upon which digital enclosures are predicated, they also manifest an alienating imbalance of power towards their subjects. A striking asymmetry has emerged, in which interactive systems have access to a significant amount of informa-

Final Draft

tion about their users, while their users have very little means to scrutinize the surveillance practices embedded within those very systems.

Trends in HCI design have recently turned towards the creation of transparent systems that, rather than presenting materially obtrusive interfaces, blend into the background, seamlessly integrating themselves into environments (Gates 2011, 184). This turn towards immateriality and inscrutability poses significant challenges in critically engaging with the dataveillance that is conducted by interactive systems. The logic of "black-boxing" – a term introduced by Bruno Latour to describe the tendency of the inner workings of complex technologies to become increasingly concealed to their users as technologies become increasingly complex (1999, 70) – is amplified through the development of increasingly seamless and immaterial interfaces with embedded systems, broadening the critical blind spot that prevents users from understanding the extent of data collection practices. The seductive affordances of platforms like Facebook, in addition to their seamless interfaces and underlying algorithmic complexity, serve as barriers that prevent users from truly contending with the ramifications of dataveillance practices.

As technological interfaces continue to embed themselves within social life with less and less visibility, it is of increasing importance to create sites that reveal the inner workings of these processes. This paper argues that media artworks are uniquely equipped to generate sites of critical surveillance awareness. This paper will examine two methods by which interactive artworks reveal and contest surveillance systems: they can remediate surveillance technologies, making visible the often-concealed processes of such technologies; and they can provide tactics of counter-surveillance for audiences towards imagining radical alternatives to monopolistic and surveillant platforms. We present our 2018 virtual reality installation DEEP SOLUTIONS as an intervention within the digital enclosure that makes use of these methods towards a personalized participatory artwork.

3 DEEP SOLUTIONS

In the summer of 2018, we were given an opportunity to create a hybrid performance and installation work for the WRECK CITY residency, which paired artists with various buildings in Calgary, Alberta slated for eventual demolition in which to develop work for a temporary, hands-on exhibition. Considering the unique circumstances of this project, we decided to take on issues of dataveillance and privacy through a three-part installation: one part performance, one part immersive VR installation, and one part crypto-internet café.

Our work began with an examination of the data Facebook provides through its "Download Your Information" tool. Introduced in advance of Europe's GDPR data rights legislation, this tool provides users with the ability to download the entirety of their publicly shared content (posts, likes, photos), as well as much of the information that has been derived from tracking systems that monitor user behaviour (ad profiles, location data). Users are

Final Draft

given the option to download this information in machine-readable JSON, CSV or XML formats (Böhmecke-Schwafert, Niebel, and Berlin 2018, 4). While these formats are intended to maximize interoperability with other software systems and social platforms, they do little to make readable the glut of archival material for everyday users interested in understanding how their information has been collected. The sheer magnitude and codified complexity of this information, in its "raw" form, poses a significant barrier in providing any meaningful knowledge for users. "Database-generated forms of 'knowledge'", write Andrejevic and Burdon, "are not accessible in the way that other forms of knowledge are" (2015, 21). They continue: "Data mining privileges those with access to the data and the technology when it comes to generating actionable information that may neither be fully explicable … nor reverse-engineerable." Despite the Sisyphean premise of reverse-engineering big data epistemologies, we opted to create a tool for translating these massive, machine-readable archives into information that could be directly encountered.

With DEEP SOLUTIONS, we wrote custom software that extracts visual material and text from Facebook user data, which is then implemented in a customized, immersive virtual reality experience where users can directly encounter the uncanny similarities and dissimilarities between themselves and their data doubles. One component of this software analyzes the location history database that is included with Facebook's user data archive. Ordinarily, this information appears as a list of WGS84-formatted geographical coordinates, which, in their raw form, are an abstraction that conceals the social relevance of the locations contained within. The software we developed extracts panoramic Google Street View images from locations found in downloaded user data, allowing the viewer to physically explore the timeline of locations within a navigable VR environment.

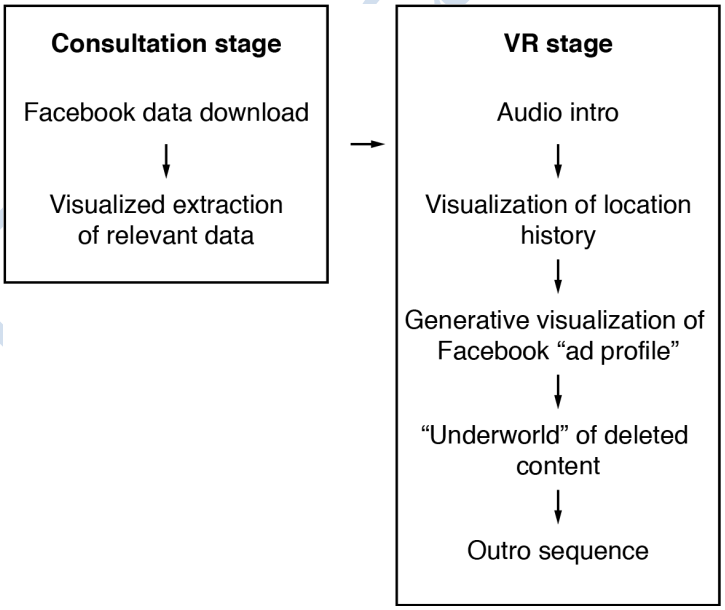

Fig. 1.
Flowchart outlining stages of interactive system

Draft

The interpretation and visualization of users' Facebook data is separated into several stages, including a hands-on consultation phase and a sequence of customized VR scenes (Figure 1). In order to accommodate the lengthy, involved process of downloading individuals' user data, *DEEP SOLUTIONS* is first presented to the audience as a consultation kiosk, in which users are invited to troubleshoot the existential quandaries of their online selves with a tech support specialist (Figure 2). In this role, we lead audience members through the process of downloading their user data. This process, which can take upwards of 20 minutes, provides a context to have discussions with visitors on issues of privacy and surveillance. Many visitors, for instance, indicated that they had no idea they had consented to giving Facebook access to location services on their phones, which was brought to light through the presentation of a stream of logged GPS coordinates on a screen in our consultation area.

Fig. 2.
DEEP SOLUTIONS consultation area

With the completion of this extraction process, the viewer is led into a VR installation, where they are invited to confront the ghosts of their data, as visualized through generative landscapes and personified through animated characters. (Figure 3) After being led through a panoramic reconstruction of their location history, the viewer descends into a series of showrooms that present imagery derived from their advertising profile, highlighting the algorithmic misinterpretations of the interests and desires of the user. These showrooms are littered with objects textured with advertising images, and their walls are plastered with interactable ads. If an ad is looked at directly, a gaze tracker triggers a scene change, leading the user to subsequent spaces that are increasingly saturated with ad imagery.

First Draft

As the experience goes on, these virtual spaces become populated with ghoulish, personified manifestations of the information that users wanted to forget, uttering the text from deleted posts and tagged with the names of "unfriended" friends. These data ghosts wander aimlessly in the virtual data-realm as a reminder that data collection systems insist on remembering even what we intend to forget. Starting with the familiar backdrop of recent activity, posts, locations and "likes," this 10-minute VR experience gradually leads the viewer into a dark, uncanny underworld populated by deleted content, targeted advertisements and excommunicated acquaintances.

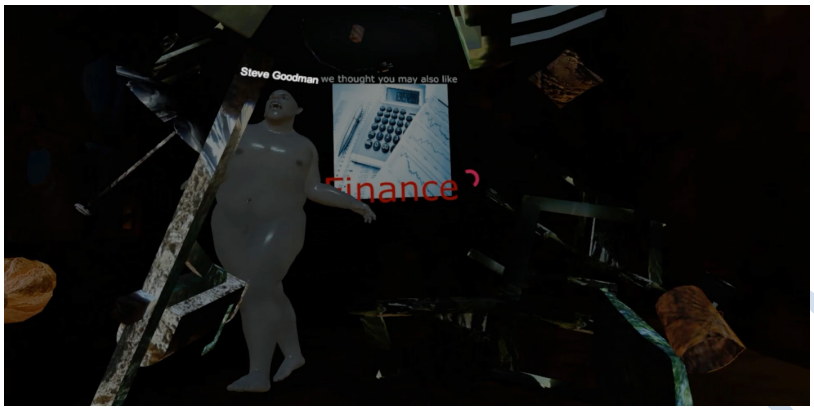

Fig. 3.
DEEP SOLUTIONS virtual reality environment

While this experience is intentionally narrativized into a sort of satirical, cinematic experience, it is followed up with a third, more pedagogical component: a crypto-internet café, in which users are presented with counter-surveillance tools that provide alternatives to the ubiquitous surveillance of popular social media (Figure 4). This "café" is situated in a room entirely clad in aluminum sheeting, functioning as a Faraday cage that prevents electromagnetic signals from entering or exiting the space and rendering devices like cellular phones mostly unusable. The only access point to the internet within the space is a computer outfitted with the Tails operating system, a Linux-based OS provisioned with built-in tools for anonymity and data security (Dawson and Cárdenas-Haro 2017, 49). The Tails OS, unlike most operating systems, deletes all files each time the computer is started up, preventing the retention of personally-identifying information. Internet traffic in Tails is routed through the TOR network, an encrypted protocol that conceals a user's location by redirecting it to a series of randomly selected, geographically dispersed "relays." As Dawson and Cárdenas-Haro describe, "The TOR is a dynamic network that is constantly evolving ... the path that our packets take changes all the time making things harder and harder for the observer" (2017, 48). The TOR network also enables the creation of hidden services, an anonymized and encrypted interpretation of the domain names and websites available on the open web.

Final Draft

Fig. 4.
Faraday Cage internet cafe

Viewers who access the computer in DEEP SOLUTIONS' faraday cage are presented with a variety of hidden services, which range from encrypted and anonymized social networks, to privacy advocacy groups, to technical instructions for installing the TOR network and the Tails OS on one's home computer. Eric Volmers, in his Calgary Herald profile of the exhibition, wrote: "it fittingly feels like being locked inside a giant, tinfoil hat" (Volmers 2018). While the paranoia and seediness commonly associated with dark web spelunking is certainly still present within this project, its intention is ultimately to reveal that, beyond these stereotypes, encryption technologies present real alternatives to mainstream internet platforms that are increasingly within reach of everyday users. "Dark web" social networks circumvent the ubiquitous surveillance strategies woven into the functionality of major platforms, providing tactics of anonymity for users concerned with privacy – in particular, the marginalized and activist communities who are disproportionately affected by surveillance (Gehl 2016, 1232).

The combined aim of the three installation approaches of DEEP SOLUTIONS was to engage with the public directly around issues of surveillance and privacy on the internet. The hands-on, face to face nature of the exhibition provided several unique opportunities for audience engagement: to facilitate highly customized visualizations of each participant's personal "data double"; to generate conversations with the public about the role of surveillance practices in everyday technological mediations; and to allow the audience to explore counter-practices that contend with ubiquitous surveillance on the web. The face to face interactive pedagogy facilitated by this exhibition allowed for a careful, personal negotiation of the trust involved in the vulnerable exchange of highly personal data. This project sought to draw audiences into a playful space of interactivity towards the facilitation of a transformative, heuristic space in which surveillance, datafication and power could be embodied, understood and critiqued.

Final Draft

4 CONCLUSION

Interactive digital artworks and participatory media platforms have much in common. They both present audiences with interfaces that solicit interactions, and they both make use of algorithms that process interactions and determine content. In this sense, artists that work with code have a unique perspective towards media systems: their own creative process is itself a process of working with the algorithmic underbelly of technology that is ordinarily left hidden behind interfaces. This algorithmic perspective comes with it unique opportunities for re-purposing and re-representing dataveillance systems towards more transparent configurations. Conversely, artists repurposing algorithmic tools to critique surveillance capitalism must be cautious not to replicate the quantifying subjectification of dataveillance by merely aestheticizing it.

Critics of surveillance art have cautioned against this sort of aestheticization of surveillance and counter-surveillance. Torin Monahan, for instance, has criticized the manner in which artworks "frame problems with surveillance as universally experienced or as needing individualized and product-based solutions to manage – rather than correct – systemic social problems" (2015, 173). How can artists expand on narrow framings of surveillance towards forms of resistance that more significantly impact the marginalized populations that are most significantly affected by surveillance? And, is the art gallery really an effective space to stage this sort of resistance? Artists working towards critical reconfigurations of surveillance technology must consider the trappings of aesthetic simplifications and expand their research into broader disseminations: beyond the limited aesthetic scope of mere playful interactivity and beyond the limited audiences of the art world and the academy, whose enclosures might further exclude communities most acutely impacted by surveillance.

Along similar lines, critics of the cryptographic solutions we have discussed have questioned the efficacy of such counter-surveillance technologies. Gurses et al. claim that the prioritization of encryption tools as fixes for the problems posed by surveillance implies that these problems can be managed with band-aid solutions, sidestepping the real critique necessary to effect actual change. "How the problem is defined already involves assumptions about whose experiences of surveillance are to be addressed," write Gurses et al, "and whether it seems possible to 'design away' the problem or whether a broader political critique is called for" (2016, 587). Counter-surveillance discourses, they argue, are disproportionately centred on technological solutions that address privacy issues rather than targeted surveillance. How, then, can counter-surveillance tactics challenge the technological elitism that frames these cryptographic solutions, seeking more equitable high-tech and low-tech solutions?

While we do not claim that counter-surveillance art can provide simple answers to the above questions, we argue that interactive artworks provide a unique experimental space in which these issues can be contended with and brought to light in new ways, and radical alternatives can be

Final Draft

proposed. The work we have presented in this essay has seized upon these experimental opportunities, seeking the pedagogical potential of participatory art to draw audiences into a space in which they are directly implicated in entanglements between interactive enclosures and their subjects. We have argued that these sorts of interactive experimental deployments are uniquely effective in making visible the logic of ubiquitous of surveillance, and furthermore, in mobilizing audiences towards the consideration of counter-surveillance tactics in their everyday lives. The task of artists, in future attempts to tackle issues of ubiquitous surveillance, is to broaden the scope of these tactical experiments towards more comprehensive visions of a future in which populations are better empowered against the imposition of surveillance.

REFERENCES

Andrejevic, Mark.
2012. "Ubiquitous Surveillance." *In Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin Haggerty, and David Lyon. Taylor & Francis

Andrejevic, Mark, and Mark Burdon.
2015. "Defining the Sensor Society." *Television & New Media* 16 (1): 19–36. https://doi.org/10.1177/1527476414541552.

Böhmecke-Schwafert, Moritz, Crispin Niebel, and TU Berlin.
2018. "The General Data Protection's Impact on Data-Driven Business Models: The Case of the Right to Data Portability and Facebook," no. 2: 8.

Dawson, Maurice, and Jose Antonio Cárdenas-Haro.
2017. "Tails Linux Operating System: Remaining Anonymous with the Assistance of an Incognito System in Times of High Surveillance." *International Journal of Hyperconnectivity and the Internet of Things* 1 (1): 47–55. https://doi.org/10.4018/IJHIoT.2017010104.

Deleuze, Gilles.
1992. "Postscript on the Societies of Control." *October* 59: 3–7.

Gehl, Robert.
2016. "Power/Freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network." *New Media & Society* 18 (7): 1219–35. https://doi.org/10.1177/1461444814554900.

Gates, Kelly.
2011. *Our Biometric Failure: Facial Recognition Technology and the Culture of Surveillance*. New York University Press.

Gürses, Seda, Arun Kundnani, and Joris Van Hoboken.
2016. "Crypto and Empire: The Contradictions of Counter-Surveillance Advocacy." *Media, Culture & Society* 38 (4): 576–90. https://doi.org/10.1177/0163443716643006.

Haggerty, Kevin D., and Richard V. Ericson.
2000. "The Surveillant Assemblage." *British Journal of Sociology* 51 (4): 605–22. https://doi.org/10.1080/00071310020015280.

Latour, Bruno.
1999. *Pandora's Hope: Essays on the Reality of Science Studies.* Cambridge, Mass: Harvard University Press.

Monahan, Torin.
2015. "The Right to Hide? Anti-Surveillance Camouflage and the Aestheticization of Resistance." *Communication & Critical/Cultural Studies* 12 (2): 159–78. https://doi.org/10.1080/14791420.2015.1006646.

Volmers, Eric.
2018. "Wreck City Residency Explores 'How We Live' with Interactive Exhibits throughout the City," August 2, 2018. https://calgaryherald.com/entertainment/local-arts/wreck-city-residency-explores-how-we-live-with-interactive-exhibits-throughout-the-city.

Zuboff, Shoshana.
2018. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. First edition. New York: PublicAffairs.

Final Draft