OTOKA

Episode #1

Privacy Techtonics

Exhibition Reader

Queen Mary University of London

NEAR NOW

BROADWAY Arts+Tech.

LEVERHULME TRUST

Privacy Techtonics Exhibition Reader

This Reader showcases the artworks exhibited at the Broadway Gallery Nottingham 11th November 2022 to 4th December 2022 together with artist interviews and specially commissioned research texts. The Reader is published in 2022 by Queen Mary University of London and OTOKA under a Creative Commons Attribution-Non Commercial 3.0 license.

Editors
Philippa Williams, Candice Jacobs and Lipika Kamra

Artist interviewers
Philippa Williams and Lipika Kamra

Text
Candice Jacobs and Philippa Williams

Artwork images
Tara Kelton, Ben Grosser, Forensic Architecture, Yuri Pattison

Exhibition Curation
Candice Jacobs and OTOKA in collaboration with Philippa Williams and Lipika Kamra and provoked by research on the geopolitics of digital privacy, WhatsApp and India

Exhibition website design
Matt Woodham

Reader design
Sian Morrell

Cover design
Candice Jacobs

Citation information
Williams, Philippa, Candice Jacobs and Lipika Kamra (2022) Privacy Techtonics Exhibition Reader. Queen Mary University of London and OTOKA.

Funders
Faculty of Humanities and Social Sciences Collaboration and Strategic Impact Fund at Queen Mary University of London 2021/2 and support from the Leverhulme Trust. Near Now at the Broadway Gallery Nottingham also hosted and funded aspects of this work.

More information
Exhibition website: https://www.otoka.org/
Research on WhatsApp: https://whatsapppolitics.com/

Reader contents

Introduction

I know what you're thinking …

I bet I know what you're thinking. I bet I know what you're doing right now and I bet I'm not the only one. I bet, like me, you've never properly read through that info that pops up on your screen all the time, you know, about whether you're happy for those people to use and abuse what you're doing, to make money. Trouble is, you already know what they're doing and you don't really care. How would you feel though, if instead I was standing outside your window peering in, or sitting on the other side of that wall, listening to you breathe. Some of you have probably already covered the camera on your computer but it doesn't matter, I've already got new ways of seeing what you're doing that you're just not able to conceal.

Your privacy is your right to control, but it's not, not anymore. The last time you searched on Google, that last message you sent on WhatsApp, the last time you watched something on YouTube, looked at Instagram, Facebook, Tik Tok, that Uber ride you took, or that time you had to show your 'covid-free pass' to that minimum waged employee who couldn't really give a damn; truth is, we're living in a world where we know that we're being watched and tracked and we're okay with it. That's what's scary. We click 'Agree' and sell our data just so that we can get on and watch that thing quicker, or find that thing that we were looking for, buy that thing that we didn't really need, download that thing that will help us feel better or do that thing that will help us remember what it was that we were doing that we can't remember anymore because we were too busy trying to find that thing that we were trying to remember.

The digital age is fuelled by data which is extracted, bought, traded and analysed for profit and surveillance. The extraction of our data - taken from our private lives - has become normalised as routine, inevitable, and is being used for the benefit of our everyday lives to make us more efficient, productive, healthier and happier. To allow our relationship with data to appear normal, the question of privacy is often kept quiet, obscured and refracted. Our right to privacy is undermined through our 'consent' to Terms of Service that are too long and too incomprehensible and leave few options but to scroll, scan and sign. We're told that our personal messages are 'end-to-end-encrypted', that they're private on Apps like WhatsApp, which they may be, most of the time, unless the state employs Pegasus spyware or the police seize your phone. Marketing our privacy to us is good for Big Tech, it helpfully deflects scrutiny away from the collection, aggregation and monetisation of your (our) metadata. But when Big Tech's growth and state control depends on exploiting unequal privacy relations, in whose interests is privacy, really?

Isn't it striking that as we emerge falteringly from a global pandemic, which brought fresh intrusions into our sociodigital lives, that the focus on privacy is shifting to centre stage. New books tell us why privacy matters, how we can take back control of our privacy and why privacy is power. The question of privacy for whom is coming up to the surface, and Big Tech don't like it.

About the reader

‘Privacy Techtonics’ comes out of a collaboration between artist and curator, Candice Jacobs and academics, Philippa Williams and Lipika Kamra. Candice has a longstanding interest in the relationship between emerging digital technologies, capitalism and societal transformations. She set up OTOKA in 2022 as a nomadic & fluid research, exhibition, residency, online platform & studio space that disrupts masculinist artworld norms and embraces real artworld lives. Philippa and Lipika’s research focuses on how ‘privacy’ is designed, talked about, regulated and experienced by WhatsApp, governments and ordinary people. This is the subject of their next book ‘Privacy Techtonics: Digital geopolitics, WhatsApp and India.’ The exhibition therefore exists at the intersection between digital technologies, privacy, politics and power, themes which surface both overtly and obliquely through the exhibits and writing to challenge us to (re)think our relationships to digital technologies and data in our digital lives through different scenes.

This Exhibition Reader brings together the show’s artworks with excerpts from interviews with the artists involved and commissioned texts to collectively explore the intrinsic and unequal relations between data, technology and people to provoke questions about our digital lives and futures, how sustainable or desirable they are and what alternative worlds we might want or need to create. Privacy Techtonics was held over four weeks and hosted four scenes which engaged global multimedia artworks and artists in the Broadway Gallery, Nottingham. Solo presentations in situ by Tara Kelton, Ben Grosser, Forensic Architecture and Yuri Pattison were exhibited on different iterations of scaffolding through a figurative nod to Ben Bratton’s ‘Stack’, comprising a computational totality of hardware and software technologies that ‘align layer by layer’ to form an ‘accidental megastructure’. These exhibits were complemented by online exhibits at OTOKA.org by Libby Heaney, Ben Grosser, James Bridle and Joey Holder.

The first scene in this reader, Silicon Lives, examines how data collection and its aggregation through digital technologies produce disciplining effects on our work-lives with a focus on Uber and Ola drivers in Bangalore, India’s ‘Silicon Plateau’ [1].

The scene begins with Tara Kelton’s critical enquiry into Uber’s opaque digital architectures and data relations presented in Black Box (2018) which innovatively surfaces the spatial and racial disconnect between Uber drivers and their digital boss. As the interview with Tara Kelton and Marialaura Ghidini further shows, digital-urban transformations produce fragmented, unanticipated and contradictory realities that raise new questions about how we creatively represent the digital-urban. The everyday, intimate effects of surveillance architectures are documented in Kaveri Medappa Kaliyanda’s ethnography of Uber and Ola drivers. In this she illuminates how drivers interpret, negotiate and reproduce uneven data relations with Uber/Ola whilst simultaneously making a living and making a home in and through their cars.

Design cultures, the second scene, is inspired by the work of Ben Grosser and his focus on the cultural, social and political effects of software; how software design subtly and powerfully shapes our

1 And the title of Tara Kelton and Marialaura’s collaborative volumes https://siliconplateau.info/

engagement with digital technologies and how design is always the product of its designers and the social, cultural and political contexts in which they are embedded. These themes are engaged through research and art practice focused on Facebook and WhatsApp. The manipulation of our attention to engage, entice and sometimes, incite is precisely how Big Tech collects vital units of data. How data relations are cultivated and sustained is the subject of Platform Sweet Talk (2021). In this recent work, Ben Grosser plays with the grammar of social media notifications to expose how our attention is captured and capitalised on by Facebook. In the accompanying piece ORDER OF MAGNITUDE (2018) we learn how Facebook's design cultures are underpinned by Mark Zuckerberg's relentless objective for growth, amplified for profound effect through a 'critical supercut' of Zuckerberg's public utterances. Philippa Williams and Lipika Kamra turn the focus on another of the Facebook Companies – WhatsApp – to examine how privacy, objectively a good thing, is being co-opted to further Facebook's, now Meta's growth. By examining WhatsApp's privacy cultures they examine how privacy narratives and design are carefully crafted to market our privacy for WhatsApp's profit.

The third scene, Digital-state infrastructures, examines the tight nexus between governments, corporations and digital technologies for surveillance and subjectification. The works collectively demonstrate how digital-state infrastructures and strategies intentionally, sometimes violently undermine our digital privacy to assert authority, power and control over our lives. The Covid-19 pandemic provided a crisis moment for states to extend their digital-infrastructures when our further reliance on digital technologies for work-life also exacerbated our digital vulnerabilities. Forensic Architecture intervene at this point to systematically document how governments are using Israeli spyware to wage 'Digital Violence' against citizen actors deemed a threat to their authority, to intimidate them into silence. As Shourideh Molavi reveals in her interview, Forensic Architecture had to negotiate their own exposure to digital violence in producing the research. Moreover, they learned that despite governments' insidious projects of 'Digital Violence', solidarity and collaboration around human rights is thriving. Yet, digital violence exists along a spectrum from the hostile, illegal targeting and intimidation of citizens to the everyday routine surveillance and digital intrusions into citizens' lives. Ram Bhat documents India's shift towards the 'platformisation of welfare' amidst the proliferation of techno-politics in everyday life which demands that citizens be digitally legible to the state, or else forfeit their rights. As Ram shows, in practice, systems errors occur, procedural exclusions are magnified and illegible citizens are rendered surplus.

In the final scene, Post privacy? witnesses the pervasive and persistent landscapes of surveillance, and the challenges to realising digital privacy. Following in the footsteps of previous 'whistle-blowers', Edward Snowden exposed to the world the routinised and intrusive practices of USA and UK state surveillance in the aftermath of 9/11. Since that moment, Snowden has been exiled to Russia while practices of state surveillance have been extended. Yuri Pattison's multi-layered film '1014' creatively plays with a world in which the Hong Kong hotel room where Snowden first shared his classified files with Laura Poitras, Glenn Greenwald and Ewan MacAskill becomes the celebrity subject of the documentary 'Citizen Four'. Conversely, the demise of

privacy communicated from that room is relegated, appearing only through motifs and redacted texts that overlay the film. The intensity of state intrusions into citizens' everyday lives is arguably unrivalled by China. Yet, as Carwyn Morris carefully documents through his research on China it is possible for everyday cultures of secrecy to flourish through creative and subversive sociodigital practices even within contexts of post-privacy.

Scene 1: Silicon Lives

Black Box (2018)

Black Box sees Indian American artist Tara Kelton interviewing Uber drivers in Bangalore, asking them to describe the company they work for – how they imagine what Uber is, what it looks like, who runs it. Using their responses as visual cues, Kelton commissioned local photography studios to produce representations from their existing image banks.

The resulting mediated images reflect the gaps between the lived reality of Uber's employees and their imagined ideas of who Uber is and what it does; to reveal a spatial and racial dissonance between Indian Uber drivers and the portrayal of largely white, western figures and settings that they feel represent Uber. Black Box speaks to the opacity, obfuscation and secrecy that surrounds Big Tech's collection of data and how data relations between workers and platforms are normalised for corporate profit.

Interview with Tara Kelton and Marialaura Ghindini

In these edited interview excerpts, Lipika Kamra and Philippa Williams speak to Tara Kelton and Marialaura Ghidini about Tara's artwork Blackbox and their collaborative volume, Silicon Plateau. The discussion touches on how they engage digital technology in their work, digital mediations and digital-urban transformations.

Lipika: How did the digital become the focus of your work?

Tara: It started quite early in my life; I spent a lot of time on computers. I didn't have a lot of friends as a kid - I was the chubby kid reading science fiction and playing video games for hours after school. This was pre-internet and technology was, you know, magical and exciting. But yeah, as a digital 'migrant', having experienced the extreme technological developments that have happened in our lifetimes and how dramatically they've changed our everyday lives - with all these changes happening in such a short span of time - I've been making work responding to it almost in real time. Initially, I was working a lot with everyday digital platforms in a more playful, experimental way, where I would explore their individual properties or mechanics, but without thinking about them too critically. I think, early on, I had this kind of assumption that I think a lot of people did, that technology was inevitable and good. And kind of neutral. And over time, I think where we're arrived is very bleak, like we are living in the techno-dystopian horrors described in my childhood books. And I started to look at all these digital platforms more critically, as many people did. One of the things I've been interested in recently is how Silicon Valley corporations treat people as just numbers, how dehumanising everything has become and my work has been observing these companies' presence and impact specifically in India / Bangalore.

Lipika: So how did these themes come up in your work?

Tara: Well, for example, I have done several projects created inside Google Street View. Google Maps presents themselves as neutral or objective, but the human still somehow makes its way back in. I used to spend a lot of time walking around virtually inside Google Street View. While I was wandering through Indian tourist sites (which were the only places India permitted Google to document), I

discovered the maps contained human narratives. I discovered, for example, that at the Taj Mahal, there was a security guard who was clearly helping the Google Street View photographer make his way through the site. In every location, if you zoomed out or turned the view, you could spot him somewhere. So, I went through the entire site and captured every image of the guard and strung the images together - the work, called "Guided Tour", became a kind of found narrative, outside of the platform's intended design.

Lipika: What did you imagine the black box as? And what was the process that you embarked upon through your work to open up this black box?

Tara: I chose the term black box for a few reasons. Earlier Uber's logo actually was a black square, which I thought was a funny choice - in computation the term 'black box' is used to describe an opaque system that you don't need to understand in order to use. I had also attended this panel where social workers were talking about the stories they had heard from Uber drivers. I was struck by how little control drivers had, how remote decisions which may not even involve a human being would be taken that would impact their income and working conditions dramatically. And they didn't have a person to talk to if they had a problem, there was no recourse. For instance, customers would run away without paying their fare, but they wouldn't have any way to contact a human being at Uber. There's so much customer service for Uber's clients, but there isn't much for the drivers. And so, then I started interviewing the drivers and asking them to describe who it is they work for. The responses were fascinating, they would pull out these fantastical descriptions, highlighting how they don't know anything at all about their employers. And they were typically describing them as a white man, sometimes in this sort of science fiction environment. Actually, it was hard to get them to talk, I think they thought I was a spy for Uber.

Philippa: How did you transform the interviews with Uber drivers into the artwork we see in Blackbox?

Tara: I have a history of collaborating with informal digital workers. I've been quite interested in less Western, unconventional uses of platforms, and software and devices. So, one of the types of workers at these local desktop publishing (DTP) shops. They provide photocopies and some graphic design services. But they don't really have formal design training. I am quite interested in the visual language they have developed. And, how there's a cultural specificity in their use of software programs. They basically have these really interesting digital image libraries of digital props and environments - people go there to have their photo taken and then they'll place them in these kinds of fantastical locations, or European cities, like Paris. They told me they get the imagery from CD ROMs from China and that they also find them online. So that's also quite interesting, how these images are circulating. So I basically went to them with the Uber drivers' descriptions. And I thought it was a nice way to visualise them. And each image has been produced by one of these DTP shops.

Philippa: What are the spaces for worker resistance and agency, whether it's Uber drivers or digital workers?

Tara: There hasn't been a lot of agency and I think it might be getting worse. Although I have heard recently that there's been some unionising. And then the government has put in some new policies and protections for gig workers. But it feels like the government can't keep up with the speed at which everything keeps changing. I actually spoke with a digital rights lawyer and she was talking about how that makes it impossible to regulate. I also heard that when Uber drivers tried to protest, Uber would send people from the company to photograph the protests, and then run the pictures through facial recognition technology, and if they identified their drivers they would permanently ban them. It's a very uneven relationship.

Lipika: Do you also see ordinary citizens resisting, if not, criticising digital technologies in their everyday lives?

Marialaura: Yes. In our collaborative project, Silicon Plateau Volume 2, each of the contributors brings out the small ways people are changing how they interact with digital technologies. We invited a wide variety of people, artists, anthropologists, writers and so on, to respond to the question: what does it mean to be an app user today—as a worker, a client, or simply an observer? The picture that emerged is that we are increasingly finding ways of going beyond the protocols of the interface and the algorithm, to do something different with them - be it in the context of the relationship with the other, with the environment or with government infrastructures. Apart from criticism, you find stories of personal agency, and forms of resistance to the standardisation of the tech industry.

Philippa: What does digital privacy mean to you?

Marialaura: Digital privacy can only exist if you can really trust, but the question is - who are you really trusting? It's a complex situation. Maybe in Europe, there is a facade of having some sort of agency with the GDPR and the declaration on digital rights and principles. But on a micro and personal level, it's a sea of interconnected services, cross-referenced data, monitoring of personal behaviours. There is very little, almost no, privacy these days. This feeling of being monitored or 'read' also emerges in some of the stories collected in Silicon Plateau.

Tara: It seems like a lot of effort to have digital privacy. Like you have to make it your full-time job to actually make it happen. There's too much individual labour involved.

‘Uber is asking for a selfie’

–Kaveri Medappa

One sunny afternoon in July 2019, I made my way towards a few drivers chatting under a manicured frangipani tree close to the ‘Ola zone’ at the city’s international airport, where many Ola cabs stood in a long, neat line waiting for their turn to pick up customers from the airport. However, fifteen minutes into my first conversation with the drivers, a young man – an ‘Ola employee’ [whose job it was to allocate customers to cabs on a first-come-first-serve basis] – was seen walking towards us with a sense of urgency, visibly unhappy at the sight he was walking towards. He told me half-panting that I could not just turn up and talk to Ola drivers at the airport. I needed permission from the corporate entity running the airport. Roughly a week later when it seemed that I was close to receiving permission from the airport authorities, I was told, rather casually by an airport official in the higher echelons of management that I needed the permission of Uber and Ola themselves to talk to drivers. ‘Errmm, but aren’t they self-employed? They’re called “partners”’. ‘Yes I know, but everyone is concerned about their image’, he had said in reply. I refused to take permission from Uber and Ola and therefore could not carry out my research at the airport.

I thought the Bangalore International Airport would have been an obvious choice for a ‘field site’ to meet Uber and Ola’s drivers for my study on the work-lives of app-based workers in the city. Afterall, this was a central pick-up place for drivers and I was keen to know how ‘partners’ were experiencing digitally mediated driving work. What did the everyday life of a driver look like, and how did drivers imagine their platform bosses? While Uber has a global reputation, Ola Cabs (Ola for short) is one of many ‘unicorns’ founded by ‘home-grown’ Indian entrepreneurs. Together, Uber and Ola entered the market in 2014-15 and now have a near duopoly over the app-based transport market in India.

Following my encounters with the Bangalore airport’s authorities I was left with the nagging feeling that I was being watched. This stayed with me throughout my research into the lives of platform workers. Indeed Uber’s infamous omniscient ‘God View’ was well-known by then. The notion that I was the subject of surveillance was reinforced by the words and actions of workers who feared retaliation by Uber or Ola for speaking critically about the platform and asked me multiple times if ‘I was sent by Uber and Ola’. And then there was the lingering anxiety about the ‘terms and conditions’ of platform apps that I had no choice but to ‘agree’ to. The sheer potential of platforms to misuse geo-location technology or deploy digital technologies to surveil people without any of us ever knowing it were some of the reasons why I could not fully shake off the feeling of being watched. It was all too apparent how digital work platforms were producing new forms of surveillance and subjectification.

On telling drivers about my experience at the airport, a few of them advised me to try the parking lot at Uber’s head office. So, there I stood, opposite Uber’s head office in Bangalore one afternoon in late August. After a few minutes of walking up and down past Uber’s office, I mustered the courage to walk into the

parking lot adjacent to Uber's tall, glass-fronted building. I walked gingerly, pulled my dupatta [1] over my head in a bid to hide at least some parts of my face from CCTV cameras and tried to look confident. With every step I took, I anticipated being stopped by a security guard or being told to 'get out' by a 'bouncer' - a figure who had come up several times during conversations with Uber drivers about their own experiences of accessing the Uber office.

Pre-empting a challenge from 'Uber officials' I had a ready 'alibi'. I would calmly say that I was curious about the pop-up tent set up by Maruti Suzuki inside the parking lot and wanted to know more about their car financing schemes for a male relative. To my surprise and relief, no one stopped me. Some men with name tags walked around the pay-and-park space, telling drivers to leave and directing new cars where to park. Many cars were empty, their drivers perhaps inside the office resolving issues. One of the people manning the car park threw a quick glance at me but thankfully no one seemed very bothered by my presence. I stopped at a white sedan, inside which a young driver, who I will call Sharan, sat scrolling through his phone.

Sharan had been driving for Uber for a little more than a year, and enjoyed driving for Uber. 'I have to do hard work but I am happy I get its rewards [prathiphala]' he said, in a Kannada that was unmistakably from north-Karnataka. He drove for both Uber and Ola, usually switching between them weekly, depending on who offered better remuneration schemes. Some drivers preferred one over the other for various reasons. 'Ola is good because you get more local customers, who pay in cash; but in Uber, there are more hi-fi customers who do online payment'. 'Uber gives better rates sometimes and their response is better [in resolving driver issues]. Ola!? Daridra nan makklu! [miserly buggers!] Always putting one penalty or the other'.

'You will not write my name anywhere, right?' Sharan confirmed again while showing me his high rating score of 4.7 on Uber and the many positive comments left by customers.[2] Sharan, a Bachelors degree holder in Commerce, had bought the sedan, against which we were leaning and chatting, through a bank loan, and had three more years to go before it would be cleared. But keen to have his own 'small business', he had recently employed three drivers from his hometown for cars that he had leased from an individual for a monthly rental. An alert on his phone briefly interrupted our conversation, he looked up from reading the screen: 'Oh, Uber is asking for selfie...one second madam', he said as he walked up to the car's bonnet. Standing in front of the car, he adjusted his phone's position to ensure his face fit the oval in the middle of the screen. Asking 'partners' to upload their selfies intermittently was a measure introduced by Uber (and in time, other platforms like food delivery apps Swiggy and Zomato followed suit) to penalise drivers who were using accounts that were not their own. Drivers had admitted to sometimes using the log-in IDs of friends or relatives to ensure continuous work on the platforms and circumvent arbitrary 'ID blocks' by platforms, or unexplained dips in rating scores, both of which had adverse repercussions on their livelihoods and earning possibilities.[3] But on discovering this worker-hack, Uber and others had deployed facial recognition (FR) technology to verify worker identity and

1 A dupatta is a long piece of fabric that usually accompanies a salwar-kameez. It is often worn by women to cover the shoulders, chest and/or head.

2 All names used here are pseudonyms

3 Except one amongst my 40 odd driver participants worked part-time, all others fully depended on app-based driving for their livelihood.

discipline their work-life practices even more pervasively. 'Partners' often had a countdown (usually less than a minute) to upload selfies, and their IDs remained active only if the selfie was 'approved' by the FR technology. While Sharan waited for Uber to accept his selfie, I looked up at the several floors of Uber's office opposite us and instinctively pulled the dupatta on my head further down.

As a testament to him being a 'fast learner' and 'intelligent', Sharan shared with me his 'plan' to earn a satisfactory income from app-based driving. He had also taught his drivers this plan. He worked for 72 hours straight, taking naps now and then on the roads or at the airport in order to complete as many rides as possible. As he explained:

> It's petrol waste to go home every night. Rates, incentives have been cut and my earnings are not as good as they were before, so we have to find ways to earn more. I go home to sleep properly on the fourth day. In this job one day you make 2000 [INR gross], one day you make 4000, so if I work like this, I can try to earn 3000 [INR gross] daily on average. That's my own target [self-set goal].

This was not the first time I heard about drivers sleeping in their cars. Another one of my participants, also a young man in his early twenties, gave up his rented room after he realised that he was hardly ever at home. He decided to save on the monthly Rs.3000 rent and live in his car. Once a fortnight he went to his hometown, a five-hour drive from Bangalore, to wash his dirty clothes and eat his mother's food. Similarly, Sharan showered at the airport and slept reclined in his driver seat on most days of the week. Walking around parking lots on Begur road, very close to the international airport, I often saw drivers asleep in their cars, wet towels and washed white shirts hanging from car windows or spread out on windshields, which also served to keep out the strong morning or afternoon sun from their faces when they caught a nap. The cars and parking lots inside the international airport and in Begur village were spaces where drivers met their needs of social reproduction – where they bathed, rested, ate fresh hot food at one of the many roadside food stalls, met fellow drivers – and regenerated their labour power for platform capital. As if to show me proof of his 'hard-work', Sharan opened the Uber app on his phone and indicated to me the trips he had done in the wee hours of the morning – 1.10 a.m., 2.45 a.m., 4 a.m. – all in the past few days.

To fill in a moment of silence during our conversation, I peeked into the car and saw a little figurine of a shiva-linga [4] on the car's dashboard and a photo of a saffron-clad, head of a religious institution – a mutt - who I did not recognise. Seeing me peer at the car, he chuckled and said 'She is my everything. My Lakshmi,[5] my home, my wife. I have everything in the car'. He took me to the boot, opened it and showed me his little backpack with an extra set of his commercial driver's uniform - white shirt and trousers – a

4 Representation of the Hindu god, Shiva
5 The Hindu goddess of wealth

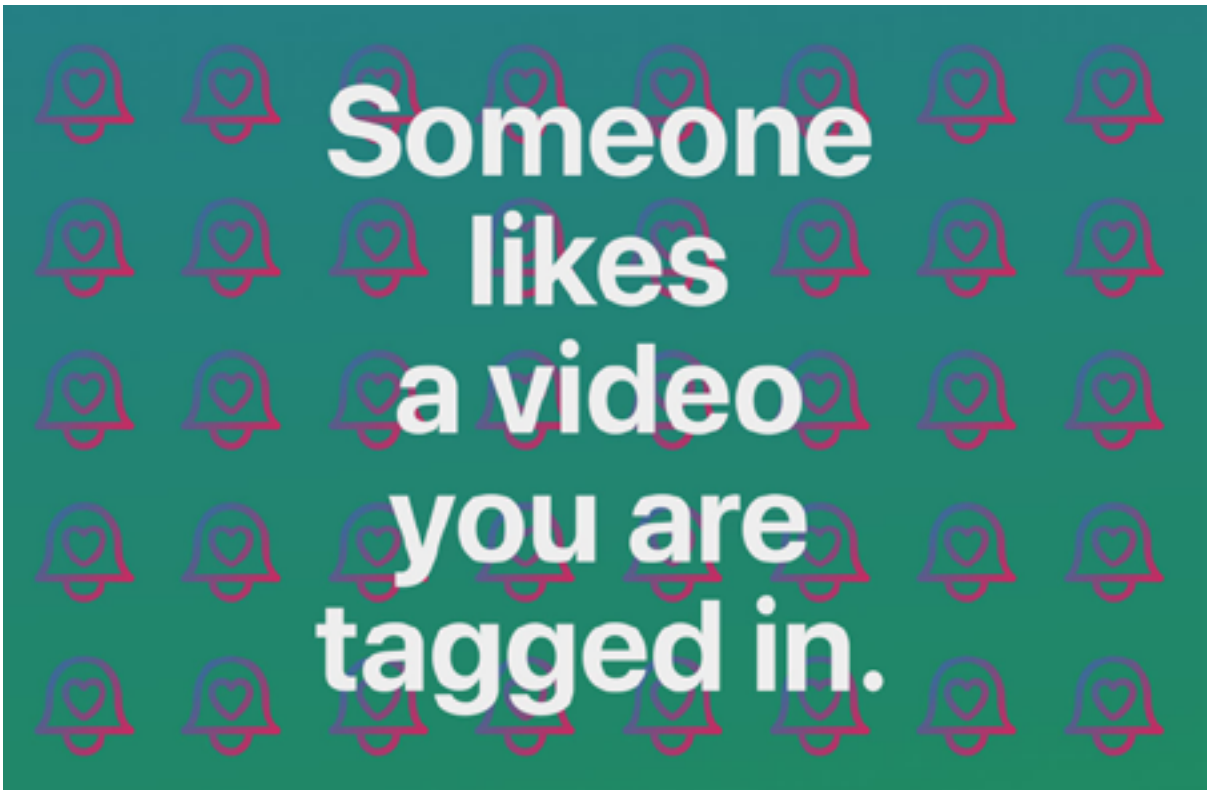
bar of soap, a comb and a small bottle of shampoo. Beside the backpack in a plastic bag was a towel, and a fleece blanket like the ones popularly sold on pavements in the markets of Shivajinagar or Majestic in Bangalore. Crumpled next to this bag was a cover for the car. 'This is for when it gets too hot. I take good care of her' he said chuckling. That was not all, for he also had to take care of himself, to keep driving. In the little pocket of his backpack were a handful of half-empty tubes of popular muscle relaxants, balms and strips of tablets. He kept a strip of Ubicar [6] next to his seat, tucked behind the gearbox. It was a tablet that helped with his chronic muscle pain. He was 24. Sharan also shared with me how the use of air-conditioning, which customers often demanded, was causing his joints to ache. 'That's why I wear these sports shoes with socks, so that they keep my feet warm'. He hoped to continue to do 'hard work' for three more years and pay off his loan instalments on his car and clear off the family's debts. His parents ran a small eatery back in Hubli district and had borrowed a lot of money for the marriage of his two sisters. 'After that, I can get married. When all these commitments get over, I won't have to work like this'.

In the car parked next to Sharan's, a man seated in the front passenger seat looked tense and was photographing a series of documents. Sharan seemed to know the man from waiting together at the parking lot. The man was 'attaching' a driver to his car because he had a family emergency but could not afford to forego the source of income from Uber for the car. In the driver's seat, a young earnest looking man held the car's steering wheel and peered around it to get himself acquainted with his new work-space. By sheer chance, Sharan and the owner of the car brought up Uber's current target and incentive scheme. Sharan saw that despite his rating score being higher than the other driver's score, Uber offered him a less competitive remuneration plan, meaning that he had to complete more trips ['target'] to earn the 'incentive' component of pay. Sharan was clearly taken aback at the perverse discrepancy. 'Your ratings are lower than mine … See madam, I told you they have their own tricks. Ah well, it's alright. They make people who work hard do more hard-work. It is good in a way…' Sharan said, outwardly justifying his relationship with Uber's algorithm whilst trying to mask the disconcerted look on his face in a moment when the uneven power relations defining the experiences of platform-dependent workers like him were revealed.

6 Ubicar is a medication used for treating muscle cramps and muscle pain

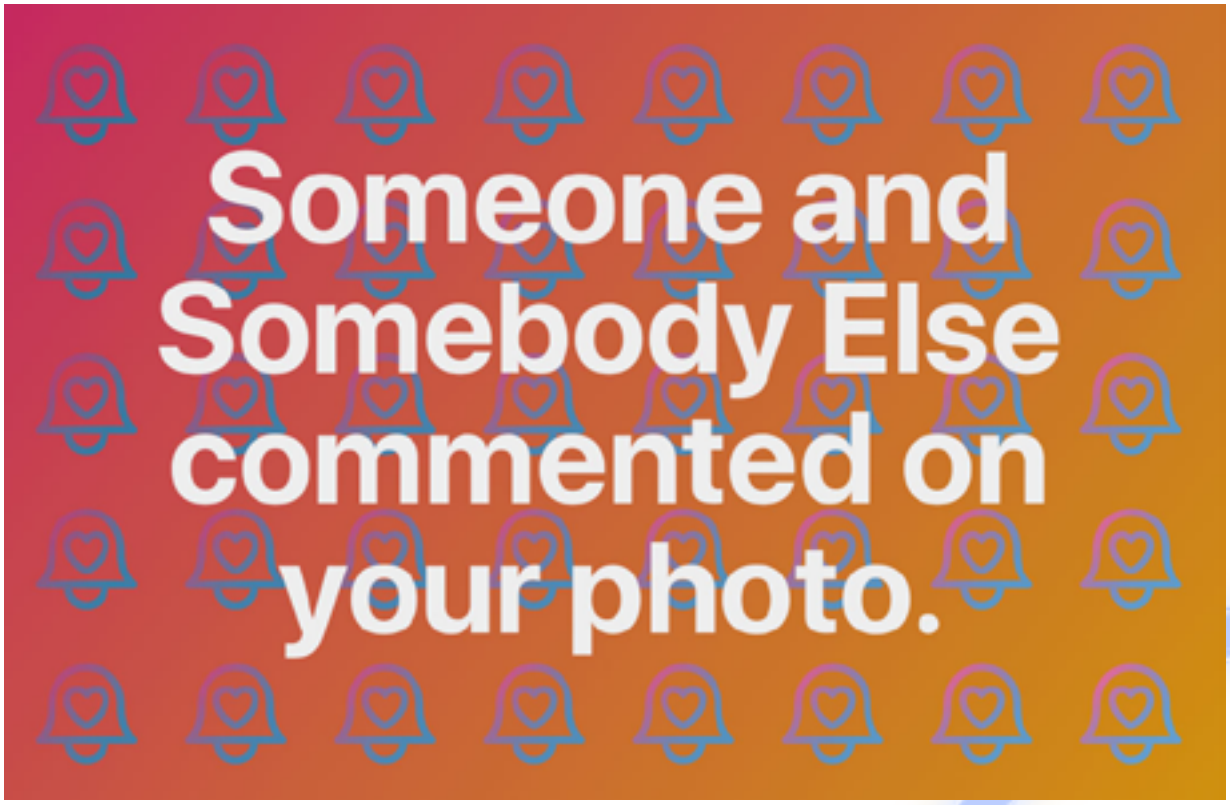
Scene 2:
Design Cultures

Platform Sweet Talk (2021)



Ben Grosser, Platform Sweet Talk (2021)

In Platform Sweet Talk (2021), Ben Grosser analyses the grammar used in messages on social media to investigate how their structure influences users' behaviour.
According to Ben, to exist in the digital is to be in 'conversation' with notifications.



Ben Grosser, Platform Sweet Talk (2021)

In this work Ben has devised a unique interface that presents these messages in a depersonalised form, highlighting the statements as empty carriers of our data which are used against us to maximise our engagement online. Platform Sweet Talk reflects Ben's characteristic method to make the normal look strange, and in this case, surface the power of software design to confront our unequal relations with data.

Platform Sweet Talk was commissioned by arebyte Gallery, London, UK.

Order of Magnitude (2019)

Ben Grosser, ORDER OF MAGNITUDE (2019)

This is a critical supercut, one that examines what matters to Mark Zuckerberg, founder and CEO of the world's largest online social network. Splicing together his every public utterance of 'more', 'grow' and larger and larger metrics, produces an affective, intense tunnel vision monologue of growth and greed.
Big tech encapsulated.

Interview with Ben Grosser

In these edited interview excerpts, Lipika Kamra and Philippa Williams speak to Ben Grosser about his art practice and research, in particular his intimate relationship with Mark Zuckerberg, the intentionality of software design to engage and entice us, the nuances of agency within Big Tech and what he thinks digital privacy is. In this Ben illuminates us about the making and thinking of Platform Sweet Talk and ORDER OF MAGNITUDE.

Lipika: What is your relationship as an artist and researcher with the digital world?

Ben: As an artist, I focus on the cultural, social and political effects of software, thinking about how the designs of a piece of software that we use every day can have dramatic effects on those who use it, and how the ideologies of those who make that software gets embedded within the software and then transmits to the users as sets of values that they take on without thinking about. So my work spans a variety of media from computationally generated video to browser extensions to sound works to performances. But much of my work takes the form of net-based artworks of some sort, whether it's a browser extension, or a website, often manipulating big tech platforms so that we can understand them in new ways, for example by manipulating big tech platforms or extracting from them. And sometimes even building alternative platforms myself, as a way of thinking through what's happening in our digital world.

Philippa: Your work has been mainly animated by Facebook over the last 11 years. Can you tell us a bit about that trajectory? How has your relationship as an artist working both with and against Facebook changed over that time?

Ben: Facebook has certainly been an active subject for me for more than a decade now. And while I had works before this, the central work I often cite as launching more than a decade's worth of work is this piece I called 'Facebook Demetricator'. And it really was a work that grew out of my realisation around 2011 of just how much attention I was paying to the visible quantifications that litter the Facebook interface. The numbers that count 'likes', 'shares', comments, how many seconds ago something happened, how many birthdays you're supposed to respond to today, etc. The 'how many' is everywhere. And I noticed that I was drawn to the numbers, that I was often having heavy emotional reactions in relation to the numbers. And that made me wonder what is the purpose of them? Why are they here? What are they doing? And so Facebook Demetricator is a browser extension that hides all of the numbers throughout the Facebook interface. And when I first made this and

put it out in 2012, a lot of people saw it as a strange and weird thing that an artist is doing. Whatever—kind of interesting, some people liked it, of course, but a lot of people just thought, well, that's the purpose of social media, right? That's how I know if I'm doing well.

I feel like this work has been the backdrop [to my later projects] because I've revived it multiple times and had to rebuild it multiple times. It animated me to hide metrics on other big tech platforms as well, such as Twitter and Instagram. And it takes something that we look at all day every day and tweaks it as a way of realising what that thing was doing. You know, many people reported, and still report, the effects of these numbers in making them anxious or compulsive, or competitive. But I think for me, the thing that I most think about is how the presence of the visible metrics in these platforms normalise the idea that it even makes sense at all for us to quantify our social lives. And you know, that value has benefit to big tech but not much benefit to individuals. So that's what animated it. And of course, along the way, I've done all kinds of other manipulations, whether it's randomising the reactions, [or] hiding all the content to look at the structure, to think about what the safety might be of a platform like Facebook in the face of disinformation, distilling it down in other ways, such as the work that will be in the exhibition: Platform Sweet Talk. I guess the one other thing I would say on trajectory is that I've also had legal tussles with Facebook along the way. They came after me for the metrics hiding work in 2016. And I was fortunate to have support from the Electronic Frontier Foundation in that conflict. And then they came after me again, in 2020, I think it was. In the middle of Instagram's test of hiding metrics. So it's been a saga, I guess.

Lipika: What relationship do you see between ORDER OF MAGNITUDE and Platform Sweet Talk, both of which we are showing in Privacy Techtonics?

Ben: Platform Sweet Talk is a web based work that is the outcome of a months-long practice of capturing and writing down the various notification messages I was getting from Facebook. I was doing it with other platforms too, but I ended up settling on Facebook because it has by far the most varied set of notification messages. And I was curious to understand what is the grammar of [of these notifications], how is the platform trying to get our attention? And anyone who still uses Facebook—which amazingly there are still people out there, still using it, even though my students don't seem to think that's true anymore—is that they're trying harder and harder all the time, you know, as their [Facebook's] numbers are going down right now. Their user metrics, the notifications are getting crazier, and they're testing more versions, and they're more varied. So I captured them all and then I abstracted them. I removed all the personal identifying information from them. And then I made an interface that presents these depersonalised notifications so it says 'Someone liked your photo' or, you know, 'This group has a new message.' — [it] doesn't tell you which group or who liked your photo, whatever it is, as a way of thinking about how there's a whole grammar of notifications. And really what makes them activate us is the way in which they insert our data from the database into them. And that's what they do for everyone.

The other work ORDER OF MAGNITUDE that you mentioned is an epic—what I refer to as an epic supercut, where I looked at every video recorded of Mark Zuckerberg in his first 15 years of public life, from 2004 to 2019. I extracted from those

every time he spoke one of three things: the word 'more,' the word 'grow,' or every time he uttered a metric, like '1 million' or '2 billion,' and I made a supercut out of that. When I started, I thought it was going to be longer than anybody would want to watch, like five minutes or eight minutes or 10 minutes—who's gonna want to watch 10 minutes of Mark Zuckerberg? By the time I was done, it was almost 50 minutes long. So I think it speaks to the obsession with growth that occurs throughout Silicon Valley over the social media era.

Philippa: What was the effect on you spending hours and hours, days and days in a very intense and intimate way with Mark Zuckerberg? What insights did you come away with about him? And what does this say not only about him, but also about big tech? And how do you then communicate that through your work?

Ben: It was an intense process. I watched and listened to every video in its entirety. It wasn't an automated process, somewhat intentionally, and also somewhat necessarily, because of the kind of work I wanted to make. I wanted refined cuts that were attentive to the rhythm and sound of the work, in addition to just the content being chopped up and assembled. But I also wanted to track all the work, to listen, to read, to watch his [Mark Zuckerberg's] progress over 15 years. And I wanted to build the most extensive archive that I could.

One of the things I learned in this process was that Facebook has worked really hard to scrub some of these videos from the Internet. In particular, a good example is Mark's first keynote at the first Facebook developer conference, in 2006 or 2007, or something like that. And you cannot find it if you just do a Google, for example, you won't find it. Facebook doesn't make it available. It won't come up on YouTube—I presume, because his ego is kind of just oozing out of his pores. He's that 21-year-old version of himself at that time in flip flops and on stage at the conference and he hasn't been coached yet in his presentation, you know his mode and method of presentation of self got locked down fairly quickly after. So I managed to find that [video] on a Chinese language YouTube clone, a version that [Facebook] hadn't tracked down and erased.

So in terms of my own experience, sometimes I felt like I almost was Mark Zuckerberg to be honest. Like I almost started dressing like him and thinking like him and talking like him. At the same time, I'm critical of him, and really seeing how his answer to every question is 'more'. No matter what the question is, if it's a question about how you're going to deal with privacy, we're going to get 'more' data, how are you going to deal with this information, we're gonna get 'more' data, we're gonna get 'more' people and get 'more' content managers. You know, whatever it is, it's 'more' — and yet, at the same time, he seems blinded to the obvious that occurs to anyone else who watches all these videos, which is that 'more' is the problem that produces the conditions upon which he's always having to answer to. It's scale that makes the problems happen in the first place. And it's the devotion to scale and the presumption that scale solves all things that leads him to the road now, where he doesn't know what to do, and he's scrambling to find a new path. So, it was a challenging time. At the same time, I was lucky to have this space to live in it [the recordings] for that period, and to really embed myself in the material and the search. And so I made it through and I'm happy with the work. It has its presence as the film, but it also ended up as an archive that's useful for research and other things.

Lipika: When you envisaged Platform Sweet Talk, to what extent was it a critique of the power of software, code design, big tech and its different implications?

Ben: So with Platform Sweet Talk, as with other works, I examine the design of software platforms, thinking about every single moment within these interfaces, every grey line, every blue box, every font, every text, every image, as an intentional design decision that is driven by what we're talking about, [which is] how do they activate users into engagement? How do they make sure we stay as long as possible? How do they make sure we don't feel we can step away. And Platform Sweet Talk looks at one specific aspect of the interface, which is how are these [Facebook] notification messages designed to woo users into a one sided relationship where we produce all the data, and they make all the profit? And, so I took these notifications and depersonalised them, like 'someone posted in a group on a day'. But you know, the someone is a friend of yours, and the group is a group you might care about. And so, it's this process of trying every possible combination, there are hundreds and hundreds of different notification messages. I captured and embedded them in Platform Sweet Talk, and I still add new ones as I find them. I don't have them all, I've just used the ones I saw personally. And what it reveals is a constant testing [ground], [where] they [Facebook] are showing you a notification message and then they are measuring exactly how effective that notification sentence is. For example, the particular way it's structured, the linguistics, the grammar of it. All of these techniques are effective at getting you to do something, so that they can continually tweak and tune and give you more of the things that activate you and give this other person more of the things that activate them. And that's what drives the whole thing, that's what the work is about. I think it's also a way of showing how, if we step away and depersonalise these messages, it gives us an opportunity to look at them in a new way. And to see how the user is one part of an ecosystem that's been designed, where things are feeding into us, and then we feed something back, and then that's measured, and it changes. It's this feedback loop that we're a part of, and I hope that the work helps people who might encounter it to get an opportunity to step out of that loop and to look at it from a bit of a distance.

Philippa: What does digital privacy mean to you?

Ben: To me, it comes down to the question of agency, and do I have agency to understand how, whatever I am providing, is being used or even do I understand what I am providing? What data is being gleaned from me, what traces am I leaving? What's going to become of it? Who has control? Where does it go? It's a question of agency. Yes, I can make decisions that there is a benefit to me, of letting some [data about] things that I've said or done, or how I'm reacting to something, be part of a system that helps me get to information I'm looking for or helps me connect to individuals I want to have conversations with. But the conditions we have now means the power differential is so vast that all the power is in the hands of the corporations. And not just the power to collect our data, but to make massive generalisations from that data that is then turned against us in the form of interface and content, algorithmic feed design, etc. So to me, it comes down to agency: do I know what's happening? Do I have any say in how it happens?

I can't really be a thinking person in society without having opportunities for privacy. The best ideas can't all emerge in the midst of surveillance. I mean, this is a basic tenet of academic understandings of surveillance, which is that we know that people can't help but act and feel differently when they know they might be in the process of being surveilled. And it limits our ability to think and to imagine, and our ability to think and imagine beyond the status quo. To think beyond the kind of the corporate line that we've been talking about is essential to changing anything, to having power to being able to push governments to do things differently, being able to erect alternative communities in whatever way we might want to.

Privacy for Profit

–Philippa Williams and Lipika Kamra

Source: Tushar Mahajan UnSplash https://unsplash.com/photos/pRtogCbgh7M

In 2019 Meta CEO Mark Zuckerberg declared that 'The future is private'. His speech to industry and accompanying public blog marked a rhetorical and technical shift in Meta's (previously Facebook's) corporate vision, away from Facebook's focus on the digital town square as a digital public space of sharing – to more private digital spaces characterised by the 'digital living room' and realised through apps like WhatsApp, a private digital messaging app. In the wake of the Cambridge Analytica scandal that exposed an economy of personal data sharing for corporate profit, the shift towards greater digital privacy is, on the face of it, a good thing. But there are also reasons to be cautious about the motives and methods that underpin why Big Tech says they 'care about your privacy' and that 'privacy matters'.

We should be under no illusions that for Big Tech, they care about privacy because they care about profit. In the last 30 years Meta, Google, Twitter and Amazon, Baidu, Alibaba Tencent and Xiaomi have become techno oligarchs, all through the trade of mainly personal data and the emergence of the data economy. In the data economy, power is derived from personal data; value is extracted to predict behaviour or influence individuals or groups and drive corporate profit. The expansion of the 'social quantification sector' through the exploitation and extraction of social resources or personal data all depends on the normalisation of 'data relations'. Naturalising 'data relations' in turn depends on ideological as well as technical work that quietly, subliminally encourages us to think, or not think, about the data produced through our interactions online.

On the one hand, data is portrayed as inconsequential 'exhaust' from our digital lives, and on the other hand, as something worth trading, whilst positioning society as the beneficiaries of Big Tech.

However Big Tech frames their relationship to our data, sustaining access to it is done through countless data privacy violations, manipulations and encroachments which are also made to look normal, benign and inevitable. The computer scientist, Jaap-Henk Hoepman draws attention to some of the 'privacy myths' that conceal from users the 'real' value of their data to Big Tech and tacitly persuade users to continue sharing their data and enable Big Tech to continue collecting personal, and other data, for profit.

Through the case of WhatsApp - a 'simple, secure and reliable' messaging app bought by Meta in 2014 - we want to draw attention to how Meta mobilises 'privacy talk' and 'privacy things' for profit. Following a public backlash to its Privacy Policy update in 2021, WhatsApp doubled down on their public commitment to users' privacy whilst simultaneously and paradoxically extending their services - such as WhatsApp Pay, WhatsApp Business and WhatsApp Cloud API - which drive data sharing to increase revenue. With over 500 million users, representing one quarter of all WhatsApp users globally, India is the company's largest market.

It is also where WhatsApp has pinned its ambition for financial growth through apps like WhatsApp Business.[1]
ProPublica reported that a 49-slide internal company marketing presentation they acquired emphasised the 'fierce' promotion of WhatsApp's 'privacy narrative.' In this context of Meta's simultaneous emphasis on privacy and opening 'the aperture of the brand to encompass … future business objectives' we examine how privacy is being constructed and mobilised, in particular: 'privacy as innate'; 'privacy paternalism' and; the 'privacy dark arts'.

1 Dave, P and K. Paul (2022) Zuckerberg says WhatsApp business chat will drive sales sooner than metaverse. *Reuters*. https://www.reuters.com/technology/zuckerberg-says-whatsapp-business-chat-will-drive-sales-sooner-than-metaverse-2022-11-18/ Last Accessed 16 December 2022.

Privacy as innate

Brian Koum and Jan Acton, WhatsApp's original founders, conceived of WhatsApp as an expressly private digital space. They sold the app to Facebook for $19 billion following assurances from Zuckerberg that their moral and technical commitment to privacy and focus on user experience rather than the extraction of users' data, would endure in the space. However, such commitments contradicted Facebook's ambitions for growth, and with their principles undermined, Koum and Acton departed Facebook in 2018 deeply remorseful about their decision to sell 'users' privacy to a larger benefit' .

Facebook have nonetheless actively evoked and capitalised on Acton and Koum's foundational privacy narratives to project privacy as something that is inherent, intrinsic and innate to WhatsApp. We see this articulated in defence of their privacy policy update where WhatsApp reassured users that 'Respect for your privacy is coded into our DNA', that it is therefore woven into its molecular structure. This message is reinforced through the implementation of end-to-end encryption 'by default' and now new 'layers of privacy', such as leaving groups silently, controlling who can see when you're online and screenshot blocking for some messages.
Digital privacy is also projected as something that is innate to our social interactions, as Will Cathcart explained: "People have been able to meet in private in person and talk privately for hundreds and hundreds of years, and there's no automatic system keeping a backup [and] relaying it to a company". And that to compromise that right to talk privately in the digital equivalent would induce an 'instinctive horrified reaction in people'. [2] By historicizing privacy norms concerning everyday conversations, Cathcart seeks to normalise private lives and the 'digital living room' as the natural and inevitable space in which we communicate today.

Will Cathcart and other Facebook executives are also seeking to make privacy, or the lack of it, an emotive and embodied force. As Avinash Pant, Director of Marketing at Facebook India, framed it: 'Our endeavour is to highlight that the privacy provided by WhatsApp through end-to-end encryption, is not just a feature, but a feeling, that leads to real human connections and to progress'. [3] That 'feeling' was communicated through WhatsApp's #MessagePrivately campaign 2021 in which they collaborated with advertising agency BBDO India, which sought to embed and vernacularise WhatsApp's effect and affect in people's everyday lives.

2 Newton, C (2021) WhatsApp CEO Will Cathcart on rocky year for app. *The Verge*. https://www.theverge.com/2021/9/13/22672756/whatsapp-ceo-will-cathcart-interview-2021-propublica-privacy-encryption Last Accessed 18 November 2022.

3 The Social Samosa (2020) Avinash Pant on making of WhatsApp's first global brand campaign. https://www.socialsamosa.com/2020/07/interview-avinash-pant-facebook/ Last Accessed 25 November 2022.

One ad shown in India called 'the golden jubilee' featured an elderly couple celebrating their wedding anniversary in the company of their grandchildren. The grandchildren ask the grandfather to kiss the grandmother but he declines, and instead moves to sit in another corner of the room.
He then sends a WhatsApp message to the grandmother who smiles to herself, then looks across to her husband and in jest raises her hand in a slap action, insinuating that he has sent her something risqué via WhatsApp.
Neither we, the audience nor the grandchildren see the message sent, reinforcing WhatsApp's message that privacy is embedded in their product ethos and design.
In the Indian context, where public displays of affection are usually seen as unacceptable even among married couples when surrounded by family, WhatsApp positions itself as the natural extension of sociodigital intimacy.

'Jubilee Wedding' BBDO for WhatsApp
Source: Screen shots https://www.thedrum.com/news/2021/08/05/whatsapp-launches-brand-marketing-campaign-message-privately-india

Privacy paternalism

WhatsApp's privacy architecture, in particular end-to-end encryption is being increasingly challenged by state governments. In the USA Attorney General William P. Barr has long fought to allow lawful access to encrypted communications, [4] India's new Internet rules demand social media companies to trace the originator of individual messages, whilst the UK's Online Safety Bill strengthens powers for Ofcom to demand encrypted messenger apps scan users' messages in suspect cases of child sexual exploitation and abuse and terrorism. [5]

WhatsApp's response has been to double down on the implementation of end-to-end encryption, pushing back against governments who they accuse of inserting a 'spy clause' in their internet regulations in the name of national security.

4 McCabe, David, Mike Issac and Katie Benner (2019) Barr pushes Facebook for access to WhatsApp messages. *The New York Times*. https://www.nytimes.com/2019/10/03/us/politics/barr-whatsapp-facebook-encryption.html Last Accessed 15 December 2022.
5 McCallum, Shiona (2022) WhatsApp: We won't lower security for any government. BBC News [online] https://www.bbc.co.uk/news/technology-62291328 Last Accessed 12 November 2022.

WhatsApp has taken the exceptional step to sue the Indian government, arguing that the new Internet rules would violate citizens' privacy: 'The threat that anything someone writes can be traced back to them takes away people's privacy and would have a chilling effect on what people say even in private settings, violating universally recognized principles of free expression and human rights.' [6]

In these cases, WhatsApp positions itself on the side of ordinary people, as Will Cathcart states in discussion with Alex Kantrowitz: 'It's why we fought so hard to bring end-to-end encryption all around the world, and defend it all around the world, at times, with scepticism from governments, or people who are opposed to that level of security saying, 'Well, do people really care about privacy of this stuff?' Yes, people absolutely care about the privacy of this stuff.' [7]

Will Cathcart projects that in ten years 'There will be even more sophisticated hackers, spyware companies, hostile governments, criminals trying to get access to it. And not having the best security means that information is stolen. I think that has real consequences for free society... My hope is that over the next few years, increasingly governments will realise that on balance, the more important thing for them to do is protect their citizens' data.' In their move to sue national governments and speak out for citizens privacy globally WhatsApp portrays itself as global protectors of privacy.

6 Issac, Mike (2021) Whatsapp sues India's government. The New York Times. https://www.nytimes.com/2021/05/25/technology/whatsapp-india-lawsuit.html Last Accessed 24 November 2022

7 Kanrowitz, Alex (2021) WhatsApp head Will Cathart dishes on Signal, India, and Apple. *Medium*. https://onezero.medium.com/whatsapp-head-will-cathcart-dishes-on-signal-india-and-apple-db81b4553718 Last Accessed 24 November 2022.

Privacy dark arts

'Privacy talk' has an important role to play in the privacy dark arts, that is, directing and deflecting our attention in ways that serve WhatsApp/Meta's interests. In the privacy dark arts, privacy talk is mobilised in combination with 'privacy things'. These are technical affordances such as 'end-to-end encryption' which means before a message even leaves your device, it's secured with a cryptographic lock, and only the recipient has the keys, which change with every single message sent. Or new privacy features introduced by WhatsApp such as disappearing messages, blocking screen shots and control over who can see when you're online. In defence of its commitment to privacy and security, WhatsApp routinely responds by emphasising the protection afforded by 'privacy things' and in particular, end-to-end encryption which, as they repeatedly tell users, 'No one can see inside that message...not even us'.

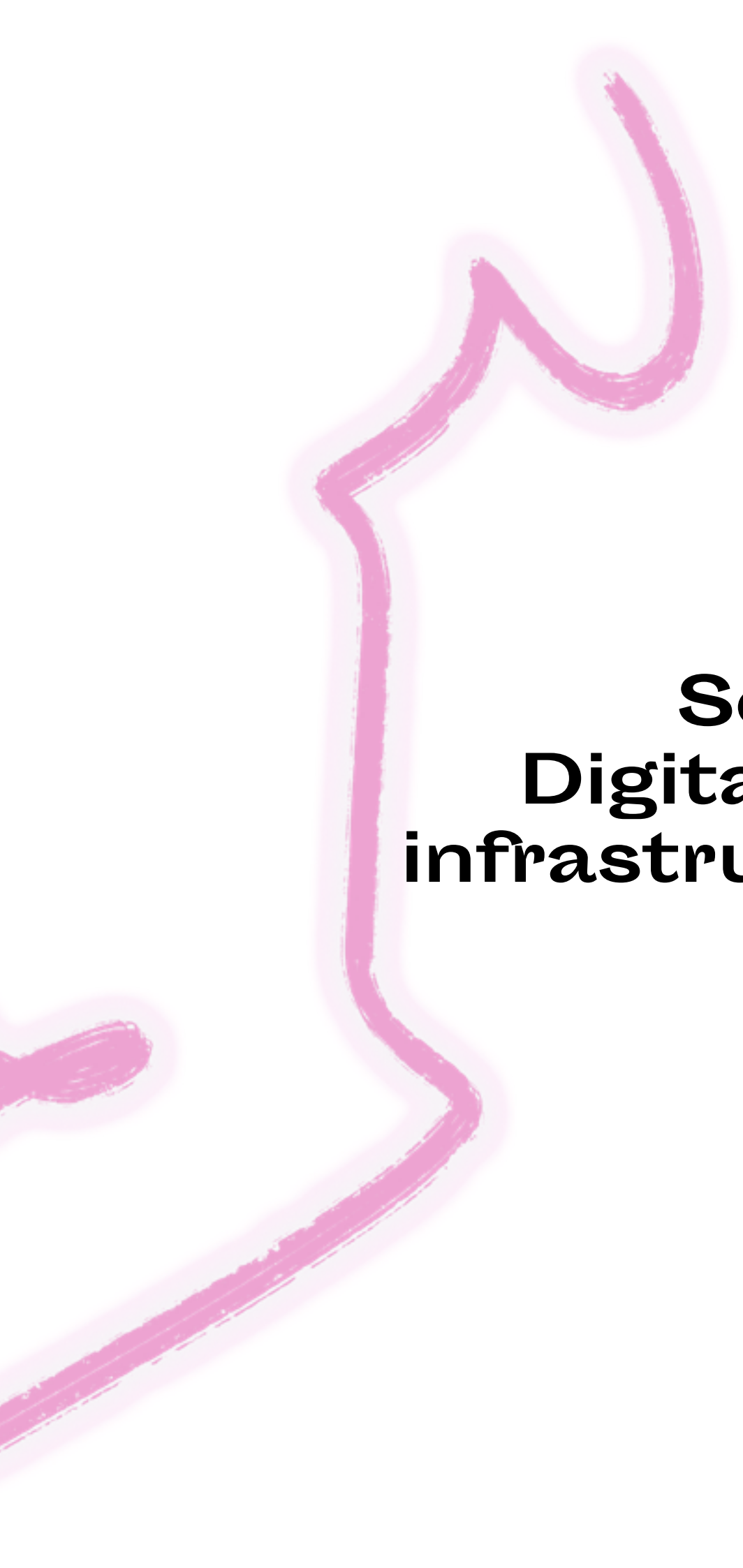
The focus on the content inside personal messages and end-to-end encryption is a conscious strategy to deflect attention away from the implications of metadata that is collected on the 'outside' of the message. Once aggregated, the metadata previously collected and shared between WhatsApp and Facebook to 'run the service', since the 2021 privacy policy update can now also be used to monetize it, in certain cases.

In this move, WhatsApp both plays down the power and value of metadata to Meta stating that it collects only basic and essential information about its users, and simultaneously plays up the importance of the interior content, repeating to users that it is the privacy of their messages

Source: Twitter @iimhamzaa

that they should be most concerned about. In so doing, WhatsApp perpetuates one of Hoepman's seven privacy myths, that it is 'merely metadata'. In its Privacy Policy, WhatsApp states that it collects information 'to operate, provide, improve, understand, customize, support, and market our Services, including when you install, access, or use our Services.' In practice, at a minimum this means collecting a wealth of data on users' handsets, IP addresses and area codes to determine location, contacts and activities on the app, such as when and whether you are online, when you last updated the 'about information', as well as your status and information about groups, such as their name, group picture and description. For users who wish to avail of location-based services and business apps the inventory of metadata collected increases, as does its value to WhatsApp/Meta.

WhatsApp collects more metadata than Signal, another privacy messaging app, does, and arguably more data than it 'needs' to, to run a private messaging app. But why? To Meta, the data on the 'outside' of your message is of far more value than its internal content. Afterall metadata is collected without people generally being aware, it's more structured and more easily analysed and most importantly, linked to other data. Memes circulating in the aftermath of WhatsApp's privacy policy update (see above) satirised the apparent duplicity of a company that both sells and protects our privacy all at once. Knowing what we know about Mark Zuckerberg's assiduous commitment to growth, the privacy pivot is really a pivot towards privacy for profit.



Scene 3: Digital-state infrastructures

Digital Violence (2021)

Forensic Architecture

Digital Violence, Forensic Architecture (2021)

Digital Violence (2021) is a global investigation by Turner Prize nominees Forensic Architecture in collaboration with Amnesty International and The Citizen Lab. It examines the cyber-weapons manufacturer NSO Group and its malware Pegasus, a piece of 'security' software sold to governments across the world. Pegasus can enable its operators to infiltrate phones, access personal and location data and surreptitiously control a device's microphone and camera. In Scene 3 we bear witness to some of 'The Pegasus Stories' video testimonials of human rights activists whose privacy has been invaded by the affordances of Pegasus.

Interview with Shourideh Molavi

Forensic Architecture

In these edited excerpts Shourideh Molavi, lead researcher at Forensic Architecture responded by voice notes to questions posed by Philippa Williams over email. She shares absorbing insights into the context and motivation behind producing 'Digital Violence', the challenges of navigating their own digital vulnerability during the pandemic and the critical spaces afforded by working at the intersection of academia, activism and art. It is fascinating to learn how the unanticipated networks and collaborations that arose through the research reinforced the project's conclusions that digital violence, although sinister and insidious is ultimately, a failed project.

Philippa: Can you introduce what 'Digital Violence' is and how it was produced? What is the relationship between digital technologies, politics and power that Digital Violence' exposes?

Shourideh: Digital violence is a project that we initiated at Forensic Architecture, just around the pandemic. And it was a product of an urgency that we found in investigating non kinetic violence … a violence that we realised many of our friends and collaborators from around the world had been subjected to. This, of course, is digital violence in the form of hacks of people's personal and work devices. And the urgency was there because we were in a pandemic - we were under lockdown forced to be behind our screens - and realised that we were making ourselves even more vulnerable to a newly developed form of state violence than we had realised. So we wanted to use our tools and our techniques at Forensic Architecture, to investigate the effect of this type of state violence on people's work around human rights and civil society organising. The relationship between digital technologies, politics and power that we then expose is the direct link between the way that physical violence and digital violence functions. Digital violence often steps in to fill in the gaps of the classical forms of physical violence applied by states, such as interrogation, arrests, intimidation, even violence, such as bullets, checkpoints, digital information that's extracted from you, using identity cards. What digital violence does is that it allows states to access individual information, even beyond the formal state setting. So when you're at home, when you're with loved ones, when you are in a recreational space, you still become vulnerable to this form of violence, and you become vulnerable through your devices that are a part of your daily activities.

Philippa: What techniques do you/ Forensic Architecture use to bring the uneven relationship between governments, people and power to the surface in the work?

Shourideh: The techniques that we used to expose digital violence by various states around the world was the production of a 3D interactive platform that plays together all of the data that we collected. And here we did open source research. We looked at everything that was available online. We organised it according to fields of operation, so countries around the world that were accessing this malicious software. And we also organised it around individuals. Every single individual that we could find who had been targeted by Pegasus was documented, what they were working on was documented, what's in the public domain was documented. We then met with over a dozen people who had been targeted by Pegasus, heard their stories, filmed them, and understood how the hack affected their human rights work. And all of the people that we spoke with were civil society organisers, anti corruption activists, journalists, lawyers, public figures, opposition figures, people who are used to different forms of state violence, and people whose existence is part and parcel of a healthy, functioning democracy. Our project Digital Violence looks specifically at the NSO group, which is an Israeli cyber weapons company established in 2010. And we look in particular at the Pegasus software that they have produced and been able to export to different parts of the world. And we realized that the governments around the world using the software were a range of liberal democratic, theocratic, monarchist, apartheid governments, and settler colonial governments. So it's a real range of governmental forms that are mobilising the software, but consistently using it against civil society activists, public figures, journalists, lawyers, and others who are working to hold state and corporate violence to account.

Philippa: What were the key challenges of designing such a project?

Shourideh: The challenge that we had in doing the investigation in 2020 and 2021, was that we were living a pandemic, we were relegated to screens which were the very same mediums that made us vulnerable to digital violence and we were very well aware of this. This completely changed our culture of working. The way that Forensic Architecture's methods were applied, the way that we worked even internally, how we communicated, the software that we use to communicate all of that shifted significantly with this project. And it made us aware of our vulnerabilities in this moment as well.

Philippa: What was your role in the investigation and production of 'Digital Violence'?

Shourideh: I am the lead researcher of that investigation, and I pushed forward the interviews with the survivors of digital violence. Working closely with our director Eyal Weizman, and filmmaker Laura Poitras, we organised a public launch and the public programme to follow the launch of the investigation in Montreal, Canada and in different parts of the world, to bring attention to this rising form of state violence. What we found consistently in speaking to people who had been targeted by Pegasus was that the intention of software like this is to break networks of collaboration. The intention is to make you doubt your colleagues, it is to make you fearful. The intention is to make you paranoid, make you feel vulnerable, exposed, make you feel

like you are exposing loved ones, family members, friends, people who are close to you, who are obviously on your devices in various forms, whether it's images or videos or contacts or messages, so that you then stop the work that you're doing. But what we realised in speaking to the people who had been targeted was that this is a failed project, consistently, any target of Pegasus with whom I spoke, were telling me that despite the violation, despite the trauma, despite the emotional damage that they faced and endured because of the Pegasus hack, they nevertheless, were continuing their work. And this is important because what it shows, is that despite digital violence being a new terrain of warfare - and cyber weapons are weapons - they kill people, they hurt people, they cause trauma and physical and emotional damage to some of the strongest people around the world. Despite the damage that this is doing, it is not preventing civil society from pushing back. And that is an important thing also to document as part of Forensic Architecture's practice.

Philippa: What is the significance to Forensic Architecture's practice, of showing Digital Violence in a gallery space or creative spaces more generally? What is the relationship between culture and politics/ethics in these moments?

Shourideh: Our practice is to use visual and spatial methodologies to investigate state and corporate violence. And in doing this, we also work with a broad sort of network of relations, we work with people who've been targeted. We work with people who are investigating that targeting. We work with lawyers, we work with artists, with architects, with developers, with theorists, with activists. And in so doing, we mobilise different fora, the gallery and the museum is one of the many fora that we mobilise. And of course, the way that we then present our work, the vocabulary, the ontology, and the grammars of enunciation, all of those change based on the fora, because as part of Forensic Architecture's work, the gallery and the museum also become political spaces. They become spaces of debate. So when we realise that the courtroom is not a space where we can affect change, we move to the university, when the university fails, we move to the streets, and when the streets fail, we move to the gallery, and so on, and so on. And we believe that this is an important way of opening up the field of accountability for human rights violations. And so far, frankly, it has proven effective.

Philippa: Either with respect to Digital Violence, or speaking personally, what does digital privacy mean (to you)?

Shourideh: So the question of what digital privacy means, to me, was one that I was grappling with throughout this investigation. And I have to say that the right to privacy is essentially the right to an identity. It is the right to thought, it is the right to have that space to yourself where you are, thinking about who you are, what you are, what you want, what you prefer, what you think what your values and your morals are. And that space, that personal, private space is sacred. It's important for us as thinking beings as social beings to have that space in order to function in a healthy way. When that space is violated, it essentially violates our ability to be full subjects. It violates our ability to think. It violates our very identity as thinking beings and as social beings.

And what it does is that it cuts our ability to connect with those around us. For me, digital violence, the project that Forensic Architecture initiated was a way to push back against that, in a landscape, where our social relations are used against us through hacks using software like Pegasus. We were then creating social networks and relations in the two years that we were doing this investigation and managed to find friends, like-minded people, organisers, thinkers, and investigators like us in different parts of the world with whom we built even deeper collaborations. So if anything, software like Pegasus and violence in the digital form that states and corporations are initiating are a failed project, because civil society groups are pushing back and are never nevertheless building the very relations, the very social ties and fabrics that this type of software targets.

Techno-politics and social surveillance in India

Ram Bhat

In 2014, Narendra Modi, leader of the Bharatiya Janata Party (BJP) came to power after a decade of Congress party rule. Modi was sold to the public as a strong and self-made man, promising honest and transparent governance. A key part of Modi's vision for a new politics was to change the architecture of governance through what he called the Digital India initiative. As part of Digital India, the union government is wiring up 250,000 village governments (Panchayats) and in effect, providing fibre optic enabled high speed internet to nearly 600,000 villages. As with much of Modi's rhetoric, this initiative is a rebranding of an earlier Congress government initiative. The Congress government, in 2012-13 had already implemented Direct Beneficiary Transfer (DBT) for a few government schemes (such as cooking gas subsidies and wages under government guaranteed employment) in 43 districts of India. This pilot relied largely on citizens having a biometric identity - called Aadhaar - used as the basis for verification of beneficiaries. Since 2014 Modi has expanded on this architecture, making it the world's largest biometric identity programme. Today, a significant portion of government welfare is routed through what his government calls the JAM trinity. The JAM stands for Jan Dhan (zero balance bank accounts), Aadhaar and Mobile phone number. This platformization of welfare and governance produces a peculiar everyday violence on the population that is subject to it. I refer to violence produced by a combination of three phenomena: expansion of social surveillance; the new forms of subjectification intimately linked to this expansion of social surveillance; and the quantitative datafication of social welfare.

A citizen's political identity is giving way to a triangulation of three data points that generate a numerical identity, in turn determining their eligibility for welfare. If eligible, money will be transferred directly from the government to the bank account of the beneficiary. This is a new architecture that will have major implications not only for individuals but also for how politics is done in India. The state is out of reach, an abstraction increasingly materialised through cash transfers. Money reaches a citizen's bank account from somewhere in Delhi, but if something goes wrong – the biometric print fails to match, the electricity supply is broken or the server is down - there is nothing the local politician, technician, bureaucrat, or citizen can do about it. The shift from paper based to digital governance, from interacting with humans to interacting with the JAM architecture has created an invisible and subtle regime of everyday violence – a violence that completely violates citizens' privacy and drastically reduces their agency to negotiate their relationship with those who govern them. Let us take two examples to illustrate what this violence looks like.

The first is an exclusion that exerts violence directly on the body. Over two decades, elites in state and civil society have been arguing against universal welfare obligations and handing over these 'sectors' to privately-owned firms. A key battleground for such arguments is the responsibility of union and state governments to organise universal provision of grains and other food essentials for citizens living in poverty. With direct cash transfers, reforming the public distribution system has come

to mean eliminating 'leakages', including by removing 'undeserving' beneficiaries. Between 2013 and 2016, more than 30 million official documents of citizens were cancelled because they failed to link their documents with their biometric identity. Linking basic needs welfare to biometric identification has been a fatal move for groups historically oppressed by caste and indigeneity. There have been dozens of reported starvation deaths taking place every year because they did not have their biometric cards available for some reason (often many citizens are forced to hand over their official documents as mortgage to access loans for emergency expenses), or biometric verification failed (fingerprints did not match). The digital architecture of welfare produces a brutal form of surveillance where the citizen must meet the gaze of the state under precisely the right conditions. Deviation and error become a matter of life and death.

The second example of the Prime Minister's Housing Scheme illustrates violence in terms of control. The housing scheme runs on two apps: Awaas Soft, a web-based electronic service delivery platform to operationalise the housing scheme; and Awaas App used to monitor real time evidence of house construction through date and time stamped georeferenced photographs of houses. This new way of doing the housing scheme gives an insight into the increasing importance of techno-politics. The process by which a citizen becomes an eligible beneficiary by meeting the standards mentioned in the socio-economic census, the procurement of materials for building a house (fly-ash, cement etc.) from local suppliers, the hiring of labour for house construction, the uploading and verification of photographic evidence mediated through mobile applications – all of these are sites of techno-politics, by which I mean politics that determines the conditions under which individuals can be included, suspended or excluded as eligible beneficiaries. A housing scheme beneficiary in Chhattisgarh told me that he had to 'build a relationship' with the local officials (code for payments in cash or in-kind) to even get listed as a beneficiary. Then his funds were 'stuck' until he hired the right suppliers for house-materials such as bricks and fly-ash. He discovered that these suppliers and contractors are relatives of the same officials who were responsible for clearing his payments from the housing scheme. In this form of social surveillance, the violence of political exclusion appears as procedural exclusions – due to technological design flaws, errors, and deviations.

The platformization of welfare is linked to the proliferation of techno-politics in daily life. New forms of social violence with devastating consequences have resulted in the quantification of politics. Notions of surveillance and privacy are turned upside down when it comes to techno-politics. Oppressed groups are forced to become radically visible and legible to the new digital architecture of politics. Not just in India but in much of the Global South, stakeholders in development such as academics, activists, policymakers, donors are valorising digitalisation and platformization of politics in the name of transparency (honest), neutrality (secular) and efficiency (speed and scale). The result is an intensification of the three phenomena I mentioned earlier: social surveillance infrastructure, new forms of subjectification and quantitative datafication of social welfare. Along with intensification of these phenomena, we will see an increase in everyday violence in the guise of procedural exclusion. Unprecedented levels of social surveillance for welfare requires us to deepen our engagement with news forms of social antagonism, inequality, and violence. Such violence needs to be recognised and exposed, a small step towards new forms of resistance.

Scene 4: Post Privacy?

1014 (2015)

Yuri Pattison

1014 (2015) gives us a tour of Room 1014 in the Mira hotel, Hong Kong that was occupied by the whistleblower turned privacy activist Edward Snowden immediately following his departure from the US in 2013, and from where The Guardian first revealed his identity to the world. Yuri Pattison created the film work two years after the event, intrigued by the transformation of this story into a revered Hollywood film called 'Citizenfour' - a highly acclaimed documentary about Edward Snowden, directed by Forensic Architecture's collaborator Laura Poitras. Pattison's guided film returns to the hotel location like one might make a pilgrimage to a movie location.

1014 is subtly annotated with diagrams and text elements borrowed from the NSA and GCHQ documents that were leaked by Snowden, while also drawing from English translations of Chinese netizen slang. These annotated elements were flattened by processing them with the anonymity tool, Anonymouth, to conceal the artist's identity and add yet further depth and layering to his critique. In a shrewd twist, the artist's source videos were hosted on the server that Edward Snowden used to store his files during the time, returning us full circle to the origin story.

Secrecy, in the ruins of privacy

Carwyn Morris

For many years surveillance anxiety occurred alongside surveillance ambiguity; many people suspected they were being surveilled by a state-corporate nexus, it was a key part of many conspiracy theories, but people were unsure of the details. The Snowden leaks laid bare the transnational scope of contemporary surveillance, highlighting how a state-corporate nexus – particularly through the PRISM programme – supported the Five Eyes countries in observing everyone from your next door neighbour to heads of state. Another noted source of digital anxiety is related to forgetting; will our online footprint be visible evermore? Will everything others share about us – even when false – be forever searchable? Will the data our activities generate be used in perpetuum? In the years that followed the Snowden leaks these anxieties coalesced into a broader data anxiety, some people and countries, Brazil for instance, looked towards Chinese hardware and software to shield them from the Five Eyes threat, while the European Union moved away from the United States vision of the 'free internet' and towards a relatively open market digital sovereignty position, most visible in its General Data Protection Regulation (GDPR).

If one were to move away from GDPR and the digital spaces owned and administered by North American companies – previously understood as Google, Apple, Facebook, and Amazon (GAFA), but now Meta and Alphabet, and arguably also Twitter – and instead speak to those embedded within the digital territory of the People's Republic of China's (China) a new landscape of anxiety emerges. During my research on activism in China, those engaged in anti-eviction map making were often less worried about being 'forgotten' and were more concerned that their activist maps and the evictions they attempted to record would never be 'remembered.' They feared that companies such as Tencent – either following state guidelines or attempting to stop politically sensitive content that could draw the ire of the state towards the company – would use surveillance technologies to censor their discussions and delete their digital places of gathering. Perversely, there was an abiding fear amongst those who discussed politically sensitive issues that the state would remember that which has (not) been said and use it against them at some point in the future. Due to these constraints, many people who may be drawn to activism avoid publicly voicing their dissatisfactions with the current state of affairs, they treat each social (media) system as compromised, and they publicly reproduce empty platitudes; "对对对对对对，好好好!" [1]

Another example of China's digital landscape of anxiety can be found in debates around privacy. Privacy from the state, as associated with Western liberal-rule-of-law or encryption and data security, is extremely limited and has been since 1949: the People's commune; the Cultural Revolution; the danwei (work unit); the residential community; violent systems of family planning; and emerging Social Credit systems are all examples of attempts to breakdown the boundaries between the state and the individual. While private space re-emerged during

1 "Yes, yes, yes, yes, yes, yes; great, great, great!"

the Reform and Opening Up period, private spaces may become spaces of state surveillance at any moment. This means that while privacy can exist, privacy does not necessarily persist.

It would be fundamentally wrong to say that privacy does not exist in China as, in the revised 2020 version of China's Civile Code, it is legally defined as 'the tranquillity of natural private persons' lives, and private and confidential spaces, activities and information that they do not wish others to know about.' But as a Civil Code, privacy here is a relationship between private individuals, not a relationship between individuals and the state. To understand the individual's relationship with the state one can look toward the Personal Information Protection Law, here the individual's data is protected from corporate entities and from rogue individuals working inside the state apparatus looking to sell personal data, though personal information is still accessible to authorities – both corporations and the state – for reasons of 'national security,' 'public security,' or 'significant public interests'. While these are lofty terms they are also linguistically flexible, and citizens who have different political imaginaries to the state, including feminist activists and those attempting to safeguard human rights, are regularly cautioned or arrested for reasons of national and public security. Therefore, while privacy does exist in the civic realm, it does not ensure citizens can make use of encrypted spaces free from state surveillance, meaning that citizens are still subject to constant surveillance during their lives in China's digital territory.

With limited personal privacy from state surveillance, secrecy has become a key aspect of life within China's digital territory. While secrecy can be defined in many ways, two useful typologies of secrecy are 'secrecy as being hidden from view' and 'secrecy as being hidden through illegibility.' The first typology means information is hidden from many but accessible to those who know where to look, while the second typology means information is shared publicly but is legible only to those who can perceive it. These typologies could also be thought of as 'secrets from the public' and 'secrets in public.' Due to China's online surveillance system and a lack of privacy, the first typology becomes relatively redundant when one wishes to evade state surveillance, with various algorithmic surveillance systems acting as detective, judge, jury, and executioner in a battle against information deemed as politically sensitive: a Cyborg Judge Dredd.

The second typology of secrecy enables sensitive and subversive knowledge to be circulated within highly surveilled environments by making the sensitivity of information illegible to surveillance systems. Some of the earliest scholarship on China's digitizing society highlighted how code words and satirical phrases were being used to evade digital governance, enabling people to discuss (and ridicule) the government (Meng 2011), leading to the rise of the 'Grass Mud Horse' and the "river crab," both used to discuss sensitive topics without censorship. [2] While textual secrecy evades attempts at keyword censorship, secrecy through images is also a common way of publicly circulating sensitive messages. As optical character and image recognition technologies became more advanced, tactics of visual secrecy have evolved to include image

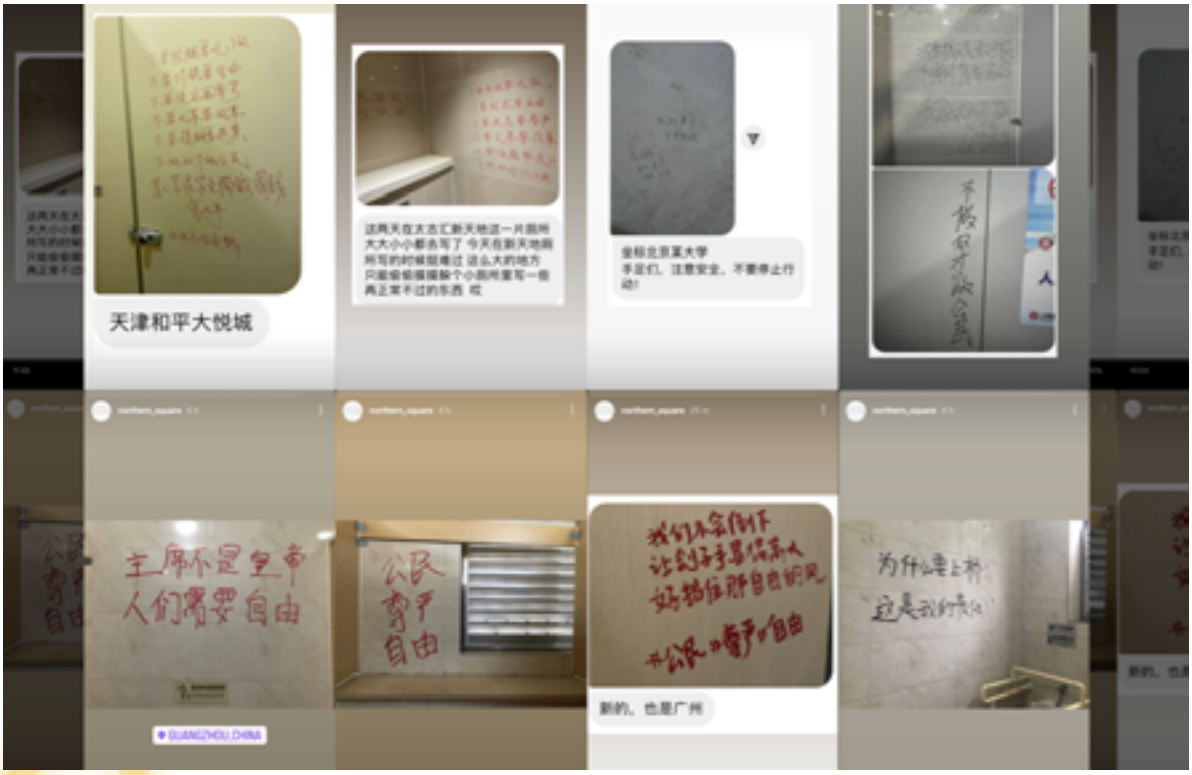
2 The 'Grass Mud Horse' is a homonym of 'Fuck Your Mother' and the 'River Crab' is a homonym of the Hu Jintao era political slogan, 'harmony.'

Print a Revolution in situ: posters from the London School of Economics, Leiden University, and Boston University, shared to and then by Instagram account northern_square
Instagram: @northern_square

manipulation techniques – flipping images, scribbling over images – and hand illustration of images. These simple-yet-effective techniques have been used for anti-eviction activist projects (Morris 2022), China's #MeToo# campaigns, [3] and attempts to highlight the failings of recent lockdowns in Shanghai. [4] Through these techniques, secrecy may at times be more about keeping the circulation of sensitive information a secret from authorities for short periods of time – secret acts – than about possessing information unknown to authorities – secret knowledge.

Evolving tactics, techniques, and geographies of secrecy have been particularly visible in the aftermath of the recent the Sitong Bridge incident. The Sitong Bridge incident took place on October 13th 2022, days before the 20th National Congress of the Chinese Communist Party, where Xi Jinping cemented his long-term rule in China was a public. It was a one-person protest against recent trends in Chinese governance and the rule of Xi Jinping as well as a public spectacle in a busy area of Beijing. The incident circulated rapidly online; images and videos of the incident (deleted) were followed by posts about the incident and its slogans (deleted). Soon cryptic allusions to the incident were posted (also deleted), including saying 'I saw', posting red box emojis, or sharing the song, Sitong Bridge, by indie band Mr Graceless.

3 For instance, the evolution of #MeToo# into #MiTu# and its English translation, #RiceBunny#.
4 China Digital Times (2022) 'Voices of April' (CDT) (blog) https://chinadigitaltimes.net/space/%E5%9B%9B%E6%9C%88%E4%B9%8B%E5%A3%B0 Last Accessed 2 Dec 2022



Print a Revolution in situ: toilet graffiti from the People's Republic of China, circulated through the Instagram account northern_square Instagram: @northern_square

While attempts at secrecy-through-illegibility were taking place and being cracked down upon within China's digital territory, outside of China, anonymous protests were taking place in ways that participants hoped would make them illegible to a state surveillance network that worked across physical and digital borders. The clearest examples of this were forms of anonymous solidarity and the Print-A-Revolution movement – 印刷一场革命 – taking place through the Instagram account, northern_square.

In support of the Sitong Bridge incident and the ideas around it, northern_square used the Instagram Stories function to become an anonymous solidarity account; messages of solidarity were sent to northern_square, they were cropped, and then they were shared anonymously to followers. In the month following the Sitong Bridge incident roughly 900 messages from all around the world were shared to northern_square, and through their Stories an anonymous community emerged where solidarity was produced in secret, where anonymous conversations mediated through northern_square could take place, and where those fearful of speaking publicly could have an anonymous public voice. At the same time, northern_square began to share posters related to the Sitong Bridge incident, posters that could be printed off and posted anywhere. To 'Print-A-Revolution,' numerous people around the world put ink to wall, by printing off and sticking up their posters. Once ink and paper were on wall users would take a photo and share this to northern_square, alongside the location and often a message. Through this act a secretive localized protest could now circulate digitally online, becoming an anonymous transnational spectacle that inspired others to find their secret-yet-public voice.

Through ink, photograph, and the circulation of digital images, Print-A-Revolution began. In the days that followed elite Beijing institution, Tsinghua University, would stop self-service printing and implement a real-name system to track printing. Fearful of sticking up posters in public, people in China began using the public Airdrop function of iOS to secretly share Sitong Bridge and anti-Xi Jinping posters to other phones around them. This resulted in Apple updating the Chinese version of iOS to limit how long public Airdrops remain accessible; coding shut a door for protest. This is not the first time Apple has made changes to its services in China that seem to aid the Chinese state in quashing activists, having previously limited device functionality and removed applications from the Chinese app store. northern_square also highlighted another secretive method of putting ink to wall: toilet graffiti. northern_square received numerous pictures of Sitong Bridge related toilet graffiti from within China, highlighting how one of the few spaces free from Chinese state surveillance may be the toilet cubicle. By putting inked messages of resistance and solidarity on the wall, public protest could be done secretly, leading to a secretive spectacle making resistance legible to those with the right positionality. Through these incidents we begin to see that while privacy could be a core concern in digital society, privacy is neither universally implemented nor defined. In the ruins of privacy, secrecy can be found, and as digital privacy is eroded – if it ever even existed – it is important to remember that secrecy is a powerful alternative to privacy, an alternative where agency is in the hands of people not states.

References

Bingchun Meng (2011), 'From Steamed Bun to Grass Mud Horse: E Gao as Alternative Political Discourse on the Chinese Internet', Global Media and Communication 7 (1): 33–51.

Bratton, Benjamin (2015) The Stack: On Software and Sovereignty. Cambridge and London: MIT Press.

Couldry, Nick and Ulises Ali Mejias (2019) The Costs of Connection: How Data is Colonising Human Life and Appropriating it for Capitalism. Stanford, Stanford University Press.

Creemers, Rogier (2022) 'China's Emerging Data Protection Framework', Journal of Cybersecurity 8(1). Online first.

Dave, Paresh and Katie Paul (2022) Zuckerberg says WhatsApp business chat will drive sales sooner than metaverse. [Online] Reuters. https://www.reuters.com/technology/zuckerberg-says-whatsapp-business-chat-will-drive-sales-sooner-than-metaverse-2022-11-18/ Last Accessed 16 December 2022.

Gilchrist, Karen (2022) 'Apple Limited a Crucial AirDrop Function in China Just Weeks before Protests' CNBC [Online] https://www.cnbc.com/2022/11/30/apple-limited-a-crucial-airdropfunction-in-china-just-weeks-before-protests.html Last Accessed 28 November 2022.

Hoepman, Jaap-Hank (2021) Privacy is Hard and Seven Other Myths: Achieving Privacy through Careful Design. Cambridge: The MIT Press.

Issac, Mike (2021) WhatsApp sues India's government. The New York Times. [Online] https://www.nytimes.com/2021/05/25/technology/whatsapp-india-lawsuit.html. Last Accessed 24 November 2022.

Kanrowitz, Alex (2021) WhatsApp head Will Cathcart dishes on Signal, India, and Apple. Medium. [Online] https://onezero.medium.com/whatsapp-head-will-cathcart-dishes-on-signal-india-and-apple-db81b4553718 Last Accessed 24 November 2022.

McCabe, David, Mike Issac and Katie Benner (2019) Barr pushes Facebook for access to WhatsApp messages. The New York Times. [Online] https://www.nytimes.com/2019/12/10/technology/whatsapp-barr-encryption.html Last Accessed 15 December 2022.

McCallum, Shiona (2022) WhatsApp: We won't lower security for any government.

Morris, Carwyn (2022) 'Digital Displacement: The Spatialities of Contentious Politics in China's Digital Territory', Transactions of the Institute of British Geographers 47 (4): 1075–89.

Newton, C (2021) WhatsApp CEO Will Cathcart on a rocky year for the app. The Verge. [Online] https://www.theverge.com/2021/9/13/22672756/whatsapp-ceo-will-cathcart-interview-2021-propublica-privacy-encryption. Last Accessed 14 November 2022.

The Social Samosa (2020) Avinash Pant on making of WhatsApp's first global brand campaign. [Online] https://www.socialsamosa.com/2020/07/interview-avinash-pant-facebook/ Last Accessed 25 November 2022.

Contributor Biographies

Ram Bhat is a visiting fellow at the Media and Communications Department at LSE and co-founder of Maraa, a media and arts collective in Bangalore. He has also worked in the community media sector for over a decade in varying capacities. His research interests include critical development, disinformation and infrastructure from a Global South perspective.

James Bridle is a writer, artist and technologist. They are the author of 'New Dark Age' (2018) and 'Ways of Being' (2022), and they wrote and presented "New Ways of Seeing" for BBC Radio 4 in 2019. They have been commissioned by the V&A Museum, the Barbican, Artangel, the Oslo Architecture Triennale & the Istanbul Design Biennial;, and been honoured by Ars Electronica, the Japan Media Arts Festival, and the Design Museum, London. They were named as one of the 1000 Most Influential People in London by the Evening Standard in 2007, and one of the 100 Most Influential People in Europe by WIRED Magazine in 2015

Candice Jacobs is an artist, curator and director of OTOKA, a nomadic & fluid research, exhibition, residency, online platform & studio space that she established after returning to Nottingham during the Pandemic and becoming a mother. Jacobs' work explores a world that exists as a mode of interrogation, drawing attention to aspects of reality that require further review and consideration, seizing and documenting behaviours that participate in spatial disturbances to create a shifting of place into angelic sphere (of exhaustion), which involves the manipulation of symbols (which are also things) and people (who are also symbolic); archetypes that supply a vocabulary for the processing of private epiphanies that shape our sense of self through contemporary capitalist frameworks and political modes of thought. Candice was nominated for the Jarman Award 2022, she co-founded One Thoresby Street, the New Midland Group & Moot Gallery in Nottingham; and she has exhibited at 56th Venice Biennale; FACT Liverpool; Camden Arts Centre; Artnight 2020; VITRINE, Seventeen and in Angelo Plessas' Eternal Internet Brother & Sisterhood in Sri Lanka for Documenta 14. She is also a Lecturer at Central Saint Martins & Chelsea College of Art.

Lipika Kamra is a Lecturer in Politics at Queen Mary University of London. She is a political anthropologist researching and teaching on digital politics, democracy and development. Her work examines how states and their citizens interact in post-conflict contexts; how rural women mediate the terrain of development and democracy in the Global South; and how digital media increasingly influences everyday democratic politics in India. She is currently co-writing 'Privacy Techtonics: Digital geopolitics, WhatsApp and India'.

Tara Kelton is an Indian-American artist based in Bangalore, India. Tara's work considers the traditional figure of the artist (and craftsperson) in relation to the digital. Working across media she reflects on the diminishing role of the human in contemporary society (replaced by automation, AI and digital mediation) and the remote algorithmic control of labour by western bodies and corporations. Tara has exhibited at the ZKM Karlsruhe, ICA Singapore and the Kochi Muziris Biennale. Tara is co-editor of Silicon Plateau, a publishing series that explores the intersection of technology, culture and society in Bangalore.

Carwyn Morris is a University Lecturer of Digital China at the Leiden Institute of Area Studies, Leiden University. Carwyn's research examines the spatialization of digital relations, including digital displacement, digital territorialization projects, digital mobilities, and wanghong (internet celebrity) urbanisms. His work has appeared in Transactions of the Institute of British Geographers, Mobility, Made in China, Mediapolis, and The China Quarterly.

Kaveri Medappa is a postdoctoral researcher in Human Geography and a Junior Research Fellow at Kellogg College, University of Oxford. She received her PhD in International Development from the University of Sussex in 2022. Her doctoral project is an ethnographic study of app-based food delivery workers and cab drivers in Bengaluru, India. Her research and teaching interests broadly fall within labour anthropology, critical mobility studies, international development, feminist political economic thought, and the intersections of everyday life with digital technologies and financialisation.

Forensic Architecture Is an interdisciplinary research agency, based at Goldsmiths, University of London. Working in the intersection of architecture, law, journalism, human rights and the environment, they investigate conflicts and crimes around the world, and are dedicated to solving crimes against civilians, in part by analysing architecture and landscapes based on the idea, and the awareness, that not only people but all matter has a memory, and that all memory is bound up with spatial perception. Forensic Architecture were nominated for the Turner Prize in 2018 and took part in Documenta 14. They recently participated in the 12th Berlin Biennial and are currently exhibiting at HKW in Berlin & Tensta Konsthall in Stockholm.

Ben Grosser creates interactive experiences, machines, and systems that examine the cultural, social, and political effects of software. His exhibition venues include Eyebeam in New York, Somerset House and the Barbican Centre in London, Centre

Pompidou in Paris, SXSW in Austin, Museum Kesselhaus in Berlin, Science Gallery in Dublin, and the Japan Media Arts Festival in Tokyo. He is an associate professor of new media at the University of Illinois and an Assembly Fellow with the Institute for Rebooting Social Media at the Berkman Klein Center for Internet and Society at Harvard University.

Libby Heaney is a London based artist, who works across moving image, performance, installation, sculpture and print, usually combining these with advanced technologies such as machine learning, game engines & quantum computing. Often drawing on surrealism and dada, Heaney's interest lies in disrupting categories and hierarchies and moving instead towards a radical interconnectedness, hybridity and a slimy belonging of both humans and non-humans. Heaney is widely known as a pioneer of using quantum computing in art. Solo exhibitions include arebyte Gallery, London; Light Art Space, Berlin (2022); Holden Gallery, Manchester; and Emmanuel Church, Radar Loughborough, Loughborough University (2021); and group exhibitions include Gwanghwa Square Mediafacade, Seoul; Ars Electronica, Linz; Zabludowicz Collection, London; Re:publica Festival, Berlin; Mimosa House, London; HMKV, Dortmund; ZKM, Karlsruhe (2022).

Joey Holder is concerned with a sense that 'everything has become a branch of computer science.' Her artwork is fuelled by continued dialogue and collaborations with researchers & practitioners from varied fields including computational geneticists, marine biologists, behavioural psychologists & investigative journalists. She has exhibited at the Harvard Museum of Natural History, Athens Biennale, Design Museum, Moscow Biennale, Transmediale & Venice Biennale. She is the Director of SPUR, an online platform which supports digital practice, Director of Chaos Magic, an arts project space in Nottingham; and represented by Seventeen, London.

Yuri Pattison connects and materialises the intangible spaces between the virtual and physical through video, sculpture, installation and online platforms. His work explores how new technologies such as the digital economy and online communication have shifted and impacted the systemic frameworks of the built environment, daily life, and our perceptions of time, space and nature. Selected recent exhibitions include Radical Landscapes, Tate Liverpool; Post Capital, Kunsthal Charlottenborg, Copenhagen (2022); The engine, Douglas Hyde Gallery, Dublin (solo); One Escape at a Time, 11th Seoul Mediacity Binnale, Seoul; No Linear Fucking Time, BAK, Utrecht; Proof of Stake – Technological claims, Kunstverin in Hamburg, Hamburg; The Ocean, Bergen Kunsthall, Bergen, Norway; and TECHNO, MUSEION, Bolzano, Italy (2021).

Philippa Williams is a Reader in Human Geography at Queen Mary University of London where she is also director of the Digital Lives Programme and a fellow of the Digital Environment Research Institute. Philippa's research is animated by everyday digital and political life in India and the UK. She was awarded the Philip Leverhulme Prize (Geography 2019) and is co-authoring her next book, 'Privacy Techtonics: Digital geopolitics, WhatsApp and India' with Lipika Kamra.

Acknowledgements

This collaboration came out of a lift at Heathrow airport. Candice and Philippa crossed paths at Level 3, Terminal 4 and a fantasy plan was exchanged to explore the intersection of art practice and research on digital technologies. That conversation was converted into reality thanks to funding from the Faculty of Humanities and Social Sciences Collaboration and Strategic Impact Fund at Queen Mary University of London 2021/2 and support from the Leverhulme Trust.

We are also very grateful to the Broadway Gallery, Nottingham and Lee Nicholls for welcoming its take-over by OTOKA for the exhibition with support from Near Now. Near Now is an Arts Council England National Portfolio Organisation and Broadway's studio for arts, design and innovation, working nationally with pioneering artists to create bold new work and drive innovation through use of emerging technologies, helping develop and showcase the skills of Nottingham's growing arts and tech community.

Huge kudos and thanks to designer, Matt Woodham for the OTOKA web design and online exhibition and to Ryan Boultbee and William Harvey of Frameworks for Practice for constructing the exhibition iterations irl. Finally, our thanks to the artists and writers for so generously showing and sharing their work in this exhibition and reader.