Everyday Surveillance

Pam Briggs
PaCTLab
Northumbria University
Newcastle upon Tyne
p.briggs@unn.ac.uk

James Nicholson
PaCTLab
Northumbria University
Newcastle upon Tyne
James.nicholson@unn.ac.uk

Elizabeth Churchill
ACM
New York
New York
churchill@acm.org

Gary W Pritchard
Open Lab
Newcastle University
Newcastle upon Tyne
gary.pritchard@ncl.ac.uk

Mark Levine
Dept. of Psychology
Exeter University
Exeter
M.Levine@exeter.ac.uk

Patrick Olivier
Open Lab
Newcastle University
Newcastle upon Tyne
p.l.olivier@ncl.ac.uk

CHI'16 Extended Abstracts, May 7–12, 2016, San Jose, CA, USA.
ACM 978-1-4503-4082-3 /16/05.
http://dx.doi.org/10.1145/2851581.2856493

Abstract
Surveillance, literally the 'close watching over' of a person or a group, was historically carried out to monitor adversaries and criminals. The digital era of sensor-rich, connected devices means that new forms of everyday surveillance – what some are calling '*dataveillance'* – are emerging. These are changing the power structures that link people, businesses and governments. In this multidisciplinary, one day workshop, we seek to rethink and understand everyday surveillance practices, asking: what are new forms of surveillance that accompany developments in Big Data and the emerging Internet of Things; what are the anticipated and unanticipated effects of a surveillance culture; how does surveillance need to be (re)configured in order to empower the citizen or contribute to social good? We will ask who 'owns' the data that arises from these everyday acts of surveillance and what can result from rethinking these ownership models. We will consider the role and place of research in surveillance data collection and analysis.

Author Keywords
Connected living; Internet of Things; tracking; logging; Big data; ethics; surveillance; dataveillance; trust; citizenship

ACM Classification Keywords
H.5.3 Information interfaces and presentation: Web-based interaction; Collaborative computing; K.4.1 Public Policy Issues: Ethics, Privacy

Background
Surveillance was the term traditionally used to describe the monitoring of activities and behaviour 'from above'. It reflected a traditional power model in which surveillance could be used to engineer a particular kind of behaviour, perhaps best captured in Jeremy Bentham's 'panopticon' model. Surveillance is usually understood as an adversarial practice, however, other forms of surveillance practices exist and the landscape is becoming more interesting. In this workshop we will explore new digital surveillance practices incorporating data-logging, tracking, crowd-sourcing, self-monitoring and peer-sharing before going on to a consideration of the societal and research value of these different forms of surveillance data.

Audience
This workshop should appeal to a wide range of researchers, designers and practitioners interested in citizen-led approaches to the governance of personal data.

Goals
The goals of the workshop are thus: (i) to reach a better understanding of the different dimensions of digital surveillance in everyday practice; (ii) to consider the design factors that underpin intended and unintended consequences of surveillance; (iii) to ask how these design factors can be used from the outset to create acceptable surveillance practices and (iv) to articulate the research value of surveillance data.

Adversarial surveillance practices
Digital surveillance first developed with the widespread deployment of CCTV and this practice continues with over 30 million surveillance cameras in the US and an estimated 4.2 million in the UK – one for every 14 people. The gradual move to a more pervasive *digital* surveillance has been accompanied by the monetization of surveillance, primarily via data brokers whose capacity to aggregate information across large datasets has been a cornerstone of the Big Data movement (Pfleeger, 2014).

Mass Surveillance
There has been much discussion in relation to the ethics of surveillance and the privacy rights of the individual citizen. It is certainly the case that machine learning and automated techniques of various kinds has removed some of the costs of surveillance, such that everyone can be subject to scrutiny – a situation liable to be exacerbated by new developments in relation to Big Data and the Internet of Things (IoT). To take just one example, according to recently leaked documents, the UK government abandoned a strategy of targeted tracking of online activities in favour of a more general 'as many people as possible' from 2007, leading to 50 billion metadata records being collected every day in 2012 (Gallagher, 2015). Such changes in the means and purposes of surveillance have created a landscape in which the costs and benefits of various surveillance practices are poorly articulated.

Activism and sousveillance
The monitoring of activities and behaviours 'from below' is described a *sousveillance* – a term that relates to the activities of individual citizens who can act collectively in documenting and sharing malpractice by those in

authority. Again, this can be seen as an adversarial practice designed to 'correct' behaviour. For example, this form of 'inverse surveillance' can help to identify police aggression, electoral malpractice or even be used to highlight neighbourhood problem areas and use documented evidence as cues for local government action. But sousveillance is another practice that is changing – in this case, largely because of the improved photojournalism capabilities of the smartphone. The rise of citizen journalism provides one example which has led to the mass dissemination of police brutality via social media networks such as *Berkeley Cop Watch* and *Cop Block* – both supported by websites that help individuals understand their rights.

Note too that the 'watching from below' is not always targeted on those in power. A number of high profile attempts have been made to harness the potential for crowd-sourcing the interpretation of surveillance video including the monitoring for evidence of illegal immigration, via a video feed from the US/Mexico border (Tewksbury et al, 2012). More recently Internet Eyes attempted to commercialize this idea by aggregating CCTV feeds from grocery stores and distributing them on their site. These two platforms attempted to open CCTV to the masses not with the aim of inclusion, but rather for economical gain (i.e. bypassing the salaries of trained surveillance monitors). A development which raises interesting questions about citizen-centric policing and vigilantism.

Employee surveillance

Employee monitoring encompasses the act of watching and monitoring employees' behaviour and performance during the working day. Digital technology has made such practices more common – effectively introducing an 'electric panopticon' (Bain and Taylor, 2000) presumably implemented in the hope that, with constant yet covert surveillance, employees will become more compliant. This can backfire in a number of ways, however. For example, workplace monitoring practices can adversely affect staff morale and can lead to unintended, unproductive or malicious consequences (Zweig and Webster, 2002). The idea of a workplace panopticon has also been tied to the introduction of Location Based Systems (LBS) that can prove beneficial to vulnerable individuals such as lone workers and which can also improve company performance – for example improving driving and reducing fraud in taxi companies (Ge et al, 2011). However these practices are also associated with unforeseen changes to time-management, workload and morale (Prichard et al., 2014).

Non-adversarial surveillance practices

Peer surveillance

Digital developments have also given rise to the process of peers 'watching each other' in a process described variously as *'veillance'; 'lateral surveillance'* (Andrejevic 2005) or '*social surveillance'* (Marwick, 2012). These developments sit alongside other initiatives such as crowdsourcing, reputation systems, peer-to-peer healthcare and citizen journalism and together they typify the trend for lay people to exchange useful 'observational' data with each other on a massive scale. Thus friends keep each other updated with shared locations, photos or videos documenting their daily lives, with recent examples including the video streaming app Periscope, which allows live video sharing. Note that the initial purpose of the app was for instant capture of real-time developing news (e.g. protests) but has the potential to be turned into a small-scale private surveillance platform.

Again, we can see a darker side - peer sharing can give rise to various forms of peer shaming and digital bullying. One example is the case of the Dog-poo girl (Krim, 2005), where a woman refused to clean up after her dog messed a subway carriage. A bystander subsequently posted a picture online, leading to a public apology after days of press coverage and online ridicule. Although meant as a means of discouraging anti-social behaviour, this could also be seen in terms of a social witch-hunt, allegedly leading the woman to contemplate suicide.

Self-Surveillance

We have also seen the rise in popularity of self-surveillance – also known as self-tracking or the Quantified Self Movement. Individuals who partake in these activities use applications to record everyday data, including diet information (MyFitnessPal), exercise diaries (Fitbit, DailyBurn), running sessions (RunKeeper), location information (Saga, FourSquare), sleep diaries (SleepCycle), mood (MoodPanda) and even music listened to (last.fm). The purpose for tracking all information varies across individuals but generally involves receiving immediate feedback for self-improvement (e.g. losing weight).

This self-generated data can be then pooled within an established or emerging social circle, and this group can then be used as a form of 'social cure' to help an individual maintain healthy behaviour. The social crowd can thus be harnessed as a motivating force for good (Sillence et al., 2015). Such developments sit within a new paradigm for the 'Social Internet of Things, where the things we surround ourselves with can be intelligently sensed and networked. Consider, for example, the kinds of elective social sharing of health information that takes place on PatientsLikeMe and imagine that the everyday health devices used to support this information sharing (thermometers, blood pressure monitors, scales) could upload information automatically. Certainly there could be some interesting gains in epidemiology and the large scale assessment of treatment efficacy, but we can see some interesting new challenges emerging around privacy and trust in such peer exchange.

Surveillance of the most vulnerable

Finally we might think of a class of *benevolent* forms of surveillance in regard to protecting the most vulnerable members of society. Again, we find that this is by no means a simple moral landscape. We can illustrate this point with reference to smart home developments in the social care of our oldest old, where sensor based means of monitoring older adults in a smart home can detect early functional impairment. For example, Lee and Dey (2015) used a range of ubiquitous sensors ('dwellsense') to collect a set of surveillance measures that could be used for patient care and decision-making while sensors embedded in a mattress or worn around the wrist can be used to detect a range of physical and mental health problems in older adults. While the benevolent intent is clearly here in such developments, we must remember that there is also an economic imperative to such developments and that sometimes sensor technology is being employed simply to save money.

The research value of surveillance data

When surveillance is an object of study, it has traditionally been with a highly critical eye. For example, researchers explore surveillance as a threat to privacy and civil liberties. They also attack the utility of surveillance – that it doesn't do what it claims and can actually have counterproductive consequences.

These stories are often told about the rise of CCTV surveillance and its domination of public spaces (particularly in the UK but increasingly across the world). Indeed the British Government's own research shows that CCTV has little impact against violent disorder – and its presence does not reassure citizens that they are in safe spaces. However, if we turn from thinking about surveillance as a threat, to thinking about surveillance as a resource, can we recover positive social benefit from surveillance technologies? What are the implications of seeing surveillance data as a resource? Participants (mostly) don't consent – in the CCTV case they often don't know they have been captured on camera and we are still developing the ethical principles that can govern our analysis of shared communication data. Can we improve on our ability to determine the nature and context for ethical use of surveillance data given with or without explicit consent?

Organizers

Professor Pam Briggs (Northumbria University): Pam has a Research Chair at Northumbria University and is Visiting Professor at Newcastle University's Open Lab. Pam is interested in new forms of digital identity management – work which addresses some of the more playful identity experiences in social media but also considers the darker side of privacy management, identity theft, identity profiling and social sorting. As part of this work she has also investigated the privacy issues in the use of LBS tracking technologies. Pam also has a strong research profile around the peer sharing of health information – asking questions about when and why we disclose sensitive information to others but also asking what health benefits accrue from this disclosure.

Dr. Elizabeth Churchill (Google): Currently a Director of User Experience at Google, Dr. Elizabeth Churchill is an applied social scientist working in the area of human computer interaction, mobile/ubiquitous computing and social media. Prior to working at Google, Elizabeth formed and managed the Human Computer Interaction research group at eBay where she looked at the use of user data for optimizing personalization algorithms for content recommendation. She is currently working on infrastructures for connected living, focusing on security and trust, and is completing a book introducing concepts in large-scale experimentation for designers.

Professor Mark Levine (University of Exeter): Mark is a Professor of Social Psychology and Head of Psychology at Exeter University. His research explores identities and group processes in pro-social and anti-social behavior. He is particularly interested in the research possibilities afforded by new technologies and digital data. This includes a systematic behavioural analysis of CCTV footage of real life nighttime violence in British town centres. He also uses virtual environments to study bystander behaviour in violent emergencies. Most recently he has used natural language processing of online data to explore how group processes shape privacy attitudes and behaviour. He is also interested in how tracking and sensing technologies can be used to explore social cohesion and intergroup relations amongst humans and between humans and robots.

Dr. James Nicholson (Northumbria University): James is a Senior Research Associate at PaCT Lab (Northumbria University) and a Visiting Researcher at Open Lab (Newcastle University). He is interested in novel applications of CCTV platforms and footage, as well as methods of including people in the online surveillance

process (e.g. crowdsourcing, open-circuit television). James has also explored the motivations behind watchers of CCTV and interfaces for improving the task

Dr. Gary Pritchard (Newcastle University): Gary is a Research Associate at Open Lab, where he brings a sociological perspective to the group's HCI research. He employs ethnographic and other qualitative methods to his work with specific experience relevant to this workshop of a long-term study on the surveillance technologies on London's bus network. This project looked at how telematics and LBS are employed to record and appraise driving remotely and showed how the introduction of digital payment created emotional stress and fears of state surveillance by passengers.

Professor Patrick Olivier (Newcastle University): Patrick Olivier is Professor of Human-Computer Interaction and founder and leader of Open Lab, Newcastle University's center for cross-disciplinary research in digital technologies (formerly Digital Interaction at Culture Lab). He is an expert in human-centered ubiquitous computing and is also active in other areas in HCI, including interaction design methods and applications, interaction techniques, social computing and usable security. Patrick leads Newcastle and Northumbria University's digital civics research initiative, and is particularly concerned with technologies and services that reframe the relationship between the citizen and government, including civic activism, grassroots service commissioning, and open government.

Website

The website www.everydaysurveillance.com will be used prior to the workshop for hosting the call for participation as well as more details about the workshop. Information about the organizers will feature on the website. Once the position papers have been accepted, they will be made available on the website for participants to view prior to attending the workshop. The schedule will also be posted once finalized. All materials created during the workshop and in its follow-up activities will be made available on the website.

Pre-Workshop Plans

We will send invitational emails to key distribution lists (e.g., CHI-announce, British HCI) and share a high level summary of the workshop through social media platforms blogs and email, and make contact with representative organizations (e.g. the UK Home Office, Facebook, Google, PatientsLikeMe; Electronic Frontier Foundation), as well as interested research groups and meet-ups (e.g., Quantified Self).

Workshop Structure

At the core of the workshop is discussion of key topics, with the outcome of an action plan for future research collaboration and an agenda for CHI relevant research. Outcomes might include a future track at CHI focused on Personal Data, Dataveillance and/or Human Data Interaction. This will be a discussion-focused workshop and not a presentation-focused one. As much as possible we will focus on current technologies, but will also reflect on the emerging technology landscape and conduct a review of current and emerging stakeholders. Participants will be asked to bring a provocation that captures the content of their paper but is not expected to be simply a slide presentation of it. Thus, films, artifacts and stories will be used to capture each participant's position.

9:00-9:15am: Welcome, introduction to the organizers, and overview of the schedule
9:15-10:00am: Quick introductions. Brief review of what each participant is bringing to the table
10:00-10:30am: Generating themes, collation of interesting resources & case studies, creation of framework for discussion (goal i)
10:30-10:45am: Coffee break
10:45-12:00pm: Break out discussions (goal ii)
12:00-12:30pm: Team project initial presentations to include 3-min lightning talks, feedback and Q&A
12:30-2:00pm: Lunch break
2:00-3:30pm: Break out groups discuss design issues for surveillance, with examples (goal iii)
3:30-3:45pm: Coffee break 2
3:45-5:00pm: Discussion of research value of surveillance data (goal iv)
5:00-6:00pm: Wrap up and poster creation/layout
6:30pm-8:30pm: Informal dinner in a nearby restaurant where discussions can continue

Our planned activities for participants involve consideration of the different types of surveillance practices we have identified. Sample videos will be searched on Youtube and other video platforms and participants will discuss the qualitative differences of each type, for instance the power-dynamics at play and the beneficiaries and casualties of each. We will then consider the nature of digital surveillance in each of these examples. Finally, we will ask each group to design a digital platform for each of these surveillance categories while complying to randomly assigned measures (privacy-preserving, data maximisation, speed of implementation, cost). Once the platform is designed, the groups will be asked to modify their design to comply with all four measures. Each group will present their original and modified designs to the whole workshop, where will facilitate further discussions on the potential for unintended social and economic consequences and ethical violations.

Post-Workshop Plans

We will publish a report on our website alongside the accepted position papers and make available a poster summarizing the main take-away messages in visual form on our website. A slide-deck will be created and made available on our website and on Slideshare (or similar service) to use in teaching.

We will discuss the appetite for either a special issue or edited book, but also talk about tangible outcomes in terms of key audiences and the formats and platforms for those audiences (e.g. the importance of blogging in cybersecurity dissemination).

Call for Participation

The aim of this workshop is to bring together researchers and practitioners to rethink and understand everyday surveillance practices. Topics include: new forms of surveillance that accompany developments in Big Data and the Internet of Things; self and peer surveillance via data-logging and wearable sensors; the anticipated and unanticipated effects of a surveillance culture; reconfiguring surveillance so as to empower the citizen or contribute to social good.

We invite interested researchers to submit a 2-page position paper in CHI ACM Extended Abstract Format relating to any of the topics identified above or related themes, e.g. novel ways of implementing surveillance platforms, the ownership of surveillance data, or the role of research in data collection and analysis. The

deadline for submissions will be 12th January 2016 and at least one author of each accepted position paper must attend the workshop and register for one day of the conference.

Accepted position papers will be published on the workshop website prior to the start of the event for attendants to read and we will also discuss a published output. The workshop will involve participants bringing examples of surveillance data in order to develop a new theoretical framework with which to consider surveillance. We will also discuss the requirements for new research and design tools and methodologies for surveillance data. For more information please visit the workshop website at www.everydaysurveillance.com. Please direct queries and paper submissions to person (first.last@organisation.ac.uk).

References

1. Mark Andrejevic. 2005. The Work of Watching One Another: Lateral Surveillance, Risk, and Governance. *Surveillance & Society* 2(4): 479–497
2. Peter Bain and Phil Taylor. 2000. Entrapped by the 'electronic panopticon'? Worker resistance in the call centre. *New Technology, Work and Employment* 15, 1: 2-18.
3. Ryan Gallagher. 2015. From Radio to Porn, British Spies Track Web Users' Online Identities. Retrieved October 6, 2015 from https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/
4. Yong Ge, Chuanren Liu, Hui Xiong, and Jian Chen. 2011. A taxi business intelligence system. In *Proceedings of SIGKDD 2011*, 735-738.
5. Jonathan Krim. 2005. Subway Fracas Escalates Into Test of the Internet's Power to Shame. Retrieved October 6 from http://www.washingtonpost.com/wp-dyn/content/article/2005/07/06/AR2005070601953.html
6. Matthew L. Lee, and Anind K. Dey. 2015. Sensor-based observations of daily living for aging in place. *Personal and Ubiquitous Computing* 19(1): 27-43.
7. Alice Marwick. 2012. The public domain: Surveillance in everyday life. *Surveillance & Society* 9(4): 378-393.
8. Shari Lawrence Pfleeger. 2014. The Eyes Have It: Surveillance and How It Evolved. *Security & Privacy, IEEE* 12(4): 74-79.
9. Gary W. Pritchard, Pam Briggs, John Vines, and Patrick Olivier. 2015. How to Drive a London Bus: Measuring Performance in a Mobile and Remote Workplace. *In Proceedings of the ACM Conference on Human Factors in Computing Systems (SIGCHI)*.
10. Elizabeth Sillence, Claire Hardy, Pam Briggs, and Peter Richard Harris. in press. How do carers of people with multiple sclerosis engage with websites containing the personal experiences of other carers and patients? *Health Informatics Journal*.
11. Doug Tewksbury. 2012. Crowdsourcing Homeland Security: The Texas Virtual BorderWatch and Participatory Citizenship. *Surveilance and Society* 10, 3/4: 249–262.
12. Michael Workman. 2009. A field study of corporate employee monitoring: attitudes, absenteeism, and the moderating influences of procedural justice perceptions. *Information and Organization* 19: 218-232.
13. David Zweig and Jane Webster. 2002. Where is the line between benign and invasive? An examination of psychological barriers to the acceptance of awareness monitoring systems. *Journal of Organizational Behaviour* 23: 605-633.