Crowdsourcing and Cloudsourcing CCTV Surveillance

Burkhard Schafer

Crowdsourcing and cloudsourcing CCTV surveillance

While the continuing proliferation of CCTV surveillance is a cause for concern, its impact on privacy has in the past been mitigated by certain natural limitations on the way CCTV systems operate in practice. In particular, the increased quantity of surveillance data has not been matched by a similar increase in our ability to process and evaluate it. This paper compares different models of technology enabled analysis of CCTV footage, with a focus on the emerging trend of crowdsourced CCTV analysis: In the world of crowdsourced surveillance, "Big Brother is us".

1 The Return of the Native

In 2009, I reported in my first ever contribution for DuD on the continuing love affair of the British government, British police and also the wider British public with CCTV surveillance.[1] A year earlier, and Marie-Theres Tinnefeld and Judith Rauhofer had analysed in this journal the legal and ethical implications of another aspect of surveillance that is more prominent in the UK than in (contemporary) Germany, the involvement of the wider public as "crime spotters", or "sensors" of the surveillance society.[2] Indeed, from the old fashioned "Neighbourhood watch" to the ubiquitous anonymous telephone helplines offered by the police for informing on all types of social ills, from benefits cheats to suspected terrorists, no analysis of surveillance in the UK would be complete without also discussing the role of citizen involvement in surveillance activities. Long before the term was coined in 2006 by Wired magazine writer Jeff Howe, "crowdsourcing" of surveillance played a crucial role in the UK's crime detection and deterrence strategy. This paper will bring these two ideas together, by analysing the privacy implications of a new technology assisted "business model" for the analysis of CCTV data that relies on members of the public to monitor and analyse the feed of CCTV cameras. It will argue that some of the existing legal and technological limitations of privacy intrusion through CCTV are rendered moot in this approach, raising some important legal-conceptual questions on the regulation of surveillance technology.

The idea that participating in surveillance constitutes a civic virtue is by no means restricted to the UK. As we will see, Canada and the US too have promoted the civic aspect of surveillance as crime deterrent. Rauhofer and Tinnefeld argued that the different attitude to citizen-led surveillance in the UK and Germany can be explained by the experience with the abuse of informer systems under both, the Nazi regime and the GDR. Social acceptance of informers, so their thesis, is more acceptable in societies where the social contract between government and citizenship has never resulted in manifest abuse, posing inherent cultural challenges for any attempt at top-down legal harmonisation of privacy regimes.

In a follow-up paper in this journal,[3] I indicated that while this is an important aspect of differences in attitude to surveillance, there is in addition another cultural trajectory that allows a more positive interpretation of the Anglo-American approach. From their perspective, the professionalization of policing in continental Europe is itself a potential threat to liberty, born from the centralist and autocratic approach to governance that merged the absolutist state with Napoleonic administration, and a system of a uniformed police that grew out of the military.[4] In these systems, the police acts as direct representative of the crown, and is imbued with special rights that other citizens do not have. From the UK perspective, the strict separation between a professional police and the citizenry is also indicative of the "Obrigkeitsstaat". By contrast, the historical narrative that we find in the UK, which provides a basis of the legitimacy also of the modern police, is intentionally juxtaposed to this continental European model. At its centre is the slow evolution of the police officer from voluntaristic, citizen-driven self-regulation to the "citizen in uniform" of today. Going back to the time before the Norman conquest, we find a "citizen proto-police" in the laws enacted by Alfred the Great. In particular, the pursuit of a suspect became a general obligation owed to the crown by all citizens, the law of "Hue and Cry".[5] Correspondingly, all citizens had a right to arrest a felon – the citizen arrest, based in common law and

[1] Schafer 'Schlafwandelnd in den Überwachungsstaat?' (2009) *Datenschutz und Datensicherheit* Vol. 8 pp 483-489

[2] Tinnefeld/Rauhofer, 'Whistleblower: Verantwortliche Mitarbeiter oder Denunzianten? Fragen im Feld von Ethikrichtlinien, des Datenschutzes und der Mitbestimmung" (2008) Datenschutz und Datensicherheit Vol. 32, No. 11, pp. 717-723

[3] Schafer. 'All changed, changed utterly? Privacy protection in post-Labour Britain' (2011) *Datenschutz und Datensicherheit* Vol 35 pp. 634-638

[4] In a similar vein on the cultural barriers to legal harmonisation see Legrand, "European legal systems are not converging." International and Comparative Law Quarterly 45.01 (1996): 52-81.

[5] Rawlings, Policing before the Police. In T. Newborn, Handbook of Policing, Wilan Publishing, Cullompton, (2009) p. 47-72

now codified under section 24A of the Police and Criminal Evidence Act 1984. Just how influential this system was on the attitude towards policing can be seen by the fact that more than 800 years later, "Hue and Cry" became the name of the first police gazette, first issued in 1772 by John Fielding, one of the driving forces behind the modern, professional police force in the UK. In modern terms, the Gazette was an early police Intranet – publishing mainly notices of wanted criminals with requests for information, including information about possible rewards.

2 A pair of blue eyes

In a society where every citizen had both the duty *and* the right to act in policing functions, professionalising the police and endowing officers with rights not held by other citizens was never going to be an easy task. Consequently, voluntarism remained a constant feature of policing in the UK, with a modern police force that evolved only slowly and gradually from community based (self)policing. At every step, widespread public distrust, together with powerful opposition from groups outside the capital and its political networks, had to be overcome.

After the Norman conquest, the office of "constable" was created, an official under the control of local magistrates. We find an early description of a constable in the writing of the medieval jurist Bracton:

> "In whatever way they come and on whatever day, it is the duty of the constable to enrol everything in order, for he has record as to the things he sees; but he cannot judge, because there is no judgment at the Tower, since there the third element of a judicial proceeding is lacking, namely a judge and jurisdiction. He has record as to matters of fact, not matters of judgment and law".

This means that the constable was lacking any powers a citizen would not also have, in particular no separate powers of arrest. From a surveillance perspective though, he was charged particularly with being the "eyes and ears" of the local court – though independent of the central government. For the centuries that followed, parish constables, part time, unpaid and typically elected by the local parishioners, dominate the scene of policing in the UK[6]. This system of elected, unpaid parish constables continued in England until the 19th century. It was only then, and again with considerable opposition from both lower class citizens (who feared that they were the main target of this development) and powerful gentry outside London, who feared a power grab by central government. The result was also, patchwork evolution of the citizen-proto officer to a professional police force. In London the Metropolitan Police was formed by the Metropolitan Police Act 1829, and outside London by the County Police Act 1839. However, this act only *permitted* counties to establish full-time professional police forces, it did not make it mandatory. To address widespread concern, these acts also made it clear that the new police was to be a police under the rule of law – with officers who did not necessarily have more powers than an ordinary citizen, but were held in the execution of these duties to a higher standard than the people they policed.

One particular reminder of the voluntaristic origin of the modern British police can be seen in the "special constable", citizens who volunteer to take on part time, unpaid police work. In the same year as a professional police force was finally created, Parliament also passed "An act for amending the laws relative to the appointment of Special Constables, and for the better preservation of the Police"[7]. In 1835 Special Constabulary was defined as a volunteer organisation. The modern special police constable finally was defined in law in World War 1 - with a special role at the time to protect water supplies from German infiltrators.[8]

While the historical accuracy of this "Sonderweg" of policing in the UK has to be treated with some care, it symbolic function for the understanding of the role of the police, and the source of its legitimacy, must not be underestimated. In popular understanding, policing in Britain has a dual aspect – the police officer is a mere "citizen in uniform", and conversely, every citizen is potentially an "officer in plain cloth". Both aspects are integral for ensuring that the police can't become an oppressive force – and cooperating with it, by e.g. on informing crime, is therefore not so much a collusion with an authority that is already conceptualised as juxtaposed to the ordinary citizen, but a way of ensuring that it remains rooted in the community it is meant to police. In the remainder of this paper, we will see how this duality plays out in the field of CCTV surveillance, a technology which can both undermine and reinforce this understanding of the legitimacy of the police.

3 Far from the Madding Crowd

While the continuing proliferation of CCTV surveillance is a cause for concern, its impact on privacy has in the past been mitigated by certain natural limitations on the way CCTV systems operate in practice. In particular, the increased quantity of surveillance systems has not been matched by a similar increase in our ability to process and evaluate the data that is generated by them. In Scotland alone, the number of CCTV cameras has trebled in the last decade, while the number of people employed to monitor them has remained stable. If we take an average system with 20 cameras providing around the clock surveillance, a staggering 480 hours of video footage or 43 million images are created every single day.[9] This creates considerable costs in personnel, as the number of screens that can be effectively monitored by one person is limited. While best practice would require not more than two screens per individual at any given time, some have had one operator responsible for more than 50 screens on a 12-hour shift.[10] As a result, many cameras are not monitored at all, even when the

[6] Guth, (1994). "The Traditional Common Law Constable, 1235-1829: From Bracton to the Fieldings to Canada". In Macleod, R.C.; Schneiderman, David. *Police Powers in Canada: The Evolution and Practice of Authority*. Toronto: University of Toronto Press

[7] http://www.policespecials.com/history.html

[8] Gill,/ Mawby, (1990). *A Special Constable: a study of the police reserve*. Aldershot: Avebury

[9] Surette, R. (2005) "The thinking eye: Pros and cons of second generation CCTV surveillance systems", Policing: An International Journal of Police Strategies & Management, Vol. 28 Iss: 1, pp.152 - 173

[10] Clarke (1994), "Blind eye on the street?", *Police Review*, August, pp.29-39.

technological ability exists.[11] In addition, a significant number of cameras is operated by private individuals, typically shopkeepers who install them mainly as a response to the demands by insurance companies. The quality of the images that are recorded is low, tapes are reused frequently, resulting in an implementation of the "right to be forgotten" by operational default, and most of the images are therefore never seen by a human eye. While the density of CCTV surveillance in the UK is higher than in any other country, counting the mere number of cameras paints therefore a misleading picture. Even CCTV with "man in the loop", where live feeds are transmitted to an adequately staffed operation centre, faces the problem that continuous surveillance of the data finds its limits in the human ability to cope with boredom and over-exposure to information. In this situation, the operator "sees" the individuals on screen, but loses the ability to identify or recognise them, or to categorise their behaviour correctly.[12]

Dealing with an ever increasing amount of data whose analysis is a highly repetitive, labour intensive task is a typical scenario for Artificial Intelligence solutions. If we can computationally model the analytic abilities of the best CCTV operator at his or her peak, we can replace human operators at least for the pre-processing of the material, leaving human judgements reserved for those situations that have been identified automatically as worthy of more detailed attention. This overcomes the limitations set by the storage and retrieval capacity of human memory and our low boredom thresholds. One approach to tackle the relative underuse of CCTV images has therefore been unsurprisingly the development of more intelligent image interpretation and data mining tools.

The earliest examples of AI enhanced CCTV surveillance modelled global properties of crowds, such as the density and flow of crowds of pedestrians in rail-stations during 'rush-hours'. A camera that "understands" for instance how a typical crowd moves after a train reaches the station can then alert a human operator when the actually observed movements vary from those predicted, for instance when a panic results in a sudden rush of bodies.[13] These techniques did not identify individuals, – rather, average properties of the typical crowd where modelled, just as the theory of idealised gases for instance models not the individual trajectory of molecules, but treats the gas as one single entity.[14]

Once the behaviour of a crowd is computationally captured, the logical next step is to contrast the behaviour of individuals against that crowd. A single person moving in the opposite direction from the main flow can be as much reasons for concern (e.g. a pickpocket, or a mother separated from her children) as an individual who stays much longer than the average person at the same place (indicating e.g. a drug dealer in a subway station). From this, the logical next step lead to the identification of individuals, and automated categorisation of their activities. Second generation CCTV will therefore have the ability to detect the presence of people, track individuals across multiple cameras, and to analyse individual behaviour. This should allow automated identification of wanted fugitives, identify automatically behaviour (an arm pointing perpendicular from the body at another person e.g. is a "red flag" for a robbery with a gun), and object recognition, e.g. when a person leaves a possible bomb behind in an airport environment.[15]

From a privacy perspective, this automated analysis of images is a double edged sword. On the one hand, it increases the utility of data, and with that also increases the possibility of its abuse. Police officers could for instance in principle query the data held cumulatively in the CCTV centres of a city so that the software first identifies the faces of participants at a lawful demonstration, and then traces back the journey they took to reach the demonstration, identifying in the process their home addresses, or where they dropped off their children for school.

On the other hand, automated data processing addresses one of the most frequent concerns found in the UK population, the inherent voyeurism of CCTV surveillance. While approving of CCTV in principle, concerns have been raised about human operators training the cameras on windows, restrooms, „funny" looking people, or certain parts of the (mostly female) anatomy. [16] The psychological effect of the „voyeuristic gaze"[17], rather than an intellectual concern about data misuse, features foremost in concerns about CCTV. This means also that the smaller the number of human operators, the less intrusive the technology is perceived to be.

There is a third, less discussed and more unexpected negative effect of CCTV surveillance. Criminological theories of crime reduction that focus on routine activities theories of crime emphasise the importance of "guardianship", informal social surveillance conducted by residents of shared public spaces.[18] CCTV is feared by some to reduce the incentive for citizens to exercise guardianship, by limiting their "stake" in public spaces.[19] As Groombridge and Murjui put it:

> "Instead of worrying about "Big Brother" watching them, the public may perceive that "big father" has sorted everything out."[20]

We have argued above that the UK police derives its legitimacy also from the notion of the citizen in uniform, and the policemen in every civilian. In the long run, loss of guardianship has therefore the potential to undermine this legitimating function. With this, finally, we can move on to a different model of using CCTV surveillance, one that puts the human element firmly back into the picture.

---

[11] Norris/ Armstrong, (1999), The Maximum Surveillance Society: The Rise of CCTV, Berg, Oxford, p. 210-211

[12] Davies,/ Thasen, (2000), "Closed circuit television: how effective an identification air?", *British Journal of Psychology*, Vol. 91 pp.411-26

[13] Velastin/Yin/ Davies/ Vicencio- Silva/ Allsop/ Penn, "Automated measurement of crowd density and motion using image processing," *7th Int. Conf. on Road Traffic Monitoring and Control, London,* 1994, pp. 127-132.

[14] Davies/ Velastin, (2005). A progress review of intelligent CCTV surveillance systems. *Proc. IEEE IDAACS*, 417-423; for a legal analysis see also Gerrit Hornung und Monika Desoi, "Smart Cameras" und automatische Verhaltensanalyse, Kommunikation und Recht, 153-158, März 2011.

[15] Davis, (2001), Real Time Computer Surveillance for Crime Detection, National Institute of Justice, Washington, DC

[16] a comprehensive analysis is in Surette, R. (1985), "Video street patrol: media technology and street crime", *Journal of Police Science and Administration*, Vol. 13 pp.78-85

[17] South, (1987), "The security and surveillance of the environment", in Lowman, J., Menzies, R., Pays, T. (Eds),*Transcarceration: Essays in the Sociology of Social Control*, Gower, Aldershot, pp.129-52.

[18] Cohen,/Felson, (1979), "Social change and crime rate trends: a routine activities approach", *American Sociological Review*, Vol. 44 pp.588-608

[19] Fyfe, (1996), "City watching: closed circuit television surveillance in public spaces", *Area*, Vol. 28 No.1, pp.37-46.

[20] Groombridge/ Murji, (1994), "As easy as AB and CCTV", *Policing*, Vol. 10 No.4, pp.283-90

4 A cloud of many-coloured idealities

In the previous section, we have seen a traditional AI approach for the problem of data overload. By modelling the skills of the best human CCTV operators, the aim is to make their expertise available if and when needed. While this approach to knowledge engineering gained prominence in the early days of the computer revolution, the emergence of the internet has made an alternative model available. Rather than building monolithic expert systems, it is now much easier, and often also much cheaper, to find all the needed expertise on the web, where it is furthermore often offered for free. We see this in Wikipedia, where people donate their time and knowledge for a collective endeavour, or in projects such as SETI at home, where participants donate processing power of their computers to analyse data from radio telescopes. "Crowdsourcing" and "virtual volunteering" are technology enabled methods to harness the contribution of large number of people, dispersed over a large geographic area, for shared goals. This can also result in a division of labour where boring or repetitive tasks are split up into smaller, more manageable parcels, for instance when proofreading scanned copies of works of literature for Project Gutenberg, or carrying out routine science work in the field of data analytics.[21] Jeff Howe's original definition of "crowdsourcing" is of interest in this context:

> "Simply defined, crowdsourcing represents the act of a company or institution taking a function once performed by employees and outsourcing it to an undefined (and generally large) network of people in the form of an open call. This can take the form of peer-production (when the job is performed collaboratively), but is also often undertaken by sole individuals. The crucial prerequisite is the use of the open call format and the large network of potential laborers."

As the definition shows, while the participation of the crowd can be on a volunteer basis, it is also possible to develop commercial business models based on this idea. This gave rise of a new job profile: the "clickworker" is self-employed, offers his services online and typically works together with many thousands of others on small parts of a larger project, co-ordinated by a computer.[22] One of the best known examples is Amazon's "Mechanical Turk", a name that also indicates that crowd sourcing sees itself indeed in the tradition of Artificial Intelligence research: the original Mechanical Turk was a (fraudulent) precursor of a robot capable of playing chess. Computer programmers co-ordinate through the Mechnical Turk the use of human intelligence to perform tasks that computers are currently unable to do, but which don't merit to employ full time staff. Clickworker.com is another such platform that provides a "virtual workforce, worldwide and on demand". Interestingly for our context, one of the jobs they offer is "Categorization and tagging of your video and audio content, as well as image materials."[23] The implications for the problem of data analysis from CCTV cameras should by now be obvious: rather than making the cameras more intelligent, disperse the monitoring task across as wide a crowd as possible. Because every observer only watches as much of the footage as he or she chooses, the problem of boredom and attention shift can be addressed. If the CCTV footage is streamed online, typically on a cloud based server, people from different time zones will monitor the footage, which enables around the clock coverage.

The idea to crowdsource the monitoring of CCTV streams online was pioneered in applications other than crime prevention or detection. TV nature programmes such as the BBC's "Autumnwatch" and wildlife publishers such as National Geographic began to provide life streams of webcam footage from cameras placed in the wild online. The potential of entertainment is often combined with more serious scientific purposes, as this approach can recruit an almost unlimited number of volunteers to monitor around the clock e.g. the nests of rare birds, and so help in their protection.[24] Even more unusual, though very British, are the "ghostcams" that have been installed in some of the UK's most "haunted houses". Again, the idea is to provide around the clock monitoring of these cameras on the web, on the off chance that they may spot an inexplicable phenomenon.[25] While not even the most ardent of animal rights advocates,[26] or advocates of post mortem personality rights for that matter, will be concerned about the privacy implications of these applications, their potential for surveillance CCTV did not remain unnoticed. After the London Riots in 2011, which also saw the use of social media as a means to organise large scale criminal activity, the Metropolitan Police showed that it was at least as comfortable with social media as the rioters. It used crowd-sourcing to identify people suspected of committing crimes during the events, developing a smartphone app that gives access to 2,800 CCTV images taken during the disorder in August. The app comes with several data mining features, and can for instance order images by location. The user of the free "Facewatch ID app can then send through an app functionality name and address of any person they identify to the police. Assistant commissioner Mark Rowley:

> "This is a great opportunity for the public to help us fight crime and bring those who remain outstanding to justice. My hope is that the two-thirds of Londoners who own smartphones will download this app, and help us identify people we still need to speak to. We need Londoners to browse through the app every week or so as new images will appear regularly. This is a fantastic way for Londoners to help us to fight crime."[27]

While this revival of the "Hue and Cry" in the age of social media only involved images of actual perpetrators, prescreened by the police, and in that sense not conceptually different from displaying images of wanted suspects in the

[21] Kanefsky/ Barlow/ Gulick. "Can distributed volunteers accomplish massive data analysis tasks." *Lunar and Planetary Science* 1 (2001)

[22] See e.g. Ickler, (2012). *Wertschöpfung durch webbasierte kollektive Intelligenz*. BoD–Books on Demand.

[23] http://www.clickworker.com/en/

[24] http://news.bbc.co.uk/1/hi/england/devon/7388767.stm

[25] An example, provided by a local council, is here: http://services.salford.gov.uk/ghostcam/ An Irish version, looking for leprechauns, here , http://www.irelandseye.com/leprechaun/webcam.htm

[26] It should be noted though that the webcam monitoring the pandas in Edinburgh zoo was recently switched ff to "ensure privacy during the 26hrs window were they can mate".

[27] http://www.bbc.co.uk/news/uk-england-london-18589273

above mentioned police gazette, other applications take the idea of crowdsourced, cloud enabled CCTV analysis a step further. In the aftermath of 9/11, Jay Walker, founder of Priceline.com proposed the „USHomeGuard" system.[28] Ordinary citizens would get paid $10 an hour to view CCTV footage from safety critical installations such as nuclear power stations or military installations, in particular at spots where no human activity is supposed to take place. Spotters have to register, and can then log on to view surveillance images. They would then vote "yes" if there was unusual activity, "no" if nothing was happening, and "maybe" in case of doubt. Every yes vote was circulated to a wider group of spotters. If enough also voted yes, an auto alert was generated. Randomly inserted fake images keep the spotters alert and quality controlled. While this proposal ultimately failed to garner enough support from the owners of the CCTV installations, more recently a similar approach was implemented at the border between Texas and Mexico, to combat drug smuggling and illegal immigration. The "Texas Virtual Border Watch Program", an initiative by a group of sheriffs from border towns, provided streaming CCTV footage, both day and night vision, on a cloud based server, to enable the public to report suspicious activity via e-mail.[29] Unlike HomeGuard, the challenges for the spotters here is to distinguish suspicious from legitimate behaviour, as the cameras would routinely also film innocent third parties crossing the border. According to one of the activists behind the system, more than 43,000 people logged on to BlueServo.net, the website hosting the footage in the first month alone, "donating" some of their free time scanning streaming video of border hot spots and acting as what the Web site calls "Virtual Texas Deputies." However, after initial enthusiasm, the project was abandoned when it became clear that data quality was in insurmountable problem – including a suspicion that criminals were using the technology to predict police raids.

Undeterred by this experience, the UK too moved from CCTV to OCTV, the Open Circuit TV, in a pilot scheme in Shoreditch, London. Residents were able to watch CCTV cameras on a special TV channel, a project that proved so popular with residents that it gave rise to new commercial ventures. One of these is "Internet Eyes". Presented as an 'event notification system', companies that subscribe to the scheme provide CCTV footage from their security cameras. Internet Eyes then act as a broker between the companies and people willing to look for a few minutes or hour at the footage, not unlike the clickworker businesses described above. While the US systems combined an appeal to patriotism with some financial incentive, the UK approach relies on financial incentives together with the "gamification" of reality[30] - 'players' not only earn £10 for every correct alert, they also earn points for spotting suspected crimes and lose points for false alarms. Correct identifications earn the player an entry into the monthly prize draw for up to £1000. The website of Internet Eye contains a reference to the relevant data protection legislation: it states in particular that "Payment of the membership fee helps prevent misuse of the system and acts as a barrier to entry to stop voyeurism. Internet Eyes Ltd. has therefore established a rewards policy as outlined below so that membership fees and more can be returned to Viewers."

This approach seem to have been successful. Even though Internet Eyes was referred to the Data Commissioner, only a caution was issued when one of the videos was uploaded by a spotter to YouTube. The business model itself remained untouched. We can now see how new technologies do indeed disrupt traditional legal concepts, creating normative problems in their wake. Neither HomeGuard nor Internet Eye *publishes* CCTV footage on the web – that would be illegal. Instead, they *hire* deputies (US), self-employed clickworkers or indeed employees (UK) to process the data on behalf of the data controller. Since this serves the original function for which the data was collected – crime prevention – and might furthermore be necessary in the light of the data processing problems discussed above, this remains formally permissible. However, this data protection regimes is premised on the idea that there is a de-facto difference between the public and the data processors, the inside of a company charged with a specific task, and the wider world. Crowdsourcing and clickworking calls this inside-outside distinction into question, and thus undermines the normative ideal of the law. In a world where it takes just the click of the mouse to become "employed" by a company, the distinction between employee and public, inside and outside world all but collapses.

However, it would also be problematic to analyse this as just another failure of the DO regime that can be addressed through legislation. As I argued in the introduction to this paper, the notion of the deputy/special constable as civilian in aid of the police, or the idea of a civic duty to act as a police officer in times of need, not just to assist them are deeply imbued in the common law "mentality". What looks for the continental observer as just another attempt to play fast and loose with private can therefore on closer inspection also been seen as an emancipatory act that establishes ownership of public spaces, and therefore wrestling authority *away from* the formal police. Harmonisation through EU directives, or so I argued, finds its limits when fundamental, historically mediated and contradictory value judgements of this type are involved.

5 Life's little Ironies

As we have seen, there is something deeply ironic about the role of CCTV as a surveillance tool. From the fear of a loss of guardianship and abdication of duties to Big Brother, OCTV , Open Circuit TV and the technologies that underpin it facilitate a return of a pre-modern policing model, where everybody is a police officer, and the "Hue and Cry" of old becomes the "Look and notify" of the internet age. There is one final irony though. While I argued that European Union laws find their limitations when running against deeply held cultural differences, regulation through technology remains a viable option to protect privacy. Privacy Enhancing Technologies in turn can benefit from the crowdsourcing paradigm just as much as surveillance technologies do. While some people may find it satisfactory to watch CCTV footage from supermarkets to look out for shoplifter, we could harness the same instincts for privacy protection – for instance by volunteering to obfuscate

[28] http://www.wired.com/wired/archive/11.06/start.html?pg=11

[29] http://thelede.blogs.nytimes.com/2009/03/26/thousands-sign-up-for-virtual-border-patrol/

[30] Huotari/ Hamari. 2012. Defining gamification: a service marketing perspective. In Proceeding of the 16th International Academic MindTrek Conference (MindTrek '12). ACM, New York, NY, USA,

images of faces on Google Earth, another technology where the amount of data created presents problems for traditional methods of processing. Using crowdsourcing for privacy protection is as a research field still in its infancy. Amazon's Mechanical Turk mentioned above has been used for studies to help us better understand privacy risks.[31] The ambivalent nature of crowd sourced privacy threats and crowd sourced privacy protection has also been discussed for crowdsroucing surveillance in the field of environmental protection.[32] So far, the most adventurous use of the crowd for privacy protection is made in the field of testing PETs. Here, our paper comes full circle, with systems that protect us from the prying eye of CCTV cameras subject of crowdsourcing evaluation and enhancement studies.[33] Whatever the outcome of these studies is, neither privacy advocates not surveillance experts can overlook any longer the technological, social and political dimension that crowd sourcing technologies have brought to the field.

Literatur

Clarke, M. (1994), "Blind eye on the street?", *Police Review*, August, pp.29-39.

Cohen, L., Felson, M. (1979), "Social change and crime rate trends: a routine activities approach", *American Sociological Review*, Vol. 44 pp.588-608

Davies, A. C., & Velastin, S. A. (2005). A progress review of intelligent CCTV surveillance systems. *Proc. IEEE IDAACS*, 417-423; for a legal analysis see also Gerrit Hornung und Monika Desoi, "Smart Cameras" und automatische Verhaltensanalyse, Kommunikation und Recht, 153-158, März 2011.

Davies, G., Thasen, S. (2000), "Closed circuit television: how effective an identification air?", *British Journal of Psychology*, Vol. 91 pp.411-26

Davis, L. (2001), Real Time Computer Surveillance for Crime Detection, National Institute of Justice, Washington, DC

Fyfe, N. (1996), "City watching: closed circuit television surveillance in public spaces", *Area*, Vol. 28 No.1, pp.37-46.

Gill, M. L., & Mawby, R. I. (1990). *A Special Constable: a study of the police reserve*. Aldershot: Avebury

Groombridge, N., Murji, K. (1994), "As easy as AB and CCTV", *Policing*, Vol. 10 No.4, pp.283-90

Guth, D J. (1994). "The Traditional Common Law Constable, 1235-1829: From Bracton to the Fieldings to Canada". In Macleod, R.C.; Schneiderman, David. *Police Powers in Canada: The Evolution and Practice of Authority*. Toronto: University of Toronto Press

Ickler, H. (2012). *Wertschöpfung durch webbasierte kollektive Intelligenz*. BoD–Books on Demand.

Kai H. and Juho H. (2012) Defining gamification: a service marketing perspective. In Proceeding of the 16th International Academic MindTrek Conference (MindTrek '12). ACM, New York, NY, USA,

Kanefsky, Bob, Barlow, N. and Gulick, V. (2001) "Can distributed volunteers accomplish massive data analysis tasks." *Lunar and Planetary Science* 1

Kelley, P. G. (2010). Conducting usable privacy & security studies with amazon's mechanical turk. In *Symposium on Usable Privacy and Security (SOUPS)(Redmond, WA*.

Korshunov, P., Cai, S., & Ebrahimi, T. (2012) Crowdsourcing approach for evaluation of privacy filters in video surveillance. In Proceedings of the ACM multimedia 2012 workshop on Crowdsourcing for multimedia (pp. 35-40). ACM.

Legrand, P. "European legal systems are not converging." International and Comparative Law Quarterly 45.01 (1996): 52-81

Monahan, T, and Mokos, JT, (2013). "Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks." Geoforum

Norris, C., Armstrong, G. (1999), The Maximum Surveillance Society: The Rise of CCTV, Berg, Oxford, p. 210-211

Tinnefeld, M-T./ Rauhofer, J. 'Whistleblower: Verantwortliche Mitarbeiter oder Denunzianten? Fragen im Feld von Ethikrichtlinien, des Datenschutzes und der Mitbestimmung'' (2008) Datenschutz und Datensicherheit Vol. 32, No. 11, pp. 717-723

Rawlings, P: Policing before the Police. In T. Newborn, Handbook of Policing, Wilan Publishing, Cullompton, (2009) p. 47-72

Schafer, B. 'Schlafwandelnd in den Überwachungsstaat?' (2009) *Datenschutz und Datensicherheit* Vol. 8 pp 483-489

Schafer, B. 'All changed, changed utterly? Privacy protection in post-Labour Britain' (2011) *Datenschutz und Datensicherheit* Vol 35 pp. 634-638

South, N. (1987), "The security and surveillance of the environment", in Lowman, J., Menzies, R., Pays, T. (Eds),*Transcarceration: Essays in the Sociology of Social Control*, Gower, Aldershot, pp.129-52.

Surette, R. (1985), "Video street patrol: media technology and street crime", *Journal of Police Science and Administration*, Vol. 13 pp.78-85

Surette, R. (2005) "The thinking eye: Pros and cons of second generation CCTV surveillance systems", Policing: An International Journal of Police Strategies & Management, Vol. 28 Iss: 1, pp.152 - 173

Velastin, J. H. Yin, A. C. Davies, M. A. Vicencio- Silva, R. E. Allsop A. Penn, "Automated measurement of crowd density and motion using image processing," *7th Int. Conf. on Road Traffic Monitoring and Control, London,* 1994, pp. 127-132

[31] Kelley, (2010). Conducting usable privacy & security studies with amazon's mechanical turk. In *Symposium on Usable Privacy and Security (SOUPS)(Redmond, WA*.

[32] Monahan/ Mokos. "Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks." Geoforum (2013).

[33] Korshunov,/Ebrahimi, (2012) Crowdsourcing approach for evaluation of privacy filters in video surveillance. In Proceedings of the ACM multimedia 2012 workshop on Crowdsourcing for multimedia (pp. 35-40). ACM.