Surveillance as public matter

Revisiting sousveillance through devices and leaks

van der Velden, L.C.

Publication date
2018

Document Version
Other version

License
Other

3 A forensic device for activism

How activists use metadata tracking for the production of public proof

3.1 Introduction: Surveillance in the context of human rights activism

This first case study deals with a classic example of sousveillance.[26] It is about a project that re-appropriates surveillance methods in order to document human rights atrocities. WITNESS, one of the organisations involved with building the tool, is a video advocacy group that was founded in response to the filmed police violence against Rodney King: one of the key illustrations of sousveillance. According to WITNESS, the introduction of mobile cameras has changed the playing field of witnessing: '[a] world with "cameras everywhere" now gives us millions of potential witnesses to the Rodney King incidents of our time' (WITNESS 2014). But this is not just a matter of multiplication: as mobile cameras are also tracking devices they allow for a new perspective on sousveillance.

Increased access to digital technologies and distribution networks has enhanced the potential for citizen journalism to monitor and report human rights abuses (Center for Research Libraries 2012). However, the widespread use of these technologies and that of mobile devices in particular, has also raised a new set of concerns. Firstly, these concerns relate to fears about surveillance and security (WITNESS 2011), because governments can easily track mobile phone use. Secondly, digital reporting also raises the issue of authentication because digital material is highly vulnerable to manipulation (Center for Research Libraries 2012, 64). This is further complicated by the volume of images and video that is captured and uploaded, which leads to a third issue: a 'fire hose' that needs to be sorted through, evaluated and maintained (ibid.). The credibility of digital reporting is not only an issue for activists but for (international criminal) courts as well (The Human

26 A previous version of this chapter has been published as "Forensic devices for activism: Metadata tracking and public proof" in *Big Data & Society* (2015).

Rights Center at the University of California 2012, 13). According to the *Human Rights Electronic Evidence Study* by the Center for Research Libraries (2012, 64), 'the resulting profusion of digital documentation has created new challenges of managing and authenticating vast amounts of evidence, from a multitude of sources, many of them unidentified.' Against the backdrop of these concerns citizen journalists and human rights activists and organisations are faced with the question of how to investigate and document an event using digital technologies while at the same time avoiding the risks of traceability that might endanger citizen journalists. In this chapter I discuss the ways in which the InformaCam project tries to deal with these issues.

InformaCam is a mobile phone application 'in the making' for managing metadata embedded in photo and video files.[27] It is designed to resolve two, sometimes paradoxical, dimensions involved in documenting conflicts: the need to document violence, and the need to protect oneself from online surveillance. To do this, the project developers have deployed special methods for producing and curating metadata. Couldry and Powell argue that 'emerging cultures of data collection deserve to be examined in a way that foregrounds the agency and reflexivity of individual actors as well as the variable ways in which power and participation are constructed and enacted' (2014, 1). The InformaCam project serves as a good example of how actors engage with data collection and analysis for the very specific purpose of investigation and evidence production.

To highlight this investigatory dimension, I introduce InformaCam as a 'forensic device'. First of all, it is important to stress that the term 'forensic device' stems from a particular reading of the term forensics, not as a disciplinary practice of the forensic sciences, but as the 'production of public proof'. According to Weizman et al.: 'Etymologically, "forensics" is derived from a Latin term meaning "before the forum" and refers to the practice and skill of making propositions through objects before professional and political gatherings or courts of law' (2010, 59). In the reading of the term as proposed by Weizman et al. the focus shifts from scientific practices, which serve legal procedures, to the skills and the (spatial) settings of evidence production beyond the disciplinary institutions of the law only. Secondly, the term 'device' refers to a particular form of action. A device, according to Callon and Muniesa (2005), is a way of arranging things to make something work. As elaborated upon in the second chapter (§2.3.2), a device establishes what in Actor Network Theory (ANT) is called a 'translation' (Latour 1983; Latour 2005b, 143; Law 1992).

27 The app was 'in the making' when this study was conducted and was later launched as 'CameraV'.

This chapter is a story on 'making networks hold' (§2.5). In line with ANT-allied studies on devices (Barry 1999, Callon 2004; Callon and Muniesa 2005), I look at how connections are being made between elements from diverse fields and settings, in my case, these are connections between (meta)data and requirements from the domain of law. The material for this case study consists of the project's (online) repository, consisting of developers' documents and public explanations about the app.[28] I also did personal semi-structured interviews with developers of InformaCam and read some of their (academic) writings. As suggested by Latour, I follow their 'methods-making' practices, their 'typologies', the way they 'design standards', and the way they 'spread their machines as well as their organizations, their ideologies, their states of mind' (Latour 2005b, 149-150).

By not only looking at the application itself, but by tracing the project back to the philosophy of and writings of the developers, I show how InformaCam is an assemblage in which technical practices are tied to the domain of the law in such a way that something innovative emerges. InformaCam has created a particular form of producing evidence relating to digital images, through a range of interventions. In his work on protest sites, Andrew Barry has shown how activists re-organise public space for the demonstration of facts (Barry 1999; Callon 2004, 125). Analogously, I will point out how the developers of InformaCam set the conditions for metadata to gain greater evidentiary capacity. The metadata are not ready made, nor do they speak for themselves, but they are constructed in such a way that they gain evidentiary capabilities. In other words, it has 'space-making capacities' (Marres 2012a, 154) because it makes space for the production of public proof.

In the following paragraphs, I first explain the basic idea behind InformaCam. Then I provide some background to the use of the term 'forensic device'. After that I describe the metadata categories deployed in the project and the interventions made by the developers. Concluding, I state that InformaCam translates metadata from a potential surveillance risk into a method for the production of public proof, and in that way, it acts as a 'forensic device' referring to the move that is made through this device. Looking at InformaCam in this way, allows one to make explicit that activism in the context of surveillance not only focuses on awareness raising and protection measures, but has an investigatory dimension as well. Hence in this case study I emphasise the 'research side' of sousveillance, something that, as I argued in the first chapter (§1.3), is underemphasised in sousveillance analyses.

28 See the page "SecureSmartCam » CameraV (InformaCam Project)" (The Guardian Project n.d.) on which the developers track the implementation.

3.2 What is InformaCam?

InformaCam is an application developed by *The Guardian Project* (not to be confused with the newspaper The Guardian). The Guardian Project is an open source software company that helps mobile device users to protect their communication from intrusion and monitoring. One of the developers describes the twofold goals of the company as follows: 'to give users control over how much data they provide as they pass media along the pipeline and to increase awareness and visibility of the various issues that converge around their data as it circulates' (Holmes 2011, 56). Part of the project is to provide people with useful tools that can be used by non-specialists. As stated on their website:

> The Guardian Project aims to create easy to use apps, open-source software libraries and operating system modifications, and customized mobile devices that can be used and deployed around the world, by any person looking to protect their communications and personal data from unjust intrusion and monitoring. (The Guardian Project 2013a)

For the InformaCam project, the developers of The Guardian Project teamed up with WITNESS, a video advocacy group which focuses on witnessing and human rights. The organisation supports people to use video 'safely, ethically and effectively' (WITNESS 2015). The project is supported by the International Bar Association (IBA). The IBA was established in 1947 and connects more than 50,000 legal practitioners and two hundred bar associations (International Bar Association).

InformaCam is designed to support people in managing metadata that come with making images and videos. In a general sense, metadata can be defined as 'data about data'. Metadata can be defined in a very specified sense as well, depending on the setting in which they play a role. In the digital context, the simplest description would be data about the context in which a file was produced, edited or stored. Metadata can be distinguished on different levels, such as 'system metadata, file system metadata, application metadata, document metadata, email metadata, business metadata, geographical metadata and many more' (Raghavan 2013, 101). The type of metadata that is relevant for our discussion is 'application metadata', data embedded in the file, which 'describes and moves with the file when it is moved or copied' (Sedona Principles 2007, 4).[29]

29 Application metadata is often contrasted with system metadata: '"system metadata" is not embedded within the file it describes but stored externally. System metadata is used by the computer's file system to track file locations and store information about each file's name, size, creation, modification, and usage' (Sedona Principles 2007, 4).

Metadata can pose a surveillance risk. When an image is created with a mobile phone, the image is stored with an extra layer of information that can include things such as the model of the phone and GPS data. When posting images or videos online one also uploads the metadata embedded in the file along with it, creating an online 'record', thus enabling those with the right tools or expertise to extract the metadata and gain certain information about the creation of the file. This can prove highly risky for the producers of documentary material in oppressive or security-obsessed regimes, because if they are targets they can potentially be tracked down. (For example, by connecting different images made by the same device that is owned by a journalist known by name or by using the GPS data to determine the location of a person on a picture.) [30]

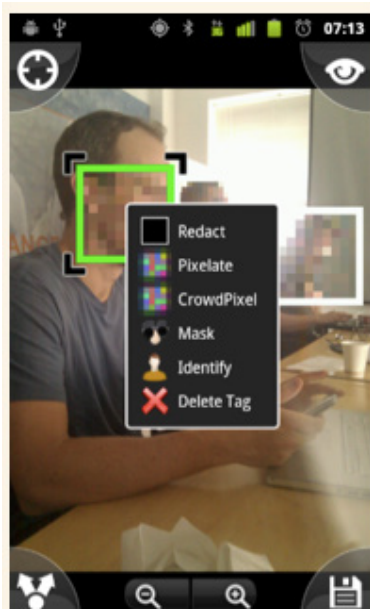
InformaCam is part of a larger project, SecureCam, in which InformaCam's predecessor, the anti-surveillance app ObscuraCam, allows users to remove identifying metadata. ObscuraCam can strip metadata and obscure faces. If somebody wishes to share an image, ObscuraCam diminishes the chance that the producer of the image, or the persons depicted in the image, can be identified or located (The Guardian Project 2013b). Technically speaking, InformaCam is based on similar principles, but it makes an additional and opposite move: metadata are not obscured but deliberately captured and safely stored in case one wants to make this information public in the future. InformaCam enhances mobile devices with a 'witness mode', that is, an extra functionality that uses the sensors of the mobile device to make the registration of contextual metadata available to, and manageable for, the user. When activated, the app registers 'sensory and atmospheric data throughout the session' (ibid.). This includes data types such as current timestamp, user's public (PGP) key, Image Regions created in the image/video, current latitude & longitude, all cell IDs that are visible, altitude, compass bearing, WIFI-networks (ibid.; personal communication).[31] After having made an image or video, one could add specific metadata about the setting in which the image was taken as well, as for instance, information about the content and the producer of the footage. The contextual metadata and the annotations can be

30 A famous example: Vice Magazine revealed John McAfee's hidden location accidently through the location data embedded in the photo (Honan, 2012).

31 Current timestamp: record date/time; User's public (PGP) key: algorithmically generated key that functions as a digital signature; Image Regions created in the image/video: user-demarcated regions in the visual image (or: Regions of Interest) Current latitude & longitude: geographical coordinates; Cell ID: Identification GSM base station; Altitude: (vertical) distance measurement; Compass bearing: orientation camera; WIFI: wireless local area network.

valuable for authenticating the image.

The application, therefore, provides the possibility of making two versions of the documentation: one version is produced without the identifiable metadata and another is safely stored with all the metadata. The 'data-poor' version (figure 1) can be distributed to any network of choice, whether that is YouTube, friends' networks or (citizen) journalists. The 'data-rich' version (figure 2) can be sent to a trusted party, which could be for example one's own e-mail address, a friend or a support organization such as WITNESS. This is automatically encrypted via Tor. Tor is a free software and open network known for anonymous browsing also known as 'onion routing'.[32] It can be used to obfuscate the trajectory of communication for intermediaries between the sender and the receiver.



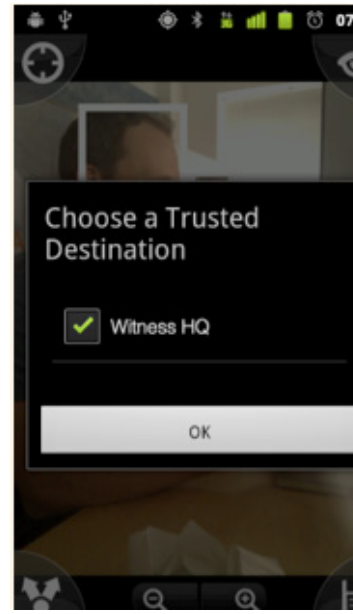


Figure 1. Screenshot of the interface of InformaCam.

A 'data-poor' version without potentially identifying data suitable for sharing. Image provided by The Guardian Project, 2015.

Figure 2. Screenshot of the interface of InformaCam.

A 'data-rich' version with contextual metadata for encrypted storage. Image provided by The Guardian Project, 2015.

32 The idea of the onion stands symbolically for a system of layers of protection that hide the content of the message and which are peeled off one by one after every transmission. A receiver only knows one node it is communicating with, but not the one before or after that neighbouring one. (Tor 2015)

The layer of metadata and the image can be disentangled when posted online, but they are stored together if one ever needs them in court or for other evidentiary purposes. In this way, InformaCam has merged two of the problems mentioned at the start of this chapter, that of mobile tracking and that of digital authentication. (The third problem, the one of sorting through a large volume of images, will be addressed later.) The developers have produced a tool that allows users to take control over the circulation of data by intermediating between two different settings that have different requirements, the risky environment of online public space and the evidentiary setting of public proof. In other words, the tool allows two different ways of 'making data public'. It is the second setting that I will focus on now. For it is here that the app enters the world of forensics.

3.3 Forensics as the production of public proof

Forensics is usually understood as 'forensic science'. It refers to the scientific practices, methods and techniques that are related to the investigation of crime (Oxford Dictionaries, 2015). The forensic sciences are those sciences that investigate, on behalf of the court, on behalf of the principal investigator, or on behalf of the defence (depending on the legal system), specific material assumed to be related to a criminal offence. The forensic sciences can offer potential evidence for a decision that is subsequently to be made by the court. Forensics are, therefore, associated with highly specialised laboratory work conducted by experts that make material visible, which is otherwise invisible for 'untrained eyes', to be presented publicly in court (Jasanoff 1998b). However, studies into how scientific and technologically mediated data become *witnessed facts* tell us that the objects of the forensic sciences never speak for themselves. Scientific and technologically mediated data are in need of particular translations to become convincing in the courtroom when data are presented in front of the judge and jury (Jasanoff 1998b, 719).

Although studies into science and law have shown that the forensic sciences do not operate in isolation from publics or social practices (M'charek 2008; Toom 2010), the notion of forensics can be understood in an even broader sense. This interpretation of forensics goes back to the etymological understanding of the term. The Latin word 'forensis' refers to 'the art of the forum' (Forensic Architecture Project 2013), and can also be translated as 'public speaking'. Weizman explains how the meaning of forensics has shifted over time:

> The Roman forum to which forensics pertained was a multidimensional space of politics, law, and economy, but the word has since undergone a strong linguistic drift: the forum gradually came to refer exclusively to the court of law, and forensics to the use of medicine and science within it. This telescoping of the term meant that a critical dimension of the practice of forensics was lost in the process of its modernization—namely its potential as a political practice. (Weizman 2014, 9)

Weizman et al. (2010) speak in terms of 'forensic architecture'. This reading takes the practices and settings of evidence giving as a central point of departure – and not the scientific or legal institutions. From this perspective, forensics refers to a relational practice in which evidence giving can be organised and so it widens up the range of actors and sites in which forensics can arguably take place. Forensics can therefore be reframed, as suggested by Latour (2012) responding to the Forensic Architecture project, as the production of public proof.[33]

As the practice of forensics centres around a piece of material, the concept also invites one to take questions concerning the relevance of this material very seriously. To explain this point better I draw on the work by Susan Schuppli on forensic media (forthcoming). Schuppli shows how technical objects can contain 'trace-evidence': inscriptions of (violent) events. Her examples include documentary material that is degraded by radiation (a Chernobyl documentary by Shevchenko in 1986), film material that has been copied and edited (the 'Loshi video' depicting a massacre in Kosovo in 1999; for an analysis see Schuppli 2014), and video footage that has metadata embedded (an anonymous execution video shot in Sri Lanka in 2009). In her framing, the object becomes 'informed material', a term inspired by the philosopher of science Isabelle Stengers, and it denotes the way 'their internal composition is enriched by information' (Schuppli 2013). Such material can depict events not only in representative terms, but the materials themselves become enriched as well through the inscriptions along the way. Schuppli shows the different ways in which matter that has archived traces of events articulates itself as a witness of these events. Her concern is with how matter that is 'informed' takes on the role of a witness, that is, how matter can speak and testify. She uses the concept of 'material witness' as an operative concept to describe the process by which that happens (ibid.). This term is rooted in legal jargon (from the US context). When a witness becomes 'material' to a case it means it holds crucial information (Leonardi 2010). In Schuppli's case studies, the question about the material witness becomes one that is concerned with the inscriptions being made along the trajectory of material becoming a piece of relevant evidence. These inscriptions can

33 See also footnote 16.

be accidental influences, but they can also be legal formats with which materials need to comply in order to gain credibility in court (Schuppli 2013).

What I take from the reading of 'forensics' as proposed by Weizman et al. (2010) is the displacement of forensic practices, which allows one to grasp the participation of actors other than scientists and lawyers in the investigation of affairs. Schuppli's work directs attention to how material, including digital material, changes along a trajectory and how that requires us to rethink procedures of evidence giving. This is relevant because, as I will explain, InformaCam is concerned with practices of archiving trace evidence and with the issue of how to make documentary material relevant through particular inscriptions. However, InformaCam is also an experimental application: it is, at the time of writing, 'in the making'. That also means that it does not (yet) deal with passed events that can be documented. In fact, it is the organisation of public proof in future that the application directs itself towards. It is also the organisation of public proof about which ANT-scholars have produced fruitful studies.

3.4 Devices for arranging the production of public proof

Classic examples of ways to organise public proof are legal trials and scientific demonstrations (Latour 1983; Jasanoff 1998b; Shapin and Shaffer 1985). These endeavours are 'devices' as in social-material arrangements, constructed to show or prove particular states of affairs. These devices require solidity because they build on rules or protocols that stay more or less the same and which allow a replication of testing and decision-making (Callon 2004, 125). A less procedural way of thinking about public proofs, and therefore relevant to this case study, is Andrew Barry's understanding of the 'demonstration' (1999). Barry starts by with drawing an analogy between scientific demonstrations and political demonstrations. The scientific demonstration has always been an important object of study in science. These studies have shown that scientific demonstrations heavily depend on the participation of witnesses and controlled behaviour, and thus, on a controlled public space (Epstein 1995; Latour 1983; Shapin and Schaffer 1985). According to Barry, political demonstrations share a family resemblance with scientific demonstrations because they require a similar reorganisation of public space. In Barry's understanding, 'to conduct a political demonstration can be a matter of making visible a phenomenon to be witnessed by others' (1999, 77). As Callon rephrases Barry's work:

> Demonstration, as the origin of the word indicates, makes visible for an audience, constructed contemporaneously with the demonstration, an object about which a discourse is articulated. It therefore simultaneously implies a putting-into-words, the construction of a referential chain (which enables the object to be articulated) and the organization of a public space in which the solidity, robustness, relevance and interest of the demonstration can be tested (possibly by other demonstrations). (Callon 2004, 123)

One of Barry's examples is an extra-parliamentary action: an occupation in a forest against potential road constructions. The site of the occupation, the landscape, was not just the background for the protest. As a 'setting' it became an actor in the protest itself because it exposed a potential truth claimed by the protesters. It showed that 'the existence of humans, animals and the land were, in whatever way, mutually implicated' (1999, 81) and the emerging reality of environmental destruction. In this way, the activists crafted a space in which there emerged something to point to. As can be taken from the title of Barry's piece, 'site' and 'sight' become interconnected. Barry describes at length the style of conflict resolution between the activists, the literature they produced and the material and social discipline needed to organise the camp. He also describes how the protest involved an 'art of demonstration' and a careful orchestration of how (electronic) media participate in the way the demonstration is witnessed.

In sum, Barry shows that devices for public proof can also be displaced from the formal arenas of public proof giving. At the same time he describes that, although these settings might be less formally organised in terms of rules and protocols, spaces for public proof giving still need a lot of work and effort to be established. Barry's take on the matter provides useful pointers for analysing InformaCam. As I will argue, the InformaCam project is, in an experimental way, involved with a range of interventions through which it tries to establish such spaces and connections. Thus, in line with more 'formal devices' such as the trial and the experiment, InformaCam can also be seen as a device that is engaged with creating the conditions for the production of public proof. As InformaCam is experimental, it provides insights into how a forensic device is being set up.

3.5 A demonstration of InformaCam

3.5.1 Enriching and ordering metadata

As will be explained in more detail, the InformaCam project turns metadata from a risky matter of surveillance into data with potential evidential value. Metadata can have evidential value because '[m]etadata refers to data about the data that is stored within a source of digital evidence' (Raghaven, 2013, 101). Metadata offer a narrative potential: a piece of evidence can tell something about itself through its metadata because contextual information is captured within the (digital) object itself. However, as mentioned earlier, data often need narrative techniques to become witnessed as facts. Framed in more philosophical terms, following Schuppli (forthcoming), only capturing data is not always sufficient to turn it into a 'witness': the material has to be able to articulate its relevance to a case. Similarly, InformaCam does more than merely 'capturing' data. The specific way by which data are captured and organised is crucial for turning it into a witnessing machine. The following paragraph describes in more detail through which categories the InformaCam project organises code and why. It also shows how software developers draw together concepts about digital networks, law, and ethical perspectives, into the same project.

The lead developer of the project, Harlo Holmes, reflects upon The Guardian Project's app development in her master's thesis (2011). She describes how EXIF data contain various specified fields and allow for free comments. EXIF stands for 'Exchangeable image file format' and is the standard used for specifying and annotating image files by digital cameras. Holmes argues that a large amount of the EXIF data fields are filled up with intellectual property data. Referring to Manovich's concept of 'cultural transcoding', a concept that addresses the translation of cultural formats into computer code (Manovich 2001, 64), she states that:

> The EXIF specification's treatment of the copyright tag is a remarkable example of the process of "cultural transcoding" posited by Lev Manovich. In the specification, the EXIF tag descriptions are usually no more than 3 lines in length; the copyright section, however, occupies quadruple the space. (Holmes 2011, 30)

It is this insight that metadata are formatted to an intellectual property regime, that for Holmes opens up the question about possible alignments with other regimes – such as human rights. If EXIF metadata take part in a particular material legal culture, why wouldn't this be extended to other domains of legal culture as well? Holmes

refers also to the anthropological research of Gabriella Coleman on how software developers approach code and intellectual property law. Coleman has shown how the software community has contributed to a form of 'jurisgenesis' (Coleman 2009, 421). The concept of jurisgenesis, originally defined by Robert Cover in 1983, refers to 'the collective construction of new legal meanings and artefacts that diverge from statist or dominant interpretations of the law' (Coleman 2009, 421). Holmes situates The Guardian Project's app development in this context. She states: 'This interaction with justice through technology can be viewed as a form of digitally enabled jurisgenesis' (Holmes 2011, 57). But in her view 'technological laws' undergo similar processes of re-appropriation:

> Obscura openly challenges the law of the smartphone by overriding its unencrypted media database and by allowing users to rein control over the embedded EXIF data. To interact with the app encourages direct exposure to the new laws of images, allowing users to actively participate in the politics newly embedded into the photographic act. (Holmes 2011, 57-58)

One can now begin to sense how Holmes and her co-developers creatively appropriate the role of metadata by stretching up the space for EXIF data and reaching out to formats that are directed at evidentiary settings. In making this move, the developers relate to the human rights arena specifically.

The interaction between human rights and software is of central concern to the Project Director of WITNESS (which is the NGO that collaborates on InformaCam), Sam Gregory. Gregory (2012) presents some of his ideas in a publication that discusses alternative ways of making human rights visible. One example is a proposal for a new kind of licensing system, one that recognises intentionality (556). His proposal is to give a twist to digital material, but one that is different from copyright or Creative Commons licenses that deal with intellectual property rights and the possibility for remixing. His type of license would embed a proposed human rights use into the metadata. His second example relates to rethinking witnessing in the digital age 'in line with the primary principle that every human being is possessed of "inherent dignity"– a concept that runs through every right included in the UDHR' (Gregory 2010, 11). An important concern in this context is the avoidance of re-victimisation of victims on film through the widespread circulation of media. Gregory continues to argue that this comes with an ethical obligation for the one who is witnessing to do so carefully with respect for the victim: 'Contemporary thinking on testimony, witnessing and trauma also places a heavy emphasis on the responsibility of the witness to abuse to represent it responsibly and

with ethical integrity – to be, so to speak, the "ethical witness"' (ibid., 11-12). WITNESS wants to contribute to ethical forms of witnessing by translating professional notions of informed consent (inspired by medical practices, social science and international human rights and humanitarian law) into the design and usage of technological devices (ibid., 2010, 12).[34]

InformaCam is an implementation of some of the ideas mentioned above. This is done by what one could call 'enriching metadata': InformaCam structures how metadata are embedded in the image. A (early) blog post on the project mentions four metadata categories: Data, Consent, Intent, Genealogy.[35] The category 'Data' sounds very general, but it represents the data that 'captures the moment of capture'. As explained by The Guardian Project's website: 'This category includes all standard metadata (timestamp, acquired sensory data, location and movement data) that have been collected during the lifetime of the image, from the moment it was opened to the instant it was saved' (The Guardian Project, 2012). InformaCam does not capture traffic but only publicly visible identifiers. 'Consent' resonates most explicitly with human rights culture. A user of the application can add free text to images indicating whether the subject has given consent to be filmed. As touched upon earlier, the approach of WITNESS is to translate ideas of consent into technical devices, by for example developing tools that give 'prompts on consent during those filming/upload processes' (Gregory 2010, 15). This is an implementation thereof. 'Intent' is more experimental and is directed to the circulation of digital material. It indicates 'information about the media's creator and the permissions for sharing' (The Guardian Project, 2012), and could therefore be considered as a materialisation of what Gregory (2012) proposed: 'a licensing system that recognizes intentionality'. This 'tag of intent' will say something about what kind of 'use' the producer envisions with a particular digital object and is an attempt to create 'human rights media' as a particular piece of media and bring that into circulation (personal communication with Gregory in 2013). 'Genealogy' refers to the main indicator of the chain of custody (or 'data integrity' which means that data should be left intact until it reaches the court). This is addressed through a digital hash embedded into the file at the moment the image was made in order to indicate its

34 Whilst acknowledging that full informed consent can never be assured, and training and the provision of training material is invaluable (Gregory 2010, 15).

35 It is good to keep in mind that these are working concepts and InformaCam will have different deployments for different settings, so not all of them will be implemented in final use.

original state.[36]

Besides these main categories, the developers make use of an ordering format entitled 'J3M' (JSON Evidentiary Mobile Media Metadata), which is described as 'a format that can be used to easily describe the origins, context, and content of any image or video taken with a mobile device' (j3m.info 2013). This is to be understood as a way of structuring metadata. The aim of J3M is to:

> [m]aintain a trusted record of a media object's chain-of-custody (…); Express the context surrounding the media object's capture (…); Embed extra user input from forms or surveys into the media object as signed metadata (…); Provide metrics for analyzing the content of the media object to mathematically determine that it was created by the device indicated in its metadata. (j3m.info 2013)

The image on the next page (figure 3) is an example of how this would look in code. Technical specifications are given on the website of the Guardian Project including a Java library to help developers to use J3M.

Figure 3. Screenshot of metadata ordered through the 'J3M-library' (JSON Evidentiary Mobile Media Metadata).

Image provided by The Guardian Project, 2015.

36 Please note that in the end, the data integrity should be decided upon by an analyst reviewing the J3M-data (personal communication with Gregory, 2013).

The above-mentioned categories and J3M give an early insight into how the people involved with InformaCam actively shape metadata. They do so in a way that would help forms of narration emerge; firstly, concerning the context of the event (the contextual metadata); secondly, with respect to the content of the material, the relation between the producer of the image (through the annotations) and the people depicted; finally, his or her relation with the digital object itself (or intent). It is an example of an emerging culture of data collection in which actors on the ground exercise their agency by constructing and curating data for particular purposes (Couldry and Powell 2014).

3.5.2 Organizing the conditions for public proof

At the time of writing, InformaCam just released its beta-implementation. Therefore, real life experiences of how InformaCam is put into use are not yet available. However, InformaCam allows for organising the settings for the production of public proof in multiple ways. I discuss three of these ways below.

A first intervention, which consists of tying images to regimes of evidence, has already been discussed. As highlighted in the previous paragraph, the categories of InformaCam show how the project developers pull together different kind of formats into the application. The chain of custody, an important issue for investigatory purposes in legal settings, is accommodated with a digital hash that J3M embeds in the file. In addition, notions of ethical witnessing from the human rights arena are redesigned as an awareness prompt. In this way, in Holmes' words, the developers are 'ingraining' categories borrowed from legal and human rights discourse into the metadata (personal communication with Holmes, 2013). It is interesting to see how these inscriptions organise the capturing of data before the images are even being made. This is analogous with other legal practices. In his investigation into the workings of law, Latour (2010) explains how, in the context of the French Council of State, some (governmental) documents are prepared for legal use before being used in a legal setting. They already carry certain references that follow legal formats and establish legal trust, such as certified copies, witness statements (ibid., 75). These documents are, in other words, already 'profiled' before arrival at court and 'made ripe for use' (ibid., 70). The operation of law, he argues, cannot be understood without these preparations. Similarly, software developers are undertaking preparatory work to 'ripen up' digital data for legal use.

Whether this material will eventually make it to the international human rights courts is difficult to foresee. In the context of this

discussion, it is important to take note of the different legal systems with respect to the admission and evaluation of evidence (Jasanoff 1998a; Van Koppen 2007. The adversarial system in the United States has specified legal requirements for scientific evidence (the Daubert Criteria).[37] It has been claimed that these admissibility rules, together with the litigation structure in the United States, provide opportunities for the critical evaluation of science and technology, especially when compared to inquisitorial systems found in many continental countries (Jasanoff 1998a; Van Koppen 2007). In inquisitorial systems, the prosecutor is responsible for the 'dossier work' and the admissibility of scientific and technological data is less subject to public discussion in the courts.[38] International human rights courts consist of a mixture of legal systems, but tend to follow civil (continental) law in relation to the admission of evidence. This implies that the threshold for the admissibility of evidence is low. With respect to electronic evidence the international tribunals, at the time of this study, require no particular standards and in terms of admissibility trial chambers are relatively free in their assessment (O'Neill, Sentilles and Brinks 2011). The rules for (electronic) documentary evidence therefore vary from court to court and the development of standards proceeds very slowly (Center for Research Libraries 2012: 65): '[R]equirements are better established for national and local courts than for international courts and tribunals' (Center for Research Libraries 2012: 51). In their review of a series of human rights courts O'Neill, Sentilles and Brinks state that 'procedural rules at international courts and tribunals offer little guidance on what must be shown to authenticate new forms of E-evidence' (O'Neill, Sentilles and Brinks 2011, 9).[39] The number of cases in which metadata have played a role is still small, and there is little case law to draw conclusions from about what to expect in the near future. A request by the International Criminal Court Prosecutor for a protocol for 'born-electronic evidence' was denied by the Chamber (ibid., 51). However,

37 These requirements were formulated in the landmark 1993 decision on Daubert v. Merrell Dow Pharmaceuticals, Inc., which determined the admissibility standards for scientific evidence in court, giving the judge greater agency in determining the validity of the testimony of the expert witness. See the website of the Legal Information Institute (2013).

38 This statement should be nuanced a little bit, as scholars have argued that sometimes this 'dossier work' is a result of a controversial trajectory as well (Bal 2005).

39 The review included the International Criminal Court (ICC), the ad hoc tribunals for the Former Yugoslavia and Rwanda (ICTY and ICTR respectively), the Special Court for Sierra Leone (SCSL), the Extraordinary Chamber of the Courts of Cambodia (ECCC), and the Special Tribunal for Lebanon (STL), and the investigatory process at the Office of the High Commissioner for Human Rights.

as explained in the same report (ibid., 42), the authentication of e-evidence can play an important role in opening up investigations into human rights violations. Despite the lack of existing standards, there is a realisation that they might develop in the years to come. According to the authors of the same review, the potential future development of restrictive demands concerning e-evidence, which might be inspired by the more extensively documented (commercial) US litigation context, could be dangerous for international human rights proceedings, since the burden placed on people bringing in evidence may preclude those without access to equipment of sufficiently high standards. That is the reason why InformaCam is a significant project: whereas requirements for metadata in the legal domain of international human rights procedures are not yet fully defined, the developers of the project are already working towards developing a specific socio-technological standard of which they hope will also become accessible for activists.

In this context it is important to know that The Guardian project has launched the InformaCam system as the 'CameraV App'.[40] In June 2015 the IBA launched a spin-off project called 'Eyewitness for Atrocities App'. This (closed-source) app is built on the open source implementation that was made in collaboration with the Guardian Project.[41] The concepts behind the project are now being put into practice. Besides offering the tools, the developers of InformaCam do also try to find ways to familiarise courts with their techniques. According to Sam Gregory, they are looking for what they call 'demonstration projects' that can help demonstrate the evidentiary value and applicability of J3M data and the InformaCam project (personal communication with Gregory, 2013). At the same time they are aware of the dangers of placing a weight of responsibility on people presenting evidence who may not have access to the right equipment to secure such standards: 'We're also cautious though not to create a situation where there is an insistence on extra metadata for proof since we know that there will be many contexts where valuable evidence is missing this' (personal communication with Gregory, 2013).

The second intervention InformaCam makes relates to the capacities mobile devices have to organise forms of witnessing on the ground. Through activating Bluetooth InformaCam can detect other devices that have the same app activated nearby. In this way the app can show that multiple devices were present at the same place at the same time, or that people have made similar documentation at the same time

40 For an extended user guide see "CameraV app and the InformaCam System" (2015).

41 It is important to note that the Eyewitness app works quite different from InformaCam as described in this chapter and has different security consequences. For a comparison, see the blogpost by Watson (2015).

with regards to the same event (personal communication with Holmes, 2013). One potential user group is the Georgia Legal Services Program that helps migrant workers (Making Cameras Count 2013). It happens that bosses deny that people came to work, leaving workers without payment. It is for such situations that InformaCam could mobilise self-tracking: through the simultaneous use of Bluetooth detection. People would thus be able to try to prove their presence, or at least, that of their phones. Therefore, the application does not only aim to produce images of events, it can also put oneself, or one's collective, on the map. So one way in which InformaCam invites material to become more 'informed' is by capturing (collective) presence. It captures not only contextual metadata that refers to location, device number etcetera, but it enacts a collective body of witnesses. Figure 4 is an example of how the presence of devices can be visually mapped with Bluetooth data.

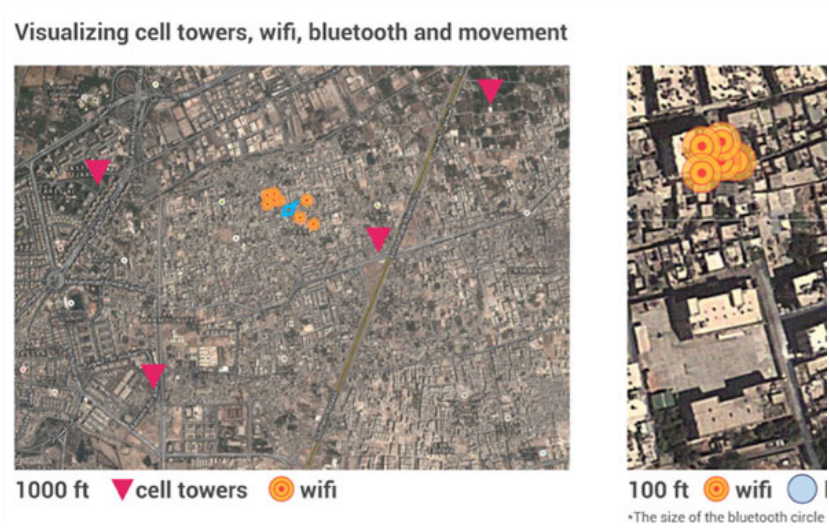


Figure 4. Map that visualises cell towers, wifi, Bluetooth and movement on the basis of data captured by InformaCam.

Image provided by The Guardian Project, 2015.

With a third intervention, InformaCam's J3M-library makes a particular form of forensic data analysis possible. According to Harlo Holmes, it is not the app itself she expects to do all the work: it is the openly available library that makes it possible to distribute J3M to other applications and platforms such as YouTube (personal communication

with Holmes, 2013).42 Gregory adds that the distribution of J3M into the public domain aims to open up research possibilities through J3M itself. The library is inscribed into the files and subsequently read out again. So the device works by structuring data in such a way that material can be pulled together after capturing it. According to Gregory, multiple J3M-sources embedded in InformaCam material can be used for timeline mapping and comparison between multiple angles. It could enhance constructing a chain of explanation of what happened in an event (personal communication with Gregory, 2013). There are already several projects that map events on the basis of (EXIF) metadata online. See for instance 'the Rashomon Project', an open-source online toolkit that assembles and analyses videos and photos from 'contested events', such as demonstrations that clash with the police. The aim of the project is to enhance a nuanced understanding by providing multi-perspective timelines and interactive viewing features (Rashomon Project 2015). This approach is therefore an example of how actors 'on the ground' could challenge 'conventional data collection' (Couldry and Powell 2014, 4). Figure 5 presents the InformaCam System Architecture. From the left to the right it shows the app, the two versions of the documentary material that the app produces, the methods for verification, and lastly, the analysis dimension in the project ('J3MScan Advanced Search and Analysis').

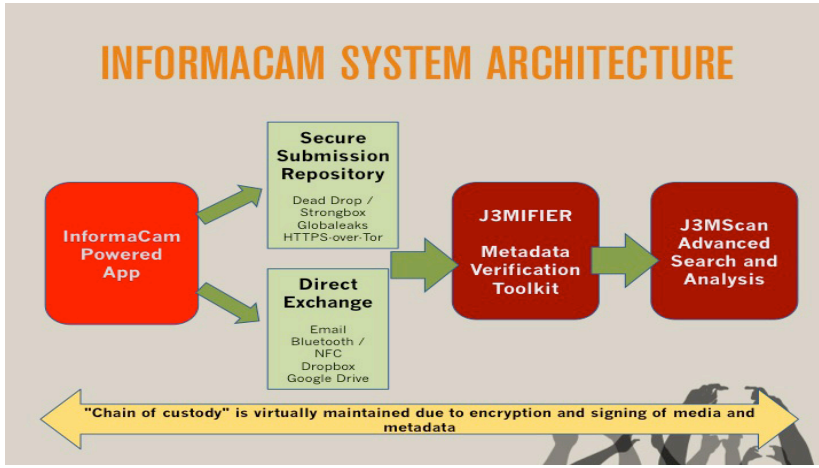


Figure 5. InformaCam System Architecture.
Image provided by WITNESS and The Guardian Project, 2015.

42 YouTube has already included a Human Rights Channel and a Face Blurring Tool (WITNESS, 2012).

3.5.3 A forensic device for activism

InformaCam is part of an emerging trend of projects that aim to enhance the verification of online information. There exist websites for tracking users' location footprint on the basis of GPS data, tools for revealing EXIF data attached to images, and tools for showing whether images have been altered. (See, for instance, the website of the *Verification Handbook* for an overview (Silverman 2014)). On the other side of the spectrum there are plenty of tools that help users to protect their identity, to browse anonymously or to securely encrypt their data. (See for instance, the websites securityinabox.org and http://prism-break.org). According to the developers, InformaCam is, as far as they know, the only app that combines these many capabilities ('enhanced metadata through sensors, cryptographic verification/hashing/signing, secure storage and transmission') and that is offered as a free and open source app that runs on inexpensive smartphones (personal communication with Freitas 2013).

Moreover, InformaCam is pre-figurative to legal standards. As mentioned earlier, Andrew Barry has shown how activists can be involved in carefully modifying and constructing spaces that allow proof to emerge, and how they can invent new forms of demonstration. The actors involved with the InformaCam project do a similar thing with respect to networked technologies. They actively engage with how data can be handled by making InformaCam intervene in different parts in the trajectory of an image. By transcribing law into code before the event, by controlling how data are captured on the ground, and by the enhancing research capabilities for post-event analysis, the InformaCam project invents a form of what we could call 'sensory data forensics'. Mobile phones, sensory data, users' interaction with technology, legal formats and code are tuned in such a way that together they allow for the production of public proof, and so operate as a forensic 'device' in the Actor Network Theory sense. It also indicates a medium-specific collaborative practice for witnessing, which can be better understood when taking into consideration that particular software communities have particular approaches to code (Coleman 2009; Kelty 2008). The people behind InformaCam are not waiting for jurisprudence to catch up with new evidentiary modes, but are already intervening through the media landscape.

The idea that images should remain 'in tact' to retain the chain of custody on the one hand and the practice of adding data-points to structure images for analysis on the other hand seems paradoxical, but, as Kelly Gates shows, this paradox characterises the practice of video forensics by forensic experts as well. Looking at the disciplinary practice of video forensics in particular, Gates describes how in preparing

CCTV video material, forensic investigators use narrative techniques like annotating, zooming and composing timelines, sometimes with the use of sophisticated software. Metadata can also be attached to images to enhance search and retrieval and cross-referencing (2013, 251; 255). As Gates critically points out, the practice of video forensics points to a new conceptualisation of (computational) objectivity:

> Here I want to suggest that the use of digital imaging technologies to make visible what is invisible and invest images with indexicality points to a new conceptualization of objectivity. This way of thinking about objectivity holds that neutral, scientific results can be achieved through the application of computational forms of analysis – automated, algorithmic techniques performed by computers. (2013, 252)

Just like forensic investigators, the developers of InformaCam 'invest images with indexicality' to condition computational analysis. It is what Thomas Keenan (inspired by the use of the concept by the photographer Sekula) calls 'counter-forensics'. This concept refers not to countering forensic investigations, but to the tactical adoption of forensics in the context of activist struggles (Keenan 2014, 69). Whether projects such as InformaCam, just like forensic state investigators, also participate in the establishment of what Gates calls a 'computational objectivity' (Gates 2013, 252) would be an interesting topic for future research. (See Brucato (2015) for including the notion of mechanical objectivity in the study of sousveillance.) This is especially interesting because the developers, at least of the InformaCam project, do not hide the fact that the computational analysis of data requires an extensive preparation and shaping of design including choices, concepts and ethics.

InformaCam shows in what direction activism in the context of surveillance can develop. This investigatory dimension raises a few critical questions: Does the project become too much of a surveillance project itself? Does it also perform analytic work in service of authorities that attempt to monitor people? Do people who use this tool, by collectively mapping events and their devices, endanger themselves? When asked about this, Harlo Holmes admitted this constitutes a potential risk, but she also argued that many states have access to this kind of data already (as InformaCam captures only public data) and many people are not aware of it yet. She regarded using InformaCam as taking a step forward in terms of the 'equality of arms' (personal communication with Holmes 2013). Recent developments have underlined the invasiveness of state surveillance. The NSA disclosures by Edward Snowden in 2013 (Greenwald 2014) have shown that the NSA uses many techniques for the analysis of data leaked by 'leaky apps' (Larson, Glanz and Lehren 2014), including mobile phone

location data and the co-presence of devices (Soltani and Gellman 2013a) (see also Chapter six). These are exactly the things InformaCam intervenes with. Tools such as InformaCam, therefore, can be seen as a timely response to the unequal distribution of power over data.

3.6 Conclusion: The investigatory dimension of sousveillance

In the first chapter I stated that sousveillance analysis does not properly address the question of what is the 'laboratory' (or database) of the sousveillance practitioners. This case study demonstrates one example of how these practitioners construct knowledge. The InformaCam tool not only allows for personal surveillance (self-tracking and mapping) and hierarchical sousveillance (documenting authorities), it also has an interesting back-end story to attend to, in which knowledge infrastructures make counter-forensics possible and make space for new forms of public proof.

The 'camera' is an icon that has informed a particular strand of surveillance theory, in which the gaze was central for practices of surveillance and sousveillance. But the camera has now become a 'camera app' and a tracking device, which seems to do away with the gaze as the central organising principle. Instead of being primarily concerned with *what* can be seen (on an image), the project shows how attention shifts to the 'art of looking', which is concerned with how to organise which data counts (including one's own position, location, etcetera). In short, it becomes engaged with investigatory practices through code.

The InformaCam project also signals an innovative way of thinking about surveillance risks: For the people involved in the InformaCam project, the circulation of data is a problem but at the same time it is material that can be analysed and used for other things. Surveillance risk is not just something to be 'informed of' or to be avoided; it is something that can be hacked in order to become an empirical object. The project has re-articulated what used to be a problem into its working material. This is a first step in understanding surveillance as 'public matter': The InformaCam project turns surveillance into research material with public ends.