The Fibreculture Journal
DIGITAL MEDIA + NETWORKS + TRANSDISCIPLINARY CRITIQUE

issn: 1449-1443

FCJMESH-005 Technology and Citizen Witnessing: Navigating the Friction Between Dual Desires for Visibility and Obscurity.

Sam Gregory
WITNESS

WITNESS has been training and supporting rights activists and citizen witnesses around the world to use video for over 20 years. Since this time they've trained people from 100 countries, supported successful advocacy campaigns and advocated for innovation in human rights technology. In this article, Program Director at WITNESS, Sam Gregory, discusses the events, reasons and philosophies that have informed their work and enabled them to support many people to use video and related technologies effectively, safely and ethically.

doi: 10.15307/fcj.mesh.005.2015

Put yourself in the shoes of an activist: perhaps a long-term Human Rights Defender or a first-time citizen witness. You are filming on your cell phone in a repressive regime—capturing the testimony of someone assaulted by the police or documenting a protest.

After recording your video you are faced with choices about how your video should be used. You can upload your footage to a popular consumer platform like YouTube or Facebook. This option offers the capacity for rapid dissemination, which might help secure timely media and public attention; but these platforms also pose a risk, as they are readily accessible to the police and military. Because of this, the faces of the people you have filmed and the

metadata describing the location and timing contained within the image might incriminate both you and them. Metadata captured by your mobile carrier and by the real-name-based social media service you have used, will likely add to this risk. This option means thinking through risk and the precautions you might take—like blurring faces and attempting to remain anonymous.

To avoid being incriminated or incriminating others, you might instead choose to hold onto your footage and to only share it with people you trust, as part of an investigation or even as potential evidence in a prosecution. In that case, it is important that you don't blur the faces of the people you have filmed, or obscure any vital authenticating information on location, timing or the chain of custody. This information will all become vital for your video to pass basic authentication tests [1].

Perhaps though you want to do both of these things: you might want to share information safely in the moment—so that it will quickly inform as many people as possible on what is happening—while also securing your information and metadata for later use and long-term accountability. This third option will see you challenged by the competing demands of obscurity and visibility, while negotiating consumer communications technologies that are not built for either of your needs, let alone for both.

These different choices illustrate one of the many frictions that emerge when we use contemporary consumer communication technologies in an expanding activist ecosystem that involves new participants, new approaches and new technologies: the friction between staying hidden and being found. This is a particular concern for those of us working in the area of human rights documentation since these services have not been designed with any awareness of the different needs and contexts of rights advocates and most often have in-built hidden surveillance and monitoring capabilities.

As one activist, 'Rafeeq' (2012) noted in the early days of the Syrian uprising:

> *Many of my friends were arrested for protesting. However they weren't arrested from the protest sites, but rather from the checkpoints spread across the city.*

But how did Assad forces know they protested? Government forces have special teams

dedicated to monitoring protests that we film and upload to the Internet. One of my friends who was detained for a short period told me that as he was undergoing torture in detention, he was asked by the investigator if he ever participated in rallies against the regime. When my friend denied protesting, the investigator showed him footage where his face clearly appeared in a protest.

This raises important questions about how much control creators, sharers, as well as people included in images, have over their identity when knowledge of their identity may bring real risks from perpetrators and state oppressors. These questions highlight the ways that the desire for immediacy in human rights reporting is compounded by expectations embedded in social media and in 24/7 news reporting. Immediacy is usually critical for getting coverage of rights violations, while this content also needs to 'stand out' and be findable. Added to this, if this content is going to have legitimacy it must stand up to scrutiny by news analysts, NGOs and other justice institutions, courts as well as informed citizens.

This means, a citizen activist in Syria like 'Rafeeq' who shares a witnessing video must weigh up the risks of further exposing the identity of him or herself, allies, victims and testimony-sharers, with an awareness that their heart-breaking, powerful testimony to gross war crimes violations, may well get lost, ignored or mistrusted amidst the half a million plus videos and images of human rights violations that have emerged from that conflict over the past four years, let along lost amidst a much larger sea of non-human rights content.

When evaluating the risks and benefits of sharing human rights documentation of rights violations, media producers need to make assessments at multiple levels. Firstly, they need to consider what is or might be revealed by the pixels and audio recording; but secondly, they will need to consider the metadata that is attached to the recording. This underlying and often obscured data can tell us so much about the what, where, who and when. [2]

Each of these risk assessment levels is enabled or constrained by the tools that an individual uses, the media literacy they have in using them, and the policy scope and limits of the platform they use. Legal and extra-legal government surveillance applied at the aggregate level—to both multiple users (through dragnet surveillance) and to individual users (through targeted surveillance)—add an additional layer of risk.

In our work at WITNESS, we have grappled with these levels of risk and opportunity in the

course of advocating around the issues of ‘visual anonymity’ [3] and ‘metadata for good’ in our work in preparing training materials, designing technology tools (with our partners at the Guardian Project), and advocating to major consumer technology platforms. In our work with companies like YouTube we have used our own work designing activists tools with the Guardian Project such as ObscuraCam to provide reference designs for the introduction of new tools [4] that allow individuals to more easily blur faces, and we continue to advocate for tools to strip out metadata from within platforms. We have also actively argued for the converse: we advocate for ‘eyewitness’ and ‘proof’ modes and functionalities based on our InformaCam tool that enable the ability to add in metadata to enable video to be more easily found and trusted by news journalists and human rights advocates and to provide verification that it comes from the stated user and has not been tampered with (which is critical if video is to be used as evidence in court proceedings).

In advocating for these changes to the design and functionality of technology platforms we are challenging some underlying tenets of the current generation of popular Internet platforms. These platforms—including popular social network sites—have an emphasis on pushing for the use of ‘real-name’ identities and in preventing or resisting anonymity; this trend has been made manifest by Facebook’s well-publicised battles with people who use pseudonyms. In this way, Silicon Valley’s expectations around transparency and safety needs are very distant from the on-the-ground realities of vulnerable individuals in many parts of the world and in their own backyard; yet widely-used global consumer platforms like Facebook constantly push everyone to operate with the same norms of visibility and accountability. The emergence of popular platforms and tools from outside Silicon Valley may not necessarily change this, particularly when these tools and platforms emerge from authoritarian contexts like China, or countries with strong regimens of surveillance like South Korea.

Added to this, is the challenge of an emerging dominant cultural discourse that tends to frame metadata negatively. Metadata—the information such as geotags, timestamps, names, dates and locations that is associated with media we create—has been developing a bad name of late and has all but become synonymous in the popular imagination with government surveillance. In the post-Snowden moment, there is growing public distrust and disquiet about the use of “metadata for bad” not only by extra-legal government surveillance but also ranging from poachers using metadata in Instagram photos of wildlife shot by tourists, to drone strikes authorised on the basis of patterns of mobile metadata, to women being stalked after the metadata contained in the images and video they have generated has revealed their location.

At WITNESS, our response to these valid concerns about metadata is that much depends on how much control we have. Technologies, and the affordances they limit or support, can put control in the hands of the creator and sharer by incorporating a starting point of privacy-by-design and default and by allowing users to be as visible and discoverable as they want to be; or it can take away control and prevent us from blurring faces, stripping out metadata, and operating under a pseudonym. While allowing privacy-by-design and default, platforms can also allow individuals to choose to add in additional metadata and markers of trust that can help content to be found and be more likely to be trusted by people who are looking for real-time information in a sea of content.

At WITNESS we advocate that the frictions that emerge between technology, activists, anonymity and visibility can be better negotiated if all of us share some basic capacities and knowledge. In the expanding realm of human rights documentation, visual imagery is not just created by professional investigators or journalists, but by citizen witnesses and media activists as well as accidental, incidental and intentional witnesses. There is a resource allocation question around broadly building witnessing and documenting literacies and this raises the question: does everyone need to have a better understanding of how to make informed choices about the visibility and obscurity contained in the video and images we record and share?

We would argue yes. In an age where communication is increasingly visual and where citizen witnessing is used not just in human rights contexts but also for news and social media discussion, new capacities and skills are critical if we are to support the privacy rights of others and protect the most vulnerable from harm. But if citizens are to be capable and empowered technologically and personally to make the most appropriate choices about what they share and what they don't, we have to ground new citizen media literacies in the context of more responsible corporate practices and accessible, useable values-manifesting technologies that are part of the platforms that regular people utilise and not just in activist niches. And ultimately these mainstreamed technological choices and widespread literacies need proportional and human-rights respecting legal protections and sound public policy if citizens are to be capable, empowered (technologically and personally) and protected to make the best choices for themselves.

Biographical Note

Sam Gregory helps people use the power of the moving image and participatory

technologies to create human rights change. He is Program Director at WITNESS, the leading organisation focused on empowering millions of people to use video for human rights effectively, safely and ethically, and he teaches on human rights and participatory media as an Adjunct Lecturer at the Harvard Kennedy School. He launched the Webby-nominated Human Rights Channel on YouTube, and leads the WITNESS team working on the award-winning ObscuraCam and InformaCam tools. Sam has worked on impactful campaigns worldwide (particularly in South-East Asia and Latin America), and created innovative training programmes and teaching texts. Sam was a 2010 Rockefeller Foundation Bellagio Resident on the future of video-based advocacy, a 2012 Young Global Leader of the World Economic Forum, and in 2013 was named a 'Future for Good' Fellow at the Institute for the Future, working on 'co-presence for good' and live and immersive witnessing for human rights. Sam has a Masters in Public Policy from the Harvard Kennedy School, which he attended on a Kennedy Memorial Scholarship, and a BA First Class from the University of Oxford.

Notes

[1] For more information on the demands of evidentiary citizen media see 'Video As Evidence: Basic Practices', Kelly Matheson on WITNESS Blog, http://blog.witness.org/2015/02/video-as-evidence-basic-practices/

[2] For more on how these risks can play out see Sam Gregory and Elizabeth Losh. 'Remixing Human Rights: Rethinking civic expression, representation and personal security in online video', First Monday 17.8–6 (August 2012).

[3] For more on the concept of 'visual anonymity' see Sam Gregory. 'Human Rights Made Visible', in Meg McLagan and Yates McKee (eds) Sensible Politics: The Visual Culture of NonGovernmental Activism (Zone Books: 2012).

[4] For more information see 'Visual Anonymity and YouTube's New Blurring Tool', Sam Gregory on WITNESS blog, http://blog.witness.org/2012/07/visual-anonymity-and-youtubes-new-blurring-tool/

References

Gregory, Sam. ‘Human Rights Made Visible’, in Meg McLagan and Yates McKee (eds) Sensible Politics: The Visual Culture of NonGovernmental Activism (Zone Books: 2012).

Gregory, Sam and Elizabeth Losh. ‘Remixing Human Rights: Rethinking civic expression, representation and personal security in online video’, First Monday 17.6–8 (August 2012).

‘Rafeeq’, ‘The camera in Homs: a double-edged sword’, Al Jazeera Blogs, published 28 June 2012, http://blogs.aljazeera.com/blog/under-siege-syrian-diary/camera-homs-double-edged-sword

OPEN HUMANITIES PRESS

The Fibreculture Journal is published by The Fibreculture Journal Incorporated in partnership with Open Humanities Press.