



EngageMedia's Secure My Video Guide – a work in progress

Draft version: EM-Secure-My-Vid-Guide_3.1.1

Welcome to the *Secure My Video Guide*, the first stage in EngageMedia's effort to provide video activists with tools to make their work safe and secure. The *Secure My Video Guide* has an Indonesian focus, however the issues and strategies recommended are universal. This Guide is a *work in progress* and your input is encouraged. You will find notes where more research is required, particularly in the last issue area, Hosting Securely (page 10). If you wish to contribute to its ongoing development, simply write your thoughts, ideas, corrections and recommendations as comments [to this site](#).

Table of Contents

1. Introduction.....	2
2. Background.....	2
3. Indonesian context.....	4
4. Summary of issues.....	5
Shooting securely.....	5
Case study.....	5
Known issues and what you can do.....	6
Resources:.....	7
Storing securely.....	7
Known issues and what you can do.....	7
Resources:.....	8
Publishing securely.....	9
Case study.....	9
Known issues and what you can do.....	9
Outstanding issues / research questions.....	9
Visual anonymity.....	10
Known issues.....	10
Outstanding issues / research questions.....	10
Hosting securely.....	10
Case study.....	10
Known issues and what you can do.....	11
Outstanding issues / research questions.....	11
5. References.....	12
6. Acknowledgements.....	12
7. About EngageMedia.....	12

1. INTRODUCTION

This *work-in-progress* guide is the result of a one day sprint held in Jakarta on 27 July 2011. Where possible information gathered during the sprint has been reviewed, cross-referenced, re-drafted and added to the most appropriate issues and solutions. Where possible, the guide provides known issues and recommendations for how best to deal with them. In other instances the guide points to where additional research is required, or where outstanding questions may best be answered.



Video surveillance sign, Tallinn, Sweden
(Photo by Hans Põldoja, CC BY)

We did not set out to provide answers to all the questions raised nor provide a comprehensive response to the issues videographers face. What we did achieve, however, is a contribution towards the work being done by groups such as [WITNESS](#) and [Tactical Tech](#), specifically noting the issues faces by video activists in Indonesia.

What was clear from this process was the need for more training, more consciousness raising to the issues raised throughout this guide. There is a paucity of security and media literacy knowledge in Indonesia, there is even less access to the skills to secure video from inception through to distribution and archiving.

As an open *work-in-progress* we encourage the ongoing development through review and contributions from our networks, friends and colleagues of EngageMedia's *Secure My Video Guide*.

2. BACKGROUND

An impossible to imagine number people and plenty of utilities, it seems, are doing video. Children, teachers, sports professionals, activists, workers and the unemployed, radio and print journalists, the police, military and security firms are all swinging cameras some where on planet earth. In many countries now we are videoed in trains, elevators, in our cars in traffic, from the skies and even from space!



Police officers in Washington video protesters, April 11, 2011
(Photo by Andrew Bossi, CC BY-NC-SA)

Video has become, as WITNESS's Sam Gregory describes, spreadable, mailable and accessible by more means than ever. It has become, in less than half a decade, ubiquitous. It's portable, potent and powerful. Hollywood and the largest media corporations in the world, Disney and News Limited, no longer command the public's total attention at the screen. No country and no individual is immune from the lens.

In a country where internet security issues are either unknown or are not taken seriously, where more and more people are using video to document abuses and record first-hand testimonials, and where Facebook has become *the internet* for millions of citizens, the means to both securely publish and access video in and from Indonesia is more critical than ever.

Along with the opportunities afforded by new technologies, there too are the threats. Creators of social justice video, for instance, can be located if they use an internet cafe and are not aware of how easily their location can be traced. The video they carry on USB sticks can be read on any computer and the people they capture on video may not be aware that they could be seen by thousands of people, all over the world, including the perpetrators of the injustices they may describe or have been subjected to. Anonymity and consent are little understood in Indonesia.

People have a right to free expression, but they too ought to have the right to anonymity should they wish it. Being seen and heard is one thing, being recognised and literally hunted down is another. It happens. Israeli authorities used Facebook to gather names of pro-Palestinian protesters and had them black-listed to prevent them travelling to Israel¹. Iran's authorities scrutinised mobile phone footage on Youtube to identify demonstrators whom they later arrested along with passers-by who just happened to be in shot². Iranians are also using crowd sourcing, a common social networking technique, encouraging the general public to identify alleged protesters in photos and video found on the web³. A more recent initiative has seen the general public swarm to Tumblr and Facebook offering their videos and photos of the hockey riots in Vancouver that raises serious questions about "name and shaming" and whether this constitutes "vigilantism or community policing⁴."

1 Last, J. Associated Press (July 2011), [Israel blocks airborne protest, questions dozens](#)

2 Gregory, S. (May 2011), [Watch: Cameras Everywhere – Presentation at Re:Publica 2011](#)

3 [GERDAB.IR](#) lists photos and stills grabbed from videos found on the web and calls for citizens to identify those individuals circled in red.

In addition to these ethical issues, many of which are being tackled through international forums and public discussion at every conceivable opportunity, there are immediate concerns regarding the day to day practise of video activists. For example, video files can be large and they can take time to upload. Getting them to a server from an internet cafe in Aceh, for example, can pose problems, particularly if connections are not secure, or more commonly, slow and costly. People need to be prepared, they need time and they need to be anonymous. Additionally, once online how secure and / or reliable is the site one publishes to? Youtube looks like a public space, but it isn't. Facebook encourages openness and sharing, but why does Julian Assange describe it as “the most appalling spying machine that has ever been invented⁵?”

As more video is produced and as more people, from all sectors of society use what ever means available to them hold up their cameras and send their images across networks and devices the means to do so ethically and securely needs to be both understood and readily available. The *Secure My Video Guide* contributes to this pool of knowledge and resources.

3. INDONESIAN CONTEXT

(Compiled from VIDEOCHRONIC and GISWatch 2011 Indonesia Country Report)



Camera phone in Kebayoranbaru, Jakarta
(Photo by nSeika, CC BY-NC-SA)

Since 2000 Indonesia has seen a dramatic increase in the use of video as a social change tool by community, campaign and activist organisations. Access to the tools for producing video have become increasingly democratised over this period, and rapidly adopted. Since the fall of Suharto's New Order regime, space has been opened up for a host of new media projects to emerge. Individuals and organisations dealing with issues such as the environment, human rights, queer and gender issues, cultural pluralism, militarism, poverty, labour rights, globalisation and more have embraced video as a tool to communicate with both their bases and new audiences.

4 Gruszko, M. WITNESS Blog (July 2011), [Crowd-Sourcing Surveillance: When Does Little Brother Get Too Big?](#)

5 Reisinger, D. C-Net News (May 2011), [Assange: Facebook is an 'appalling spy machine'](#)

The experience of the 1998 political uprising that overthrew the Suharto regime demonstrated the power of digital video in generating extensive socio-political changes by mobilising people in support of a new government. In the build up to the end of the regime, footage of the shootings of Trisakti University students in Jakarta, much of which was 'amateur' footage shot by bystanders, was aired on television inside and outside Indonesia. These images sparked sentiments of national solidarity, leading to mass student protests in several cities across Indonesia, denouncing the New Order regime.

However, today, without the same momentum of mass direct action on the streets that characterised the end of the 20th century in Indonesia, the ways that video can be used to affect change are more ambiguous. Realising that they cannot rely on the foreign press to expose humiliating human rights violation cases, campaigners push their videos through other avenues, such as EngageMedia, YouTube, and Facebook, where, instead of relying on news corporation producers activists can become the producers and distributors themselves. In becoming more independent, however, this also shifts their responsibilities, particularly concerns regarding security, both in relation to themselves and whomever they bring to screens across the planet.

Not only is there little knowledge of internet and digital data security issues throughout Indonesia, there is poor understanding of the implications of uninformed consent, particularly in the case of footage that could undermine the security of those interviewed and by-standers who just happened to be in shot.

With broadband concentrated in major capitals, inconsistent internet access elsewhere, humidity that can play havoc with all forms of data storage from tape to the organic dye layer of writable CD-ROM and DVDs and increasingly sophisticated forms of digital surveillance pervading social media spaces the challenges are many, but not insurmountable.

4. SUMMARY OF ISSUES

Shooting securely

In the field one can either plan ahead or, if in the wrong place at the right time, work quickly to document events as they play out. If you have the luxury to plan your shoot you can decide on the most suitable camera for the task and prepare it accordingly. You can also inform those whom you might interview of the implications of their appearance on camera, giving them to choice to consent to being seen or to remain anonymous. But if you don't, then you have to make do with what you've got and be prepared to take minimise the risk to yourself, your sources and your subject(s).

Case study

On Sunday 6 of February the minority Ahmadiyah sect in Cikeusik, Indonesia, sustained a brutal and fatal attack by some 1500 people carrying and bamboo, rocks and machetes⁶. In spite of the presence of up to 30 armed police officers, the Ahmadiawere overwhelmed. The entire attack was captured on video in graphic detail. The uploader, wanting to support the Ahmadi, published the video almost immediately after, however some of the Ahmadiyah members captured on camera were further terrorised. Even so, with so much evidence available and the video screened on national Indonesian television days after the case has languished in the courts and the perpetrators yet to be brought to justice.

6 Rayda, N. Horrific Video Shows Brutality of Attack on Ahmadiyah, Jakarta Globe, <http://www.thejakartaglobe.com/home/horrific-video-shows-brutality-of-attack-on-ahmadiyah/421214>

In this example the intention to raise awareness encouraged reprisals on those identified on video. In addition, that the video was published at all has not aided in the Ahmadi case, one of many such cases that has lowered the public's faith in Indonesia's court system.

Known issues and what you can do

- **Identification:** Cameras are ubiquitous. Each can identify the user in the own way. If you wish to remain anonymous consider the following conditions and the precautions you can take.
 - Touch screen interfaces, on smart-phones and pads capture traces of not only commonly used features but characters too. A high-contrast photocopy of a touchscreen may yield fingerprints and even passwords. Wipe frequently!
 - Lenses too, if not handled correctly, can reveal fingerprints and unique forms of grime that can identify and / or locate where devices have been. Clean lenses frequently. Wipe with a lens cloth in a circular motion from the centre of the lens out.
 - Meta data on all digital camera devices can locate the geographical location of any shoot. This can be useful when needing to validate what has been recorded, but it can also put people at risk. If risk is an issue ensure all location recording is switched off.
- **Visual anonymity:** Not everyone wants to be recognised on video. As evidenced in the case study surviving victims sustained reprisals as they were easily identified once the video went online and viral.
 - If you've captured a critical event weigh up the implications of getting it online. Will it help or hinder the cause? What can I do to protect the identities of those I've filmed? Who have I filmed that has nothing to do with the event, and will their appearance implicate them in the incident?
 - Make the time to think through these issues. If identification is an issue, take the trouble to blur the faces off all those people you feel may be at risk if identified. If in doubt, blur that face out!
 - The development of applications, such as [ObscuraCam](#) by [The Guardian Project](#), are particularly useful for people without a background and / or training in video production. That is, individuals who have little knowledge to mitigate the ethics of filming in critical situations and how to prepare videos prior to publishing online. These applications are designed to blur/disguise faces either whilst filming or directly after.
- **Securing consent:** In some countries videoing someone without their knowledge or consent could land you with a lawsuit, or worse, for invasion of privacy. It could also do more damage for the cause you intend to support if those you intend to video have no idea what your intentions are. Implied consent, where someone indicates they're aware they're on camera, may be enough to get you over the privacy issue hurdle, but may not protect those you're going to have appear in your video. You may not even know where your video could end up. In the spur of the moment you may not have time to secure anyone's consent, but if you do, it's your responsibility to ensure people are well informed.
 - Ask yourself these few questions:
 - Do the people you have in mind to film know your intentions?
 - Do they know your video will be published, where it might be seen and how far it may spread?
 - Do they know what the Internet is?
 - How can you best protect your sources?

- Advise your subjects about your project's intentions. What is it, why are you making it and where do you intend it to go?
- Make sure people are aware that if it goes onto the Internet it may be viewed by not only supporters to their cause, but by their perpetrators too.
- Finally, you can secure their consent by having them:
 - Sign a consent, or release form;
 - If you're not carrying hard-copy release forms, get their consent on video;
 - Alternatively, if you're smart-phone savvy, have their photo, audio or video consent appended to a pre-prepared consent template. Tools such as [Evernote](#) can be used for such purposes, and particularly useful because you can back these materials up online.
- **On-location security:** If you're holding a video camera and you're in a volatile situation you could be a target and so to any one that may be with you. Even journalists, with press passes, are no longer safe in some areas of conflict. It pays to be discrete. Here's a few suggestions.
 - Do you really need to video the even that's playing out in front of you? It might be just as effective, and less dangerous to record audio. Ensure you have options.
 - The smaller the camera the more discrete you can be.
 - In some situations it might be prudent to have two cameras available. Another person would carry a hidden camera whilst you carry the more obvious one. This way, if your camera is confiscated not only can your team keep shooting there's a record of anything that may happen to you.

Resources:

- [Informed Consent](#) (WITNESS)
- [Safety and Security Tips](#) (WITNESS)
- [Tips on How To Film With Your Mobile Phone](#) (WITNESS)
- [The Guardian Project](#)
- [Release Form Templates](#) (open licensed)

Storing securely

Storage devices are conceivably more easily concealed, but even-so, any device can be easily read for its contents. Almost every digital device, from a cell phone to a GPS is a store for data. The general rule of thumb is to back everything up. However, in some cases even backups may be compromised.

Known issues and what you can do

- **Environmental conditions:** High temperatures and humidity can affect some forms of storage. Commonly known as **bit rot**, CDs and DVDs are known to grow mould rendering them unusable. Magnetic tape is also pre-disposed to deterioration in these conditions.
 - Air tight and water resistant, re-sealable plastic bags can be used to protect video tape, SD cards, USB sticks and other digital media. Carry such bags with you at all times.
 - Tapes can also be risky for the Indonesian humid environment. Make back up every 5 years, and store in re-sealable, water resistant plastic bags. Make sure the air in the bag is sucked out with a vacuum cleaner. Store in a cool, dry place. If possible use a dehumidifier.

- Unstable electricity supply should be avoided. If possible, use an uninterrupted power supply (UPS) at your work place. In the field protect your devices with power surge protectors and limit the use of external drives. Sudden loss of power can result in corrupted or loss of data.
- **Resource limitations:** If you don't have access to low-cost broadband, nor secure access and funds to cover storage on cloud based back-up services, such new storage mediums are out of reach to most Indonesian activists.
 - **Resource limitations solutions noted for further research.**
- **Video files are huge:** Video consumes much more data than other digital mediums. Under Windows operating systems storing large files can be tricky. Many drives are formatted as FAT32. FAT32 will not support files larger than 2GB. This is not common knowledge.
 - Using H.264 codec to achieve smaller video file size without losing too many details (http://en.wikipedia.org/wiki/H.264/MPEG-4_AVC)
- **Unencrypted data:** Without data encryption all digital data, including Blue Ray, can be retrieved no matter the format. Tapes offer no encryption.
 - One of the most secure forms of data encryption, for both storage and when one is on the move, is [TruCrypt](#). Available for all platforms you can carry TruCrypt files on any device. Picture or video files can be camouflaged as different file types by using True Crypt, stored on any device including data DVDs.
 - Encrypt entire data and drives for both Mac and PC (note neither options have been tested):
 - Mac / Encrypting an entire hard disc.
Select Security & privacy > filevault
 - Windows 7 Pro / Bitlocker is available with the operating system.
<http://technet.microsoft.com/en-us/magazine/2007.06.bitlocker.aspx>
- **Storage options – too many choices:** There are so many storage options available to use now, but which are the safest and most secure? SD cards, for instance, have a known life span of around 100,000 write cycles. You may need back-up for your back-ups!
 - USB memory sticks, SD cards, external drives and video tape (DV, HDV) are preferred by activists and videographers in Indonesia.
 - Portable, quick to transfer data, cheap, unaffected by magnetic fields and can be stored in high humidity conditions and have been known to survive washing machines.
 - Digital tape can be a useful storage option if you have the means. Easily store raw, uncompressed video data, storage is time based, not volume based. However, tape deteriorates in humidity, requiring temperature controlled storage in high humidity conditions.
 - Magnetic will eventually break. For long-term storage, use SSD devices (read only, write once) because it does not uses magnetic components, however the price is expensive.
- **How secure is *the cloud*?** In September 2011 South Africa's MyVideo lost thousands of of their uses videos due to poor server maintenance and back-ups. GoogleVideo closed its doors early 2011 and countless videos are no longer accessible. In both instances large numbers of people relied on these services to keep their videos accessible in perpetuity. If you don't have reliable data storage of your own, relying on a third party provider can be perilous.
 - **Cloud computing alternatives / solutions noted for research.**

Resources:

- **Resources to be researched.**

Publishing securely

You need time to upload video and the internet may know who and where you are. The IP address from where you publish a video can be concealed, but if your video contains recognisable faces they can and will be identified. Facial recognition software is now widely spread.

Additionally, publishing via mobile devices can be risky. Carriers may collude with authorities to shut down networks, intercept video uploads and provide details of individual users. Mobile phones, for instance, may also embed your location within video meta-data.

Case study

The problems for activists in Papua are many and perilous. When Papuan leader Agus Alua died, text messages were blocked for almost 24 hours in Jayapura preventing, for instance, any coordinated response. Intelligence officers are known to act as phone credit sellers in order to obtain the numbers of suspected Papuan activists which are then alleged to be shared with the Special Forces (Kopassus).

Getting online comes with its own complications. The fastest and most reliable networks are only accessible nearby government buildings and military commands. As such, using poor bandwidth as an excuse, many internet cafes in Papua block YouTube.

Then there are the costs. In some remote areas certain Internet cafes charge a fee simply for opening a Facebook account.

Once you're there, do you publish under your name or anonymously? Publishing anonymously is little known in countries like Indonesia and in many other countries it is not encouraged.

Known issues and what you can do

- **Bandwidth constraints:** Whilst there are bandwidth constraints in Papua, many other parts of Indonesia are better serviced.
 - Publish preview clips and provide an alternative means to distribute the entire video. For example, ICT Watch publishes short clips on YouTube and post CDs or DVDs on email request.
 - Shared directories on services such as Dropbox are a viable option so long as you can afford storage costs and rely on the service to keep your videos online.
 - Establish a trusted offline network to assist in distribution.
- **Publishing without the consent of your subjects:** Responsible shooting and distribution.
 - Refer to *Securing consent*, page 4.
 - To secure the safety of their members some NGOs urge their members to upload videos under the name of their organisations so that the liability falls to them, not individuals producers who may not have the resources to combat any likely repercussions.

Outstanding issues / research questions

- Uploads from mobile phones can be intercepted and / or meta data provided to authorities. How can such practices be mitigated?
- What can online service providers do to assist in mitigating the threat to publishers (see WITNESS, [Recommendations for Online and Mobile Service Providers](#))?
- How can we address bandwidth constraints? Is this purely a technical problem, or can video producers employ more sophisticated compression tools, or limit themselves to shorter clips?

- What are the most efficient compression tools that provide the smallest file sizes and clearest image? Noting clarity is required for authentication purposes.
- What are the regulatory requirements of mobile phone carriers in Indonesia in terms of user / client privacy? What kind of information are carriers required to make available to authorities and under what circumstances?
- Which mobile phones geo-locate by default and which are optional?

Visual anonymity

The right to free expression sits side-by-side with the right to remain anonymous. However, not all governments value this and many are still debating the pros and cons of a charter of rights that supports anonymity on the internet.

People want to speak out, but not everyone may want to be recognised. The question is, how can we work within such a powerful and visual medium and yet remain anonymous?

Known issues

- Many citizen journalists are not aware of the potential reach of their work, nor issues of consent. Hence, they are unable to forewarn their subjects, nor seek their consent in using an identifiable image.
- Multiple devices may cover the same issue putting everyone within view at risk of being identified whether associated with the event or not.
- Multiple views can, in spite of the risks, ensure a single event may be more positively authenticated.
- The use of paper-based clearance forms, the practice of one-to-one consent, may not be a feasible tool in remote practice, and certainly not in immediate response situations. They too can pose a security threat by the mere fact of their physical properties.

Outstanding issues / research questions

- What means are there to easily explain these complex issues to both citizen journalists and, for example, their interviewees (e.g. WITNESS and YouTube collaboration⁷)?
- Is there a role for online service providers (see WITNESS, [Recommendations for Online and Mobile Service Providers](#))?
- Explore the notion of embedding the idea of consent into the process of video documentation.

Hosting securely

Hosting video content is not a minor task. Unlike text based content backing up discs crammed with videos can take hours, if not days. If an independent video hosting site goes down what can be done to ensure its content is available elsewhere and within an acceptable period of time?

Case study

To research: case study recommendations from spring are the film 'Fitnah' and the 'Mohammad cartoon' as well as the Elga and Arus Pelangi sites that were blocked early 2011.

⁷ WITNESS Blog (June 2010), [Protecting yourself, your subjects and your human rights videos on YouTube](#)

Known issues and what you can do

- **Websites are vulnerable to all manner of threats, from take-down-orders to DDOS attacks.**
 - Organisations are urged to regularly conduct monitoring of their whole website system as preventive measures.
- **Backing up server content is critical, but also time consuming if not done frequently.**
 - Don't rely on just one mirroring location.
 - There are bloggers who create several mirrors to protect their blogs.
- **What are the least time-constrained means to ensuring an independent video hosting site such as EngageMedia and its primary content can be effectively mirrored during a period of crisis?**
 - Issues to consider:
 - Bandwidth
 - The targeted audience
 - Networking
 - Things to do:
 - Caching content using reverse proxy
 - Tuning maximum connection on web server
 - Use mod_security, [how to implement mod_security](#).
 - Use rsync to synchronize to another server
- **Is it feasible to co-locate video content at the point of publication?**
 - Establish network between organisations
 - Improvise with domain name
 - See MalaysiaKini case
- **What networks and projects are available that can respond to threats a video hosting site (e.g. APC Rapid Response).**
 - [Team Cymru](#)
 - [Rise Up](#)

Outstanding issues / research questions

- The cost of transferring a video hosting sites data to a voluntary mirror may be prohibitive.
- There are local regulations which threaten video publications.
- Facebook status can be liable.
- There are many similar cases that sit in the police and courts without getting much publicity.
- Are there regulatory protections available to hosting providers in Indonesia and if not, for instance, under what circumstances can a take-down-order be issued?

- What are the regulatory tools authorities can implement to prohibit video hosting in Indonesia? For example, what kind of subject matter would be consider in violation of Indonesian communications law?

5. REFERENCES

The following materials have been provided as a means to assist in either improving on, contributing to or identifying gaps in video security.

- [Human Rights Video, Privacy and Visual Anonymity in the Facebook Age](#)
- [The Secure Smart Camera App for Human Rights Video](#)
- [WITNESS Blog - all articles on security](#)
- [Cameras Everywhere: Our New Leadership Initiative](#)
- [Watch: Cameras Everywhere – Presentation at Re:Publica 2011](#)
- [Collaboration with YouTube on The Power of Human Rights Video](#)
- [The Guardian Project](#)
- [Tor on Android](#)

6. ACKNOWLEDGEMENTS

This *work in progress* guide would not have been possible without the support and participation of the following:

Sam Gregory and Chap Day (WITNESS), Yerry Niko Borang, Enrico Aditjondro, Alexandra Crosby, Cheekay Cinco and Andrew Lowenthal (EngageMedia), Ahmad Yunus (WatchDoc), Wempie (JPIC), Lexy (Off Stream), Ahmad Aminudin, Ian Keikai, Donny Budhi Utoyo (ICT Watch).

Secure My Video Guide was researched and authored by Andrew Garton (EngageMedia).

7. ABOUT ENGAGEMEDIA

[EngageMedia \(www.engagemedia.org\)](http://www.engagemedia.org) is a non-profit media, technology and culture organisation. We use the power of video, the internet and free software technologies to create social and environmental change. We believe independent media and free and open technologies are fundamental to building the movements needed to challenge social injustice and environmental damage, as well as to provide and present solutions.

EngageMedia works with independent filmmakers, video activists, technologists, and campaigners to generate wider audiences, demystify new video distribution technologies, and create an online archive of independent video productions using open content licenses.

Australia office:

6/225 Bourke Street
Melbourne, 3000, Vic
Australia

Indonesia office:

Jl. Pati Unus no. 9
Kebayoran Baru, Jakarta Selatan
Indonesia, 12120