CAMERAS EVERYWHERE

CURRENT CHALLENGES AND OPPORTUNITIES AT THE INTERSECTION OF HUMAN RIGHTS, VIDEO AND TECHNOLOGY

WITNESS

SEE IT
FILM IT
CHANGE IT

WITNESS WOULD LIKE TO THANK ALL THE INTERVIEWEES AND EXPERT READERS WHO GAVE THEIR TIME AND EXPERTISE TO INFORM THE ANALYSIS AND RECOMMENDATIONS IN THIS REPORT. THIS REPORT WOULD NOT HAVE BEEN POSSIBLE WITHOUT THEIR GENEROSITY AND OPENNESS.

REPORT TEAM

SAMEER PADANIA
Director, Macroscope & Consultant to WITNESS

SAM GREGORY
WITNESS Program Director

YVETTE ALBERDINGK-THIJM
WITNESS Executive Director

BRYAN NUNEZ
WITNESS Technology Manager

For further information, please contact:

WITNESS
80 Hanson Place, Fifth Floor
Brooklyn, NY 11217
+1-718-783-2000
cameraseverywhere@witness.org
www.witness.org

BIOGRAPHIES

SAMEER PADANIA runs Macroscope (http://blog.sameerpadania.com/), a research, policy and advocacy consultancy working on the future of human rights, media and technology. From 2006 to 2010, he worked for WITNESS, running the HUB, the world's first online platform dedicated to human rights video, and co-conceived the *Cameras Everywhere* Leadership Initiative. Prior to this, he worked at *Panos* London for six years to support and strengthen radio and online journalism in the developing world, and published policy reports on British public interest media and on local radio and journalism in Africa. Sameer has also worked as a documentary researcher and film writer, and is on the Board of New York-based archaeology foundation, Archaeos.

SAM GREGORY helps people use the power of moving images to create change. He is the Program Director of WITNESS where he oversees WITNESS' programmatic work, including supervising the Campaign Partnerships, Tools and Tactics, and Leadership initiatives. Over the past decade he has worked extensively with human rights activists, particularly in Latin America and Asia, to use video to push for changes in policy, practice and law.

Within WITNESS *Cameras Everywhere* Leadership Initiative, he identifies solutions to the challenges, and ways to capitalize on the opportunities presented by increasingly ubiquitous video for human rights. Sam has created training tools and programs, including the WITNESS Video Advocacy Institute, was lead editor on "Video for Change" (Pluto Press, 2005) and teaches a course called, "Human Rights Advocacy Using Video and Related Multimedia", as an Adjunct Lecturer at the Harvard Kennedy School. Sam graduated from the University of Oxford and completed a Masters in Public Policy as a Kennedy Memorial Scholar at Harvard. He currently serves on the Board of the U.S. Campaign for Burma, and the Advisory Board of Games for Change.

YVETTE ALBERDINGK THIJM is Executive Director of WITNESS. Prior to serving as head of the organization starting 2008, Yvette was on the WITNESS Board for four years. She has nearly two decades of experience in media, strategic partnerships and new technologies, which includes serving as Executive Vice President of Content Strategy and Acquisition at Joost, a global online video platform start-up launched by the founders of Skype. Yvette also spent more than a decade at MTV Networks International focused on its international growth and forays into digital media. She is a member of the Board of Trustees of the Foundation Center, a leading authority on organized philanthropy, and serves on the Board of Access, a global movement for digital freedom and the Advisory Board of Uncensored Interview, a digital platform for independent musicians.

BRYAN NUNEZ is the Technology Manager at WITNESS. He oversees technology for the organization as well as the development of projects like the HUB, a site for citizen human rights media, and the Secure Smart Cam, a camera-phone app for human rights activists. Prior to WITNESS, he was a technology strategist and consultant on a variety of projects ranging from online banking to interactive television. He is an alumnus of the Interactive Telecommunications Program at NYU and has a BA in anthropology from UC Berkeley.

ABOUT WITNESS

WITNESS is the global pioneer in the use of video to expose human rights abuses. We empower people to transform personal stories of abuse into powerful tools for justice, promoting public engagement and policy change. Founded in 1992, WITNESS has partnered with more than 300 human rights groups in over 80 countries, trained over 3,000 human rights defenders, developed widely-used training materials and tools, created the first dedicated online platform for human rights media, the HUB, and supported the inclusion of video in more than 100 campaigns, increasing their visibility and impact.

Videos made by WITNESS and our partners have told dozens of critical human rights stories, and have galvanized grassroots communities, judges, activists, media, and decision-makers at local, national and international levels to action. They have called attention to stories of slavery, trafficking and war crimes. They have secured basic rights to education, employment, housing and health care. They have improved the lives of children, the disabled, indigenous peoples, minorities, workers and women. WITNESS campaigns have empowered individuals and their communities to secure and protect their rights. They have shown us where governments and non-state actors have failed to meet legally-binding obligations. They have pressured those in power to act. And they have engaged millions of ordinary citizens in the struggles for human rights taking place every day all over the world.

TABLE OF CONTENTS

FOREWORD

FOREWORD

When people have suffered human rights abuses, it seems extraordinary that their experiences can then be effectively denied, buried and forgotten. Whenever there is video, their experience and stories are not only captured, but the video becomes a tool for change. WITNESS was founded in 1992 to bring video and technology into the human rights movement.

Today, almost 20 years later, technology is enabling the public, especially young people, to become human rights activists. With the global distribution of mobile phones, our original dream of getting cameras to the world is being realized and with that come incredible opportunities. Activists, developers, technology companies and social media platforms are beginning to realize the potential of video to bring about change, but a more supportive ecosystem is urgently needed.

This report asks the hard questions about how to protect and empower those who attempt to expose injustices through video. It provides specific recommendations for immediate and future actions that can reduce danger for those risking their lives. This report is an important step to understanding how we can harness the power of video and technology to empower activists to protect and defend human rights. This is the age of transformative technology.

PETER GABRIEL
Co-founder, WITNESS

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

From the Arab Spring, with its use of social media, cell phones and the internet, to the release of confidential documents by Wikileaks, new technologies and new approaches are challenging long-held assumptions about how human rights documentation and advocacy functions, and who does it.

Video has emerged as a key means through which human rights abuses can be exposed, while also contributing more broadly to ensuring that transparency, accountability and good governance are upheld.

But while video and other communications technologies present new opportunities for freedom of expression and information, they also present challenges and expose vulnerabilities. In the video age, more people, intentionally or inadvertently, have become human rights advocates than ever before. Those seeking to create lasting impact will need to develop new skills and systems for creating and handling human rights video, online and off. But their access, privacy and safety is dependent on a wider range of people too, from governments and international organizations, to companies such as Google, Facebook, Yahoo, Microsoft, Twitter and Nokia. Access to information, technology, skills and networks shapes who can participate – and survive - in this emerging ecosystem of free expression.

WITNESS' *Cameras Everywhere* aims to ensure that the thousands of people using video for human rights can do so as effectively, safely and ethically as possible. This report is based on discussions with over 40 senior experts and practitioners in technology and human rights. It presents a roadmap to emerging trends in policy and practice at the intersection of human rights, technology, social media, and business. *Cameras Everywhere* goes on to make specific recommendations on how important players in the new human rights landscape can take specific, manageable steps to strengthen the practical and policy environments for human rights video, and other information and communication technologies (ICTs) used for human rights.

There are five areas that present the most pressing challenges: Privacy and Safety; Network Vulnerabilities; Information Overload, Authentication and Preservation; Ethics; and Policy.

PRIVACY AND SAFETY

It is clear that new technologies, particularly the mobile phone, have made it simpler for human rights defenders and others to record and report violations, but harder for them to do so securely. The ease of copying, tagging and circulating images over a variety of platforms adds a layer of risk beyond an individual user's control. All content and communications, including visual media, leave personal digital traces that third parties can harvest, link and exploit. Hostile governments, in particular, can use photo and video data – particularly that linked with social networking data–to identify track and target activists within their countries, facilitated by the growth of automatic face-detection and recognition software.

Without proactive policymaking, legislative or regulatory loopholes will be taken advantage of where they exist. Technology companies, for example, must ensure that their products, suppliers and services protect users' privacy and data by default, and should place a greater focus on privacy by design.

It is alarming how little public discussion there is about visual privacy and anonymity. Everyone is discussing and designing for privacy of personal data, but almost no-one is considering the right to control one's personal image or the right to be anonymous in a video-mediated world. The human rights community's understanding of the importance of anonymity as an enabler of free expression must now develop a new dimension – the right to visual anonymity.

NETWORK VULNERABILITIES

Technology providers like Google and Facebook have recently been pushed to the forefront of human rights debates. The responsibility of these providers as intermediaries for activist and human rights purposes have been brought into focus by the Arab Spring. Though activists have long been using websites, like Dailymotion and YouTube, to rally and inform their supporters, almost none of these sites has a *human rights* content category, whether for user contributions or for curators or editors. Providers do not have publicly available editorial policies or standards specifically focused on human rights content. Some activists have faced content, campaign or even account takedown for "violating" terms of use policies. Video content is vulnerable to interception, takedown and censorship, and needs active protection. Mechanisms are evolving to make automatic censorship of video content more widely possible. On commercial platforms videos showing graphic violence or killing are vulnerable to takedowns. Copyright policy, backed by powerful music/film industry lobbies, impacts public interest content using parodies or remixes.

Surveillance technologies that can have a legitimate law enforcement use, such as in tracking child exploitation online, can also be used to block or censor political or human rights content or to covertly monitor advocates. International standards for scrutiny and export control of such dual-use technologies do exist, but these need revision and strengthening.

We must increase the resilience, reach and accountability of communications networks, public and private. The human rights community must also invest in alternative means of communicating, preserving and distributing human rights content.

INFORMATION OVERLOAD, AUTHENTICATION AND PRESERVATION

With more video material coming directly to the public from a wider range of sources, it is increasingly urgent to find ways to rapidly verify or trust such information. Alongside more manual, forensic techniques of verification, technology-driven initiatives are underway to provide technical verification and digital chain-of-custody footage, and to help underpin the use of video in evidentiary, legal, media and archival contexts. However, significant questions remain over how to vouch for authenticity, protect safety, and communicate the original intention of human rights footage. Civil society organizations may need to develop common information standards or shared protocols –or adapt them from journalism.

As the store of human rights content grows, curating and aggregating it in ways that are clear and appealing becomes a major challenge. In addition, ensuring that human rights video remains persistently available is important for awareness, advocacy and justice – and commercial organisations cannot be relied upon to do this. Neither is it easy for individual users of commercial platforms and technology to understand how to back up their human rights content, especially in crisis situations.

ETHICS

The place of ethics in social media content and conduct is increasingly under the spotlight, primarily around usage by young people and other potentially vulnerable

groups. Human rights needs, including how consent of video participants is secured, can come into conflict with the free flowing spread of content and identity through social media. Ethical frameworks and guidelines for online content are in their infancy and do not yet explicitly reflect or incorporate human rights standards.

More needs to be done to tie together ethics in digital spaces with ethics in the physical world, which might prove helpful both for those "born digital" and those that are not.

POLICY

Technology, and the internet in particular, evolves much more quickly than legislative and policy responses to it. When policy responses are introduced, they are often inconsistent across different policy domains and, moreover, developed behind closed doors, beyond public debate and scrutiny.

United States and European Union policy towards the internet and mobile communications strongly influences similar policies in other parts of the world. Yet neither the United States nor the European Union routinely applies human rights standards in forming internet policies. Intergovernmental organizations such as the UN are–in general–not yet agile players within the policy-making arena of the internet, though some specific agencies and Special Rapporteurs are developing new, widely-consulted frameworks. Meanwhile some governments, notably China, are making headway both shaping policy against freedom of expression domestically, and seeking to influence international standards bodies.

KEY RECOMMENDATIONS

Long-term and sustainable change for the effective use of video for human rights requires genuine engagement between civil society, business and government to be impactful. We outline several key steps–for technology companies and developers, investors, human rights organizations, funders and policy makers–that must be taken to enhance the potential of video for human rights, and more broadly, to ensure that all people can use technology safely, effectively, and ethically.

TECHNOLOGY COMPANIES

Recommendations to technology companies and developers focus on four sets of changes–to policy, functionality, editorial content, and engagement. Making these changes would not only positively affect the entire environment for online and mobile video, but would also free up resources in civil society.

1. **Put human rights at the core of user and content policies:** Reevaluate current policies using human rights impact assessments, create human rights content categories that are not vulnerable to arbitrary takedowns and highlight key values around context and consent, and ensure content is preserved wherever possible.
2. **Put human rights at the heart of privacy controls and allow for anonymity:** Make privacy policies more visible and privacy controls more functional using principles of *privacy by design*, and allow for visual privacy and anonymity with the help of new products, apps and services.
3. **Create dedicated digital human rights spaces:** Support curation of human rights videos, facilitate user education and understanding of human rights issues, make takedown and editorial policies transparent, employ Creative Commons licensing, and support users in dealing with ethics and safety issues.
4. **Engage in wider technology-human rights debates and initiatives:** Draw on expertise across companies in order to collaborate on human rights guidelines, participate in multi-stakeholder initiatives, such as the Global Network Initiative, and address supply chain and environmental impact issues.

TECHNOLOGY INVESTORS

Venture capitalists and investors play a critical role in bringing high-quality technology products and services that could yield major gains to the human rights community.

1. **Put human rights at the forefront of investment:** Work to understand the human rights implications of technologies.
2. **Collaborate with human rights funders:** Use joint funding mechanisms for technology development for human rights.

HUMAN RIGHTS ORGANIZATIONS

The fight for human rights is increasingly intertwined with technology usage and policy. In the digital age, it is proving to be increasingly critical for human rights organizations to collaborate more with non-traditional partners, while standing firm on core universal human rights values, standards and principles until they take root in the technology sphere.

1. **Engage with technologists:** Dedicate resources and expertise to strengthening own capacity and communicating and collaborating with technologists on human rights issues.
2. **Support training and learning on using technology for human rights.**
3. **Collaborate more, compete less:** Create a human rights-technology network, coordinate cross-platform discussions and engage with key policymakers, civil society, media, business and technology funders/investors, and develop human rights principles for investments in information and communications technologies.
4. **Invest in research:** Develop more effective monitoring and evaluation systems, create predictive models that can anticipate trends in technology and policy that may impact human rights policy, and share findings with key players.

FUNDERS

Governmental, foundation and private donors play a critical role in conducting and supporting research, activism and advocacy on issues related to human rights and technology. To increase impact, their funding need to become more transparent, accessible, harmonized and less risk-averse.

1. **Increase transparency in funding around who is funding what and how.**
2. **Collaborate with other funders, investors and technology developers:** Create multi-donor spaces on technology and human rights, including emerging crowd-funding platforms, as well as new donors outside U.S./Europe, and create both joint funding mechanisms with investors and review boards that can assess risk in proposals.
3. **Lead in developing effective monitoring and evaluations methodologies for human rights and technologies.**

POLICY MAKERS

Policy and lawmakers play a central role in guaranteeing that citizens have access and the capability to use information technologies in a manner that protects and promotes their rights. They also often set the frameworks within which ICTs are governed and held accountable. The recommendations below are an initial subset primarily centered on the U.S. and EU.

1. **Review existing legislation for consistency:** Ensure policies are human rights-compatible across key areas of legislation and policymaking, both domestically and internationally.

2. **Update legislation on visual privacy issues:** Review the Safe Harbor Principles and EU Data Protection Directive and incorporate visual privacy data into existing restrictions on the transfer of personal data between countries.
3. **Review national legislation and international agreements on dual-use technologies:** Scrutinize and update monitoring practices for dual-use technologies, particularly those used by repressive regimes and other governments for repressive purposes.

WITNESS NEXT STEPS

WITNESS will work to ensure that the millions of people turning to video for human rights can do so as effectively, safely and ethically as possible. Never before has there been such potential for diverse stakeholders to harness the possibilities of human rights video. As video becomes more central to human rights struggles, WITNESS will deepen our global leadership role by fostering a more conducive environment for video to support human rights. We plan to:

1. **Create WITNESS Labs:** Support a series of collaborations with technology developers to create innovative tools that support human rights and address the challenges raised by the increasing use of video, particularly within grassroots human rights campaigns.
2. **Engage with key stakeholders in technology and human rights:** Advocate on the key recommendations outlined in this report through private advocacy, public discussions, events, blogs and online debates.
3. **Build broad-based digital media literacy and advocacy skills for effective use of video:** Develop comprehensive training tools, effective guidelines and spreadable media to support a growing number of human rights video-users.
4. **Promote public policy solutions:** Review participation in multi-stakeholder initiatives, push for further discussion around visual privacy, and facilitate collaborations with key players on critical issues outlined in this report.
5. **Mobilize support for a growing field–"Why Video Matters":** Through collaborative research and reporting, further deepen the evidence-based understanding of the challenges and opportunities that video and related technologies can play in facilitating social change.

INTRODUCTION

CAMERAS EVERYWHERE: CURRENT CHALLENGES AND OPPORTUNITIES AT THE INTERSECTION OF HUMAN RIGHTS, VIDEO AND TECHNOLOGY

Video is increasingly central to human rights work, campaigning and advocacy. It has been critical in drawing worldwide attention to corruption, torture, denial of rights and repression around the world. More human rights video is being captured, produced and shared by more people in more places than ever before, often in real-time. It is happening in organized and spontaneous ways, by people with training and without. In this video-saturated environment, those seeking to create lasting impact will need to develop new skills and systems for creating and handling human rights video online and off.

Video has a key role to play, not just in exposing and providing evidence of human rights abuses, but across the spectrum of transparency, accountability and good governance. Video and other communication technologies present new opportunities for freedom of expression and information, but also pose significant new vulnerabilities. As more people understand the power of video, including human rights violators, the more the safety and security of those filming and of those being filmed will need to be considered at each stage of video production and distribution. Access to information, technology, skills and networks shapes who can participate–and survive–in this emerging ecosystem of free expression. Poverty, inequality, marginalization, discrimination and repression reinforce the significant divides between those that can access this ecosystem, and those that can't.

New information and communications technologies (ICTs) –the internet, mobile phones, social networking sites, mapping and geospatial technologies like satellite imaging– are playing a powerful role in contemporary human rights work. From facilitating and strengthening networking among local activists to building international solidarity for a cause, from unearthing street-level eyewitness footage to providing satellite evidence of attacks on civilians, these new technologies are challenging long-held assumptions about how human rights documentation and advocacy functions and who does it. More and more people, including many who might not see themselves as human rights activists, are now using video and social media to create, share and organize around issues they care about.

This is, in turn, bringing a new range of players into the human rights field, many of whom never before regarded themselves as having a stake in human rights–most notably, leading social networks, social media platforms, internet companies, mobile manufacturers and operators, including companies such as Google, Facebook, Yahoo, Microsoft, Twitter and Nokia. By virtue of the sheer numbers of people using their products to document, share and expose human rights violations, these companies have both a stake and a say in how human rights are understood and handled worldwide and are increasingly being pressed to meet these responsibilities. What's more, local and international laws and policies that govern these companies often take little account of human rights needs or standards. This has been made much more apparent as the Arab Spring has unfolded.

The WITNESS *Cameras Everywhere* initiative aims to ensure that the thousands of people using video for human rights can do so as effectively, safely and ethically as possible. This report–accompanying other aspects of the initiative–is based on in-depth discussions with over 40 senior experts and practitioners in technology, media and human rights. We engaged decision-makers at major content publishers and technology platforms, senior staff at international human rights groups, policy-makers and legislators, journalists, experts and researchers in technology, privacy, and media. In some discussions we focused particularly on the opportunities presented by the growth in the use of video, in others, the broader context of the internet and technology. The report presents a roadmap to emerging trends in policy and practice at the intersection of human rights, technology, social media, and business.

While grassroots movements and human rights organizations are vital and remain at the heart of WITNESS' work, we must also recognize that the media, policy and technology sectors shape many of the standards and structures for the creation and distribution of human rights video. Opportunities for new kinds of thinking, partnerships and solutions to the challenges posed by new technologies are abundant. By setting the parameters within which video is created, seen and shared, these new human rights actors have the power to influence how grassroots activists can operate – and the scale of their potential impact. This report makes specific recommendations on how important players in the new human rights landscape can take specific, manageable steps to strengthen the practical and policy environments for human rights video, and other ICTs used for human rights.

We have identified key challenges in relation to:

- Privacy and Safety
- Network Vulnerabilities
- Information Overload, Authentication and Preservation
- Ethics
- Policy

These are shaping the immediate future of the human rights sector as it relates to visual media, and to ICTs more generally. In particular, the events of 2011 in the Middle East and North Africa have brought some of these challenges into sharper focus and highlighted the need for a more comprehensive lens trained on the intersection of human rights, the internet, new communications technologies and technology policy. The reality is we no longer have the luxury of treating these different sectors in isolation from each other. They increasingly intertwine and human rights run through all of them–we can no longer collectively pretend that this is not the case.

KEY CHALLENGES

KEY CHALLENGE: PRIVACY AND SAFETY

VISUAL PRIVACY AND ANONYMITY

With cameras now so widespread, and image-sharing so routine, it is alarming how little public discussion there is about visual privacy and anonymity. Everyone is discussing and designing for privacy of personal data, but almost no-one is considering the right to control one's personal image or the right to be anonymous in a video-mediated world. Imagine a landscape where companies are able to commercially harvest and trade images of a person's face as easily as they share email addresses and phone numbers. While it is technically illegal in some jurisdictions (such as the EU) to hold databases of such images and data, it is highly likely that without proactive policymaking, legislative or regulatory loopholes will be exploited where they exist. So far, policy discussions around visual privacy have largely centered on public concerns about surveillance cameras and individual liberties. But with automatic face-detection and recognition software being incorporated into consumer cameras, applications (apps) and social media platforms, the risk of automated or inadvertent identification of activists and others–including victims, witnesses and survivors of human rights abuses–is growing. No video-sharing site or hardware manufacturer currently offers users the option to blur faces or protect identity. As video becomes more prevalent as a form of communication and free expression, the human rights community's long-standing focus on the importance of anonymity as an enabler of free expression needs to develop a visual dimension–the right to visual anonymity.

NETWORKED AND MOBILE SECURITY

Networked technologies - mobiles, social networks, cameras, media-sharing sites - are ever simpler to operate, but not to control. This is both a strength and a vulnerability of online, mobile, hardware and apps. New technologies have made it simpler for human rights defenders (HRDs) and others to record and report violations, but harder for them to do so securely. The ease of copying, tagging and circulating video, while helpful for some human rights situations, does add a layer of risk beyond an individual user's control. All content and communications, including visual media, leave personally identifiable digital traces that third parties can harvest, link and exploit, whether for commercial use or to target and repress citizens. This creates new kinds of risks for the safety and security of frontline HRDs and for those they film or work with. HRDs routinely use these platforms and tools for advocacy, or in crisis situations, but neither the HRDs nor the respective technology providers are always aware or prepared for the risks inherent in using these technologies for human rights work.

Mobile phones, while perhaps the most power-shifting device for activists, are widely regarded as introducing significant new human rights risks. In general, it is easier to be located and identified, and simpler to have your communications intercepted on mobile devices than it is on the internet. Although some responsibility clearly rests on HRDs and other users to protect themselves, the platforms and services they use bear significant responsibility to provide users with adequate warnings, guidance and tools related to safety and security. To help guard against these risks, technology providers are facing calls to integrate privacy thinking throughout their design and development processes (e.g. the principle of *privacy by design*) in order to make privacy controls easier to find and manage. They must ensure that their products, suppliers and services protect users' privacy and data by default.

CASE STUDY: FACIAL RECOGNITION, CROWD-SOURCING, PROTESTORS AND RIOTERS

Facial identification based on videos taken at protests is a growing concern for human rights defenders (HRDs). Images of crowds at protests and riots can be fed into automated facial recognition systems that can be used to identify individuals. Meanwhile, crowd-sourced identification adds to the networked risks that HRDs face.

During Iran's 2009 Green Movement protests, the Islamic Revolutionary Guard Corps (IRGC) posted to a website that was created visuals of opposition activists taken mainly from videos and photos on public video-sharing and social media sites. They asked people to contact the IRGC if they could identify the individuals shown. Since then, citizen surveillance has moved to North America and Europe. The Vancouver Police Department solicited witness footage of alleged rioters following the Stanley Cup riots in June 2011, and London's Metropolitan Police uploaded photos of alleged rioters in August 2011 to its Flickr account and asked for help identifying them. In both cases, the public responded enthusiastically and continued the work of identification outside of official channels.

KEY CHALLENGE: NETWORK VULNERABILITIES

TECHNOLOGY PROVIDERS AS HUMAN RIGHTS FACILITATORS

Recent efforts by governments across the Middle East and North Africa to block or track social media services, the takedown of technical and financial services to WikiLeaks under apparent pressure from the U.S. authorities, as well as the increasing use of social networks like Facebook for organizing, have pushed technology providers to the forefront of human rights debates. The responsibility of technology providers as intermediaries for activist and human rights-focused users has become a part of mainstream media discussion. Activists and citizens have long been using privately-owned websites and networks in the public interest, yet almost none of these sites or services mention human rights in their terms-of-use or content policies. Strict policies can restrict freedom of expression. On some leading social networks and social media platforms (notably Facebook and Google+) activists have faced content, campaign or even account takedown for using pseudonyms to protect their identities. No mass platform or provider has a *human rights* content category, whether for user contributions or for curators or editors. Providers do not have publicly available editorial policies or standards specifically focused on human rights content. Though one could argue that this offers a useful degree of flexibility and makes content less conspicuous, systems that protect public interest content on social media networks are overall ad hoc and haphazard rather than systematic.

Furthermore, personalization of web services, such as *social search*–where search results or suggestions of related content are personalized according to what your social network is viewing–could increase the fragmentation of human rights content online, reduce the reach of controversial content and adversely impact freedom of information and expression.

CASE STUDY: AMAZON AND WIKILEAKS

Days after publishing a trove of classified U.S. diplomatic cables in November 2010, whistle-blowing website, Wikileaks, came under massive Distributed Denial of Service attacks, attempting to bring the site down. Wikileaks tried moving to an Amazon cloud server, but within days was kicked off of Amazon's servers. Amazon reps stated that Wikileaks had violated its Terms of Service (ToS). At the same time. U.S. Senator Joe Lieberman also claimed that it was he who requested the Wikileaks shutdown.

If Amazon's version of the event is true, then the public's right to know was determined by a private company's individual ToS. However, if Lieberman's statement is correct, then this shows how vulnerable human rights activists are to government pressure, even in democracies.

CASE STUDY: YOUTUBE AND HUMAN RIGHTS VIDEO TAKEDOWNS

The trajectory of YouTube's policies on human rights videos–from removing videos by Egyptian activist Wael Abbas in 2007 to keeping videos of protests in Iran on the site in 2009–demonstrates both the growing role for video in human rights movements and a rising awareness of human rights activists' use of YouTube. YouTube took down Abbas' video evidence of police brutality because it featured graphic violence that violated its ToS. This meant not only that these videos instantly disappeared everywhere they had been embedded across the internet, but that the original URLs and comments associated with these videos also disappeared, taking away the viral phenomenon that his videos created. Since then, YouTube has re-considered its policy on graphic violence in videos and have decided to allow Iranians to upload their videos of state violence against protesters in 2009 and 2010, saying they consider the videos to be educational content.

VIDEO CENSORSHIP AND FREEDOM OF EXPRESSION

Video content is vulnerable to interception, takedown and censorship, and needs active protection. Because of the large file-size and easily-identifiable file suffix (.avi, .mp4, etc.), video files are becoming increasingly easy to monitor and intercept. Although less simple to censor using existing filtering technology, mechanisms are evolving to make automatic censorship of video content more widely possible. At the same time, videos showing rights violations involving graphic violence or killing can also be vulnerable to takedown or user-flagging. Encouragingly, platforms like YouTube are becoming increasingly sensitive to politically-motivated takedown.

Much video-based political and human rights

commentary actually parodies or remixes existing copyrighted images or music. This leaves them vulnerable to automatic takedowns on the basis of copyright infringement. Copyright policy, with its focus on anti-piracy messaging and powerful music/film industry lobbies, is often used to target political or human rights content. Copyright laws are coming under increased scrutiny, but policy recommendations rarely include proper consideration of public-interest and human rights-use cases, or the impact on freedom of expression and information. Alternative content-licensing or intention-signalling systems (such as Creative Commons) have yet to be adapted specifically for human rights purposes.

DUAL-USE TECHNOLOGY AND FREEDOM OF EXPRESSION

The capability to observe, filter and censor audio-visual media, as well as text-based content, is growing. Surveillance technologies that can have a legitimate law enforcement use, such as in tracking child exploitation online, can also be used by governments to block or censor political or human rights content or to covertly monitor their citizens. Such technologies are known as dual-use technologies. Online filtering, censorship and surveillance software employed and shared by governments threatens the overall environment for freedom of expression. Western companies selling communications-monitoring technologies to foreign governments such as Egypt, Iran or China have only recently come under scrutiny for complicity or collusion in censorship and repression. Similarly, companies training governments to use these technologies run the risk of making American and European companies complicit in human rights abuses and repression of free speech. China is thought to be sharing censorship technology and expertise with other states concerned about burgeoning online freedom of expression. International standards for scrutiny and export control of dual-use technology do exist, but these need revision and strengthening to meet the new and evolving challenges posed by new media.

VULNERABILITY IN THE CLOUD

Services increasingly store users' personal and other data in the digital cloud. Cloud data is processed and handled across multiple jurisdictions, creating potential inconsistencies and conflicts in how users and their data are protected. More worryingly, cloud storage renders data vulnerable to multiple attacks and data theft by any number of malicious hackers. Repressive governments, in particular, can use photo and video data–particularly those linked with social networking data–to identify, track and target activists within their countries. Legislative and ethical responses to these vulnerabilities currently range from being too restrictive to completely absent.

NETWORK CAPACITY AND ACCESS

All of us have a vested interest in keeping the Internet and other communication platforms open and free. But when mass communications are shut down or excessively filtered, activists, HRDs and other relevant stakeholders need fallback options. While it is proving harder to shut down communications networks entirely, lessons and tactics being learned in current crises need to be systematically documented and shared to enable effective ways to work around connectivity shutdowns. As video, mobiles, and other ICTs become increasingly part of the infrastructure of the human rights movement, we must increase the resilience, reach and accountability of communications networks, public and private. At a policy level, attacks on net neutrality, both on the internet and on mobile networks, pose a threat to freedom of information and expression and to the ability to access coverage of human rights abuses. The human rights community must also invest in alternative means of communication, preservation and distribution of human rights content. While extending connectivity (through greater access to technologies) is important, relying on connectivity alone will not provide sufficient resilience for the human rights community, especially in crisis situations.

CASE STUDY: ANONYMITY AND GOOGLE

In February 2011, as part of a wider conversation about privacy and the use of ICTs in support of activism in the Middle East and North Africa, Alma Whitten, Google's Director of Privacy, posted a clarification of Google's position on anonymous usage of its services. Whitten explained that users could be unidentified, pseudonymous or identified and different Google products had different types of privacy controls that might be more suited to users in each of these situations.

Several months later, when Google+ launched, it was unclear which category the service fell into. After Google began issuing warnings and shutting down Google+ accounts that used pseudonyms, it has faced a barrage of criticism from Google users opposed to this "real-name policy". But even under anonymous and pseudonymous services, Google can identify its users and their contacts, not least through services like Social Search - and it is not clear under what circumstances this information is shared with governments, other companies or other users.

As this extends into users' visual identity - via YouTube, Picasa, Image Search and Streetview, for example - it is becoming increasingly apparent that the ability to stay anonymous on Google, and more broadly online, is extremely difficult for individuals to control.

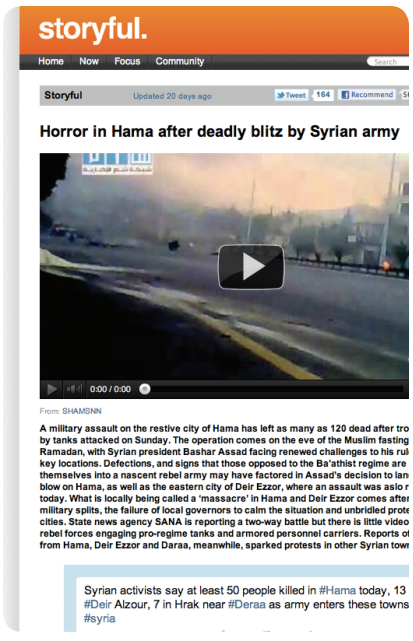
KEY CHALLENGE: INFORMATION OVERLOAD, AUTHENTICATION AND PRESERVATION

AUTHENTICATION OF CONTENT

With more video material coming directly from a wider range of sources, often live or nearly in real-time, and often without context, it is increasingly urgent to find ways to rapidly verify or trust such information. Civil society organizations may need to develop common standards or shared protocols–or adapt one from journalism–to explain how they ensure that their information is accurate and reliable. Adoption of such a shared standard could warrant new kinds of statutory protections not just for journalists, but also for other kinds of information providers.

Major journalism organisations like the BBC are learning as they go along, and are sharing emerging practices in how to sift, verify and curate social media content about human rights and humanitarian crises. Alongside more manual, forensic techniques of verification, more technology-driven initiatives are underway to provide technical verification and digital chain-of-custody of footage, to help underpin the use of video in evidentiary, legal, media and archival contexts. However, significant questions remain over how to vouch for authenticity, protect safety, and communicate the original intention of human rights footage. Initiatives to embed human rights concepts–like *do no harm*–within metadata need the involvement and backing of major video-sharing platforms, where the majority of this kind of video is seen and held, and by mobile manufacturers and networks, who supply the greatest number of cameras worldwide Without this, adoption of such standards will be niche at best. As live video streaming from mobile devices grows in prevalence, new questions will continue to arise. For example, how to reconcile expectations of total transparency and immediacy with the frequent need to edit footage to protect people's safety. Although there is near universal rejection of any further statutory regulation of content, self-regulation of content may soon emerge in the internet and social media industries in the U.S. and EU.

CURATION AND AGGREGATION



Everyone is struggling with how to present and help people make sense of the growing store of human rights content. Most widespread techniques for curating and aggregating video are still quite linear and rudimentary, such as chronological live-blogs or video playlists. Despite these limitations, news outlets, both large and small, are engaging more with eyewitness human rights material. They are providing readers and viewers with crucial context and triangulation for what they see and are ensuring that human rights issues raised by such material are debated by broader publics.

PRESERVATION OF HUMAN RIGHTS VIDEO

Ensuring that human rights footage and imagery is persistently available, whether publicly or in restricted archives, is important for awareness, advocacy and justice in the near- to mid-term, as well as for longer-term historical and research needs. The closure of the Google Video hosting service, and with it the loss of a trove of human rights video, brought the risks of relying on mass commercial platforms to the fore. At the moment, there is no systematic effort to gather and preserve online and offline human rights video and it is not easy for individual users of commercial platforms and technology to understand how to do so for themselves, especially when under time constraints in crisis situations.

KEY CHALLENGE: ETHICS

NEW ETHICAL CHALLENGES

The place of ethics in social media content and conduct is increasingly under the spotlight, primarily around usage by young people and other potentially vulnerable groups. Ethical frameworks and guidelines for online content are in their infancy, and although these are partly influenced by journalism standards, they do not yet explicitly reflect or incorporate human rights standards. Human rights needs, for example understanding how consent is secured from video participants, can come into conflict with the assumption of engineers and user experience specialists in social media companies, that content and identity must spread with as little "friction" as possible. There is still significant debate about how ethics for remixed, nonlinear media might differ from earlier types of media, specifically in how it is produced, stored, consumed and shared.

A culture of remixing (cutting existing pieces of content together into something new) presents challenges for human rights. Appropriating existing content (music/images/videos) and mixing it with fresh content in new ways is a cheap, effective, and popular form of political expression. However, remixing often relies on de-contextualizing footage that has a specific human rights purpose. More needs to be done to tie together ethics in digital spaces with ethics in the physical world, which might prove helpful both for those "born digital" and those that are not.

CASE STUDY: HUMAN RIGHTS PERPETRATORS ON FLICKR

In the aftermath of Egypt's January 25th movement, human rights activist @3arabawy uploaded a cache of videos and photos of State Security Police (SSP) officers that he had found at the SSP headquarters to Flickr. @3arabawy claimed that he had ensured that only SSP officers (many of whom are accused of committing torture) were visible in the images.

Subsequently, Flickr removed the images from its servers. It stated that @3arabawy had posted them in violation of Flickr's Community Guidelines, which require that images be created and owned by those who upload them. Activists pointed out that seeing non-original images on Flickr is common. Yahoo!, Flickr's parent company, wrote on its blog that it relies on users' reports to enforce its Community Guidelines.

Flickr took down the image set after a flurry of reports triggered a review of the set. Yahoo! argued that Flickr had the right to enforce rules that support the community of content creators it seeks to create. Yahoo! also claimed that creating an *human rights* category for images was overly restrictive and might endanger activists more than content moderation does.

KEY CHALLENGE: POLICY

POLICY IS SLOW, TECH IS FAST

Technology, and the internet in particular, evolves much more quickly than legislative and policy responses to it, often leaving the law out of step with practice. Policies that address technology are inconsistent both within and between particular policy domains. For example, trade, security and human rights policies each treat technologies differently and sometimes contradictorily. Laws and policies targeting content piracy under trade frameworks facilitate surveillance and erosion of privacy for citizens and activists, and constrain the space for free expression. Development of these laws is often done behind closed doors, beyond public debate and scrutiny. This can lead to repressive and aggressive, rather than protective and progressive, uses of technology. The Anti-Counterfeiting Trade Agreement (ACTA) for example, uses a trade framework to target copyright 'offences' like those of remixing in human rights video.

INCONSISTENT INTERNATIONAL STANDARDS

The internet is not borderless. It is increasingly governed and shaped on a national or regional level. However, U.S. and EU policy towards the internet and mobile communications strongly influences similar policies in other parts of the world–in both progressive and regressive ways. Yet neither the U.S. nor the EU routinely apply human rights standards when forming internet policies. Some governments, notably that of China, are shaping their domestic internet, openly and tacitly, and at the same time seeking to shape the broader environment of internet and technology standards through influencing international standards bodies. Governments, democratically elected or otherwise, argue that protecting national security entails sacrificing elements of individual privacy, and that this justifies measures they take to control or monitor the internet and mobile communications–or against transparency activists like WikiLeaks. Until the Tunisian and Egyptian uprisings of early 2011, online debate and dissent was seen as something of a safety valve by governments such as China, but this too is now being constrained.

Intergovernmental organizations such as the UN are not yet agile players within the policymaking arena of the internet. Select individual agencies (for example UNICEF) have placed a premium on innovation, and some Special Rapporteurs, individuals at the United Nations and other intergovernmental bodies tasked with oversight on particular human rights issues, have undertaken to understand the new landscape. They have developed new, widely-consulted, frameworks for how networked communication interacts with freedom of expression, as well as with business and human rights. Unfortunately, national human rights institutions are, in particular, ill-equipped to participate in and influence such debates. Additionally, around the world national-level civil society, legal communities and judiciaries lack the capacity to absorb, analyze and advocate around all these issues and need systematic strengthening.

RECOMMENDATIONS

RECOMMENDATIONS

In the past, businesses, governments and other stakeholders have been made aware of their impact on other global challenges–such as women's rights and the environment. Through pressure and support from civil society and citizens they have emerged to take a leading role in finding solutions. Long-term, sustainable change requires genuine engagement between civil society, business and government to be impactful. Below we outline several key steps–for technology companies and developers, investors, human rights organization, funders and policy makers–that must be taken to enhance the potential of video for human rights, and more broadly, to ensure that all people can use technology safely and effectively.

TECHNOLOGY COMPANIES

1. Put human rights clearly into content and user policies.

- **Create *human rights* content categories**
  - Create categories and build specific content review mechanisms (including an assessment of informed consent by individuals being filmed or uploaded) to deal with content tagged and flagged as human rights related. This should relate to a workflow addressing account deactivation requests related to human rights content.
- **Build-in human rights prompts**
  - For any content categorized or tagged as *human rights* related, build in prompts to encourage responsible usage of human rights content. This could include nudges for adding more context, confirming the consent and protecting the identity of individuals featured, and communicating how the uploader intends footage to be used.
- **Reevaluate current policy**
  - Conduct a human rights impact assessment of existing site policies, including mobile products, in consultation with relevant stakeholders, and make public the findings, along with recommendations for modifications.
- **Make human rights and privacy policies more visible**
  - Announce and highlight changes (additions or removals) to site, mobile or product policies that specifically address human rights and privacy vulnerabilities or concerns raised in human rights impact assessments or through other means.
  - Ensure policies relevant to human rights and privacy vulnerabilities are clearly presented, and in multiple languages.
  - Discuss clearly, publicly and transparently–to the extent possible–editorial decisions that illuminate human rights content guidelines.
- **Allow anonymity**
  - Explicitly permit, or at least tolerate, anonymous usage of sites and platforms, and pseudonymous use of user accounts.
- **Preserve human rights content**
  - Ensure that human rights content, wherever possible, is preserved and accessible across all platforms, languages and markets, including mobile. In light of recent service closures, such as Google Video, this is particularly important.

2. Improve functionality around visual privacy and anonymity.

- **Build visual privacy checks**
  - Incorporate data masking, such as that encoded into images (e.g. location, time, type of camera), as well as standard privacy checks into product design, development and marketing workflows.
- **Draw on risk scenarios outlined through human rights impact assessments.**
  - Follow the principle of *privacy by design*, and for products already in circulation, *privacy by default*. This is particularly important for products, apps and services that share this data with third parties that may not exercise the same diligence.
- **Build new tools**
  - Enable users to selectively blur faces, voices, and redact specific words and to use other relevant anonymization/privacy protection techniques directly at the point of upload (for platforms or social networks) or acquisition (for hardware or mobile apps), and to alter videos in this way after they have been published if necessary.

3. Create dedicated digital human rights spaces.

- **Curate content**
  - Support curation of human rights-related video content selected by appropriately qualified, trained or experienced individuals.
- **Create space for human rights content**
  - Create blogs/ toolkits/ discussion forums dedicated to strengthening user education and promoting broader understanding of human rights in the digital era.
- **Transparent takedowns and editorial decisions**
  - To the extent possible, document, make public and discuss transparently content or account takedown requests from all sources, identifying where these relate specifically to human rights situations. Explain publicly and transparently editorial decisions related to human rights content.
- **Employ Creative Commons licensing**
  - Encourage the most permissive licensing possible that corresponds with human rights concerns, so that content produced can be circulated and translated widely at the same time as being correctly attributed.
- **Make ethics and security easier**
  - Provide links at appropriate points in the mobile and online user flow to downloadable, mobile-ready video guides, supporting users to deal better with (informed) consent, protecting safety and security of those filmed and those filming, and vicarious trauma for those filming and those watching.

4. Engage with the wider technology-human rights debates and relevant multi- stakeholder initiatives.

- **Collaborate on human rights guidelines**
  - Participate in wider initiatives to develop, share and refine ethical codes or codes of conduct for increasingly ubiquitous video. These guidelines should specifically address human rights use cases.
- **Involve legal, product managers, executives and engineers, and customer-facing staff**
  - A range of these perspectives can best inform discussions and analysis on human rights and technology.
- **Participate in multi-stakeholder initiatives**
  - Participate in multi-stakeholder initiatives, such as the Global Network Initiative, that address human rights in the technology sphere.
  - Ensure that these processes, deliberations and decisions are–to the extent possible–transparent and public.

- **Address supply chain and environmental impact issues directly and transparently**
    - Utilize Human Rights Impact and Environmental Impact Assessments and make similar requirements of sub-contractors.

TECHNOLOGY INVESTORS

Venture capitalists and investors play a critical role in bringing high-quality technology products and services to market. Thus, incorporating small changes to product development and refinement processes could yield major gains in human rights terms, as has been shown from other socially-responsible investment strategies.

1. Put human rights at the forefront of investment.

- **Understand human rights implications**
    - Work with Global Network Initiative (GNI) and/or other multi-stakeholder groups to understand human rights implications of technologies.
    - Develop a simple human rights impact checklist for VCs for development of new products, especially in personal data or geolocation space.
    - Help developers understand and take into account the potential impacts of their work, and to consistently apply industry standards for cross-border data security and other protections.

2. Collaborate with human rights funders.

- **Create joint funding mechanisms**
    - Focus on technology development specifically for human rights, bringing expertise on technology investment to funding field.

HUMAN RIGHTS ORGANIZATIONS AND CIVIL SOCIETY

The fight for human rights is increasingly intertwined with technology usage and policy. However, human rights organizations, and civil society more widely, do not understand or integrate technology well enough to wield as credible influence as needed when advocating on issues of technology and tech policy. They must collaborate more and compete less, as well as learn to work with and learn from non-traditional partners, like technologists, technology companies, hackers, government, media and the security/intelligence community. But even as changes in technology appear to indicate shifting values, human rights organizations must continue to stand firm on core universal human rights values, standards and principles and help these values take root in the technology sphere.

1. Engage with technologists.

- **Invest in expertise**
    - Invest in in-house and external expertise to strengthen analysis and advocacy related to technology and ICTs.
    - Dedicate resources to engagement with technology developers and investors.
- **Develop collaborative spaces**
    - Engage and share expertise (virtually or otherwise) with technology developers and producers to help address human rights issues and use-case scenarios in technology development.
- **Create technology-specific human rights training**
    - Collaborate on common, open-source factual curricula for human rights workers to understand how emerging technologies impact human rights.
    - Provide training/support networks and training capacity/tools grassroots organizations to enable them to participate fully in the use of ICTs and other technologies.

- Encourage digital media practitioners to introduce or update elements that are relevant to technology and human rights into media literacy initiatives and educational curricula, in multiple languages and across teaching contexts.

- **Continually reassess the landscape**
  - Regularly reassess how to make security and safety procedures for technology products more streamlined and accessible.
- **Accelerate efforts to preserve human rights content and make it accessible**
  - Push for broader efforts to digitize and preserve the wealth of visual human rights content held by civil society, online and offline.
  - Develop long-term ways to preserve and make accessible human rights content online.

2. Collaborate more, compete less.

- **Create a Human Rights Tech Network**
  - Create a virtual network of human rights organizations–including freedom of expression, right to information, women's rights, and other domains–committed to tracking and prioritizing technology policy issues.
  - Engage with National Human Rights Institutions on how transnational internet issues impact on human rights domestically and internationally.
  - Engage in GNI and similar processes.
- **Coordinate cross-platform discussions**
  - Increase joint informational meetings for policy-makers in key policy-making, standards-setting and legislative spaces (e.g. European Parliament, U.S. Congress, ISO, ITU) on major upcoming legislation and decision-making processes.
  - Increase coordinated participation in relevant fora and decision-making venues (e.g. the Internet Governance Forum) with an eye on collective action.
  - Encourage engagement in the GNI from a wider cross-section of global civil society, media, business and technology funders/investors.
- **Employ a *big-tent* strategy**
  - Engage with sectors of civil society that address other areas of internet policy–such as media development, governance, transparency, human and national security.
  - Develop human rights principles for investments in ICT by major institutional and private donors and investors, and/or strengthen existing sets of principles with human rights perspectives.

3. Invest in research in partnership with academic and other research organizations.

- **Document and analyze**
  - Systematically review cases and trends relating to the intersection of technology and human rights.
  - Develop new or refine existing monitoring and evaluation systems for technology and technology-based approaches now embedded in human rights documentation, campaigning and advocacy practice.
- **Create predictive modeling**
  - Invest in regular scenario development or other kinds of predictive research, to model and anticipate trends in technology and policy that may impact specific areas of human rights policy and practice.
- **Share findings**
  - Collect, collate and publish case studies illuminating and providing new actionable insights into the interaction between human rights, video and technology.

FUNDERS

Governmental, foundation and private donors play a critical role in conducting and supporting research, activism and advocacy on issues related to human rights and technology. To increase impact, their funding needs to become more transparent, more accessible, more harmonized and less risk-averse. They should continue to support–through funding, networking grantees and open-sourcing their materials and research–the integration of technology and ICTs into human rights work. However, they must also focus on widening user access, education and participation, and on strengthening advocacy using new ICTs. Funders also need to cross-pollinate with a wider cross-section of practitioners involved with new ICTs outside the human rights field, including private investors. By doing this, they can develop new cross cutting funding and transparency mechanisms, providing a more balanced perspective on failure rates and value generation in technology investments.

1. Make funding transparent.

- **Map the funding landscape**
  - Publish a study of the international and regional funders for technology and human rights.
  - Make explicit the quantity, direction, focus, overlap and speed of funding flows, as well as potential donor bias.
  - Include new donors based outside U.S./Europe (e.g. India, Middle East, Singapore) and large regional donor networks like Ariadne or IHRFG.

2. Collaborate with other funders, investors and technology developers.

- **Create multi-donor spaces on technology and human rights**
  - Involve the largest international private and governmental donors and smaller individual philanthropists and family foundations.
  - Involve emerging crowd-funding platforms such as Kiva.
- **Create joint funding mechanisms**
  - Focus on technology development specifically for human rights.
- **Assess human rights risks**
  - Appoint or support the creation of an independent technology review board that will assess proposals involving large ICT investment for human rights risk and appropriateness–and vice-versa, a human rights advisory board that will assess technology-led proposals.

3. Be thought leaders.

- **Evaluate methodology**
  - Lead a wide consultation on how to adapt, refine or develop monitoring and evaluation methodologies for human rights and technology.
  - Consider making shared requirements across groups of funders, so as to strengthen collective impact assessment and to ease the reporting burden on organizations working increasingly in real-time environments.

POLICY-MAKERS AND LAWMAKERS

Policy and lawmakers have a central role to play in guaranteeing that citizens have access to information technologies and that they can do so effectively, safely and ethically.

Policy-makers, regulators and legislators considering technology in any domain or sector need to take into account the human rights implications of these technologies, through conducting credible Human Rights Impact Assessments. All human rights

stakeholders need to provide better information and analysis as well as actionable advocacy to help them do this better. Local judiciaries and legal communities need support to develop and strengthen their analysis of how technology and human rights interact and intersect, both on the local level and internationally. Intergovernmental, regional and national legislative and policy-making bodies need to take more inter-sectoral approaches to their analysis, particularly in incorporating human rights assessments. Encouragingly, some within the U.S. technology sector are calling for trade talks to incorporate free expression, while some are advocating that foreign aid should be dependent on recipient countries meeting good governance indicators such as a free press or an open internet.

The recommendations below are an initial subset primarily centered on the U.S. and EU.

1. Review existing legislation for consistency.

- **Conduct a comprehensive review of European legislation.**
    - Ensure human rights-compatible policies are consistent applied across key areas of EU legislation and policy-making, notably business, trade, arms, counter-terrorism, cyber warfare and other relevant sectors.

2. Review legislation in relation to visual privacy issues.

- **EU Data Protection Directive and Safe Harbor Principles**
    - Review the directive in respect to the rise of visual privacy issues.
    - Initiate a mechanism to update the directive in line with relevant findings and recommendations.
    - Other regional or international groupings of governments having similar legislations must consider similar reviews.
- **Focus on human rights dimensions of privacy, and particularly visual privacy in meetings of Privacy Commissioners**

3. Review export controls on technologies at the national level as well as the international Wassenaar Arrangement.

- **Scrutinize monitoring practices for dual-use technologies.**
    - Review and update mechanisms of scrutiny for so-called dual-use technologies in line with recent developments in the interaction between technology and human rights.
    - Include more clearly the technology hardware and software products produced by Western companies–particularly those used by repressive regimes and other governments for purposes contrary to human rights principles.
    - Engage other governments–notably China and Israel–that foster innovation in these kinds of technologies, with a view to encouraging them to adopt similar or shared oversight of this kind.

PROGRAMMATIC NEXT STEPS– WITNESS

PROGRAMMATIC NEXT STEPS–WITNESS

To enable the growing number of people using video for human rights to do so effectively, safely and ethically, WITNESS plans to:

1. Develop tools in *WITNESS Labs*.

- *WITNESS Labs* initiative will support a series of collaborations with technology developers to create innovative tools that support human rights.
    - These tools will have an initial focus on enhancing the safety and security of people using video for human rights by:
        - Concealing the identity of those filmed;
        - Protecting relevant metadata;
        - Integrating human rights standards of consent and intent into filming workflow and
        - Where possible, collecting relevant metadata for evidentiary authentication.
    - Other areas of likely focus include additional modes of evidentiary authentication, secure upload, and information management with multiple video sources.
    - Our initial collaboration is with the Guardian Project (www.guardianproject.info) to develop the *Secure Smart Cam*, which focuses on securing video, data, and the visual privacy of those in front of and behind the camera. See: https://docs.google.com/present/view?id=ddr5dm94_467vh6sz6cm.
- *WITNESS Labs* will create a small advisory committee of leading technologists, technology investors and human rights advocates to guide this process. The initiative will use a small seed grant process to solicit new apps or enhance and improve existing apps or web functionalities to address the challenges raised by the increasing use of video, including specific situations emerging from grassroots human rights campaigns.

2. Advocate and engage with key stakeholders in technology and human rights.

- Advocate and engage with technology providers on the key recommendations outlined in this report around usage and content policies, codes of conduct, user education, tools and functionalities, and support curation/discussion of human rights material.
- Coordinate with partners a series of public discussions involving human rights activists and technologists on the core topics emerging from this report and accompanying recommendations–both in online venues (invited blog posts and online debates), and in real-world discussions (shared via live-stream).
- Use key existing sectoral events (technology, social change and human rights) to present key findings and build debate in the public sphere.
- Commission and support detailed recommendations and relevant information on key aspects highlighted–for example, in relation to issues of informed consent in the digital age.
- Propose collaborative spaces for practical dialogue between technology developers and human rights organizations, so that mutual expertise can be shared in practical, real-time contexts.

3. Build citizen activists' digital media literacy and advocacy skills.

- Continue to develop comprehensive training tools that address key issues of how to film, edit, circulate and distribute human rights video safely and ethically, and most importantly, effectively.
- Ensure these tools are made available to both traditional and non-traditional human rights video-makers (for more information on existing materials see http://blog.witness.org/training-resources/).
- Collaborate with digital media literacy experts to develop effective, shareable guidelines for a range of human rights situations, including short spreadable/ viral media that concisely communicate key points and are easily consumed and shared.
- Utilize WITNESS' social media and blogging presence, other publication and discussion venues, and key sectoral events to promote dialogue, sharing of lessons learned and cohesive action around issues within the *Cameras Everywhere* initiative.

4. Promote public policy solutions.

- Review participation in the GNI.
- Push for further discussion around policy questions of visual privacy, including in relation to the Madrid Privacy Declaration.
- Consider a range of approaches for collaboration with other civil society organizations working in this field, in order to better maximize resources.

5. Mobilize support for a growing field–"Why Video Matters".

- WITNESS will use a strand of collaborative research and reporting entitled "Why Video Matters" to explain, on the basis of sound research, case studies and document the critical role that video and related technologies play in facilitating social change, further deepening understanding of the challenges and opportunities identified in this report.

PHOTO CREDITS

COVER
Photo left: NOUR EL REFAI
Photo top right: GEORGE HENTON/DEMOTIX
Photo bottom right: NOUR EL REFAI

PAGE 16
Photo: AUTOPAUTA/DEMOTIX

PAGE 22
Photo top: NOUR EL REFAI
Photo bottom: http://storyful.com/stories/1000005936

PAGE 23
Photo left: AUTOPAUTA/DEMOTIX
Photo top right: MOHAMED ELMAYMONY/DEMOTIX
Photo bottom right: NAMEER GALAL/ DEMOTIX

WITNESS | 80 Hanson Place, Fifth Floor | Brooklyn, NY 11217
+1-718-783-2000 | cameraseverywhere@witness.org | www.witness.org