Reflections on digital technologies, repression, and resistance: Epilogue

Anita R. Gohdes*
University of Zurich

May 2018

When the first images of citizens protesting their autocratic governments across the Middle East and North Africa flooded the Internet in 2011, a flurry of op-eds, news reports and academic articles hailing the new digital revolution as the great democratiser of the twenty-first century was quick to follow. The initial euphoria emphasising the liberating aspect of technology – whereby individuals were finally able to collectively mobilize against repressive rulers, while simultaneously documenting the atrocities committed by them – led many tech optimists to believe that it was only a matter of time until technology helped to overturn despotic governments all over the world.

Fast forward to 2018, where the ongoing conflict in Syria, the global surveillance disclosures leaked by Edward Snowden, and rising right-wing populism in Europe and the US have significantly dampened the public's enthusiasm over the role of digital technologies. Both the effusive optimism of the early days of the Arab Spring and today's overly dramatic headlines claiming that the Internet is to blame for all recent political developments are likely wrong. They are wrong because they tend to overestimate the role and impact of digital technologies on societal developments. But more importantly, they fail to take a nuanced look at the complex ways in which digital technology is in fact amplifying and changing politics today.

Amid these broader developments, the authors in this Special Issue bring together important reflections on the precarious relationship between digital technology, state repression and local resistance. The individual contributions span a number of important aspects pertaining to the ambiguity of digital technology, whereby precisely the characteristics that make it so useful for mobilization, self-empowerment and resistance allow it to be controlled and abused by repressive authorities. In the following, I will briefly reflect on some of the common themes that emerge from this collection.

Exposing Surveillance as an Act of Resistance

The contributions in this Special Issue highlight the different ways in which digital state surveillance violates fundamental human rights, and presents one of the key challenges for human rights defenders working on resisting abuse of power in the current political climate. Human rights defenders and researchers alike are faced with the fact that digital surveillance tends to occur in secret. Unless governments choose to strategically disclose the extent of their surveillance activities, researchers and activists are oftentimes only able to uncover information about surveillance practices through methods deemed illegal by the state itself. Both Colvin (2018) and Nyst (2018) therefore highlight

*Published in *State Crime Journal 7(1). Spring 2018*. Email: gohdes@ipz.uzh.ch.

the important yet precarious position in which digital whistleblowers find themselves. A large part of our current knowledge of global and local surveillance practices has been informed by individuals who have disclosed information at great personal risk, by hackers who have sought to expose the work of surveillance software companies (such as the leaked emails of the Italian *Hacking Team*), and by researchers working on reverse-engineering malicious software (such as the work by the Citizen Lab).

Understanding and analysing how government surveillance works is important for a number of reasons. First, for those seeking to protect themselves from intrusive state behaviours, the mechanisms by which these technologies work present a crucial first step in designing their own tools of resistance. Second, researchers interested in investigating how surveillance capacities are integrated into the larger repressive toolkit of governments are dependent on information about the technical infrastructure and actual usage of these surveillance systems. Third, activists working to challenge the status quo require knowledge of both the technical details as well as the broader context in which these technical solutions are employed.

The (Often Invisible) Work of Digital Documentation

Much has been written about the important role citizen journalists – local participants and observers documenting the evolvement of contentious political events through the use of digital media – take on in the context of resisting repressive state authorities. Kasm (2018) and Deutch and Al Khatib (2018) describe the manifold ways in which local reporting helps sustain and build resistance movements. Digital documentation allows those who are absent from the dominant discourse to make their voices heard, can help build community and a new public sphere, and has the potential to provide visual documentation of human rights violations that may otherwise remain hidden.

In his case study on the Egyptian *Mosireen*, Kasm reflects on an important point that was vital in the success of the Egyptian collective: local ownership of the produced documentation. Grassroots initiatives that build local content and capacity can work towards providing an alternative display of events to that propagated in state-controlled media. Where local observers of contentious events remain in the position of the producers of "raw" material, which is then exclusively processed, evaluated, and interpreted by international audiences, such formations of new public spheres may be seriously stifled in their ambition to provide a genuinely local perspective and conversation.

A further challenge local groups face is that in response to the increased popularity of citizen-supported journalism, state and state-supported groups are increasingly adopting the techniques spearheaded by those protesting the authorities. Digital spaces originally used to mobilize and organize resistance are oftentimes flooded with content that is supportive of the regime, thereby attempting to control the predominant discourse both domestically and internationally. Content may be newly generated, reappropriated or forged, and as a consequence, publicly available information becomes highly contentious and oftentimes requires expert knowledge to analyse and contextualize. Digital technology employed in conflict documentation has elevated the role of visual evidence of human rights violations, making the organization, search-ability and verification of said material more important than ever before. The work by groups such as the Syrian Archive (described by Deutch and Al Khatib) demonstrates the level of methodological innovation, attention to detail, contextual knowledge and ethical consideration that is required if visual documentation is to be included into official accountability processes.

Dealing with an Increasingly Corporate Internet Infrastructure

In the past decade, individuals and groups have sought to collect and memorialise vital documentation on social media platforms during many episodes of social and political unrest. Amid political instability, and in particular in contexts where more traditional media outlets remain inaccessible, the preservation of content in online spaces brings with it many advantages. However, corporate platforms operating on the Internet should not be mistaken for a permanent archive of information. Social media platforms were never intended for the purpose of securely saving important content over long periods of time. Platforms are shut down for financial reasons, others are bought up and their infrastructure changed along the way, while others are hacked and content is removed by third parties. Open or closed groups or channels regularly used by resistance groups may be shut down for political reasons, users suspended, content flagged as inappropriate and removed; all this resulting in the loss of stories, evidence, and memories. In many contexts, relying on infrastructure provided by large Internet-based companies is the only viable choice local resistance movements have, and yet the willingness of such companies to cooperate with repressive regimes can present an immediate risk for their personal safety, and the archival of their digital memories.

Recently, YouTube started implementing machine learning algorithms to help identify extremist content, and in the process thereof ended up deleting a substantial number of videos documenting the Syrian conflict. Given the transient nature of most social media content and the growing importance of visual documentation, the work by groups such as the Syrian Archive is thus becoming increasingly fundamental for resistance and accountability processes. And the case study on the Egyptian *Mosireen* shows how groups can strategically make use of international platforms, such as YouTube, to share their content, yet manage to maintain control of the production process of their own work.

Franklin (2018) addresses a further dimension on which increasingly corporate Internet infrastructures threaten vulnerable groups, by analysing the outsourcing of digital surveillance from state actors to private sector corporations in the context of EU border controls. The delegation of border control missions that are supported by digital technologies traditionally used by state authorities to private contractors has allowed national and regional authorities to deny responsibility for the increasingly repressive policies employed.

The context referred to in these contributions is very different, and yet, all implicitly or explicitly address the complexity of dealing with both corporate and state involvement in digital controls when attempting to resist state repression. The contributions to this Special Issue highlight the ways in which the usage of digital technologies critically influences the ever-evolving dynamics between non-state, state and private actors. On one hand, it is virtually impossible to think about digital resistance and repression as detached or separate from more traditional forms of contentious politics (Gohdes 2018). On the other hand, we observe that all actors involved in such politics are continuously learning to adapt and adopt new technologies for their own purposes, sometimes to their advantage, sometimes at considerable initial cost. Future research programmes will necessarily have to pay close attention to these changes and learning processes.

References

Colvin, N. (2018) 'Whistle-blowing as a Form of Digital Resistance: State Crimes and Crimes Against the State', in State Crime and Digital Resistance, Kasm, Saeb and Anne Alexander, eds, State Crime 7(1): 24–45.

Deutch, J. and Al Khatib, H. (2018) 'The Syrian Archive: A Methodological Case Study of Open- Source Investigation of State Crime Using Video Evidence from Social Media Platforms', in State Crime and Digital Resistance, Kasm, Saeb and Anne Alexander, eds, State Crime 7(1): 46–76.

Franklin, M. (2018) 'Refugees and the (Digital) Gatekeepers of 'Fortress Europe'', in State Crime and Digital Resistance, Kasm, Saeb and Anne Alexander, eds, State Crime 7(1): 77–99.

Gohdes, A.R. (2018) 'Studying the Internet and Violent Conflict', Conflict Management and Peace Science 35(1): 89–106.

Kasm, S. (2018) 'Redefining Publics: Mosireen, State Crime and the Rise of a Digital Public Sphere', in State Crime and Digital Resistance, Kasm, Saeb and Anne Alexander, eds, State Crime 7(1): 100–140.

Nyst, C. (2018) 'Secrets and Lies: The Proliferation of State Surveillance Capabilities and the Legislative Secrecy Which Fortifies Them – An Activist's Account', in State Crime and Digital Resistance, Kasm, Saeb and Anne Alexander, eds, State Crime 7(1): 8–23. State Crime 7.1 Spring 2018