Dialogue | Introduction: Surveillance in Conflict and Crisis

Keith Spiller

University of Southampton, UK
k.spiller@soton.ac.uk

Bryce Clayton Newell

University of Oregon, USA; Utrecht University, The Netherlands
bcnewell@uoregon.edu

Introduction

This Dialogue sought contributions from surveillance studies scholars that examine how surveillance is part of, or has grown out of, contemporary conflicts around the world. The ongoing war in Ukraine stimulated the initial idea for the section, but we also remained mindful of the wider global scope of conflicts around the world, the history of such conflict, and the ways in which surveillance has become integral to many forms of domestic and international conflict. We wanted to extend the engagement of surveillance studies research with issues of surveillance and its relationship to conflict and to push debate and conversation about the practices, technologies, and ethics of how surveillance has been situated in moments and longer periods of conflict. We have four distinct contributions as part of this specific Dialogue, and they draw upon issues of privilege, longevity, control, organizational power, and discrimination that are placed within case studies from conflicts in Columbia, Palestine, and Ukraine.

In the first paper, Daniela Silvestre Jorge Ayoub examines how video footage emerging in the aftermath of the murder of Palestinian-American journalist Shireen Abu Aqleh in May 2022 was used as evidence of what occurred and to counter the official claims by Israeli authorities. Daniela analyzes how data taken from real-life contexts are interpreted, articulated, and given meaning as "objective, even neutral, material evidence." Ayoub argues that amid "the spectacle of political rhetoric and military theatrics, an asymmetric interpretation and subsequent instrumentalization of digital archives obstruct the inclusion of those subjected to harm as interpreters of their own experiences, shaping public perceptions and further exposing oppressed populations to continued violence." Ultimately, this paper frames the case of Abu Aqleh's murder as an example of how "surveillance and selective framing of data" can be used to "distort conflict and structure warfare."

Next, Aaron Martin examines ways in which private surveillance firms have embedded themselves within humanitarian crises and argues that these activities involve the exploitation of "humanitarian crises as a means to 'aidwash' their technologies and services." Martin employs two primary examples, that of Palantir and its ongoing partnership with the United Nations' World Food Programme and Clearview AI's interventions into the ongoing Ukrainian war with Russia. Using these examples, Martin argues that these firms, among others, use corporate social responsibility initiatives or public-private partnerships to justify the deployment of their surveillance platforms and services within war and humanitarian crises with the aim of "aidwashing" their otherwise controversial surveillance activities—or, as Martin writes, "corporate misbehavior, ethical misdeeds, and dubious data practices."

Then, Camilo Tamayo Gomez challenges surveillance studies scholars "to rethink and reimagine the meaning of surveillance activities and practices during long-term armed conflicts." There are, as Tamayo Gomez notes, seemingly never-ending wars on multiple continents. And these prolonged conflicts, in which ongoing violence may be of more interest to various armed groups than ultimately "winning," hold the potential to create "new sociocultural conditions for the development of surveillance activities and practices, where battles between armed groups are rather rare and most violence is directed against civilians." Tamayo Gomez uses the example of long-term kidnapping during the former armed conflict in Colombia to illustrate some of these themes. Ultimately, Tamayo Gomez's piece is a call to action for surveillance researchers to engage and develop new theories, methods, and concepts for explaining and investigating how surveillance develops and plays out in these extended conflicts.

Finally, Simon Hogue investigates how the use of surveillance technologies, including cell phones, by civilians in the Ukraine-Russia war to document war crimes and human-rights violations while also providing open-source intelligence for Ukrainian and other Western governments puts these civilians at significant risk. Indeed, Hogue argues that "Ukrainian government and its Western allies mobilize civilian surveillance for operational purposes and to build the narrative of the war against the Russian aggressor. In the process, they put civilians at risk of retaliation by Russian forces and endanger the independence of investigators." For Hogue, this places these civilians squarely as actors within the politics of war, with their digital evidence offered as "narrative weapons."

To build on the contributions each of these short papers make to this Dialogue, we organized a virtual call with all of the contributors. The conversation occurred online, using Zoom, after all of the papers had been fully drafted and each contributor had been able to review the contributions from the other authors. It was designed to extend the actual dialogue and conversation amongst the contributors to this issue and to channel a discussion on some of the themes that emerged from the respective papers. The conversation was structured around a series of pre-planned questions based on the draft papers. Several questions were directed at specific contributors, while the other participants were also then free to engage in the conversation that ensued. The portions of the transcript that we include below are edited for brevity, readability, and to keep focus on some of the more insightful exchanges from the conversation, but we did try to remain faithful to the general conversation as it unfolded. The conversation took place in late January 2023 and included the following contributors: Keith Spiller (moderator and guest editor of this Dialogue), Daniela Silvestre Jorge Ayoub (University of Coimbra, Portugal), Aaron Martin (Maastricht University, The Netherlands), Camilo Tamayo Gomez (University of Huddersfield, UK), and Simon Hogue (Royal Military College Saint-Jean, Canada).

We began the conversation by asking the contributors to identify commonalities or common themes that emerged across the papers. Simon opened the conversation by noting it was not necessarily the themes he identified, rather "ways into which other texts related to my own areas of questions," and the conversation then developed a little something like this:

Daniela: I think my paper offered a good case study to further some of the discussions that other authors submitted. I think that, in that way, it made it easier for me to understand my own work and furthered the fundamental nature of surveillance as opportunistic, and not just in conflict but also as a structural component.

Camilo: After reading the papers and reflecting a little bit, I think it is the tensions and the challenges of the public and the private actors doing surveillance activities in different conflicts. I think, especially, reading Simon's paper regarding the use of technology and how civilians are being more active in order to conduct surveillance from the States, or the work of Daniela about how the different narratives that different organizations can create in order to portray or create different narratives about what is going on.

Aaron: I think for me one of the key insights is that they're very different papers and they're all addressing very different problems within the conflict frame. There's a lot of diversity in the contributions, and I think

that diversity probably speaks to what is an underexplored but potentially very rich research domain, surveillance in conflict or crisis situations. I also think each of the papers speaks to the importance of methodology and appropriate research design for understanding what surveillance means in a very particular context where doing empirical work is not so easy. One of the connecting threads is the recognition that methodology is really essential here and that it's not always straightforward to understand surveillance in these very challenging contexts.

Keith: There's a geographical spread in the contributions and the examples of surveillance cited in the papers. What similarities or differences do you think there are in terms of the surveillance examples, and particularly considering some of those physical distances that may be involved?

Camilo: I think both the case that my colleagues are addressing and my research about Colombia, I think the social cultural context can shape different social cultural practices of surveillance. So, for me, it's interesting to reflect on conditions of power, inequality, poverty, and access to technology. But in other geographies, they don't have the same resources, or they have not reflected enough about the role of technology in how to address those particular cases.

Simon: I would say it's not geography per se, but it's linked to geography. If we look at the case of Ukraine, I didn't push it that far in the paper, but I think… it is important to understand [the Ukrainian society], the response of the population to the use of surveillance and digital technologies in the conflict. Ukraine is a very connected country, and its connectivity has increased massively in recent years. So, it's not so much a surprise because it is also the same in other countries. But what is specific in Ukraine is that they invested in the IT industry. So, there are lots of startups, and the economy of new technologies is increasing and developing very fast in Ukraine. So that gave people on the ground knowledge and technical tools to be able to become surveillers.

Keith: **There's a sense of privilege in the papers. Was that about those with access to resources of various kinds and their ability to use them to their advantage? How in your mind does surveillance facilitate this?**

Aaron: The privilege of the companies that I'm describing is reflected in their taking advantage of the opportunity—of the crisis. I think this is especially apparent in the case of Palantir, which is very much an extension of their original market, which was the security and defense industries. But I think Palantir have really done well to find crises globally and to use their connections with the defense apparatus in countries like the United States and in the UK to become the first port of call with respect to the use of data and analytics in terms of responding to crises. So, for sure, there is this very privileged position that they occupy within the security and defense establishment within global north countries that's allowed them to become— by extension—humanitarian responders. But more than that, I think with respect to the World Food Program partnership in particular, Palantir has entered into this sphere, into this sector, which is supposed to abide by very different principles than defense and military operations. The humanitarian principles around neutrality, impartiality, and independence are supposed to distinguish humanitarians from others involved in conflict.

Simon: I think another group of people who have privilege, and we may not see them, is the open-source investigators. They can act as onlookers, but from the outside, and… have, or sometimes maybe it's not so real, but they have the subjectivity in looking at the conflict or looking at the violations all around the world, because they can pretend to be outside of that conflict or they can look at it from the outside. This is a very important privilege that we should not also forget in claiming disruption and, so, resistance. I'm not saying that I don't totally support what they do, don't misinterpret me here, but I think we have to recognize this privilege.

Aaron: Now that I reflect a bit more on the term privilege, there's another interpretation, which is actually quite interesting. In the humanitarian space, there are certain international organizations like the World Food

Program and other UN agencies—that is, organizations with a mandate under international law—that enjoy legal privileges and immunities. Essentially, they operate in a different legal space, which affords them a lot of protections. So, when things go wrong, these organizations normally can't be held unaccountable under domestic law. While there are good reasons for these agencies to be afforded legal privileges and immunities, it's become a big issue in the responsible data debates in the sector, because when there are data breaches or other kinds of data harms, legal recourse for data subjects is limited. When negative things happen with data, UN agencies and other international organizations are basically immune from prosecution because they don't have to follow, for example, GDPR or similar domestic legislation.

Keith: **Another theme that emerges from the papers is control and power asymmetry. As well as the physical control that surveillance hardware enables, there is a control of the narrative in moments of conflict. What are your thoughts about truth and political rhetoric that perhaps formulate or mold this asymmetry?**

Daniela: Historically, there have been two political narratives. One which reiterates the insistence of colonization and another that reiterates the importance of autonomy of populations and of decolonization within a larger history of decolonization since the 1950s, particularly in North Africa moving towards Southwest Asia. The political narrative that hasn't actually received much attention stems from resistance groups, a term I use more broadly. One that hasn't received that kind of attention has of course been the narratives that Palestinians hold of their own stories and of their own experiences, which have been dominated by documentation processes that deem themselves to be official narratives, which is the issue with having proof and what having proof means.

This ties a lot to Eyal Weizman's work. In my paper, I point to the work of Goldsmith's Forensic Architecture, which is led by Eyal Weizman. In his book, *The Least of All Possible Evils*, Weizman (2011) reflects on the processes that determine who is deemed the bearer of truth and the role of official documents and material evidence in constructing truth. Ultimately, how together these components build what is considered an objectively true narrative. What organizations like Forensic Architecture offer, what social media offers, and what open-source investigations now offers on a larger scale, is a different kind of narrative that can contest dominant power dynamics and also be considered "truth."

Camilo: I think it's a link with the construction of political identities during armed conflict as a result of power struggles. Because I can see in cases like in Ukraine or Palestine and Colombia, how different groups start to create and to move to different political spectrums and to construct different political identities as a result of these challenges of narratives. I was just thinking about what Daniela is saying about this particular NGO that architect forensics architectures, because they have been doing a lot of work for the Colombian Truth Commission and especially try to know what happened with two or three key moments during the conflict. And some people that used to support, in the case of Colombia, the military army and the Colombian Armed Forces, started to change the political perspective because of the outcomes of this research and to show in these narratives about how, in that case, the Colombian Army behaved during the times of the conflict. So just to highlight this, how the construction of political identities and the changing of this construction can be an outcome of these struggles for power, and how of course all these technologies can help to create new narratives to move and to construct different political identities during conflict.

Keith: **As the war in Ukraine moves towards its first anniversary, what surveillance lessons have been learned? And particularly, what we can be perceived as the positives, for example, the documentation of war crimes, the use of data by the "just" side? (What I mean by the "just" side is the Ukrainian forces with the support of the West.) Give us an idea of some of those lessons that may have been learned over the last year.**

Simon: I think that people on the ground can be very efficient collectors of evidence, and in using the right methods, can share this evidence so that we can actually know what is happening on the ground, so that can lift this infamous fog of war, at least in part. We can really understand how the conflict is developing and

what violence is there. I think that without these individuals and these technologies, it wouldn't be possible to access this form of truth and to be really able to build a narrative and to be able to rebuild or contest the ongoing narrative. Because it wouldn't be easy just to be stuck between the Ukrainian official narrative, versus the Russian official narrative. There wouldn't be any space in between. So, having civilians using surveillance there is extremely valuable to be able to understand, but then to be able to follow up in courts, and hopefully to be able to bring the people who committed war crimes to justice.

Keith: **Then my follow-on question is, what surveillance lessons are negative?**

Simon: Well it's been instrumentalized by the Ukrainian, and I would say also by the US, side at least, and probably also from the Russian side, but I couldn't say here. The Ukrainian state is well aware that it's very important for them to have information about how the Russians are moving and to be able to collect these data about violence so that they can build up their own narrative. But that puts people on the ground at risk, because for a foreign army, foreign invaders, and the Russians, having somebody with a phone or recordings or finding photographs and videos of things on a telephone, on a phone, it makes that person a security threat. It puts all the risk, transfers the risk from the state or the army or the security officials of that country towards its population—who should be in practice protected by humanitarian law in that conflict. So, it brings those civilians into the conflict in ways that wouldn't have been otherwise. One last thing, I think this helps us highlight the privilege that people in the US and in Europe and Canada and everywhere else in the world have, because they can use this evidence that has been gathered at risk, but in the comfort of their offices or their couch. They're doing good things, but there are inequalities there.

Daniela: It also points to what Simon was discussing before about the privilege of open-source investigators, investigations, and the kind of gaps that are created between. They're also truth determiners. We can see with organizations like Bellingcat that have done a lot of work on Ukraine in particular—what they determine to be the truth is what is often reproduced in mainstream media and, therefore, in public discourse. So, what information they are able to access and subsequently deem legitimate has consequences as to both who is at more risk and who is then possibly going to be prosecuted. Definitely building into the kind of themes that you were talking about, the patriotism issue, revving up the drive of conflict even further, especially for civilians already at risk, maybe even motivating people to continue if not expand their surveillance practices.

Aaron: I just wanted to respond to Simon's point about the importance of mobile phones and other devices in conflict and how their use blurs the line between civilian and combatant, which is a very important problem. I think it speaks to a couple issues. One is the ways in which these technologies lend themselves to surveillance of different kinds in these contexts and what that means for the end user. Ukraine is a military conflict, but it's also a humanitarian crisis. You can look at other contexts where the crisis is primarily of a humanitarian nature, where mobile phones are ever present because they're now basically becoming the platform for the distribution of humanitarian aid. That becomes very important for aid agencies that want to, for example, deliver information to crisis-affected populations, provide cash assistance to people who are affected by crisis and so on. Connectivity as aid is now a thing, meaning providing people with a mobile connection as a form of aid so that they can contact relatives, etc. But what happens is, as these people migrate, become refugees, try to enter other jurisdictions, etc., those devices themselves become the object of suspicion. Authorities want, for example, to look at the location history of the devices to see whether an asylum claim is "legitimate" or not. Is this person actually Somali or are they Kenyan? Who is in their contact list? Is it primarily Kenyan numbers, Somali numbers, etc.? So, through forensics of different kinds, these mobile devices become yet another thing that can be analyzed, hacked, etc. I think we need to question the neutrality of these devices—or rather the presumed neutrality of the devices—in conflict, humanitarian aid, and so on.

Keith: **The papers touch upon longevity of conflict and, building on the last question and what we were just talking about there, what we can see are situations of conflict that have allowed or**

encouraged a playground of technological or surveillance development. What is the difference presented by the short term or the long-term conflict?

Camilo: Well, the main characteristic is of course the social relations that actors can develop over time because of the conflict. As I try to explain in my paper, I am researching kidnapping in Colombia and especially situations of long-term kidnapping. In that particular example, time is important.… When you take technology as part of all these discussions, of course technologies can disrupt time. This is something that the field of surveillance can [investigate], to see how some technologies of surveillance can affect the perception of time during long-term captivity, or in this case, or long-term actions in conflict. So, for me, it's an invitation to reflect and to think about the role of all these notions and categories, to create and to better address our objects of research, how we can think more about the role of time, technology, but how they are creating a different ecosystem of surveillance during armed conflicts.… Just reflecting on something that Aaron was saying before, is the transnational element and international nature of what we're talking about here.… How they disrupt time as well, because if some particular group is resisting, or I don't know for a battle or whatever, some civilians in another part of the planet can still be doing activities for them. But this transnational connection and this nature with time is interesting for me to start to reflect and see how we can better address our objects of research.

Daniela: I did just want to say I think that it's really interesting, also thinking about the diaspora in many of these conflicts and how the role of memory also plays a huge part in how conflict is approached, funded, and continued in different contexts and the relationship to time.

Keith: Another theme that can possibly be seen in the papers is the influence of organizations or big business. Where do issues of corporate social responsibility [CSR] or more generally ethics and morals sit within the interventions of surveillance within conflicts?

Aaron: I do see a trend towards leveraging CSR, and in particular CSR efforts aimed at humanitarian crises of different kinds. I think this is only going to get bigger and bigger. There is a major iris biometrics company known as IrisGuard who have basically become the de facto biometrics "solutions" provider for the humanitarian sector. They make a pretty penny doing biometric authentication of refugees and other displaced people in places like Jordan and elsewhere and have become the provider of choice for the World Food Program and other UN humanitarian agencies. But even for a company with a sound business model, there's still value even for them in CSR initiatives and the performance of being an ethical business. I think there is a very much a performance aspect to a lot of this for these firms, especially where there's doubts about the operational value of the partnership, for example in the case of Clearview AI's involvement in Ukraine. It's not just surveillance firms, of course. I think the tech industry writ large is quite keen on using these opportunities to improve their image. But I think it's particularly concerning when it is surveillance companies or at least companies whose primary business is surveillance. I think at least in the two cases that I try to cover in the paper, there's a lot of significance in the fact that these are free offerings. Palantir and Clearview AI are giving away access to very expensive platforms and services. So, you have to ask yourself for what? I think that "for what" makes a lot of people uncomfortable, in particular within the aid sector.

Camilo: I think that can be an example of cannibal capitalism, like how these private companies just find an opportunity to make business and to make profit just by trying to be the good guy. How in some particular conflicts, by supporting one particular actor or one particular army or one particular state, it's not just because they believe in the cause or they believe in whatever, it's just another way to make business and to make profit. It's just basically surveillance as another way to make more money for private actors.

Keith: **Can the oppressed, controlled, invaded, or those that rebel truly repurpose the practice of data collection and management to their advantage?**

Daniela: Well, that's the question I think. There's always a deep contradiction of using a tool that oppresses you. Of course, jails offer a good example of that historically. That would exactly be what needs to be looked

into: Could the use of a particular tool be so detrimental to those that benefit most, in terms of power and control, that its counter-use would deem it useless? That would be the purpose, eventually making it useless. But historically, we know that technology doesn't stop just because the usefulness changes for a particular group. Instead technology becomes more sophisticated, it develops into new monsters per se. Ideally, some surveillance practices and tools could at least be used to a certain degree, particularly given the correct alliance. For example, Forensic Architecture. They are just one ally, one institution in a sea of many, many institutions and organizations that could also be doing similar work but don't. Many of these organizations that facilitate any sort of rights-based work, whether data or otherwise in the Palestinian context are actively repressed and shut down. The need for Israel to ensure their inactivity certainly points to the fact that they do have power. Are they able to use it for total liberation? I'm not sure. Are they able to use it to make it so ineffective that that tool becomes useless per se? Maybe. Hopefully. But maybe not. Tying to something that Aaron was saying, investigating private interests is extremely important. These entities construct entire ways of living, entire ways of seeing. At least in the United States, which none of the papers specifically point to, but there are entire cities being built on these private-public partnerships and that designate surveillance as the only model of social engagement, especially in very poor urbanscapes.

Simon: I think that the idea of total liberation is maybe, we might hope it, but it's most unlikely. And especially with surveillance, I think it highlights very well the very fundamental issue, that surveillance and visibility are both something for control but also for care. So, I think we can link resistance and reframing narrative as a form of care here, but we're stuck with this. It's a tool that can be dangerously both, and this is why it makes it so interesting to study, I think.

Keith: **Is agency withering in the face of automation, or even things like AI, or is it just as important to the functioning and understanding of conflict and surveillance?**

Simon: It's disappearing? Well, I don't think so because people will always have to act, and of course automation directs actions or takes action for us. But we'll always be involved in these actions somehow. We will always relate to these machines, and these machines will take directions that will influence how we will behave. So, I think rather than saying that agency's withering, we could at most, I think, say that agency's enlarging and that these technologies are becoming agents that we partly control and that we partly don't control. And that they act on us in ways that we haven't planned for, as in ChatGPT, just to name something that maybe we are all bored of hearing of, that fantastic AI writing exams for our students that we have to mark. So, this is a new form of agency that we have to find a solution to, but the agency is not disappearing, it's just transforming and broadening.

Keith: **Is there anything that we may have missed or is any kind of contribution somebody wants to make or a point that they want to raise that may have not come up earlier on?**

Camilo: Maybe just to highlight that we can reflect more about the nature of conflict and how surveillance studies need to explore more the changing nature of armed conflicts and long-term conflicts. That will be just something to highlight that we definitely need to make an effort to explore more. Because I think we are having, at least from my perspective, a really superficial approach to understanding armed conflict in general. Maybe surveillance can be a key element for understanding the dynamics of new wars and new conflicts. Especially as my colleagues are saying, in their cases, what happened in Ukraine or what happened in Palestine or what happened in Colombia or in Germany, if we analyze more the role of surveillance in all those conflicts, [we could generate] better tools for understanding the new nature of wars and the new nature of contemporary wars.

***

In conclusion, the contributions to this Dialogue examine how surveillance is part of, and has grown out of, contemporary conflicts and humanitarian crises around the world. The papers address conflicts ranging from the ongoing war in Ukraine, the Israeli-Palestinian conflict, the long history of kidnappings in Colombia,

and how surveillance firms are exploiting humanitarian crises to "aidwash" their technologies and services. We hope these interventions encourage or inform additional research and novel new studies into the role and development of surveillance and surveillance technologies in long- and short-term conflicts and humanitarian crises around the world, and the multifaceted ways in which surveillance, technology, and informational politics intersect within these conflicts.

References

Ayoub, Daniela Jorge. 2023. Returning the Gaze of Surveillance: The Murder of Shireen Abu Aqleh. *Surveillance & Society* 21 (1): 91–95.

Hogue, Simon. 2023. Civilian Surveillance in the War in Ukraine: Mobilizing the Agency of the Observers of War. *Surveillance and Society* 21 (1): 108–112.

Martin, Aaron. 2023. Aidwashing Surveillance: Critiquing the Corporate Exploitation of Humanitarian Crises. *Surveillance & Society* 21 (1): 96–102.

Tamayo Gomez, Camilo. 2023. Beyond Battlefields and Conventional Research Agendas: The Importance of Understanding Surveillance Activities and Practices During Long-Term Armed Conflicts. *Surveillance & Society* 21 (1): 103–107.

Weizman, Eyal. 2011. *The Least of All Possible Evils.* New York: Verso.