Surveillance & Society

Dialogue

# Aidwashing Surveillance: Critiquing the Corporate Exploitation of Humanitarian Crises

**Aaron Martin**

Maastricht University, The Netherlands
aaron.martin@maastrichtuniversity.nl

## Abstract

Private sector actors have long been involved in surveillance. This extends to surveillance undertaken in crisis contexts and conflict situations, where humanitarian needs commonly arise. Prior research has problematized the surveillance-industrial complex's involvement in aid initiatives and humanitarian interventions, but new dynamics are creating novel dilemmas. This contribution to a dialogue on surveillance in contemporary conflict discusses how surveillance firms are exploiting humanitarian crises as a means to *aidwash* their technologies and services. In this context, aidwashing practices involve the use of corporate social responsibility initiatives and forms of public-private partnership with aid actors to burnish surveillance firms' reputations and distract the public from corporate misbehavior, ethical misdeeds, and dubious data practices. In this piece, I draw on two recent cases—a partnership to develop advanced data analytics for the optimization of humanitarian food assistance and the donation of facial recognition services in an ongoing armed conflict—to interrogate the surveillance industry's public relations activities in humanitarian emergencies and conflict situations and reflect on the inner workings of—and resistance to—aidwashing.

## Introduction

In this article, I argue for a critical assessment of the involvement of surveillance firms in humanitarian crises. I draw attention to what I term *aidwashing,* which in the surveillance-industrial context (Ball and Snider 2013) describes the use of corporate social responsibility initiatives and forms of public-private partnership involving aid actors to burnish surveillance firms' reputations and distract the public from corporate misbehavior, ethical misdeeds, and dubious data practices.

I present two contemporary examples of surveillance firms aidwashing their technologies and services. First, I highlight the case of Palantir (a controversial software company specializing in big data analytics) and its ongoing partnership with the World Food Programme (WFP) in which the UN agency is leveraging the data analytics firm's software to optimize humanitarian food assistance. Second, I present the case of Clearview AI (a similarly controversial provider of facial recognition services) making its platform available to Ukrainian authorities during the conflict with Russia. While the provision of free or subsidized technology for humanitarian uses, such as in Palantir's relationship with WFP or Clearview AI's involvement in Ukraine, is a common type of partnership in the aid sector, distinct concerns emerge in cases where the software is explicitly designed for surveillance purposes or where the firms involved are widely seen as exploiting a humanitarian crisis for reputational gain.

I argue that the main driver for Palantir's involvement in humanitarian action is to launder its reputation. Similarly, Clearview AI is exploiting the Ukraine crisis—not for experimental purposes or to normalize the use of its technology, which is already in widespread use by police departments and other law enforcement

Martin, Aaron. 2023. Aidwashing Surveillance: Critiquing the Corporate Exploitation of Humanitarian Crises. *Surveillance & Society* 21 (1): 96-102.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487

agencies around the world—but rather primarily to aidwash its sullied public image. Like Palantir, it sees opportunity in demonstrating how its platform can also serve humanitarian aims, thus further complicating the tensions inherent in surveillance as representing both control and care.

## Background

In 2013, the global civil society organization Privacy International published groundbreaking research documenting how aid initiatives pursued by international development and humanitarian agencies were enabling the surveillance of crisis-affected people in multifaceted and often problematic ways (Hosein and Nyst 2013). The Aiding Surveillance report covered a range of critical issues including different forms of tracking enabled by electronic cash transfers (cf. Martin 2019), digital identity and biometric technologies (cf. Weitzberg et al. 2021), mobile phone monitoring tools, and the proliferation of border security systems through technology transfer initiatives (cf. Frowd 2018, 2021). Hosein and Nyst (2013) also criticized the involvement of commercial actors in aid initiatives for extending, deepening, and adding legal and technological complexity to the surveillance of aid beneficiaries, for example where major payment processors like Mastercard become central players in the distribution of humanitarian cash assistance.

A decade later, these concerns are still highly salient, but the phenomenon of *aiding surveillance* has evolved to incorporate new dynamics. This contribution to a dialogue on surveillance in contemporary conflict discusses how surveillance firms are exploiting humanitarian crises as a means to "aidwash" their technologies and services.

## What is Aidwashing?

Aidwashing—sometimes referred to as "humanitarian washing" (Kaurin 2019) or "bluewashing" when it involves UN agencies (Berliner and Prakash 2015)—generally describes how the private sector uses corporate social responsibility initiatives and forms of partnership involving aid actors to burnish their reputations and likewise distract the public from corporate misbehavior or ulterior motives.

Berliner and Prakash (2015) detail how firms have gamed the United Nations Global Compact (UNGC), a prominent international voluntary program launched in 2000 based on ten principles related to human rights, labor standards, the environment, and anti-corruption. Signatories are expected to incorporate the principles into their strategies, policies, and procedures to help uphold their "basic responsibilities to people and planet." Berliner and Prakash (2015) found that the lack of monitoring and enforcement in the UNGC allows members to shirk their commitments while still being able to enjoy the goodwill benefits of program membership. Their analysis of the bluewashing phenomenon within the UNGC—while not specific to the technology sector or surveillance firms—does inform a critique of the distortion of corporate social responsibility campaigns by the surveillance industry aimed at addressing operational needs in fragile and conflict-affected situations.

Homing in on the technology initiatives specifically, these public relations activities often intend to divert attention away from companies' dubious data practices. Kaurin's (2019) critique of the failed Libra cryptocurrency is instructive. Libra (later rebranded as Diem) was a social impact project to develop a payment platform to benefit the poor and "unbanked." Led by Facebook, the consortium originally included several corporate partners such as Mastercard, Visa, PayPal, Uber, and others. Kaurin (2019) questioned the role played by the project's sole humanitarian partner: Mercy Corps, a global non-governmental, humanitarian aid organization. As Kaurin (2019) states, "Libra is being branded as a tool that will help millions around the world, and it needs Mercy Corps for this humanitarian washing." Despite its short-lived existence, the Libra proposal is significant not only because it represents a failed attempt at aidwashing a cryptocurrency with major corporate backers by framing it as a financial inclusion initiative but also because its failure was largely due to sustained regulatory pushback fueled, in part, by doubts about Facebook's true motivations.

Building on these critiques by Berliner and Prakash (2015), as well as Kaurin (2019), in what follows I present two contemporary examples of surveillance firms aidwashing their technologies and services. First is Palantir's ongoing partnership with the World Food Programme in which the UN agency is leveraging the data analytics firm's surveillance platform (cf. Ilidais and Acker 2022) to optimize food aid distribution; I also comment on Palantir's recent activities in response to the Ukraine conflict. Second, I discuss the case of Clearview AI making its facial recognition platform available to Ukrainian authorities during the conflict to support the identification of Russian soldiers—living or dead—and to verify that travelers in the country are who they claim to be. While some facets of these cases have been documented elsewhere (Latonero 2019; Martin et al. 2022; Hill 2022; Thylstrup et al. 2022: 3), this piece is the first to reflect on their significance in terms of aidwashing.

## "Bad Times Are Very Good for Palantir."[1]

In 2019, the World Food Programme (WFP) announced it was entering into a five-year partnership with the data analytics firm Palantir to "use [WFP's] data to streamline the delivery of food and cash-based assistance in life-saving emergency relief operations around the world" (World Food Programme 2019a). The announcement was notable, among other reasons, because the software, services, and expertise being offered to the UN agency at no cost were reported to be valued at forty-five million USD (Parker 2019). WFP is leveraging Palantir's Foundry platform for a new "data engine" that "collates operational data into a central platform" for WFP staff "to access crucial information such as beneficiaries' food ration quantities, transportation and food costs" (World Food Programme 2020).

In a follow-up statement on the partnership following initial civil society outcry due to Palantir's controversial history including contracts with agencies whose values are antithetical to the humanitarian cause (Easterday 2019), WFP emphasized that Palantir would not be able to access data about its beneficiaries, that the partnership was dedicated solely to improving operational efficiencies, that Palantir would not use WFP's data for commercial benefit, and that the UN agency would retain "full control over the data, the analysis and derivative work" (World Food Programme 2019b). In other words, WFP's partnership with Palantir is aimed at supply chain optimization (ostensibly unrelated to personal data), with controls being implemented to prevent unauthorized data collection or further processing.

All of which begs the question: why would Palantir partner with a humanitarian agency at its own expense especially if it is contractually prohibited from extracting direct value from WFP's data (or any analytical or derivative products related thereto)? While the partnership could be understood as a way for Palantir to develop future commercial opportunities in a new market, namely the humanitarian domain, by leveraging the multiyear experience of working with WFP (the world's largest humanitarian agency) to approach other organizations in the sector to pitch new business, there are other possible explanations. Palantir's relationship with WFP may help the firm attract a more diverse pool of data analysts, including talent with political sensibilities who would otherwise shy away from working with the company's core clientele, i.e., intelligence, law enforcement, and immigration authorities. While this is a form of aidwashing aimed at strengthening the firm's recruitment efforts, a more blatant example of Palantir benefitting reputationally from its work with WFP is in its public celebration of its partner winning the 2020 Nobel Peace Prize shortly after the company's initial public offering (IPO) (see Figure 1).

[1] Quote from Alex Karp, Palantir's CEO (qtd. in Ponciano 2022).

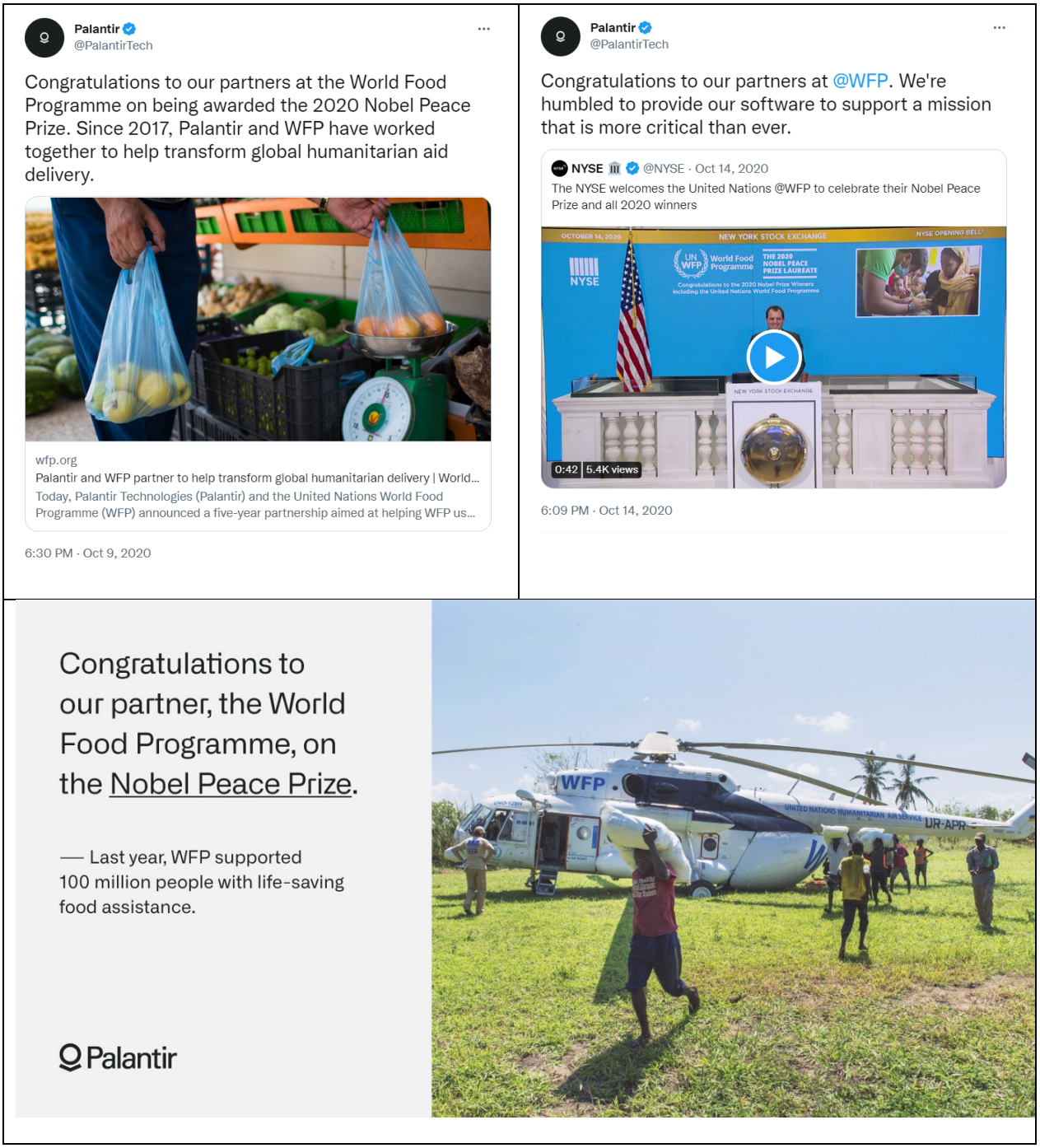


***Figure 1:*** *Palantir's public celebration of WFP's 2020 Nobel Peace Prize.*

Aside from its partnership with WFP, Palantir has also emerged very publicly during the 2022 conflict in Ukraine, with its CEO being the first chief executive to visit the country since the Russian invasion (Fedorov 2022). In June 2022, the company's leadership and the Ukrainian president, Volodymyr Zelenski, met to discuss "how Palantir can continue to use its technology to support Ukraine" (Chapman 2022). Beyond the country's borders, Palantir is also involved in helping European countries (Poland, Lithuania, UK, etc.) manage the influx of Ukrainian refugees.

## Clearview AI in Ukraine

Palantir is not the only surveillance firm that has found opportunity in the Ukraine conflict. The controversial facial recognition software provider, Clearview AI, has also sought to aidwash its tarnished reputation by offering access to its product to Ukrainian authorities at no cost. Clearview AI has faced repeated legal challenges, regulatory actions, and fines in the United States, Canada, Australia, United Kingdom, across the European Union, and elsewhere due to the companies' illegal use of people's photos scraped from the web without consent (cf. Hogue's dialogue contribution on open-source intelligence in the Ukraine conflict, in this issue). The Ukraine conflict thus provides an opportune moment for a public relations exercise.

In March 2022, Reuters revealed that Clearview AI was providing Ukrainian authorities with free access to the company's facial recognition search engine to "vet people of interest at checkpoints, among other uses" (Dave and Dastin 2022). A month later, it was reported that Clearview AI had created "more than 200 accounts for users at five Ukrainian government agencies," as well as translating its app into Ukrainian (Hill 2022). The provision of free or subsidized technology for humanitarian uses like in the Palantir relationship with WFP or in the Clearview AI case in Ukraine is a common type of partnership in the sector (UN OCHA 2020: 2), but it raises unique sensitivities where the software is explicitly designed for surveillance purposes or in cases in which the firms involved are widely seen as exploiting a humanitarian crisis for reputational gain. To be clear, the Ukraine case is different in the sense that the end user of Clearview AI's platform is the government, not a humanitarian organization, but as one of the main applications of the service is reported to be the identification of dead Russian soldiers so as to inform their family members and facilitate the return of bodily remains—an activity governed by international humanitarian law[2]—it is worth interrogating Clearview AI's aims.

The UN Office for the Coordination of Humanitarian Affairs (OCHA), which serves as the humanitarian arm of the UN Secretariat with primary responsibility for the provision and coordination of humanitarian aid to affected populations, has acknowledged these risks. OCHA's Center for Humanitarian Data has published guidance that highlights, among other risks emanating from public-private technology partnerships, that "for humanitarians, reputational damage can occur if a private sector partner has been associated with human rights infringements in a past project, or is perceived to be 'whitewashing' by collaborating with a humanitarian partner. This can lead to restrictions in access and erosion of trust with affected populations, which could undermine the ability of humanitarian organizations to deliver assistance" (UN OCHA 2020: 4).

## Concluding Remarks

Despite such formal guidance, there are scant public examples of humanitarian organizations deciding against a proposed data or technology partnership following a due diligence or risk assessment or discontinuing such a partnership following civil society pushback or emergent concerns related to harmful surveillance practices or aidwashing by technology vendors. In August 2022, UN Women ended a partnership "to cooperate in promoting the growth of gender lens investing" with the investment company BlackRock only three months after it was formed, citing "concerns raised by civil society" (De Wei and Konotey-Ahulu 2022). A collective of feminists and women's rights activists had mobilized to argue that "UN Women ha[d] been recruited to BlackRock's image-cleansing efforts—this time it is seeking to 'pinkwash' itself… If this is a 'partnership', it looks like it works in just one direction. It gives BlackRock a veneer of feminist approval that it clearly does not merit" (Association for Women's Rights in Development 2022).

While the UN Women case is unrelated to the surveillance industry (at least directly so), it does demonstrate the potential for civil society contestation where values between partners do not align. But it also raises the

[2] See Rule 114. Return of the Remains and Personal Effects of the Dead: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule114.

question of why civil society resistance to the World Food Programme's partnership with Palantir has been ineffective in ending the relationship. One suggestion is that its operational focus and emphasis on supply chain logistics (as opposed to beneficiary's personal data) has made it harder for civil society to articulate a convincing problematic. In the case of Clearview AI offering its facial recognition tools to Ukrainian authorities during the conflict with Russia, civil society voices seem to have missed the point. For example, a representative from the digital rights group Fight for the Future has argued that: "War zones are often used as testing grounds not just for weapons but surveillance tools that are later deployed on civilian populations or used for law enforcement or crowd control purposes. Companies like Clearview are eager to exploit the humanitarian crisis in Ukraine to normalize the use of their harmful and invasive software" (Evan Greer of Fight for the Future qtd. in Hill 2020). I would instead argue that, while Clearview AI is indeed exploiting the Ukraine crisis, it is doing so primarily to aidwash its reputation, not for experimental purposes (Sandvik et al. 2017) or to normalize the use of its technology, which is already in widespread use by police departments and other law enforcement agencies around the world. Rather, like Palantir, it sees opportunity in demonstrating how its platform can also serve humanitarian aims, thus further complicating the tensions inherent in surveillance as representing both control and care.

Finally, it is not just Palantir and Clearview AI that are in the business of aidwashing. In January 2023, IrisGuard (2023)—an iris biometrics firm that handles "around $1.2 billion a year of humanitarian cash, the equivalent of ten percent of global distributed humanitarian aid" (Hersey 2022)—announced that it was becoming a member of the UN Global Compact Network UK (which serves as a point of contact for UN Global Compact signatories in the UK). We should expect to see further cases of these public relations activities by surveillance firms as humanitarian crises grow in number and complexity.

## Acknowledgments

While based at the Tilburg Institute for Law, Technology, and Society, the author received funding from the European Research Council under the EU's Horizon 2020 research and innovation programme (grant agreement n° 757247). The author would like to thank Kristin Bergtora Sandvik for organizing the June 2022 roundtable where the idea for this paper emerged following interventions by Faine Greenwood and Stuart Campo, as well as Linnet Taylor, Silvia Masiero, John Warnes, Ziad Al Achkar, Keren Weitzberg, Emrys Schoemaker, and Margie Cheesman for sharing their insights.

## References

Association for Women's Rights in Development. 2022. Feminists Demand End of UN Women's Partnership with Blackrock, Inc.. https://awid.org/news-and-analysis/feminists-demand-end-un-womens-partnership-blackrock-inc [accessed February 14, 2023].

Ball, Kirstie, and Laureen Snider. 2013. *The Surveillance-Industrial Complex*. London: Routledge.

Berliner, Daniel, and Assem Prakash. 2015. "Bluewashing" the Firm? Voluntary Regulations, Program Design, and Member Compliance with the United Nations Global Compact. *Policy Studies Journal* 43 (1): 115–138.

Chapman, Lizette. 2022. Palantir CEO Alex Karp Met with Zelenskiy in Ukraine. *Bloomberg*, June 2. https://www.bloomberg.com/news/articles/2022-06-02/palantir-ceo-alex-karp-met-with-zelenskiy-in-ukraine [accessed September 29, 2022].

Dave, Paresh, and Jeffrey Dastin. 2022. Exclusive: Ukraine Has Started Using Clearview AI's Facial Recognition during War. *Reuters*, March 14. https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13 [accessed September 29, 2022].

De Wei, Low, and Olivia Konotey-Ahulu. 2022. UN Women Group Ends Partnership with BlackRock after Criticism. *Bloomberg*, August 26. https://www.bloomberg.com/news/articles/2022-08-26/un-women-terminates-partnership-with-blackrock-after-criticism [accessed September 29, 2022].

Easterday, Jennifer. 2019. Open Letter to WFP re: Palantir Agreement. Responsible Data, February 8. https://responsibledata.io/2019/02/08/open-letter-to-wfp-re-palantir-agreement [accessed September 29, 2022].

Fedorov, Mykhailo. 2022. Today me and President @ZelenskyyUa hosted Alex Karp CEO @PalantirTech. Alex is the first CEO, who came to Kyiv after the start of the full-scale war. Impressive support and faith in credibility of investments: agreed on office opening and digital support of Army. Twitter, June 2. https://twitter.com/FedorovMykhailo/status/1532343175087591425 [accessed February 14, 2023].

Frowd, Philippe M. 2018. *Security at the Borders*. Cambridge, UK: Cambridge University Press.

———. 2021. Borderwork Creep in West Africa's Sahel. *Geopolitics* 5: 1131–1351.

Hersey, Frank. 2022. IrisGuard Looks to New Tech for Further Use Cases as It Handles 25M Interactions a Day. Biometric Update, May 24. https://www.biometricupdate.com/202205/irisguard-looks-to-new-tech-for-further-use-cases-as-it-handles-25m-interactions-a-day [accessed January 9, 2023].

Hill, Kashmir. 2022. Facial Recognition Goes to War. *The New York Times*, April 7. https://www.nytimes.com/2022/04/07/technology/facial-recognition-ukraine-clearview.html [accessed June 27, 2022].

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.

Hosein, Gus, and Carly Nyst. 2013. Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives Are Enabling Surveillance in Developing Countries. Privacy International. https://privacyinternational.org/report/841/aiding-surveillance [accessed February 14, 2023].

Iliadis, Andrew, and Amelia Acker. 2022. The Seer and the Seen: Surveying Palantir's Surveillance Platform. *The Information Society* 38 (5): 334–363.

IrisGaurd. 2023. We are proud to be joining the UN @globalcompactUK and work with other organisations that share our commitment to accelerating sustainability efforts and scaling up impact. Twitter, January 6. https://twitter.com/IrisGuard/status/1611364619183964160 [accessed February 14, 2023].

Kaurin, Dragana. 2019. Why Libra Needs a Humanitarian Fig Leaf. *Berkman Klein Center Medium Collection*, July 8. https://medium.com/berkman-klein-center/why-libra-needs-a-humanitarian-fig-leaf-79ae6a463c8 [accessed June 27, 2022].

Latonero, Mark. 2019. Stop Surveillance Humanitarianism. *The New York Times*, July 11. https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html [accessed June 27, 2022].

Martin, Aaron. 2019. Mobile Money Platform Surveillance. *Surveillance and Society* 17 (1/2): 213–222.

Martin, Aaron, Gargi Sharma, Siddharth Peter de Souza, Linnet Taylor, Boudewijn van Eerd, Sean Martin McDonald, Massimo Marelli, Margie Cheesman, Stephan Scheel, and Huub Dijstelbloem. 2022. Digitisation and Sovereignty in Humanitarian Space: Technologies, Territories and Tensions. *Geopolitics*. https://doi.org/10.1080/14650045.2022.2047468.

Parker, Ben. 2019. New UN Deal with Data Mining Firm Palantir Raises Protection Concerns. *The New Humanitarian*, February 5. https://www.thenewhumanitarian.org/news/2019/02/05/un-palantir-deal-data-mining-protection-concerns-wfp [accessed June 27, 2022].

Ponciano, Jonathan. 2022. Palantir Stock Collapses after Disappointing Earnings—CEO Warns Threat of Nuclear War 'Significantly' Underestimated. *Forbes*, May 9. https://www.forbes.com/sites/jonathanponciano/2022/05/09/palantir-stock-collapses-after-disappointing-earnings-ceo-warns-threat-of-nuclear-war-significantly-underestimated/ [accessed December 1, 2022].

Sandvik, Kristin Bergtora, Katja Lindskov Jacobsen, and Sean Martin McDonald. 2017. Do No Harm: A Taxonomy of the Challenges of Humanitarian Experimentation. *International Review of the Red Cross* 99 (1): 319–344.

Thylstrup, Nanna Bonde, Kristian Bondo Hansen, Mikkel Flyverbom, and Louise Amoore. 2022. Politics of Data Reuse in Machine Learning Systems: Theorizing Reuse Entanglements. *Big Data & Society* 9 (2). https://doi.org/10.1177/20539517221139785.

UN OCHA. 2020. Data Responsibility in Public-Private Partnerships. United Nations Office for the Coordination of Humanitarian Affairs, February 3. https://centre.humdata.org/guidance-note-data-responsibility-in-public-private-partnerships [accessed February 14, 2023].

Weitzberg, Keren, Margie Cheesman, Aaron Martin, and Emrys Schoemaker. 2021. Between Surveillance and Recognition: Rethinking Digital Identity in Aid. *Big Data & Society* 8 (1). https://doi.org/10.1177/20539517211006744.

World Food Programme. 2019a. Palantir and WFP Partner to Help Transform Global Humanitarian Delivery. February 5. https://www.wfp.org/news/palantir-and-wfp-partner-help-transform-global-humanitarian-delivery [accessed February 14, 2023].

———. 2019b. A Statement on the WFP-Palantir Partnership. February 7. https://medium.com/world-food-programme-insight/a-statement-on-the-wfp-palantir-partnership-2bfab806340c [accessed February 14, 2023].

———. 2020. Digital Transformation: Beyond the Annual Performance Report 2019 Series. June. https://docs.wfp.org/api/documents/WFP-0000116930/download/ [accessed February 14, 2023].