Surveillance & Society

Article

The Art of Screening: Reasonable Efforts and Measures at the Nexus of Aid Work and Counterterrorism

Beáta Paragi

Corvinus University of Budapest, Hungary
beata.paragi@uni-corvinus.hu

Abstract

Surveillance in the context of aid work refers to control over procedures, supplies, goods, and people that is deemed necessary for providing care. It is widely considered an inalienable, albeit criticized, part of care provision. International non-governmental organizations implementing aid projects in the Global South (hereafter INGOs or aid organizations), however, also screen individuals based on either conditional clauses in funding agreements in the context of counterterrorism or on their pursuing other organizational interests. While this opaque practice has raised increasing concerns both in humanitarian and development circles, it is much less known how screening is implemented and if it can be construed as (harmful) surveillance. Therefore, qualitative methods were used to explore a screening tool, the description of which is the core empirical part of this study, and to map INGO experiences and dilemmas with screening. As findings indicate, vendors delivering surveillance technology can help INGOs to navigate the complexity of sanctions and enforcement lists, ensure legal compliance, and demonstrate accountability towards donors, while the transparency obligation prescribed in data protection laws poses huge challenges. Furthermore, the right to be recognized, supported, assisted, and employed—either in the humanitarian or the development context—depends on how INGOs categorize individuals before screening and how they make decisions based on the results. The article contributes to earlier research by including screening in the conceptualization of (counter)surveillance in aid work.

Introduction

In Autumn 2021, six Palestinian human rights organizations were designated as terrorist organizations by Israel, the government of which officially asked donors to stop funding them. European Union (EU) member states hesitated to provide a straightforward answer to this "call" in the absence of convincing evidence (Ziv and Abraham 2022). They also had to be cautious because any official response would have entailed consequences, such as terminating funding to aid projects, in line with the so-called reasonable measures expected in the context of anti-money laundering and combating the financing of terrorism (AML/CFT) (Sullivan 2020; Rébé 2020). However, little is known about how non-state actors implement "reasonable measures" in the era of surveillance societies and "commercialized suspicion" (Lyon 2007: 67).

Being simultaneously recipients of official donor money and potential donors to local beneficiaries, international non-governmental organizations implementing aid projects in the Global South (hereafter INGOs or aid organizations), humanitarian organizations (HOs) included, are expected to prevent the use of donor money for illicit purposes. To minimize transactions with designated organizations, sanctioned

Paragi, Beáta. 2024. The Art of Screening: Reasonable Efforts and Measures at the Nexus of Aid Work and Counterterrorism. *Surveillance & Society* 22(2): 138-159.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487

persons, or anyone affiliated with listed entities, INGOs conduct screenings.[1] While screening of *final* beneficiaries has been widely discussed in the context of international humanitarian law by practitioners (Gillard 2021a, 2021b), screening *in general* also raises questions with regard to privacy and surveillance. Recalling the synergies between surveillance (law) and privacy studies (Goold and Neyland 2009; Skinner-Thompson 2022), these domains are linked by their common interest in individuals and personal data. Screening, indeed, can be conceptualized as a series of data processing operations, at the core of which are personal data (Paragi 2023).

International financial surveillance has enjoyed academic attention for more than a decade due to the controversial politics of listing (De Goede 2012; De Goede and Sullivan 2016; Minella 2019; Sullivan 2020); the involvement of private actors, financial institutions, lawyers, and corporations in securitization and AML/CFT activities (Amicelle 2011; Amicelle and Favarel-Garrigues 2012; De Goede 2017; Helgesson and Mörth 2019); and the emergence of the reg-tech and fin-tech industry (Arner, Barberis, and Buckley 2016; Hanley-Giersch 2019). The participation of INGOs in surveillance–like activities, however, is much less highlighted or somehow mischaracterized, for surveillance is seen as an inalienable, albeit criticized, part of care provision in various contexts.

Terms such as digital humanitarianism (Duffield 2016), financial humanitarianism (Tazzioli 2019), surveillance humanitarianism (Latoreno 2019), humanitarian dataveillance (Sandvik 2020), and surveillance funded by foreign donors in Global South countries (Hosein and Nyst 2013; Martin 2023) reflect the controversial manner in which aid organizations engage with technologies and data. As digital innovations, especially in humanitarian fields, are not without harmful consequences (Sandvik, Jacobsen, and McDonald 2017), increasing attention has been paid to the blurred borders of control and care (Fast and Jacobsen 2019; Paragi and Altamimi 2022) and those of recognition and surveillance (Weitzberg et al. 2021; see below).

Therefore, to contribute to earlier research, the purpose of this article is to extend the understanding of surveillance in the context of aid work by exploring how screenings conducted by larger aid organizations can be interpreted within the conceptual framework of (critical) surveillance studies. Surveillance in this latter domain means "a focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction" (Lyon 2007: 14) and of governing populations' activities (Haggerty 2009: 278). It usually involves "relations of power in which watchers are privileged," where the watched may also play a role by participation (Lyon 2007: 15). The traditional sites of surveillance—military, governmental, employment, police and crime control, and consumer spaces (Lyon 2007: 25–45)—as well as their sister- and sub-spaces, have not only received widespread scholarly attention but also have been increasingly scrutinized in the context of privacy and personal data protection. The civil space, however, is only included in the analysis in two main cases: when NGOs are targets of governmental or financial surveillance, or when they advocate for human rights to prevent harmful surveillance, in many cases by implementing countersurveillance measures.

On one hand, financial institutions conduct financial surveillance over the international transactions of aid organizations in line with international standards and domestic legislations (Amicelle 2011; Rébé 2020). Such control over international financial transactions potentially implies the criminalization and securitization of aid NGOs by governments, treating "the boundary between civil society and the state as a matter of security, particularly in relation to 'foreign influence'" (Watson and Burles 2018: 4; see also Howell and Lind 2009; Howell 2014; Jackson 2015; Lazell and Petrikova 2020). While at least 140 governments adopted counterterrorism legislation between 2001 and 2018, such measures can also be used against civil society actors (Human Rights Council 2019: 2). Indeed, aid NGOs are not only subject to

[1] While wealth screening conducted by aid INGOs for fundraising purposes is not the subject of this article, the conceptual difference between vetting and screening also deserves to be mentioned. While the latter is carried out by aid actors (INGOs) themselves, the former requires them to provide the identity information of individuals and entities to the official donor (USAID, for example), which carries out the checks itself (Gillard 2021a: 48).

surveillance as bank clients but also may be criminalized or securitized as foreign agents. While Muslim charities traditionally have been considered suspicious in Western countries (Malakoutikhah 2020), certain governments—in Russia, Turkey, Israel (Lamarche 2019), and Hungary (Nagy 2017), among others—not only rhetorically labelled but also legally designated international and local NGOs as security risks, accusing them of threatening public order or "national values" (Human Rights Council 2019). Foreign and fellow local NGOs can also be surveilled by other NGOs, sort of "vigilante" organizations, such as the pro-Israeli NGO Monitor, which aims to demonstrate how civil society actors may contribute to funding Palestinian "terrorism" (Lamarche 2019).

On the other hand, certain NGOs may also be engaged in countersurveillance activities (Monahan 2006).[2] Exploring the practices of organizations that provide assistance to migrants and refugees, Topak (2019) distinguished "humanitarian surveillance" from "human rights surveillance." While they share the ambition to "resist the spread of discriminatory and hierarchical surveillance and appropriate surveillance technologies to use them in oppositional ways" (Topak 2019: 388), human rights surveillance aims at advancing the well-being and rights of marginalized populations in ways similar to the practices of actors conducting countersurveillance. Humanitarian surveillance, however, cannot be considered countersurveillance. Rather, it is a parallel form of "surveillance that contributes to surveillance and normalizes the hierarchies between watcher and watched" (Topak 2019: 388).

To explore how aid NGOs are made into "watchers"—how they provide "focused, systematic and routine attention to personal details" (Lyon 2007: 14)—the following research questions were posed: How is screening conducted? How does technology (offered as a compliance solution by private vendors) work from an empirical perspective? What dilemmas do INGOs face considering the power imbalances embedded in aid relations (Barnett 2002: 32–46)? A detailed overview of surveillance theories (Lyon 2007; Ball, Haggerty, and Lyon 2012) is beyond the scope of this article, but the most important themes, along which different sites of surveillance can be compared, will be used to structure the findings. These include rationalization, technology, sorting, knowledgeability, and urgency (Lyon 2007: 26–27). The power relations between the watchers and the watched in the context of screening will be approached by approximating reasonable expectations of the "ignorant" watched. As findings indicate, screening strengthens and normalizes hierarchies between watcher and watched at least as much as it is potentially used as a countersurveillance measure.

The article unfolds as follows. The methods section is followed by a brief summary of the main conceptual elements of surveillance in the context of counterterrorism and aid work. The core empirical part of the research findings is the description of a tool used for screening, as contemporary surveillance can hardly be understood without considering the socio-technical dimension (Lyon 2007: 21) and knowledgeability in the context of surveillance studies (Lyon 2007: 27). As screening is also a data processing operation, data subjects' reasonable expectations are considered because not only are they inherently linked with data protection principles and the right to information (Klareen 2013; Bygrave 2014; Vrabec 2021) in the context of law enforcement and counterterrorism (Tzanou 2017) but they also illustrate power imbalances between the watchers and the watched. I then discuss the findings.

Materials and Methods

The research followed a qualitative design[3] considering that very little research has been conducted with regards to how the General Data Protection Regulation (GDPR) affected European donor policies and aid

[2] Organizations such as Privacy International and Access Now are at the forefront of anti-surveillance movements fighting for privacy rights.

[3] This article communicates the results of research whose initial purpose was to explore EU-based NGOs' experiences with the GDPR in the context of aid projects implemented in the Global South. While this article analyses screening as surveillance, a sister article (Paragi 2023) discussed the transparency dimension of screening (within the broader context of data protection and GDPR).

NGOs operating in the Global South after it had entered into force in 2016 (Gazi 2020; Franz, Hannah, and Hayes 2020; Paragi 2021). Semi-structured qualitative interviews (n=12) were conducted in spring and autumn 2021 to explore dilemmas with regards to EU GDPR (2016): screening appeared as a common concern for most interviewees, either for ethical reasons or for legal compliance. The discussions usually lasted for an hour and were not recorded; only notes were taken. Therefore, the few quotes cited in this article are not results of a content analysis of written transcripts but are only used to illustrate dilemmas shared across organizations. A workshop was also arranged in 2022, with the primary purpose to provide an opportunity for practitioners to discuss the data protection dilemmas of screening (Workshop, Septemeber 23, 2023). Participants—researchers (n=7), legal advisors, and data protection officers (DPOs) (n=11) of aid organizations (n=6)—were also notified about my ongoing research.

This article does not attempt to offer a comprehensive assessment of NGO conduct with regard to any data protection law,[4] partially because restrictions might apply in certain jurisdictions. However, relevant provisions of the EU GDPR (2016) will be used to illustrate the transparency obligations that are applicable in the case of NGOs that are registered in the EU/European Economic Area (EEA).[5] It is also established that a lot is unknown with regard to the use of various technologies by NGOs and related practices of data collection, processing, and sharing (Jacobsen 2022: 623).

The online survey was conducted from January 2021 to April 2021 (Paragi 2022). Respondents' data are summarized in Table 1.

Table 1. *Profiles of European aid NGOs participating in the online survey*

Location within Europe (n=35)	**Main area (n=35)**	**Geographic areas of operations (multiple)**	**Number of local employees (n=35)**
Scandinavia (12)	Development (9)	Middle East (21)	Fewer than 10 (10)
Central-Eastern Europe (5)	Humanitarian (4)	North Africa (14)	11–20 (3)
Western Europe (11)	Both (18)	Sub-Saharan Africa (29)	21–50 (4)
Southern Europe (3)	None, other (4)	Asia (21)	More than 51 (18)
United Kingdom (4)		Latin America, Caribbean (20)	
		EU Eastern neighbourhood (14)	
		Other (2)	

While the survey contained only two questions regarding screening,[6] the content of privacy notices was assessed for direct evidence. Terms such as (ethical) screening, vetting, background check, due diligence, fraud prevention, and AML/CFT were deemed "direct" evidence, but indirect formulation was also considered for the extent to which screening may have been inferred from other wording. Considering there are thousands of NGOs registered in the EU/EEA, aid organizations were selected based on their VOICE (n.d.) membership (n=88) as well as on a random basis (n=5) so that larger actors present in multiple areas with a diverse profile and employee pool were part of the sample. All in all, the content of ninety-two publicly available privacy notices was assessed for evidence on screening (usually under the subthemes

[4] The EU GDPR (2016) is relevant the extent to which screening can be conceptualized as a data processing operation alongside the provisions of the GDPR.

[5] See Paragi 2023.

[6] Q10 asked about the typical purposes for data collection; Q15c (a follow-up question) inquired about the specific purposes of collecting personal data for meeting donor requirements.

purposes of processing, legitimate interest, and data transfer to third parties as data processors) in November 2022.[7]

To illustrate how technology is used by aid organizations beyond stated objectives—that is, for development and humanitarian purposes (Walsham 2017: 28)—an anonymized screening ("CP-WatchList-Tech") tool will be introduced in this paper, considering that there are various products available on the market for non-profit clients too. Documentation on "CP-WatchList-Tech" obtained by email was used to demonstrate the technical side of screening. Its vendor, "CompliancePartner" (CP), offers access to a cloud-based consolidated database containing multiple and integrated watch lists.[8] This information was complemented with the description of a similar screening software, World Check (De Goede and Sullivan 2016: 76–81), information available on the corporate websites of LexisNexis Risk Solutions and CSI WatchDOG Elite and a qualitative interview with a European representative of LexisNexis (as of autumn 2021). While the latter contributed to a better understanding of the technical side, the information obtained was verified by triangulation, namely, correspondence with an advisor working at a European aid organization using the tool.

With regard to research ethics, I followed the EU (2021) guidelines and shared information on the details of the research with the participants by email based on which interviewees provided their consent for participation. Key informants were provided with the opportunity to read the original manuscript before initial submission.

Conceptual Framework

International organizations (IOs) such as the United Nations (UN) and the EU require their member states to combat terrorism by various means, such as treaties and Security Council resolutions (Rébé 2020: 18–20),[9] agencies and institutions (e.g., Financial Action Task Force [FATF] [n.d.], UN Office of Counter-Terrorism, Council of Europe Committee on Counter-Terrorism, and EU Counter-terrorism Coordinator), advisory tools (Rébé 2020: 20–23), sanctions lists, and domestic laws (De Goede and Sullivan 2016; Sullivan 2020; Rébé 2020: 107–238).

The politics of listing involves decisions about placing legal or natural persons on international or national sanctions lists or designating them as terrorists. While not every listed person is a terrorist, terms such as "terrorism" or "terrorist" do not have a universal definition. Therefore, they can be equally used, abused, or misused by those in power (Sullivan 2020). For example, while contemporary Russia doubts the legality and legitimacy of sanctions against Russian citizens, Western governments consider it problematic that even imprisoned human rights defenders and journalists can be labelled as terrorists for "spreading misinformation, leaking state secrets and insulting authorities" in many parts of the world (Amnesty International 2020: 16). Delisting is challenging even in the case of international sanctions lists (Sullivan 2020; Minella 2019).

[7] Only one privacy notice per NGO was publicly available, with the exception of two organizations (NRC and PLAN UK). Larger NGOs may have multiple privacy notices (PNs) (for internal use only) addressed to various groups of people (data subjects: candidates, employees, etc.), which may be subject to change. For example, PLAN UK has revised its privacy notices since the data collection was closed (in November 2022); it used to have six PNs, but in early 2023 there were four. Three NGOs did not have a privacy notice as of November 2022.

[8] Both the company name (CompliancePartner) and the product name (CP-WatchList-Tech) are fictional because the key informant left the company since our email-correspondence. While the original company and product names have been anonymized, the year of publication (version) and page numbers are encrypted wherever the internal documents are cited.

[9] UNSCR 1373 is particularly relevant for INGOs as it requires states to introduce laws that criminalize terrorism and the support of terrorism.

Listing has contributed to the emergence of financial surveillance by banks and other financial institutions. The implementation of customer due diligence (CDD) and know-your-customer (KYC) procedures in the context of AML/CFT required a huge investment in resources, skills, and creativity in the financial sector (Amicelle 2011; Amicelle and Favarel-Garrigues 2012). With regard to the EU, since its Directive 2001/97/EC on money laundering and Directive 2005/60/EC on AML/CFT were adopted, banks, accountants, lawyers, and a wide range of other private actors have been obligated to follow a risk-based approach in their dealings with clients (European Union 2005). As discussed by Helgesson and Mörth (2019: 258), among others, these directives "include obligations to identify and monitor clients properly" as well as "to report suspicions of illicit financial transactions to the national financial police without informing the client concerned." EU-based aid organizations—as clients of banks, and as recipients of official funding—are also legally obliged to have an overview of their transaction partners following FATF Recommendation 8/2001 (Financial Action Task Force 2014; Financial Action Task Force 2015),[10] international and related domestic laws, and contractual clauses in grant agreements. However, unlike banks, which use their websites and other means to communicate AML/CFT activities in general, no such information is available on the websites of most INGOs (Paragi 2023).

The lack of transparency does not mean that listing and related AML/CFT measures have not influenced how security is interpreted and works within the domain of donations and giving. As noted by De Goede (2012: 21), the "pursuit of terrorist monies depends on the deployment of preemptive decisions and speculative techniques that have their genealogy in financial practices" in domains of (international) charity too. As implied, bigger INGOs are not only passive objects of (financial, governmental) surveillance but also may cooperate with private actors' "aidwashing" surveillance technologies in the Global South (Martin 2023) and/or conduct screenings in-house for legal-regulatory compliance or other legitimate interests that may go beyond sanctions and counterterrorism (Hayes 2017: 28–29).

It should also be acknowledged that HOs (humanitarian organizations) concerned with human rights and principaled humanitarian work have fought against their co-optation into counterterrorism activities for many years.[11] Therefore, a recently adopted UN resolution (UNSCR 2664/2022) has come as a "relief" to HOs, as a result of which "[1]… the provision, processing or payment of funds, other financial assets, or economic resources, or the provision of goods and services necessary to ensure the timely delivery of humanitarian assistance… are permitted and are not a violation of the asset freezes imposed by this Council or its Sanctions Committees [any more]" (UNSC 2022). Yet paragraph three notes that the exemption does not apply to the expected risk-mitigation measures, such as screening, with the Security Council requesting that, "*providers* relying on paragraph 1 *use reasonable efforts* to minimize the accrual of any benefits prohibited by sanctions, whether as a result of direct or indirect provision or diversion, to individuals or entities designated by this Council or any of its Committees, including *by strengthening risk management and due diligence strategies and processes*" (UNSC 2022; emphasis added).

Screening by aid organizations operating in the Global South can be approached by considering insights from critical international relations (IR) and security studies (Duffield 2001, 2007; Howell and Lind 2009; Howell 2014; Lazell and Petrikova 2020; Pallister-Wilkins 2021), scholarship on the use of technology and data for development purposes (Walsham 2017; Qureshi 2019), cooperation between aid actors and companies delivering surveillance technologies (Hosein and Nyst 2013; Martin 2023), the nexus of humanitarian law and counterterrorism (Gillard 2021a, 2021b; Eckert 2022), and data protection (Gazi

[10] FATF Recommendation 8 says: "Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Certain *non-profit organisations are particularly vulnerable*, and *countries should ensure that they cannot be misused*: (a) by terrorist organisations posing as legitimate entities; (b) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset-freezing measures; and (c) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations" (Financial Action Task Force 2001: 4, 7; emphasis added). On the ongoing FATF-consulation with the civil society sector see Financial Action Task Force 2023.

[11] See, for example, the websites of the Norwegian Research Council (2020) and the International Review of the Red Cross (2022) dedicated to this topic.

2020; Franz, Hannah, and Hayes 2020; Paragi 2023). Critical IR and security studies have been concerned with how aid work and the operation of Northern INGOs have become securitized—to some extent even partially instrumentalized—in the context of counterterrorism. Surveillance studies, however, focuses more on visibility and ways of seeing people and watching their corresponding digital(ized) bodies. Recalling that spaces of surveillance can be explored by focusing on rationalization, urgency, sorting, technology, knowledgeability, and the power relations between the watchers and the watched (Lyon 2007: 26–27), the next section will analyse screening by NGOs against these themes.

Findings

Aid organizations use personal data collected from individuals, their (would-be) donors, employees, suppliers, partners, and (in the case of development projects) beneficiaries to check if their names can be found on any watch list (Paragi 2023). Screening is widely used in original, medical context with positive connotations, as "[s]creening tests sort out apparently well persons who probably have a disease from those who probably do not" (World Health Organization 1968). As it is about examining something or somebody to detect a fault in order to prevent harmful effects, screening is more controversial in the context of counterterrorism or homeland security (passenger screenings by airlines, customer screenings by banks) because societal or political faults are more contested than biological equivalents. In the case of NGO s, one of the "faults" is transferring donor money to individuals that are either criminalized (by law enforcement actors), securitized (listed on a sanctions list or designated as a terrorist), or simply considered a reputational hazard. As a result, regular screening may enable INGOs to distinguish persons with "normal" backgrounds from those engaged in "suspicious" activities.

Rationalization, Urgency, and Sorting

Rationalization in the case of aid INGOs operating in the Global South is related to risk mitigation.[12] While the reasons for screening may vary from context to context, risks can be overlapping even if development INGOs work under different conditions than HOs and IOs, which usually justify their actions by "emergency" situations. Hiring a politically exposed person (PEP; for a definition, see Gilligan 2009), or using donor money for a project that benefits a sanctioned person, can equally carry legal, financial, or reputational risk.

When aid NGOs receive funding from official donors, financial and legal compliance may also be enforced by funding agreements. By signing the donor contract, an NGO becomes responsible not only for the aid project it implements but also for complying with legal conditions in the context of AML/CFT. As preventing the use of donor money for illicit purposes is in the best interest of any implementing actor, the inclusion of conditional clauses in funding agreements has become a norm (European Union 2020; Norwegian Refugee Council 2018b, 2018c).[13] Conditional clauses rarely prescribe screening per se, but the expectation is implied in their wording according to experiences (Workshop, September 23, 2022). The obligation of CDD/KYC on the part of the final grant beneficiaries (international, European or local NGOs) is not without dilemmas because the interpretation of the given clauses is not always obvious (Interview 3, Zoom interview with a leader and data protection office, February 12, 2021), and because a "lot of confusion" exists about whether screening individuals prevents the misuse of funds (Interview 2, Zoom interview with an advisor working at a Norwegian NGO, January 8, 2021). Indeed, what prevention and "reasonable measures" mean is rarely specified in grant agreements (Gillard 2021a: 47); rather, it is either negotiated between the given donor and the NGO considering the humanitarian implications (Gillard 2021b: 523, 526–528) or left to the market, which offers various tech solutions (De Goede and Sullivan 2016).

[12] Screening as a surveillance-like risk-mitigating measure might also be considered alongside so-called remote management practices (Akal 2022) and profiling (Duroch and Neuman 2021).

[13] Examples of conditional clauses are provided in Norwegian Refugee Council 2018b and 2018c.

To avoid being accused of financing terrorism, even if unintentionally, and to organize this practice in a time-efficient manner, many larger aid organizations resort to technology, especially if the scope of their activities involves multiple countries and sectors in the Global South; various donors (EU, US, national); numerous projects, contracts, and financial transactions; and thousands of employees. Commercially available tools are used to make screening and, as an expected result of that, sorting—primarily the sorting out of individuals that do not deserve contacts with or benefits from aid organizations—more efficient. While INGOs screen not only beneficiaries and local suppliers in the Global South but also employees and volunteers, true positive matches are rare (VOICE 2021: 12–14). Acknowledging that little is known about the real impacts of decisions based on screening, the theoretical risk is discrimination or exclusion—not only the discrimination or exclusion of humanitarian beneficiaries but also of employers and job seekers, transactions partners on grounds that may be unclear or invisible to the concerned individuals. However, to mitigate potential discrimination and to make the process of screening simpler, most large aid organizations do mass screening by treating everyone to be screened with "categorical suspicion"—recalling Marx (2005), who distinguished five types of suspicion (categorical, personalized, behavioral, protectional, and locational)—instead of screening only certain individuals in a targeted manner.

The majority of larger INGOs that participated in earlier surveys (Norwegian Refugee Council 2018a; VOICE 2021) acknowledged using external vendors for screening. As indicated by the findings of the online survey that explored experiences and dilemmas with GDPR compliance, contractual obligations for screening (vetting, background checks of individuals, etc.) were mentioned by 60% of the respondents (n=21) as a purpose for data collection (Q10: "What are the main purposes of collecting and processing personal data of local [non-European[data subjects at your organization [as data controller] in the context of project implementation?"). When asked about the specific purposes of collecting personal data for meeting donor requirements in a follow-up question (Q15c), 60% of the respondents (twenty-one of thirty-five INGOs) confirmed that they collect personal data for "contractual obligations required by donors (background check, vetting or screening of individuals expected by our donors)"; six respondents indicated that this question was not applicable in their case, while eight organizations (22.8%) claimed that they did not collect personal data for such purposes.

The Technology Used for Screening

Screening is about running a search online that is checking whether lists of personal data match various watchlists in the consolidated database. The most popular tech solutions available on the market are FinScan, LexisNexis (former WorldCompliance), CSI WatchDOG Elite, LexisNexis WorldCompliance, Visual Compliance System (VOICE 2021: 13), and World Check (formerly Thomson Reuters, operated by Refinitiv/LSEG as of 2014) (De Goede and Sullivan 2016). These tools enable users, INGOs included, to synchronize watchlist screenings and navigate continuously shifting sanctions, financial crime compliance, and anti-bribery requirements.

While the World Check database included 1.2 million records in 2009 (De Goede and Sullivan 2016: 77), LexisNexis offered access to almost five million global "risk profiles" covering individuals, organizations, businesses, and vessels from 240 countries and territories in 2022 (LexisNexis 2021).

As personal data is involved, screening can be considered a data processing operation following the definition provided, for example, in Article 4(2) of EU GDPR (2016). The operation includes sharing personal data with the service provider by uploading names or files (lists with personal data) to the cloud, running the search online to check if lists of personal data (names of natural persons) match various watch lists in a consolidated database, and storing the records in order to document compliance.[14] Once the search is run, the system controls the data against the integrated database, which is a result of a "thorough sequence of research, vetting and data compilation" (LexisNexis 2021). The customized solutions/subscriptions also

[14] While the majority of suppliers are US-based, search results are stored in a database on AWS servers in Ireland if the NGO (as data controller) decides to store them.

enabled LexisNexis to develop and deploy simple, rule-based artificial intelligence to increase efficiency in search (Interview 13, Zoom interview with representative of LexisNexis, May 20, 2021).

Visibility, a further crucial component of surveillance, is ensured by watchlists with lists and screening tools. The lists can be grouped roughly into two sets based on the origin of the data. The first set contains lists that are available publicly on official governmental websites and integrated by LexisNexis® WorldCompliance™ Data or other tools according to categories in the database. Using the information provided by LexisNexis (2021) as an illustration, categories include:[15]

- SANCTIONS: Information on individuals and organizations from targeted sanctions lists worldwide; both national and international sanctions lists are included.

- ASSOCIATED ENTITY: information about family members and associates of sanctioned entities, when the associated entity is mentioned in targeted sanctions lists.

- LAW ENFORCEMENT: information on criminal offences based on materials published by official government agencies (courts, tax authorities, law enforcement agencies, etc.) and international organizations, among others; individuals on such lists are not designated as sanctioned (terrorists), but they can be convicted criminals.

- PEP: information about individuals who occupy a senior prominent public function; adhering to FATF global standards, the database may also contain information on family members and partners of PEPs.

- SOE (Sovereign Owned Entities): information about entities that are majority or minority owned by governments around the world.

Such categories are not unique to LexisNexis even if the labels (names of list categories) may vary from vendor to vendor. To illustrate what screening means and how it works, CP-WatchList-Tech is used in the following paragraphs. Both the company and product names are anonymized, as explained in the methods section.

The second set of sources (ADVERSE MEDIA as a single category) is composed of publicly available news, feeds, or social media appearances that are systematically gathered by the CompliancePartner's researcher team. The ADVERSE MEDIA category, seen as perhaps the most problematic, contains personal information about identifiable individuals that can be linked to illicit activities based on news that is published by news media sources or in social media in dozens of languages (CompliancePartner 20yyb: 14).[16] In other words, organizations and individuals not associated with financial crimes or terrorist organizations are also listed.[17] How information is gathered within the ADVERSE MEDIA category by the researcher teams is unclear both to users (INGOs) and to individuals, who may or may not be aware of being on such lists (Hayes 2017: 28). As these US-based service providers are supervised neither by financial nor

[15] Vendors share a long document with their customers that details the content of each category. Further sources (annex to contracts) contain the titles and sources (websites) of sanctions and enforcement lists—by country and international organization—that are integrated in the screening tools offered by the vendors. The databases are updated regularly following changes in the original (official) lists. For a description of the categories see, for example, the website of LexisNexis (2021).

[16] Reference date anonymized to protect source.

[17] Recalling De Goede and Sullivan (2016: 78) on World Check: "Inclusion in the World-Check database is based on open-source information research performed by multi-lingual teams around the world. In this process, web-based sources, public indictment records, newspaper articles and other publicly available information of very diverse quality—including blogs, news sites and online photographs—are reviewed for possible connections to 'financial crime, narcotics trafficking, money laundering, gambling and internet fraud [and] those types of things.'"

by EU data protection authorities (Interview 13, Zoom interview with a former representative of LexisNexis, May 20, 2021), the quality of information available to their customers cannot be controlled.

Screening may be conducted occasionally or regularly. As to individuals, personal data are usually obtained from the concerned person, who may or may not be aware that their data are being used for screening (Paragi 2023). Having logged into the online system, the user (authorized staff of a given aid organization) may also record identifiers (personal data: name, date of birth, etc.) in a field and select the type of entity (individual, organization) and categories (of watch lists). The result of the submitted search is a value indicating probability that can be grouped roughly into three main sets: negative (in most cases), positive (an alert with X probability), or false positive (it is also an alert).

As the alert always depends on the setting, it is a matter of organizational discretion which of the above-listed categories (which types of data) and countries are included in the FULL file or associated files. In principle, the user can exclude a country if it distrusts its sanctions lists. For example, the names of the listed Palestinian organizations mentioned in the Introduction will come up as an alert (positive hit) if the competent NGO staff member searches against their names either in the SANCTIONS list or in the ADVERSE MEDIA category (Workshop, September 23, 2022). However, the alert also depends on the settings and the extent to which the NGO can select which lists to search against. Taking our example, the Israeli list can be excluded; certain lists (Russian, Chinese) are indeed excluded in many cases (Workshop, September 23, 2022).

The absence of a positive (or false positive) match indicates that the given person, identified by their personal data, is not listed as a sanctioned individual, a terrorist or a PEP. Even in this case, the NGO may be interested in documenting the absence of persons from the lists by keeping some of their personal data. In case of alerts, however, the aid organizations need to consider if the result is real or a false positive hit and make decisions (on exclusion, not engaging in a contract, etc.) and proper documenting accordingly. The internal policies and procedures of the NGO and its organizational profile (humanitarian vs. development) will always determine what it does about an alert and how it processes the results.

While a narrow set of personal data (name, place, and date of birth) is needed for conducting screenings, the outcome of screening, presented in the form of a file in case of (false) positive matches, contains a far more detailed set of information that can be related to the person (Interview 13, Zoom interview with a representative of LexisNexis, May 20, 2021). In case of a (false) positive hit, the outcome is in the form of an integrated (pro)file (html, pdf). In such cases, the following information can also be used to identify the concerned persons: (a) a detailed set of personal data, photo included; (b) a narrative description containing references to the sources of each piece of information; (c) a section on the reported addresses; and (d) a network of relationships indicating the type of relations: family members, associated others, related companies, and organizations.[18] This outcome file also contains sensitive information (as defined in GDPR 2016: Article 9). These information types can be considered personal data following the EU GDPR (2016) and relevant interpretations by the Court of Justice of the EU (Bygrave and Tosoni 2020: 109–110; Paragi 2023).

Considering the scope of the problem, many organisations purposely overapply donor compliance requirements and screen all individuals (potential employees, contractors, suppliers and partners, beneficiaries, etc.) (Workshop, September 23, 2022) rather than just those who pass a certain spending threshold in an effort to ensure they do not omit an entity from the process inadvertently (Norwegian Refugee Council 2018a: 24). For example, the Norwegian Refugee Council conducted 7,053 searches screening partner staff, suppliers, and employees just in the Middle East in 2018 (Charny 2019).

[18] Furthermore, there is also an extensive list of sources, websites, and documents that were used by LexisNexis researchers to draw the profile (Interview 13, Zoom interview with a representative of LexisNexis, May 20, 2021; Interview 8, Teams interview with an advisor working at a Norwegian NGO, May 4 and June 20, 2021; documents provided via email correspondence by Compliance Partner, March 20–27, 20YY).

Furthermore, in addition to disclosing data to vendors, aid organizations in certain cases might also share them with other third parties, such as financial service providers (FSP) that facilitate the implementation of cash and voucher assistance (CVA) projects, for example, by issuing debit cards to beneficiaries in cooperation with INGOs. These FSPs usually receive lists of names from the INGOs and might conduct screenings—by considering the individuals as clients and not humanitarian beneficiaries (Workshop, September 23, 2022).

Knowledgeability and Reasonable Expectations

A further component needed for conceptualizing screening as surveillance is *knowledgeability* and "willing participation on the part of those whose life details are under scrutiny" (Lyon 2007: 27). Expectations and knowledge on screening—on its substance, purposes, legal basis, the involvement of third-party actors, and the consequences of decisions based on positive matches—not only determine how surveillance works but also affect human rights. With regard to the documentation requirements associated with funding agreements, record-keeping carries relevance because merely storing data relating to an individual's private life constitutes a data processing operation; as such, it is considered an interference with the right to respect for private life even without the subsequent use of stored data.[19]

Expectations are shaped by what individuals (are allowed to) know about the processing operations concerning their personal data. Recalling relevant provisions of the EU GDPR (2016: Article 5[1], Article 12, 13–14, and Recital 39), it should be transparent to natural persons that personal data concerning them are being collected, used, consulted, or otherwise processed and to what extent such personal data are or will be processed or, if applicable, further processed. The obligation of fairness, transparency, and lawfulness (GDPR 2016: Article 5[1]) is to be read in line with the interpretations of the European Court of Human Rights regarding the extent to which individuals' expectations or assumptions concerning the use and processing of their personal data are to be considered when decisions are made about the use of their data (Paragi 2023).

Humanitarian organizations consistently reject the idea of screening their beneficiaries, that is, vulnerable individuals receiving humanitarian aid on the grounds of international humanitarian law (IHL) (Gillard 2021b; Interview 8, Teams interview with an advisor working at a Norwegian NGO, June 14, 2021). If they consider themselves not well-positioned enough to negotiate the terms of the contract with a donor, the only solution is to refrain from submitting a proposal for a call. Such decisions, however, are rarely discussed with concerned individuals:

> We [as a humanitarian organization] try not to screen our beneficiaries, but we do not really consult this matter with them before making decisions.… [W]e say to our donors that screening [of beneficiaries in case of humanitarian projects] is an absolute red line, but we do not ask the local people about it. Maybe, they would not mind being screened if it was the price to be paid for the cash assistance or any other project that we, as an organization, reject for the sake of principled humanitarian action. (Interview 8b; interview with an advisor working at a regional office of a Norwegian NGO, November 3, 2021)

As noted elsewhere, the willingness to intervene in someone else's life without her/his consent is not only the hallmark of paternalism but also typical in humanitarian contexts (Barnett 2002: 35). However, while some Global South individuals may not mind being screened as a precondition for, or sharing personal data in exchange for, aid, others reject the idea of conditional funding—signing any contract with Northern donors, official aid agencies and NGOs included, with conditions—for cultural or political reasons. Recent Palestinian NGO objections formulated against EU conditions (restrictive measures, conditional clauses in grant agreements, screening and vetting) illustrate that the price of funding (being treated as a risk by

[19] *Amman v Switzerland,* appl. no. 27798/95 (ECtHR, February 16, 2000), para 69; *S and Marper v. The United Kingdom*, appl. no. 30562/04 and 30566/04 (ECtHR, December 4, 2008), para 67; *Kopp v Switzerland,* app no. 23224/94 (ECtHR, March 15, 1998), paras 51–53. The listed cases concerned data storage by public authorities.

default) can be considered too high by locals. EU conditions are deemed unfair and unacceptable because they are perceived as undermining the Palestinian right to self-determination and defending Israeli security interests (BADIL 2021).

Yet, surveillance—monitoring workers in a recruitment and employment context (Nouwt, de Vires, and Prins 2005) or consumers and clients in a commercial context (Zuboff 2019)—has been normalized worldwide (Ball, Haggerty, and Lyon 2012). Being surveilled by the police or secret service may also be considered "normal" even when someone has not committed a crime in such non-democratic settings where aid projects are usually implemented. And even if data extraction, techno-colonialism (Madianou 2019), and surveillance funded by aid or implemented in cooperation with aid organizations are known in academic and practitioner circles, screening by aid organizations is neither intuitive nor well known.

Knowledge and expectations depend on the context. Aid organizations (are allowed to) operate in the Global South on the premise that they provide morally and ethically defendable support to individuals or communities (Chatterjee 2004). How individuals relate to an aid NGO is shaped by the local cultural and political setting; the aid NGO's mandate, core activities, and image as communicated on websites or in their interactions with locals, conveying solidarity and altruism; the relationship between resource-rich Northern INGOs and individuals (characterized by strong power imbalances); and other factors. Getting/giving help in the form of charity aid or hospitality is rarely considered pure altruism by beneficiaries and recipients (Mauss 2002; Pyyhtinen 2014; Chatty 2017). Reciprocity is both perceived and conceptualized as a constitutive part of contemporary aid relations in both development and humanitarian contexts (Hattori 2001; Fassin 2007; Furia 2015; Paragi 2017). Personal data are by no means the exception, not even in humanitarian contexts. As argued by Sandvik (2019), certain digital humanitarian services and goods represent a new form of "gifting" from beneficiaries to humanitarian actors and their partners whereby the real (return) gift is the beneficiary data. Therefore, what individuals as data subjects (are allowed to) know about the purposes of and ways in which their personal data are used shape their expectations.

As aid images are conceptually far from surveillance imaginaries, it is unlikely that individuals would reasonably assume that aid organizations "assess" individuals not only by considering their needs or (in employment or supplier contracts) merits, vulnerability, and resilience capacities but also by checking their personal data against a database to see if they are reliable or risky. The use of third-party service providers for screening or sharing personal data of beneficiaries with FSPs that may screen them before they provide CVA should also be considered as an activity *beyond* the reasonable expectation of the data subjects.

To sum up, expectations with regard to mass screening conducted by aid organizations in any context likely do not exist. It is not intuitive that personal data are systematically and routinely checked against various watch lists by actors who are otherwise interested in providing a living in the form of employment, supplier contract, cash assistance, in-kind aid, or access to an event. However, "operations done with personal data [of Global South individuals too, by EU/EEA-registered INGOs]… [should be] within the reasonable expectations of the data subject" (summary of case law by de Terwangne 2018: 313), precisely because of the power imbalances between the controller (watcher) and the data subject (watched). Imbalances can be mitigated only if adequate information is provided in an adequate manner. Somewhat ironically, an individual can conceptualize themself as a risk that threatens the aid organization only if the person is notified about being screened.

The Art of Screening in the Context of North–South Power Relations

How INGOs navigate between their mandate, regulations concerning counterterrorism, and data protection is a developing issue. Compliance with AML/CFT laws and their perceived incompatibility with humanitarian principles has received far more attention than compliance with any data protection law. Participation in CFT activities has been a matter of discussion within the NGO sector since UN and US regulations were implemented after 9/11 (Hayes 2012, 2017; Norwegian Refugee Council 2018a, 2018b, 2018c, 2020; VOICE 2021) and due to the legal and ethical dilemmas surrounding the global sanctions regime in the context of human rights (Tzanou 2017) and humanitarian law (Gillard 2021a, 2021b). Yet, aid

organizations as beneficiaries or coordinators of aid projects are interested in demonstrating compliance to prevent exclusion from future tenders.

Although neither screening nor subscription to screening tools is prescribed by legal instruments, such as funding agreements, if screening is conceptualized as a data processing operation, the EU GDPR (2016) applies—at least in the case of those NGOs that are registered in an EU/EEA member state. Acknowledging that compliance with the GDPR is challenging (VOICE 2021: 3; Paragi 2023), EU/EEA-based NGOs as data controllers are required to provide information to individuals to meet the transparency obligation enshrined in Article 5(1) and Article 12 of the EU GDPR (2016) unless restrictions or exemptions apply.

Considering the mass amount of personal data collected by aid-implementing aid NGOs,[20] the data subjects' rights enshrined in the EU GDPR (2016) (Article 13–14, Article 15), and aid NGOs involvement in counterterrorism and related activities (Hayes 2012, 2017; Gillard 2021a, 2021b), privacy notices posted on NGO websites were analysed to see if they contain any direct or indirect reference to screening as a data processing operation. Findings indicate that the sampled NGOs almost never communicate the practice of screening to data subjects. Among the EU/EEA-based NGOs whose publicly available privacy notices were analysed for their content, only four privacy notices can be mentioned as rare exceptions (Paragi 2023).

While the information on screening as data processing may be missing from the privacy notices because the aid organizations in the sample simply do not collect personal data or do not screen individuals, it is highly unlikely in the light of earlier reports (Hayes 2017: 28; Norwegian Refugee Council 2018a: 23-25; VOICE 2021: 13; Gillard 2021a: 46–49, 2021b); responses given to my online survey also confirmed that screening is an existing practice. In-house opacity, however, became clear only during the qualitative interviews. As a legal advisor at a Norwegian NGO explained, the matter of screening is a delicate issue:

> We usually ask for personal data before a contract is signed or when an event is organized. As part of the preparation, we check if an individual is listed by using [OMITTED]. While we do such checks continuously, by verifying the identity and background of hundreds of people annually, the likelihood of a true positive hit is very low. As the risk of exclusion [from humanitarian aid] is very low, we do not provide much information on details [unless people ask about the screening clause in employment contracts, for example]. (Interview 8, Zoom interview with an advisor working at a Norwegian NGO, May 4 and June 14, 2021).

The reasons are complex, but communicating privacy and data protection matters in a GDPR-friendly manner poses a huge challenge to organizations: "It is kind of "unexplainable" [using clear and plain language] to an ordinary mother in Mozambique why or how the personal data of her daughter is collected and how it is processed or protected for the imbalance in power and knowledge between the data subject and us" (Interview 9, Teams interview with advisors working at the UK branch of an international NGO, June 17, 2021).

In addition to the problem of digital illiteracy perceived by aid organizations, lack of human capacity may also explain why screening is under-communicated to individuals in the Global South in detail (Interview 8, Teams Interview with an advisor working at a Norwegian NGO, June 14, 2021). Recalling the interviews and related observations, only one or two legal advisors or compliance officers are involved in the periodic screening of thousands of individuals, a procedure that is not necessarily known in-house either. While larger INGOs have drafted standard internal procedures for screening criteria in line with FATF recommendations, these documents are usually unavailable to the wider public.

[20] "Data protection is a huge problem within the industry for various reasons. It is common that things are not explained [to data subjects]. The industry is digitally illiterate, while we collect a lot of information, we do not understand the complexity of gathering data and the legal side of data collection" (Interview 1, Zoom interview with an advisor working at a Norwegian NGO, December 17, 2020).

In the absence of information disclosed on screening in publicly available privacy notices, most individuals, regardless of their place of residence, are familiar neither with the existence of sanctions lists nor with the fact that INGOs follow internal procedures to screen them. Furthermore, aid organizations usually fail to notify the data subjects about the implicit outsourcing of screening that is typical in CVA projects when INGOs cooperate with FSPs (Workshop, September 23, 2022), even if it is recommended by the International Federation of Red Cross and Red Crescent Societies in their guidance addressed to cash practitioners.[21]

Nevertheless, as surveillance in employment contexts is much better scrutinized and regulated in the context of privacy and data protection laws (Nouwt, de Vires, and Prins 2005) than in case of individuals living in experimental Global South settings (Sandvik, Jacobsen, and McDonald 2017), labour contracts usually contain a clause on screening. Consequently, those who have a contractual relationship (as employee or supplier) or are in charge of money transfers over internationally set standards[22] are notified about screenings when they sign the contract. However, even when information is provided on screenings (in the form of a contract), verbal explanation is usually offered only in generic terms (Paragi 2023).

Regardless of the transparency obligation of the GDPR, it was consistent across the interviews and the workshop that aid organizations have a well-founded, seemingly "legitimate" interest *not to disclose* the fact of screening. While reasons for missing transparency would require further research, opacity may be explained by the fact that INGOs cannot easily navigate between their mandate/image and the legal requirements of the controversial mission of AML/CFT. Although the technical side of screening is less artistic, navigating among donors (providing funding and expecting AML/CFT compliance), authoritarian regimes (being interested in knowing the local transaction partners, beneficiaries of Northern NGOs), other organizational interests (preventing reputational risk), the reasonable expectations of individuals (benefiting from jobs with aid organizations or from aid projects), and data protection laws (prescribing the transparency obligation) requires creativity from INGOs. Considering the power imbalances embedded in aid relations, both the acknowledgement and denial of screening might reinforce local perceptions that INGOs are foreign agents.

Discussion: Screening as Surveillance

Focusing on practices of collecting or extracting (personal, group) data for humanitarian or development purposes, an emerging scholarship deals with the instrumentalization of technology; the increased involvement of private actors in aid work through potential harms of digitalization and datafication on vulnerable people (Duffield 2016; Harris 2016; Sandvik, Jacobsen, and McDonald 2017; Madianou 2019; Lemberg-Pedersen and Haioty 2020); and the conceptualization of digital technologies as tools for biopolitics, the purpose of which is to discipline populations and control their movement. For example, digital (legal) identity management systems (Martin and Taylor 2021) and the related "financial inclusion" of the world's "unbanked populations" (Gabor and Brooks 2017) are not only about providing more freedom of consumer choice but also entail tighter-than-ever control over vulnerable people.

"Aidwashing" aside (Martin 2023), *surveillance* in the context of aid work has mostly been interpreted as being in a dialectical relationship with *recognition*, where the latter (providing increasingly digitalized *care* to people) is inherently linked with the former (exercising *control* over data describing identities, traits,

[21] "Inform beneficiaries and explain the KYC requirements or at minimum include these requirements in the privacy notice that could be consulted at any time" (IFRC 2021: 24).

[22] For example, following the Financial Action Task Force (2016: 12) recommendations, actors (addressing banks and FSPs) engaged in money transfers are required to implement preventive measures "before they (i) establish business relations; (ii) in case of those carrying out occasional transactions above the applicable designated threshold (USD/EUR 15 000)…; or (iii) there is a suspicion of money laundering or terrorist financing."

needs, movements of people, and humanitarian goods) (Jacobsen 2015; Fast and Jacobsen 2019; Weitzberg et al. 2021; Paragi and Altamimi 2022).

However, as findings indicate, screening can also be interpreted as surveillance, following Lyon (2007: 26–27), given the extent to which surveillance involves the process of screening, namely, identifying individuals that meet the criteria of various lists. Surveillance by NGOs is directed at determining if (changing) risk factors are emerging that may impact their operation or work environment, reputation or credibility, and legal-regulatory compliance. During this process, large, resource-rich aid NGOs resort to screening identify individuals deemed or designated "dangerous" by those official entities making the original lists and by service providers consolidating the hundreds of lists in integrated databases.

Screening is standardized and reasoned by legal-regulatory compliance or organizational interests and is organized by the use of tech tools. Its purpose is to categorize people according to the risk they may pose to the aid organization, that is, to sort out—exclude—potentially risky individuals from any transaction while as little information as possible is provided on screening in line with surveillance logics. Recalling that the involvement of third parties (vendors providing access to consolidated databases) has been critically discussed in the context of financial surveillance (Amicelle and Favarel-Garrigues 2012), similarities are detectable and include both internal weaknesses (the quality of data) and the external dimension of screening (how it is regulated and prescribed).

When NGOs do screenings, their advisors or compliance officers make decisions based on information available in consolidated databases. Even if they can exclude certain lists through settings, individual donors, would-be suppliers, participants of events, and beneficiaries—just like listed individuals, terrorists, and leaders of violent conflicts—are represented by, if not reduced to, their personal data. Considering that decisions depend on the "quality" or "content" of the personal data, the content of consolidated databases is decisive. While official sanctions lists (available on governmental websites) are identical to sanctions lists provided in the consolidated databases (errors included), the latter also contain alternative watch lists (PEP; ADVERSE MEDIA), the content of which is the result of institutionalized or professionalized social surveillance by vendors' research teams. Social surveillance originally referred to "an ongoing inquiry that constitutes information gathering by people about their peers, made salient by the social digitization normalized by social media… encompass[ing] using social media sites to broadcast information, survey[ing] content created by others, and regulating one's own content based on perceptions of the audience" (Marwick 2012: 397). In the case of consolidated watchlists, this content is edited by the research teams managing the screening databases based on news articles and media appearances available online (De Goede and Sullivan 2016: 77). Making decisions based on this content has created complications for compliance officers at banks (Amicelle and Favarel-Garrigues 2012: 112). Legal advisors and compliance officers at INGOs face similar dilemmas.

The fact that (knowing) data (the digital double) is increasingly considered more important than (knowing the) real person (customer, client) in contemporary fin-tech and reg-tec (Arner, Barberis, and Buckley 2016) also seems relevant in the case of NGOs. Errors are bound to occur because personal data are by no means identical to the person themself and such lists do not necessarily offer comprehensive knowledge on the context (in the case of five million profiles, the probability of error is high). Yet an individual's trajectory and profile, if interpreted against a given social-political context, might lead to understandings and decisions alternative to what is supported by (false) alerts.

Acknowledging that little is known about how international aid organizations make decisions internally (whom to screen, against which watch lists exactly, when and how often), the securitization argument deserves further research to understand how hierarchies and power imbalances—between aid organizations and individuals, between the Global North and Global South—are strengthened by screenings. While dilemmas stemming from screening as a normalized securitized activity are acknowledged by practitioners (Norwegian Refugee Council 2018a; VOICE 2021), the problem is usually framed in the context of

international humanitarian law (IHL). Preventing beneficiary exclusion (Gillard 2021a, 2021b), however, is only part of the problem.

Due to the financial risks (potential loss of funding), screening by international organizations, the civil sector included, is self-regulated at least as much as KYC procedures of financial institutions were ten years ago (Amicelle 2011). Indirect—hidden or covert—interventionism "does not impose rigid measures but promotes techniques of self-regulation that provide autonomy while simultaneously delegating responsibility and 'risks' in relation to the translation and implementation of abstract rules" in the financial sector (Amicelle 2011: 166). Self-regulation, however, also represents a particular kind of interventionism (by states, IOs) in which key concepts are autonomy and responsibility (Amicelle 2011: 166). Compliance is self-regulated and self-enforced in humanitarian (and, to some extent, development) spaces too.

Firstly, aid organizations voluntarily subscribe to commercially available solutions to demonstrate "reasonable efforts." Secondly, just as compliance officers working in banks distinguish "between at-risk sectors of activity [and] the geographical zones which they believe are particularly exposed to money-laundering practices" (Amicelle and Favarel-Garrigues 2012: 113), legal advisors at international and national NGOs include or exclude individuals on one hand and watch lists on the other hand in line with their own values and organizational norms. The burden of responsibility explains perceptions (Workshop, September 23, 2022), such as that they are expected to do the "dirty work" while donors "are 'put at ease' by [INGOs'] use of screening procedures (and software)" (VOICE 2021: 13). These non-profit perceptions resonate to some extent with the perceptions of lawyers who also experience AML/CFT regulation as invasive and hegemonic with regard to certain norms guiding their relations with their clients, such as confidentiality and professional secrecy. However, while such actors may resist being proactive in relation to security threats in spite of delegated powers and obligations (Helgesson and Mörth 2019), further research would be needed to explore the manoeuvring room of NGO advisors vis-à-vis authorities.

While screening is deemed to be in conflict with humanitarian principles, ineffective considering the low rate of true positive matches, and entailing too high subscription fees and reputational risks (VOICE 2021: 12–14; Newhouse 2021), perceived inconveniences are likely to be outweighed by the benefits. Given the extent to which the number of INGOs cooperating with service providers is increasing (Gillard 2021b), the sector is contributing to the normalization of risk-based thinking and regulation. It does so either by accepting regulatory arguments that security threats (e.g., terrorism) can be prevented by reasonable measures, or by responding to organizational experiences gathered in the Global South (Duroch and Neuman 2021; Akal 2022).

Donor conditionality (mitigating risks by demanding the implementation of reasonable measures) combined with self-regulated screening by international INGOs contributes to social and political control in global terms, which has long been a concern for critical IR and security studies. While screening may increase "public and governmental confidence" by ensuring compliance with norms and rules set by donors, it can also "exert coercive and normative pressures" by regulating, that is, constraining NGO behaviour (Hayes 2012) and securitizing and politicizing their role (see also Watson and Burles 2018). Following Madianou (2019), it may also make INGOs complicit in maintaining a techno-colonial order that benefits already privileged segments of the population. If actors considered "violent, corrupt, and criminal are neutralized" or removed (Duffield 2001: 132) in line with donor expectations of INGOs' reasonable efforts, screening can contribute to implementing or resuming "normal" aid-financed activities serving the interests of privileged populations. Screening as surveillance can also be considered a tool of biopolitics that facilitates legibility (Scott 1998) and governmentability similarly to other contemporary digital technologies, such as digital ID systems (Martin and Taylor 2021) or solutions mapping people's needs by extracting their data (Madianou 2019).

While screening is far from "normal" from the perspective of the watched, and even if humanitarian NGOs are critical of donors' expectation of their participation in AML/CFT, their compliance teams systematically gather information not only about designated persons but also about individuals that may be a potential risk

in the civil sector (sexual offenders, for example). As indicated by the discussion with practitioners, individuals may be screened against law enforcement lists by some NGOs but not by others. While there are usually no (donor) contractual obligations to do it, donors may require NGOs not employ people who have committed fraud or were involved in human trafficking, which is a criminal offence, not a terrorist crime. Screening in such cases is for due diligence and "it is the NGO's legitimate interest to know if a (would-be) supplier committed a criminal offence or did not paid tax" (Workshop, September 23, 2022).

Considering that the narrative of counterterrorism and even legal instruments are used to marginalize political opposition, journalists, civil society leaders, activists, or anyone critical of state policies (Hayes 2017; HRC 2019; Amnesty International 2020), the question emerges of whether screening can be considered not only a surveillance (ensuring legal-regulatory compliance) but also a *countersurveillance* measure (Monahan 2006), providing access to information precious to international or national NGOs under control and surveillance. The answer likely depends on what kind of information aid NGOs access, what they do with the data gathered (beyond documenting what is required in line with funding agreements), how they share it with authorities, if at all, and under what conditions. While further research would be needed to answer these questions, it is highly likely that some aid NGOs are simultaneously engaged in humanitarian and human rights surveillance (Topak 2019).

While beneficiary exclusion (as a result of screening) is a bigger concern for HOs than for development NGOs (Malakoutikhah 2020; Gillard 2021a, 2021b), no aid project is implemented in an apolitical context. The real harms can be understood by recalling the mainstream "Third World" critique of international law (Mutua 2000) and Ariella A. Azoulay's (2017) provocative argument for illustration. The idea and enforcement of universal human rights are usually promoted for securing international peace and stability by the UN, funded by OECD Development Assistance Committee members as main donors, and implemented mostly by Northern aid organizations. Yet this noble aim can also be read as an opportunity for "imperial powers to bestow upon themselves a general amnesty without having to pay for the crimes committed and rights violated during centuries of human trafficking, genocide, forced displacement" (Azoulay 2017: 467). Such critique is relevant in the case of screening given the extent to which entities and individuals in the Global South are routinely securitized in the name of (inter)national security by privileged states and actors under their legal-regulatory power. And while compliance is performed by law-abiding NGOs registered in the Global North, affected populations in the Global South have not been provided the opportunity to shape AML/CFT norms, rules, and laws, such as IHL and IHRL, data protection regulations included, on equal terms.

Conclusion

Screening as a form of surveillance is about sorting out those who might pose a risk before a contract is signed and for as long as the legal relationship lasts. Screening against sanctions, terrorist, and enforcement lists is considered necessary because of the high prevalence of financially suspicious transactions that may lead to terrorism financing or financial crimes. It may be conducted by following legal obligations prescribed by law, funding agreements, or alternative organizational interests. While the findings section of this article summarized the practices and the realities of screening by NGOs, the discussion focused more on the underlying effects of screening in the context of North–South relations.

The article contributed to earlier research not only on aid NGOs' controversial involvement in securitization agendas (Duffield 2001, 2007; Howell and Lind 2009; Howell 2014; Lazell and Petrikova 2020; Pallister-Wilkins 2021) and participation in financial humanitarianism (Tazzioli 2019; Lemberg-Pedersen and Haioty 2020) by expanding the meaning of surveillance in the context of aid work (Weitzberg et al. 2021; Martin 2023) but also to research on the complexity of NGO accountability (Jordan and Van Tuijl 2006).

INGOs do not want to be accused of contributing to conflict by channelling money to "risky" individuals that may be associated with terrorist organizations. Therefore, individuals (job applicants, employees, suppliers, beneficiaries of development projects, etc.) are treated with "categorical suspicion" by INGOs.

Being screened only once or regularly, certain people are categorized "suspicious" and "hardly innocent until proven guilty" (following Marx 1988: 227) or as a financial-regulatory risk by default. It implies that the right to be recognized, supported, assisted, and employed—either in a humanitarian or a development context—depends on how INGOs categorize and classify individuals *before screening* and how they make decisions *after* it, based on the results of screening. Both would require further research.

As demonstrated by the findings, European aid NGOs equally seem to "overapply" legal and donor requirements in the context of AML/CFT compliance and under-communicate screening both in-house and publicly. The risk-based approach characterizing financial surveillance is particularly problematic in the case of HOs as performing humanitarian principles "contributes to organizational security by alleviating two common reasons for security incidents: mistaken identity and misperceptions regarding the roles and motivations" of HOs (Vaughn 2009: 269). However, "if aid actors cannot be distinguished from political and military [security or counterterrorism] actors, the claim that HOs merit special treatment disintegrates (Vaughn 2009: 270).

Access to information (by screening) may equally mean opportunities and risks as long as European NGOs may also be required, expected, or coerced to share this data (or lists) with third parties, with the latter meaning US governmental agencies or authoritarian governments in the Global South. As implied, screening and its communication are delicate issues not only for the reasonable expectations and human rights of data subjects but also because they further politicize (humanitarian) assistance. This likely explains why this practice is rarely discussed with or disclosed to concerned individuals. However, "screening in secret"—if no or very little information is shared with the data subjects—is at odds with the fairness and transparency principles guiding most data protection laws (Paragi 2023). By not providing (general, but clear) information on their efforts and measures to individuals that are considered risky by default (Paragi 2023), aid organizations obviously control the discursive space. By doing so, they further strengthen fixed hierarchies of generosity and gratitude between the watchers and the watched by screening. The "watched," playing the role of the grateful, are not well positioned to ask questions and hold aid organizations accountable. If they do, they bite the helping hand.

While further research would be needed to map the reasons for the lack of transparency, certain limits of the methods used in this study should be acknowledged. Interviews and discussions provide valuable but limited access to information considering the fact that neither vendors within the surveillance industry (Lauterbach 2017) nor legal advisors, DPOs, or compliance officers working at NGOs are interested in or authorized to disclose details of internal decisions for independent academic research. Confidentiality among business partners, reputational hazards, and loyalty between the employer and the employee are among the factors that prevent honest discussions outside the informal circles of practitioners and consultants.

Regardless of research methods, there is a certain irony in the fact that while most civil society organizations praise the values of transparency and privacy (protection) as opposed to surveillance practices (Lyon 2007: 169–171), considerable opacity prevails around screening (Paragi 2023). Conducting AML/CFT-related surveillance on one hand and delivering aid to the Global South on the other hand, represent distinct domains both in practice and in theory. While surveillance implies, if not permits, certain secrecy and opacity, at least in the case of governmental agencies working for public and national security, aid work is to be guided by principles such as transparency and accountability for the sake of aid effectiveness—regardless of the data protection dimension. Common to them, however, is the power imbalance between the watcher and the watched (in the case of surveillance) and between the aid organization and the beneficiaries at the receiving end of aid relations.

Acknowledgments

I owe thanks to practitioners that shared their experiences during the research as particpants of the interview and workshop, to researchers affiliated with NCHS and PRIO who not only facilitated but also encouraged professional

discussion on this topic, and to the anonymous reviewers and editors of *Surveillance & Society* whose kind and constructive feedback contributed to the development of this text. The responsibility for any mistake is mine.

References

Akal, Ayse Bala. 2022. Tacit Engagement as a Form of Remote Management: Risk Aversity in the Face of Sanctions Regimes. NCHS Paper. https://www.humanitarianstudies.no/resource/tacit-engagement-as-a-form-of-remote-management-risk-aversity-in-the-face-of-sanctions-regimes/ [accessed November 8, 2022].

Amicelle, Anthony. 2011. Towards a "New" Political Anatomy of Financial Surveillance. *Security Dialogue* 42 (2): 161–178.

Amicelle, Anthony, and Gilles Favarel-Garrigues. 2012. Financial Surveillance: Who Cares. *Journal of Cultural Economy* 5 (1): 105–124.

Amman v Switzerland. 2000. Appl. no. 27798/95 (ECtHR, February 16).

Amnesty International. 2020. *AI Report 2020/2021: The State of the World's Human Rights*. https://reliefweb.int/sites/reliefweb.int/files/resources/POL1032022021ENGLISH.PDF [accessed November 12, 2021].

Arner, Douglas W., Janos N. Barberis, and Ross P. Buckley. 2016. The Emergence of Regtech 2.0: From Know Your Customer to Know Your Data. *Journal of Financial Transformation* 44 (79): 17–63.

Azoulay, Ariella Aïsha. 2017. *Potential History: Unlearning Imperialism*. New York: Verso.

BADIL. 2021. European Union Conditional Funding: Its Illegality and Political Implications. Badil Position Paper. Bethlehem, IL: Badil. https://www.badil.org/cached_uploads/view/2021/04/20/europeanunionconditionalfunding-positionpaper-april2020-1618905422.pdf [accessed November 18, 2022].

Ball, Kirstie, Kevin D. Haggerty, and David Lyon, eds. 2012. *Routledge Handbook of Surveillance Studies*. London: Routledge.

Barnett, Michael. 2002. *Empire of Humanity. A History of Humanitarianism*. New York: Cornell University Press.

Bygrave, Lee A. 2014. Core Principles of Data Privacy Law. In *Data Privacy Law: An International Perspective*, 145–168. New York: Oxford University Press.

Bygrave, Lee A., and Luca Tosoni. 2020. Article 4(1). Personal data. In *The EU General Data Protection Regulation (GDPR): A Commentary*, edited by Christopher Kuner, Lee A. Bygrave, Christopher Docksey, and Laura Drechsler, 103–115. New York: Oxford University Press.

Charny, Joel R. 2019. Counter-Terrorism and Humanitarian Action: The Perils of Zero Tolerance. War on the Rocks, March 20. https://warontherocks.com/2019/03/counter-terrorism-and-humanitarian-action-the-perils-of-zero-tolerance/ [accessed April 8, 2022].

Chatterjee, Deen K. 2004. *The Ethics of Assistance*: *Morality and the Distant Needy*. Cambridge, UK: Cambridge University Press.

Chatty, Dawn. 2017. The Duty to Be Generous (Karam): Alternatives to Rights-Based Asylum in the Middle East. Lecture on Africa, Asia and the Middle East, 14 March 2017. *Journal of the British Academy* 5: 177–199.

CompliancePartner. 20yy. *Categories for* CP-WatchList-Tech. Email attachment sent to the author of this paper by CompliancePartner. March 27, 20YY.

De Goede, Marieke. 2012. *Speculative Security: The Politics of Pursuing Terrorist Monies*. Minneapolis, MN: University of Minnesota Press.

———. 2017. The Chain of Security. *Review of International Studies* 44 (1): 24–42.

De Goede, Marieke, and Gavin Sullivan. 2016. The Politics of Security Lists. *Environment and Planning D: Society and Space* 34 (1): 67–88.

de Terwangne, Cecilie. 2018. Principles (Articles 5–11) Article 5: Principles Relating to Processing of Personal Data. In *The EU General Data Protection Regulation (GDPR): A Commentary*, edited by Christopher Kuner, Lee A. Bygrave, Christopher Docksey, and Laura Drechsler, 309–320. New York: Oxford University Press.

Duffield, Mark. 2001. *Global Governance and the New Wars: The Merging of Development and Security*. London: Zed.

———. 2007. *Development, Security and Unending War: Governing the World of Peoples*. London: Polity Press.

———, Mark. 2016. The Resilience of the Ruins: Towards a Critique of Digital Humanitarianism. *Resilience* 4 (3): 147–165.

Duroch, Françoise, and Michaël Neuman. 2021. Should We Discriminate in Order to Act? Profiling: A Necessary but Debated Practice. HPN Paper. https://odihpn.org/publication/should-we-discriminate-in-order-to-act-profiling-a-necessary-but-debated-practice/ [accessed April 8, 2022].

Eckert, Sue E. 2022. Counterterrorism, Sanctions and Financial Access Challenges: Course Corrections to Safeguard Humanitarian Action. *International Review of the Red Cross* (No. 916–917): https://international-review.icrc.org/articles/counterterrorism-sanctions-and-financial-access-challenges-916#footnote81_27rk033.

European Union. 2005. Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0060 [accessed April 8, 2023].

———. 2020. ANNEX II. General Conditions Applicable to EU-Financed Grant Contracts for External Actions. Version: August 2020, 3h2_gencond_en. https://ec.europa.eu/europeaid/prag/document.do?nodeNumber=1 [accessed March 28, 2022].

———. 2021. *Ethics in Social Science and Humanities*. European Commission. https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-in-social-science-and-humanities_he_en.pdf [accessed October 12, 2021].

EU GDPR (European Union General Data Protection Regulation). 2016. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data. https://eur-lex.europa.eu/eli/reg/2016/679/oj [accessed April 8, 2022].

Fassin, Didier. 2007. Humanitarianism as a Politics of Life. *Public Culture* 19 (3): 499–520.
Fast, Larissa, and Katja L. Jacobsen. 2019. Rethinking Access: How Humanitarian Technology Blurs Control and Care. *Disasters* 43 (S2): S151–S168.
Financial Action Task Force. N.d. The FATF. https://www.fatf-gafi.org/en/the-fatf.html [accessed May 12, 2022].
———. 2001. Special Recommendation VIII (SR VIII) – Recommendation 8 (Measures to Prevent the Misuse of Non-profit Organisations). https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/BPP-combating-abuse-non-profit-organisations.pdf.
———. 2014. Risk of Terrorist Abuse in Non-Profit Organisations. https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-of-terrorist-abuse-in-non-profit-organisations.pdf [accessed November 18, 2022].
———. 2015. Best Practices Paper on Combating the Abuse of NonProfit Organisations: Recommendation 8. https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Bpp-combating-abuse-npo.html [accessed April 8, 2022].
———. 2016. Guidance for a Risk-Based Approach: Money or Value Transfer Services. Paris: FATF. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-money-or-value-transfer.html [accessed October 8, 2022].
_____ 2023. Public Consultation on the FATF Best Practice Paper to Combat the Abuse of Non Profit Organisations. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/FATF-BPP-Combat-Abuse-NPOs-Public-Consultation.html [accessed May 3, 2024].
Franz, Vera, Lucy Hannah, and Ben Hayes. 2020. *Civil Society Organizations and General Data Protection Regulation Compliance: Challenges, Opportunities, and Best Practice*. Brussels: Open Society Foundation. Available at: *civil-society-organizations-and-gdpr-compliance-20200210.pdf (reliefweb.int) [accessed December 8, 2021].
Furia, Annalisa. 2015. *The Foreign Aid Regime: Gift-Giving, States and Global Dis/Order*. London: Palgrave.
Gabor, Daniela, and Sally Brooks. 2017. The Digital Revolution in Financial Inclusion: International Development in the Fintech Era. *New Political Economy* 22 (4): 423–436.
Gazi, Teodora. 2020. Data to the Rescue: How Humanitarian Aid INGOs Should Collect Information Based on the GDPR. *Journal of International Humanitarian Action* 5: https://doi.org/10.1186/s41018-020-00078-0.
Gillard, Emanuela-Chiara. 2021a. IHL and the Humanitarian Impact of Counterterrorism Measures and Sanctions: Unintended Ill Effects of Well-Intended Measures. Chatham House Research Paper. https://www.chathamhouse.org/sites/default/files/2021-09/2021-09-03-ihl-impact-counterterrorism-measures-gillard_0.pdf [accessed June 8, 2022].
———. 2021b. Screening of Final Beneficiaries – a Red Line in Humanitarian Operations. An Emerging Concern in Development Work. *International Review of the Red Cross* 103 (916–917): 517–537.
Gilligan, George. 2009. PEEPing at PEPs. *Journal of Financial Crime* 16 (2): 137–143.
Goold, Benjamin J., and Daniel Neyland. 2009. *New Directions in Surveillance and Privacy*. Portland, OR: Willan.
Haggerty, Kevin. 2009. Methodology as a Knife Fight: The Process, Politics and Paradox of Evaluating Surveillance. *Critical Criminology* 17: 277–291.
Hanley-Giersch, Jennifer. 2019. RegTech and Financial Crime Prevention. In *The REGTECH Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries in Regulation*, edited by Douglas W. Arner, Janos N. Barberis, and Ross P. Buckley. 20–26. New York: Wiley and Sons.
Harris, Roger W. 2016. How ICT4D Research Fails the Poor. *Information Technology for Development* 22 (1): 177–192.
Hattori, Tomohisa. 2001. Reconceptualizing Foreign Aid. *Review of International Political Economy* 8 (4): 633–660.
Hayes, Ben. 2012. Counter-Terrorism, "Policy Laundering," and the FATF: Legalizing Surveillance, Regulating Civil Society. *The International Journal of Not-for-Profit Law* 14 (1–2): https://www.icnl.org/resources/research/ijnl/1-introduction-2.
———. 2017. *The Impact of International Counter-Terrorism on Civil Society Organisations: Understanding the Role of the Financial Action Task Force*. Berlin, DE: Bread for the World.
Helgesson, Karin Svedberg, and Ulrika Mörth. 2019. Instruments of Securitization and Resisting Subjects: For-Profit Professionals in the Finance–Security Nexus. *Security Dialogue* 50 (3): 257–274.
Hosein, Gus, and Carly Nyst. 2013. Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives Are Enabling Surveillance in Developing Countries. SSRN, September 16. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2326229 [accessed March 8, 2023].
Howell, Jude. 2014. The Securitisation of INGOs Post-9/11. *Conflict, Security and Development* 14 (2): 151–179.
Howell, Jude, and Jeremy Lind. 2009. *Counter-Terrorism, Aid and Civil Society: Before and After the War on Terro*r. Basingstoke, UK: Palgrave Macmillan.
Human Rights Council. 2019. Impact of Measures to Address Terrorism and Violent Extremism on Civic Space and the Rights of Civil Society Actors and Human Rights Defenders. Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism. A/HRC/40/52, March 1.
IFRC. 2021. Practical Guidance for Data Protection in Cash and Voucher Assistance. https://www.ifrc.org/document/practical-guidance-data-protection-cash-and-voucher-assistance [January 18, 2023].
International Review of the Red Cross. 2022. Counterterrorism, Sanctions and War: A Collection of 32 Articles. International Review of the Red Cross 916–917: https://international-review.icrc.org/reviews/irrc-no-916-917-counterterrorism-sanctions-and-war.
Jackson, Paul, ed. 2015. *Handbook of International Security and Development*. New York: Routledge.
Jacobsen, Katja L. 2022. Biometric Data Flows and Unintended Consequences of Counterterrorism. *International Review of the Red Cross* 103 (916–917): 619–652.
———. 2015. *The Politics of Humanitarian Technology: Good Intentions, Unintended Consequences and Insecurity*. London: Routledge.
Jordan, Lisa, and Peter Van Tujil. 2006. *NGO Accountability. Politics, Principles and Innovations*. London: Earthscan.

Klareen, Jonathan. 2013. The Human Right to Information and Transparency. In *Transparency in International Law*, edited by Andrea Bianchi and Anne Peters, 223–238. Cambridge, UK: Cambridge University Press.
Kopp v Switzerland. 1998. App no. 23224/94 (ECtHR, March 15).
Lamarche, Karine. 2019. The Backlash against Israeli Human Rights INGOs: Grounds, Players and Implications. *International Journal of Politics, Culture and Society* 32 (3): 301–322.
Latoreno, Mark. 2019. Stop Surveillance Humanitarianism. *New York Times*, July 11. https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html [accessed November 18, 2023].
Lauterbach, Claire. 2017. No-Go Zones: Ethical Geographies of the Surveillance Industry. *Surveillance & Society* 15 (3–4): 557–566.
Lazell, Melita, and Ivica Petrikova. 2020. Is Development Aid Securitized? Evidence from a Cross-Country Examination of Aid Commitment. *Development Policy Review* 38 (3): 323–343.
Lemberg-Pedersen, Martin, and Eman Haioty. 2020. Re-assembling the Surveillable Refugee Body in the Era of Data-Craving. *Citizenship Studies* 24 (5): 607–624.
LexisNexis. 2021. LexisNexis® WorldCompliance™ Data. https://risk.lexisnexis.com/global/en/products/worldcompliance-data [accessed March 12, 2022].
Lyon, David. 2007. *Surveillance Studies: An Overview*. Cambridge, UK: Polity Press.
Madianou, Mirca. 2019. Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises. *Social Media + Society* 5 (3): 1–13.
Malakoutikhah, Zeynab. 2020. Financial Exclusion as a Consequence of Counter-Terrorism Financing. *Journal of Financial Crime* 27 (2): 663–682.
Martin, Aaron. 2023. Aidwashing Surveillance: Critiquing the Corporate Exploitation of Humanitarian Crises. *Surveillance & Society* 21 (1): 96–102.
Martin, Aaron, and Linnet Taylor. 2021. Exclusion and Inclusion in Identification: Regulation, Displacement and Data Justice. *Information Technology for Development* 27 (1): 50–66.
Marwick, Alice E. 2012. The Public Domain: Surveillance in Everyday Life. *Surveillance & Society* 9 (4): 378–393.
Marx, Gary T. 1988. *Undercover: Police Surveillance in America*. Berkley, CA: University of California Press.
———. 2005. Seeing Hazily, But Not Darkly, Through the Lens: Some Recent Empirical Studies of Surveillance Technologies. *Law and Social Inquiry* 30 (2): 339–399.
Mauss, Marcel. 2002. *The Gift: The Form and Reason for Exchange in Archaic Societies*. London: Routledge.
Minella, Carlotta M. 2019. Counter-Terrorism Resolutions and Listing of Terrorists and Their Organizations by the United Nations. In *International Human Rights and Counter-Terrorism*, edited by Eran Shor and Stephen Hoadley, 31–53. New York: Springer.
Monahan, Torin. 2006. Counter-Surveillance as Political Intervention? *Social Semiotics* 16 (4): 515–534.
Mutua, Makau W. 2000. What Is TWAIL? *Proceedings of the ASIL Annual Meeting* 94 (31): https://digitalcommons.law.buffalo.edu/journal_articles/560/ [accessed December 12, 2022].
Nagy, Veronika. 2017. How to Silence the Lambs? Constructing Authoritarian Governance in Post-Transitional Hungary. *Surveillance & Society* 15 (3–4): 447–455.
Newhouse, Nina. 2021. Screening Recipients of Humanitarian Cash and Voucher Assistance: Necessary Precaution or Wasted Resources? Calp Network (blog). https://www.calpnetwork.org/blog/screening-recipients-of-humanitarian-cash-and-voucher-assistance-necessary-precaution-or-wasted-resources/ [accessed April 8, 2022].
Nouwt, Sjaak, Berend R. de Vires, and Corien Prins, eds. 2005. *Reasonable Expectations of Privacy? Eleven Country Reports in Camera Surveillance and Workplace Privacy*. The Hague, NL: T. M. C. Asser.
Norwegian Refugee Council. 2018a. Principles under Pressure: The Impact of Counterterrorism Measures and Preventing/Countering Violent Extremism on Principled Humanitarian Action. https://reliefweb.int/sites/reliefweb.int/files/resources/nrc-principles_under_pressure-report-screen.pdf [accessed April 18, 2021].
———. 2018b. Understanding Conditional Clauses. https://www.nrc.no/shorthand/stories/understanding-counterterrorism-clauses/index.html [accessed June 18, 2022].
———. 2018c. Examples of Counterterrorism Clauses. https://www.nrc.no/globalassets/pdf/reports/toolkit/nrc_toolkit_02_examples-of-counterterrorism-clauses.pdf.
———. 2020. Toolkit for Principled Humanitarian Action: Managing Counterterrorism Risks. https://www.nrc.no/toolkit/principled-humanitarian-action-managing-counterterrorism-risks/ [accessed June 18, 2022].
Pallister-Wilkins, Polly. 2021. Saving the Souls of White Folk: Humanitarianism as White Supremacy. *Security Dialogue* 52 (1): 98–106.
Paragi, Beáta. 2017. Contemporary Gifts: Solidarity, Compassion, Equality, Sacrifice and Reciprocity From the Perspective of NGOs. *Current Anthropology* 58 (3): 317–339.
———. 2021. Digital4development? European Data Protection in the Global South. *Third World Quarterly* 42 (2): 254–273.
———. 2022. Challenges in Using Online Surveys for Research Involving Sensitive Topics: Data Protection Practices of European NGOs Operating in the Global South. *SAGE Research Methods Cases – Doing Research Online.* https://doi.org/10.4135/9781529604146.
———. 2023. Opacity or Transparency? Screening by NGOs in the Context of Aid Work. NCHS Paper, April 10. Oslo, NO: Norwegian Centre for Humanitarian Studies. https://www.humanitarianstudies.no/resource/opacity-or-transparency-screening-by-ngos-in-the-context-of-aid-work/ [accessed July 18, 2023].
Paragi, Beata, and Ahmad Altamimi. 2022. Caring Control or Controlling Care? Double Bind Facilitated by Biometrics between UNHCR and Syrian Refugees in Jordan. *Society and Economy* 44 (2): 206–231

Pyyhtinen, Olli. 2014. *The Gift and Its Paradoxes: Beyond Mauss*. London: Ashgate.
Qureshi, Sajda. 2019. Perspectives on Development: Why Does Studying Information and Communication Technology for Development (ICT4D) Matter*? Information Technology for Development* 25 (3): 381–389.
Rébé, Nathalie. 2020. *Counter-Terrorism Financing: International Best Practices and the Law*. Leiden, NL: Brill.
S and Marper v. The United Kingdom. 2008. Appl. no. 30562/04 and 30566/04 (ECtHR, December 4).
Sandvik, Kristin B. 2019. Making Wearables in Aid: Digital Bodies, Data and Gifts. *Journal of Humanitarian Affairs* 1 (3): 33–41.
———. 2020. Wearables for Something Good: Aid, Dataveillance and the Production of Children's Digital Bodies. *Information, Communication & Society* 23 (14): 2014–2029.
Sandvik, Kristin B., Katja L. Jacobsen, and Sean M. McDonald. 2017. Do Not Harm: A Taxonomy of the Challenges of Humanitarian Experimentation. *International Review of the Red Cross* 99 (1): 319–344.
Scott, James C. 1998. *Seeing Like a State. How Certain Schemes to Improve the Human Condition Have Failed.* London: Yale University Press.
Skinner-Thompson, Scott. 2022. Introduction: Privacy Studies, Surveillance Law. *Surveillance & Society* 20 (3): 294–296.
Sullivan, Gavin. 2020. *The Law of the List: UN Counterterrorism Sanctions and the Politics of Global Security Law*. Cambridge, UK: Cambridge University Press.
Tazzioli, Martina. 2019. Refugees' Debit Cards, Subjectivities, and Data Circuits: Financial-Humanitarianism in the Greek Migration Laboratory. *International Political Sociology* 13: 392–408.
Topak, Özgün E. 2019. Humanitarian and Human Rights Surveillance: The Challenge to Border Surveillance and Invisibility? *Surveillance & Society* 17 (3–4): 382–404.
Tzanou, Maria. 2017. *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*. Oxford, UK: Hart.
UNSC (United Nations Security Council). 2022. S*/RES/2664. Adopted by the Security Council at its 9214th meeting, on 9 December 2022*. http://unscr.com/en/resolutions/doc/2664 (accessed April 17, 2023).
Vaughn, Jocelyn. 2009. The Unlikely Securitizer: Humanitarian Organizations and the Securitization of Indistinctiveness. *Security Dialogue* 40 (3): 263–285.
VOICE. N.d.. Our Members. Voluntary Organisations in Cooperation in Emergencies, https://voiceeu.org/our-members [accessed October 13, 2021].
———. 2021. Adding to the Evidence: The Impact of Sanctions and Restrictive Measures on Humanitarian Action. Survey Report, March. https://voiceeu.org/search?q=adding+to+the+evidence [accessed October 8, 2021].
Vrabec, Helena U. 2021. The Right to Information. In *Data Subject Rights under the GDPR*, 64–103. Oxford, UK: Oxford University Press.
Walsham, Geoff. 2017. ICT4D Research: Reflections on History and Future Agenda. *Information Technology for Development* 23 (1): 18–41.
Watson, Scott, and Regan Burles. 2018. Regulating NGO Funding: Securitizing the Political. *International Relations* 32 *(*4): 430–448.
Weitzberg, Keren, Margie Cheesman, Aaron Martin, and Emrys Schoemaker. 2021. Between Surveillance and Recognition: Rethinking Digital Identity in Aid. *Big Data & Society* 8 (1): 1–8.
World Health Organization. 1968. Principles and Practice of Screening for Disease. https://apps.who.int/iris/handle/10665/37650 [accessed March 8, 2022].
Ziv, Oren, and Yuval Abraham. 2022. Israel's New Secret Document Still Fails to Tie Palestinian INGOs to "Terrorism." *+972Magazine*, January 13. https://www.972mag.com/israel-document-palestinian-ngos/ [accessed March 8, 2022].
Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism*. New York: PublicAffairs.