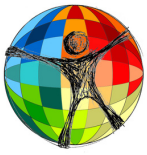
INTERNATIONAL HUMAN RIGHTS INTERNSHIP PROGRAM | WORKING PAPER SERIES

VOL. 11 | NO. 1 | SUMMER 2022

Refugees and the Digital Passage to Europe: Navigating the Right to Privacy within the EU Border Infrastructure

Angela Yang

McGill Centre for Human Rights and Legal Pluralism



Centre sur les droits de la personne et le pluralisme juridique de McGill

McGill FACULTY OF Law

ABOUT CHRLP

Established in September 2005, the Centre for Human Rights and Legal Pluralism (CHRLP) was formed to provide students, professors and the larger community with a locus of intellectual and physical resources for engaging critically with the ways in which law affects some of the most compelling social problems of our modern era, most notably human rights issues. Since then, the Centre has distinguished itself by its innovative legal and interdisciplinary approach, and its diverse and vibrant community of scholars, students and practitioners working at the intersection of human rights and legal pluralism.

CHRLP is a focal point for innovative legal and interdisciplinary research, dialogue and outreach on issues of human rights and legal pluralism. The Centre's mission is to provide students, professors and the wider community with a locus of intellectual and physical resources for engaging critically with how law impacts upon some of the compelling social problems of our modern era.

A key objective of the Centre is to deepen transdisciplinary collaboration on the complex social, ethical, political and philosophical dimensions of human rights. The current Centre initiative builds upon the human rights legacy and enormous scholarly engagement found in the Universal Declaration of Human Rights.

ABOUT THE SERIES

The Centre for Human Rights and Legal Pluralism (CHRLP) Working Paper Series enables the dissemination of papers by students who have participated in the Centre's International Human Rights Internship Program (IHRIP). Through the program, students complete placements with NGOs, government institutions, and tribunals where they gain practical work experience in human rights investigation, monitoring, and reporting. Students then write a research paper, supported by a peer review process, while participating in a seminar that critically engages with human rights discourses. In accordance with McGill University's Charter of Students' Rights, students in this course have the right to submit in English or in French any written work that is to be graded. Therefore, papers in this series may be published in either language.

The papers in this series are distributed free of charge and are available in PDF format on the CHRLP's website. Papers may be downloaded for personal use only. The opinions expressed in these papers remain solely those of the author(s). They should not be attributed to the CHRLP or McGill University. The papers in this series are intended to elicit feedback and to encourage debate on important public policy challenges. Copyright belongs to the author(s).

The WPS aims to meaningfully contribute to human rights discourses and encourage debate on important public policy challenges. To connect with the authors or to provide feedback, please contact human.rights@mcgill.ca.

ABSTRACT

Global spending on border management has grown exponentially and the primary focus of that spending has been on the establishment, extension, and enhancement of border management technologies. In the face of the ever-growing digital border infrastructure in different countries around the world, this paper explores the interplay between technology, refugees, and the digitized border through a human rights lens, filling in a particular gap in the literature. Taking the European border as my primary case study, I argue that there remains an unresolved tension between the right to privacy, which is a fundamental human right that in theory should extend to all, and the increasingly digitized border. All the while, refugees are acutely aware of the privacy implications throughout their journey, though their concerns are not necessarily always conceptualized as about "privacy." As a result, they are continuously engaged in processes of negotiation and contestation with the digital infrastructure in which they have no choice but to be embedded. By situating refugees' individual acts of micro-resistance along their journey in the broader digital infrastructure of the border, I aim to adopt Fischer and Jørgensen's mission to "speak back to system" and to make visible the structures of the border and of technologies.

CONTENTS

I. INTRODUCTION *6*

II. PRIVACY AS A HUMAN RIGHT *11*

III. THE REFUGEE PASSAGE AND THE SMARTPHONE *18*

IV. THE DIGITAL BORDER *26*

V. CONCLUSION *37*

BIBLIOGRAPHY *38*

I. Introduction

A. *The Landscape*

In migration research, most discussions begin with data. These are usually statistics regarding the number of people who were on the move for international protection, meant to illustrate what displacement looks like on the international stage. I, too, want to start with data. This year, President Biden requested increases in discretionary funding for the US' two main immigration enforcement agencies: $15.3 billion for Customs and Border Protection, an increase of 4% from its 2022 funding, and $8.1 billion in discretionary funds for Immigration and Customs Enforcement (ICE), an increase of 1% from its 2022 funding.[1] The budget of these two agencies "rivals total spending by some of the world's largest militaries."[2] According to the US Homeland Security Secretary, the budget is focused on making "smart investments in technology to keep our borders secure."[3] In Europe, as part of its 2021-27 Multi-annual Financial Framework which allocates European public money for security and defense purposes, the Integrated Border Management Fund will receive €6.2 billion, an increase of 131% from the previous budgetary cycle from 2014-2020.[4] Frontex, the European Union's (EU) Border and Coast Guard Agency, will receive €5.6 billion, an increase of 194%, representing an overall increase of 13,200%

[1] See Rafael Bernal & Rebecca Beitsch, "Biden budget accelerates shift from Trump policies on immigration", *The Hill* (28 March 2022), online: <thehill.com/latino/600074-biden-budget-accelerates-shift-from-trump-policies-on-immigration/>.

[2] Mizue Aizeki et al, "Smart Borders or A Humane World?" (October 2021) at 3, online: *Immigrant Defense Project's Surveillance, Tech & Immigration Policing Project, and the Transnational Institute* <tni.org/en/publication/smart-borders-or-a-humane-world>.

[3] Bernal & Beitsch, *supra* note 1.

[4] See Chris Jones, Jane Kilpatrick & Yasha Maccanico, "At what cost? Funding the EU's security, defence, and border policies, 2021–2027" (April 2022) at 3, online (pdf): *Statewatch and the Transnational Institute* <eubudgets.tni.org/wp-content/uploads/2022/05/At-what-cost-Statewatch-TNI.pdf>.

in less than 20 years.[5] Much of the funds allocated to border management will be dedicated to acquiring, maintaining, and training new technologies, which are central to achieving the aim of "ensur[ing] strong and effective European integrated border management at the external borders."[6] In Australia, its 2022-23 federal budget allocated $136.7 million to maintaining Operation Sovereign Borders, "the Australian government's multi-agency military-led 'border security operation,'"[7] an increase of 120% from its budget in 2018-19.[8] The activities that Operation Sovereign Borders engages in include maritime surveillance.

On the one hand, it is important to note that the overall number of people who are displaced each year, either across national borders or internally, continues to rise.[9] On the other hand, the aforementioned numbers perhaps tell an even more striking story about what mobility looks like today. Global spending on border management has grown exponentially and much of the funds are dedicated to extending and enhancing the use of technologies at the border. Rather than focus on the number of displaced people, these numbers present some small insight into how much countries around the world are investing to sustain an infrastructure of control, management, and outright deterrence.

In this paper, I explore that infrastructure and the refugee journey within, through, and against it. I add my voice to the expanding literature by bringing together discussions on the makeup of the modern border, intertwined with various forms of technology, and the literature on the now familiar phenomenon

---

[5] See *ibid* at 5.

[6] *Ibid* at 27.

[7] Claire Higgins, "Budget 2022: What it means for Australia's refugee system" (30 March 2022), online: *Kaldor Centre* <kaldorcentre.unsw.edu.au/news/budget-2022-what-it-means-australias-refugee-system>.

[8] See Khanh Hoang, "Asylum seekers and refugees in Australia's 2018-2019 Budget" (9 May 2018), online: *Kaldor Centre* <kaldorcentre.unsw.edu.au/news/asylum-seekers-and-refugees-australia%E2%80%99s-2018-2019-budget-0>.

[9] See United Nations High Commissioner for Refugees, "UNHCR - Refugee Statistics" (last visited 23 September 2023), online: *UNHCR* <unhcr.org/refugee-statistics/>.

of the "connected migrant."[10] My paper draws on Sara Dehm's transnational migration law framework, which she conceptualizes as "making visible the production, enactment, and maintenance of particular sets of structural relations and the enactment of an assemblage of legal practices that shape how people move in the contemporary world."[11] In the face of the ever-growing digital border infrastructure in different countries around the world, I am interested in analyzing the interplay between technology, refugees, and the digitized border through a human rights lens, filling in a particular gap in the literature.[12] As such, this paper examines the question:

How is the right to privacy negotiated, contested, or abandoned, as refugees and asylum seekers navigate digital devices and networks that facilitate their journeys, as well as the border security apparatus that is designed to surveil, police, and curtail their rights?

The paper is structured as follows. In Part II, I examine the definitions of privacy and consider how privacy has been established as a human right. In particular, I highlight how the literature has developed on the human right to digital privacy, and I contend with the tension between privacy and security. In Part III, I draw on digital migration scholarship which has examined how refugees engage with the digital infrastructure during their journeys through their use of smartphones. I emphasize the critical necessity of digital devices and staying connected, and at the same time also explore how privacy considerations complicate the straightforward narrative of smartphones as an unqualified "good" for refugee empowerment. In Part IV, I examine the forms of digital governance at the border and the privacy implications of these technologies for refugees and asylum seekers.

Taking the European border as my primary case study, I argue that there remains an unresolved tension between the right

---

[10] Koen Leurs, "Communication rights from the margins: politicising young refugees' smartphone pocket archives" (2017) 79:6–7 Intl Comm Gazette 674 at 676.

[11] Sara Dehm, "Transnational Migration Law: Authority, Contestation, Decolonization" in Peer Zumbansen, ed, *The Oxford Handbook of Transnational Law* (Oxford: Oxford University Press, 2021) 682 at 4.

[12] See Leurs, *supra* note 10 at 677.

to privacy of refugees and asylum seekers, this fundamental human right that in theory should extend to all, and the increasingly digitized border. All the while, refugees are acutely aware of the privacy implications throughout their journey, and as a result, they are continuously engaged in processes of negotiation and contestation with the digital infrastructure in which they have no choice but to be embedded.

B. The Scope

The scope of this paper looks primarily at the EU border and EU border controls. While the digitization of borders is a worldwide phenomenon, the EU is an important region to study because its border infrastructure is one of the most sophisticated, if not the most sophisticated, in the world. Moreover, the EU has also established a constitutional and legislative framework for the protection of data and privacy that is widely considered as the global benchmark,[13] which means the questions that sit at the intersection of the right to privacy and the right to seek asylum are particularly relevant.

Without a doubt, the increasing securitization and digitization of borders affects all travelers. However, these impacts are not equal:[14] Structural inequalities make "some individuals more susceptible to privacy violations, and help explain why violations of privacy may be more dire for vulnerable individuals."[15] As such I choose to focus on refugees and asylum seekers, who are the most vulnerable of migrants. As will be elaborated in more detail in Part IV, refugees and asylum seekers

---

[13] See Federico Fabbrini & Edoardo Celeste, "The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders" (2020) 21:S1 German LJ *55* at *55;* Ben Hayes, "Migration and data protection: Doing no harm in an age of mass displacement, mass surveillance and 'big data'" (2017) 99:904 Intl Rev Red Cross 179 at 195.

[14] See Petra Molnar, "Robots and refugees: the human rights impacts of artificial intelligence and automated decision-making in migration" in Marie McAuliffe, ed, *Research Handbook on International Migration and Digital Technology* (Cheltenham: Edward Elgar Publishing Limited, 2021) 134 at 144.

[15] Nora McDonald et al, "Privacy and Power: Acknowledging the Importance of Privacy Research and Design for Vulnerable Populations" (Paper delivered at CHI '20: CHI Conference on Human Factors in Computing Systems, Honolulu, 25 April 2020) at 2.

must provide data to all kinds of institutions throughout their journey and at the border, in order to receive the protections afforded to them under international law. And yet refugees and asylum seekers are for whom privacy considerations may be especially sensitive, given the contexts from which they fled and the reasons why they are seeking international protection.[16] This paper foregrounds the reality that refugees and asylum seekers, more than other migrants, may be more seriously affected by digitization and increasing reliance on technology at borders and the contraventions to their fundamental right to privacy.

The paper most directly examines the experiences of asylum seekers, since I focus on their displacement journey before they can acquire official refugee status according to international law. Nonetheless, I use the terms refugee and asylum seeker interchangeably to reflect the fact that they all would have had to confront the border regime and the digital infrastructures at some point.

C. *Theoretical Grounding*

There are two grounding points of theory I want to attend to at the outset. First, this paper draws from the autonomy of migration model, which is a research approach that centers the agency of migrants within the broader border regime – it presumes the right of movement, and emphasizes the everyday practices of people on the move to build a "mobile commons,"[17] a continuously-built infrastructure created by the actions of people on the move, in the face of and independent from sovereign control.[18]

Second, while I am not conducting ethnographic or fieldwork which would ordinarily require research ethics

---

[16] See Enno Steinbrink et al, "Digital Privacy Perceptions of Asylum Seekers in Germany: An Empirical Study about Smartphone Usage during the Flight" (2021) 5:CSCW2 Proceedings of the ACM on Human-Computer Interaction 1.

[17] Martin Bak Jørgensen & Leandros Fischer, "Impossible Research? Ethical Challenges in the (Digital) Study of Deportable Populations Within the European Border Regime" in Marie Sandberg, Luca Rossi & Vasilis Galis, eds, *Research Methodologies and Ethical Challenges in Digital Migration Studies: Caring For (Big) Data?* (Cham: Springer International Publishing, 2022) at 166.

[18] See *ibid* at 154.

disclosures and protocols, I consider it necessary to reflect on Leandros Fischer and Martin Bak Jørgensen's critical questions about migration research: "How does one conduct research that aims to highlight the agency of migrants without inadvertently placing them in danger? How is the question of inherently uneven power differentials played out in this case?"[19]

Fischer and Jørgensen draw attention to the predicament at the heart of research conducted through the autonomy of migration model, which is that producing knowledge about migrants' acts of resistance and subversion also runs the "risk of being abused by anti-immigrant forces, states, and security agents."[20] With this in mind, I take seriously their critical reflection towards "doing harm," rather than adhering formally to the research ethic dictum of "doing no harm."[21] That is to say, migration research should strive to be engaged scholarship that "does" harm by "locat[ing], and expand[ing], ruptures in the … border regime."[22] By situating refugees' individual acts of micro-resistance along their journey in the broader digital infrastructure of the border, I aim to adopt Fischer and Jørgensen's mission to "speak back to system" and to make visible the structures (of the border and of technologies).

II. Privacy as a Human Right

A. *A Historical Overview*

Before I elaborate on the entanglement of the refugee journey with the digital border infrastructure, I turn first to the right to privacy, which has become a central concern within any discussion of technology. The right to privacy has been enshrined as a fundamental human right in the international human rights regime since the adoption of the *Universal Declaration of Human Rights* (UDHR) in 1948. As Article 12 of the UDHR states: "*No one shall be subjected to arbitrary interference with his privacy,*

[19] *Ibid* at 152.

[20] *Ibid* at 157.

[21] *Ibid* at 163.

[22] *Ibid*.

family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[23] The right to privacy is similarly codified, almost verbatim, in the *International Covenant on Civil and Political Rights* (ICCPR) at Article 17,[24] and it is also present in the *European Convention on Human Rights* (ECHR) at Article 8.[25] It is an easily overlooked right, since it does not appear as a standalone article, but alongside other rights. Of note is that the African Charter on Human and Peoples' Rights makes no explicit reference to the right to privacy.[26]

The right to privacy seems to have followed an unusual development process. The international human rights regime typically concretizes rights at the state-level that are already well-established[27] – the development of the right to privacy happened in reverse, where it was recognized under the international human rights framework before it was ever recognized in state constitutions. In addition, Oliver Diggelmann and Maria Nicole Cleis show that in the records of the debate, revision, and drafting processes for the major international instruments protecting the right to privacy – namely the UDHR, ICCPR, or the ECHR – there exists little to no evidence as to why significant changes were made regarding the right to privacy. The final version of the UDHR positions "privacy" first in the list, signalling "privacy" to be an umbrella term, yet this was not always the case.[28] In René Cassin's first draft of the UDHR, "private life" was used in place of "privacy" and in his second draft privacy was not considered an umbrella term at all.[29] Unlike the UDHR and the ICCPR, the ECHR protects

---

[23] *Universal Declaration of Human Rights*, GA Res 217A (III), UNGAOR, 3rd Sess, Supp No 13, UN Doc A/810 (1948) 71, art 12 (emphasis added).

[24] See *ICCPR*, 19 December 1966, 999 UNTS 171, art 17.

[25] See *ECHR*, 4 November 1950, 213 UNTS 221, art 8.

[26] See "Privacy International at the 62nd Session of the African Commission on Human and People's Rights (ACHPR)" (28 April 2018), online: *Privacy International* <privacyinternational.org/news-analysis/2227/privacy-international-62nd-session-african-commission-human-and-peoples-rights> [Privacy International].

[27] See Oliver Diggelmann & Maria Nicole Cleis, "How the Right to Privacy Became a Human Right" (2014) 14:3 HRLR 441 at 442.

[28] See *ibid* at 447.

[29] See *ibid* at 445.

"private life,"[30] yet there are no reports to show whether "private life" in the ECHR is meant to be an umbrella term, or why "private life" was used in lieu of "privacy" (as is used in the other major international human rights instruments).[31]

Diggelmann and Cleis contend that it is possible the drafters of these instruments did not see these various changes in definitions as fundamental, and that changes may have also been the result of having to work in and with multiple languages.[32] Regardless, a closer review of the codification history reveals significant disagreement over the fundamental concept of privacy,[33] and this lack of clarity has persisted to this day. On the one hand, the right to privacy has been incorporated in almost every constitution in the world, in legal norms such as procedural rules,[34] and in the international human rights regime (with a notable absence of the right in the *African Charter of Human and Peoples' Rights*).[35] On the other hand, privacy has been deemed an "unusually slippery"[36] right: It has proved notoriously difficult for legal scholars, philosophers, and other academics to pinpoint an adequate definition of "privacy."

After conducting a detailed study of different concepts of privacies, Daniel Solove came to the conclusion there were six general types of conceptions of privacies: "(1) the right to be let alone; (2) limited access to the self - the ability to shield oneself from unwanted access by others; (3) secrecy - the concealment of certain matters from others; (4) control over personal information - the ability to exercise control over information about oneself; (5) personhood - the protection of one's personality, individuality, and dignity; and (6) intimacy - control over, or limited access to,

---

[30] *ECHR*, *supra* note 25.

[31] See Diggelmann & Cleis, *supra* note 27 at 457.

[32] See *ibid* at 448.

[33] See *ibid* at 458.

[34] See Alexandra Rengel, "Privacy as an International Human Right and the Right to Obscurity in Cyberspace" (2014) 2:2 GroJIL 33 at 41.

[35] See Privacy International, *supra* note 26.

[36] Rachel L Finn, David Wright & Michael Friedewald, "Seven Types of Privacy" in Serge Gutwirth et al, eds, *European Data Protection: Coming of Age* (Dordrecht: Springer Netherlands, 2013) 3 at 5.

one's intimate relationships or aspects of life."[37] We will see that the digitization of borders engages with all six conceptions of privacy, and refugees must negotiate with each of them on their journey.

Ultimately, Rachel L Finn, David Wright, and Michael Friedewald conclude that whatever it means, "privacy comprises multiple dimensions,"[38] as was also made clear in the drafting of the UDHR, and that perhaps the "slipperiness" of the concept is necessary to be able to encompass new, future technologies.[39] Feminist theorists also stress that understandings of privacy vary by culture and context,[40] as its omission from the African Charter signals. Nonetheless, as we will see in Part III, refugees recognize privacy concerns in their own ways, and come to learn about its necessity on their journey.

B. In the Digital Age

As alluded to already, technology has already made the right to privacy more urgent. New demands are being made in relation to the right of privacy, notably in the protection of personal data, and even manifesting in the recent creation of a new right, the right to be forgotten.[41] The right to the protection of personal data (conception four in Solove's taxonomy) has also taken on fundamental status on its own in the European regime under the General Data Protection Regulation (GDPR). As privacy does encompass data protection, both will be discussed together in the following analysis.

On the international stage, the Human Rights Council created the first mandate on privacy in 2015 and began

---

[37] Rengel, *supra* note 34 at 38.

[38] Finn, Wright & Friedewald, *supra* note 36 at 6.

[39] See *ibid* at 26.

[40] See Kieron O'Hara, "The Seven Veils of Privacy" (2016) 20:2 IEEE Internet Computing 86 at 87; Saskia Witteborn, "Privacy in collapsed contexts of displacement" (2022) 22:4 Fem Media Stud 883 at 886.

[41] The right to be forgotten, as a distinct right separate from the right to privacy and protection of personal data, is outside the scope of this paper.

appointing Special Rapporteurs on the right to privacy.[42] The UN Special Committee on Social, Humanitarian and Cultural Issues adopted a new resolution on the right to privacy in the digital age in 2016, which re-emphasized pre-existing international commitments to the right to privacy, and called on "states [to] address legitimate concerns regarding their national security in a manner that is consistent with these obligations," with the awareness "that personal data are increasingly susceptible to being sold without the individuals' consent or knowledge."[43] The UN General Assembly requested the High Commissioner for Human Rights to prepare a report on the right to privacy in the digital age focusing on the impacts on the right to privacy by the use of AI, which was published in 2021.[44] This report had a particular interest in the "interlinkages between the promotion and protection of the right to privacy in the context of the use of AI and the exercise of other human rights (including … freedom of movement)."[45] From this focus, it is clear that there is some, but I would argue not nearly enough, international attention on the issue of refugees and digital borders. All the while, the problem of definitional clarity has extended into the digital privacy realm. Legal scholars have not been so quick to take up Finn, Wright, and Friedewald's conclusion and are undecided on whether the international human rights framework is enough as is to be able to adapt to new technologies, or whether the realm of the digital is unique enough to necessitate a different framework under international human rights law.[46] On the national level, legislators and courts have been pressed to clarify what the right to privacy means and looks like in the digital age.[47]

---

[42] See "Special Rapporteur on the right to privacy" (last visited 23 September 2023), online: *OHCHR* <ohchr.org/en/special-procedures/sr-privacy>.

[43] Molnar, *supra* note 14 at 143.

[44] See "OHCHR | The right to privacy in the digital age: report (2021)" (15 September 2021), online: *OHCHR* <https://www.ohchr.org/en/calls-for-input/2021/right-privacy-digital-age-report-2021>.

[45] *Ibid*.

[46] See Adamantia Rachovitsa, "Engineering and lawyering privacy by design: understanding online privacy both as a technical and an international human rights issue" (2016) 24:4 Intl JL Info Tech 374 at 392.

[47] See Marko Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age" (2015) 56:1 Harv Intl LJ 81 at 86.

Two interrelated considerations with regards to the right to digital privacy arises: Who deserves privacy, and what does it mean to enforce privacy protections, given the inherent borderless nature of data and online activity? In theory, given the fundamental status of the right to privacy in the UDHR, everyone deserves privacy no matter what citizenship they hold (or do not hold). It would seem unreasonable, Marko Milanovic argues, to make the case that "non-citizens *as a class are* inherently more dangerous to the security of a state than its own citizens or permanent residents,"[48] and that their private information is inherently more valuable in ascertaining that supposed danger. However, the right to digital privacy inevitably comes up against national security concerns, as an ostensibly natural extension of an age-old debate between two concepts long considered irreconcilable.[49] In *Volker und Markus Schecke GbR, and Hartmut Eifert v Land Hessen,* the Court of Justice of the European Union ruled that neither the right to the protection of personal data nor the right to privacy were absolute rights – they must be "proportionately balanced with other fundamental rights"[50] and can be subject to restrictions of law in times of public emergencies, for example.[51] Adamantia Rachovitsa submits that in some respects, protecting online privacy in fact helps to *ensure* network, national, and international security. In practice, however, the tension between privacy and security remains unresolved because as Matthias Leese shows, security, especially border security, has become dominated by the desire to accumulate as much data as possible so as to prevent against future risks.[52] It is this security risk-oriented justification that sustains the EU border infrastructure

[48] *Ibid* at 99.

[49] See Matthias Leese, "Privacy and Security – On the Evolution of a European Conflict" in Serge Gutwirth, Ronald Leenes & Paul de Hert, eds, *Reforming European Data Protection Law* (Dordrecht: Springer Netherlands, 2015) 271 at 271.

[50] Mohamed Abomhara et al, "Border Control and Use of Biometrics: Reasons Why the Right to Privacy Can Not Be Absolute" in Michael Friedewald et al, eds, *Privacy and Identity Management Data for Better Living: AI and Privacy* (Cham: Springer International Publishing, 2020) 259 at 262.

[51] See *ibid* at 260.

[52] See Leese, *supra* note 49 at 279.

and that results in disproportionate impacts on refugees and their right to privacy, as will be expanded on in Part IV.

Concerns about data breaches and privacy infringements of refugees are not hypothetical. In November 2022, the LA Times reported that ICE had accidentally released the information – including extremely sensitive data such as names, birthdates, nationalities, and locations – of more than 6,000 immigrants who claimed to be fleeing torture and persecution and who had claimed asylum in the US, onto its website.[53] Heidi Altman, director of policy at the National Immigrant Justice Center, an immigrant advocacy organization, condemned this data leak as "illegal and ethically unconscionable, a mistake that must never be repeated," because "the disclosure of the information put lives at risk."[54]

These considerations bring the international human rights regime to the fore, as its international nature makes it the most feasible avenue to try to address and "codify potential harms [of border technologies] because technology and its development is inherently global and transnational."[55] The EU presents a unique case study too in the application of its privacy protections, because both the ECHR[56] and the GDPR[57] protect those who are on EU territory – *regardless of citizenship,* which would seem to mean that migrants fall within their protected scopes.

---

[53] See Hamed Aleaziz, "ICE accidentally released the identities of 6,252 immigrants who sought protection in the U.S.", *Los Angeles Times* (30 November 2022), online: <latimes.com/california/story/2022-11-30/ice-released-names-6252-immigrants-persecution>.

[54] *Ibid*.

[55] Molnar, *supra* note 14 at 135.

[56] See Yannis Ktistakis, *Protecting migrants under the European Convention on Human Rights and the European Social Charter: A handbook for legal practitioners* (Strasbourg: Council of Europe, 2013) at 13.

[57] See Marcus Evans & Anna Rudawski, "EDPB clarifies territorial scope of the GDPR | Data Protection Report" (6 December 2018), online: *Data Protection Report* <dataprotectionreport.com/2018/12/edpb-clarifies-territorial-scope-of-the-gdpr/>.

III. The Refugee Passage and the Smartphone

Keeping in mind that, at least on paper, the legal landscape safeguards refugees' rights to privacy, I turn now to examining their journey and what the right to privacy looks like to them in practice. For refugees and asylum seekers, navigating the digital "is no more a completely futuristic world, but rather part and parcel of the everyday of migrants:"[58] Smartphones have become "a 21st century migrant essential."[59]

Since 2015, when the aftermath of the Syrian civil war brought the image of the "smartphone refugee" into the public narrative, academics have begun to investigate how vital smartphones are for migrant journeys. Maria Gabrielsen Jumbert, Rocco Bellanova, and Raphaël Gellert found that when refugees make spur of the moment decisions to leave, the only items they carry are their phones and some money.[60] Arguably, even in these cases, money is not as important as their phone, since they never have enough money to cover all the expenses on the journey and end up needing to use their phones to make additional payments along the way.[61] Refugees and asylum seekers who had more time to plan their escapes spend a good amount of time securing their digital devices: This means preparing battery chargers and plastic bags (to keep the phone dry); this also means digitizing as much of their life to load onto

---

[58] Maria Gabrielsen Jumbert, Rocco Bellanova & Raphaël Gellert, "Smart Phones for Refugees. Tools for Survival, or Surveillance?" (April 2018) at 5, online: *Peace Research Institute Oslo Policy Brief* <repository.ubn.ru.nl/bitstream/handle/2066/221131/221131.pdf?sequence=1>.

[59] Isabel Awad & Jonathan Tossell, "Is the smartphone always a smart choice? Against the utilitarian view of the 'connected migrant'" (2021) 24:4 Inf Comm & Soc 611 at 612.

[60] See Marie Gillespie, Souad Osseiran & Margie Cheesman, "Syrian Refugees and the Digital Passage to Europe: Smartphone Infrastructures and Affordances" (2018) 4:1 Social Media + Society 1 at 7.

[61] See Tiziana Mancini et al, "The opportunities and risks of mobile phones for refugees' experience: A scoping review" (2019) 14:12 PLoS ONE 1 at 10; Bram Frouws et al, "Getting to Europe the Whatsapp Way: The Use of ICT in Contemporary Mixed Migration Flows to Europe" (2016), online (pdf): <mixedmigration.org/wp-content/uploads/2018/05/015_getting-to-europe.pdf>.

their phones, as an act of preservation.[62] Significantly, in their interviews with fourteen Syrian refugees who made their way to Germany, Enno Steinbrink et al found that *no one* escaped without access to a phone – they all made use of some makeup of phone at some point of their journeys.[63] For more proof of the critical nature of smartphones and the digital infrastructure underpinning their use, an article in the Independent compared the importance of phone credit alongside the importance of water and food.[64] In the most extreme cases, mobile phones and mobile phone coverage quite literally determined the life and death of migrants.[65]

To further examine the role of digital devices like smartphones on refugee journeys, and how refugees navigate digital connectivity, the concept of affordances provides a helpful lens. Taken from Communication and Media Studies, affordances typically describe how users are afforded or constrained depending on rational courses of action.[66] In the refugee context, Marie Gillespie, Souad Osseiran, and Margie Cheesman suggest that "smartphone affordances emerge, are recognized, mobilized, used, and disregarded by individuals, only to re-emerge in different forms in different contexts."[67]

Smartphone affordances are mobilized as asylum seekers use the smartphone for critical access to information along their journey. One of the most important uses of smartphones cited by refugees and asylum seekers is the ability to search for route information on mapping applications, such as Google Maps. The ability to load mapping information on the smartphone to use in areas or times without connectivity, or to download offline maps through certain applications, is also significant. Other information

---

[62] See Mancini et al, *ibid* at 10.

[63] See Steinbrink et al, *supra* note 16 at 8.

[64] See Samantha Lind, "Refugees need phone credit almost as much as food and water" (7 October 2018), online: *The Independent* <independent.co.uk/happylist/refugees-need-phone-credit-almost-as-much-as-food-and-water-a8572611.html>.

[65] See Gillespie, Osseiran & Cheesman, *supra* note 60 at 7.

[66] See Andrew Richard Schrock, "Communicative Affordances of Mobile Media: Portability, Availability, Locatability, and Multimediality" (2015) 9 Intl J Comm 1229.

[67] Gillespie, Osseiran & Cheesman, *supra* note 60 at 7.

smartphones provide access to include "distances, altitudes, temperature and weather conditions, currencies, possible shelters or refueling points."[68] Refugees are also able to access more meaningful information, in the sense of having access to translation apps, which can help them to understand and communicate with different actors, in different languages, at the various points along their journey.[69]

Scholars have also observed that many refugees and asylum seekers are resourceful social media users, and that social media has become one of their most important platforms for information.[70] Smartphones keep refugees and asylum seekers connected to social media either through downloaded applications or simply the ability to access the internet on the go. Social media is regularly used to crowdsource information, tips, and warnings. Refugees and asylum seekers are able to find information left behind by those who have already travelled the same, or a similar, route,[71] and are also able to find updates on road conditions, border checkpoints, and police or border guard activity. Armed with this information, refugees and asylum seekers are less dependent on smugglers throughout their journey and are thus rendered less vulnerable to exploitation and abuse. Though, scholars are careful to point out that still, none of the migrants they interviewed were able to make their full journey without the help of a smuggler.[72] Given this reality, social media also plays a key role, not only mediating connections between migrants and smugglers, but also informing migrants of particular smugglers or tactics to watch out for. With increased access to information, migrants are able to become more active participants as they traverse the "liminal space" of the refugee journey, confronting "extreme uncertainty … on the move" by making (more) informed

[68] Mancini et al, *supra* note 61 at 9.

[69] See Mirko Forti, "Migrants and refugees in the cyberspace environment: privacy concerns in the European approach" (2020) 2020:2 Eur J Privacy L & Tech 241 at 243.

[70] See e.g. Amanda Alencar, "Mobile communication and refugees: An analytical review of academic literature" (2020) 14:8 Soc Compass 1.

[71] See Mancini et al, *supra* note 61 at 7.

[72] See Steinbrink et al, *supra* note 16 at 9.

choices.[73] Some scholars have termed this ever-expanding migration phenomenon as "Uber migration."[74]

Another important use of the smartphone is to preserve contact with relatives and loved ones through communication applications, such as WhatsApp and Viber. By allowing refugees to stay connected, communication applications help to fulfill the mental and emotional needs of the people on the move. Having a smartphone also means that in some areas or countries where governments have restricted international calls, they serve as the only way for refugees and asylum seekers to maintain contact with those who stayed behind.[75] In times of extreme precarity, for example during boat crossings on the Mediterranean, the smartphone becomes a lifesaving device. The smartphone can be used to contact border authorities to provide rescue at sea, to keep contact with a relative or friend on land for them to be able to seek help from authorities, and even, simply, through the flashlight option on the phone, to indicate presence and attract the attention of authorities.

In all these ways, the smartphone facilitates the mobility of refugees and asylum seekers, allows them to assert their autonomy, and provides them with security – this can come in the form of practical security, material security, or emotional/mental security. According to Gillespie, Osseiran, and Cheesman, "the prospect of losing or damaging their own mobile phone raised a deep existential and physical insecurity in refugees."[76]

And yet, Isabel Awad and Jonathan Tossell remind us of the necessity of critically interrogating depictions of the smartphone as (always and inherently) an unqualified "good."[77] While smartphones can facilitate access to smugglers through online connections, they may not be helpful in connecting refugees to authorities to report cases of abuse. Refugees may in fact be isolated from official social structures throughout their journey,

---

[73] Gillespie, Osseiran & Cheesman, *supra* note 60 at 2.

[74] Cees J Hamelink & Maria Hagan, "Communication Rights for Migrants" in Kevin Smets et al, eds, *The SAGE Handbook of Media and Migration* (London: SAGE Publications Ltd, 2020) 373 at 377.

[75] See Steinbrink et al, *supra* note 16 at 3.

[76] Mancini et al, *supra* note 61 at 10.

[77] Awad & Tossell, *supra* note 59 at 614.

their phones offering them a false or incomplete sense of security.[78] Despite making ubiquitous use of smartphones, many refugees themselves are acutely aware of the risks of being so connected and they remain fearful and suspicious of digital surveillance[79] not only from the country they left but also the countries they are hoping to get to. Gillespie, Osseiran, and Cheesman emphasize how refugees are forced to learn and to adapt to "commuting between online visibility and invisibility,"[80] or, to go back to the concept of affordances, between using and discarding affordances. These choices are often made based on the *type* of border crossing – for example, refugees make themselves actively locatable at sea, as opposed to attempting to fly under the radar at land crossings.[81]

The privacy risks refugees face are myriad, ranging from border agents monitoring social media and collecting identifying information through communication applications, to digital surveillance by government actors from refugees' countries of origin, and even to the monitoring capabilities of the applications and online platforms themselves in terms of tracking activity and collecting data, which may be shared with authorities. We are all now familiar with the inadequacies of the privacy protections of major social media platforms and applications – platforms like Facebook were not designed with the average users' privacy in mind, let alone refugees' privacy.[82] Refugees and asylum seekers are put in even more precarious positions, because social media platforms have also been known to collaborate with governments, providing them with data and either directly or indirectly supporting migrant deterrence campaigns.[83]

---

[78] See Mark Latonero & Paula Kift, "On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control" (2018) 4:1 Social Media + Society 1 at 4.

[79] See Steinbrink et al, *supra* note 16 at 3.

[80] Gillespie, Osseiran & Cheesman, *supra* note 60 at 7.

[81] See Steinbrink et al, *supra* note 16 at 15.

[82] See Latonero & Kift, *supra* note 78 at 1.

[83] See Koen Leurs & Jeffrey Patterson, "Smartphones: Digital Infrastructures of the Displaced" in Peter Adey et al, eds, *The Handbook of Displacement* (Cham: Springer International Publishing, 2020) 583 at 587.

Many studies have illustrated the strategies refugees employ to protect themselves and their family members specifically from the dangers of using smartphones and having a visible online presence – what Gillespie, Osseiran, and Cheesman call "tap[ping] into the subversive affordances of smartphones."[84] Steinbrink et al outline four major tactics they gathered from their interviews: 1) staying anonymous; 2) adapting communications; 3) adapting behavior; and 4) renouncing the use of the phone altogether.

Firstly,[85] refugees usually create anonymous avatars or use aliases on social media, in an attempt to stay unidentified online as much as possible or at the very least to try not to have identifiable information tied to their online activity. Refugees choose to join closed groups on Facebook when seeking information, with the expectation of some degree of privacy if others are required to go through a verification step to join the group. Further, refugees also try to mask their phone numbers, purchasing online numbers that cannot be linked to their real identity. These unidentifiable numbers are useful when having to contact smugglers, to use applications such as WhatsApp, where you cannot create an account without a number (all communication apps, including Viber, Telegram, and Signal, require a phone number to create an account).

Secondly, refugees adapt their communications often by withholding sensitive information, such as details of their journey, their plans, or their thoughts on political issues. Some communicate online using "coded language."[86] Some also make selective choices to "clean" their profile if they foresee an upcoming land crossing or encounters with border patrols.[87] Thirdly,[88] refugees adapt their behavior on digital devices, which means that they prefer certain applications over others depending on privacy considerations, familiarity, and practical fears. It is common for refugees to switch between applications when communicating, for example starting a conversation on Facebook

---

[84] Gillespie, Osseiran & Cheesman, *supra* note 60 at 7.

[85] See Steinbrink et al, *supra* note 16 at 13.

[86] Mancini et al, *supra* note 61 at 8.

[87] See Gillespie, Osseiran & Cheesman, *supra* note 60 at 6.

[88] See Steinbrink et al, *supra* note 16 at 14.

Messenger and continuing it on WhatsApp. Refugees do this either for privacy protection or simply due to practical concerns such as needing to delete some applications on the phone to preserve data and battery. Some refugees prefer to use Facebook to communicate rather than mobile applications such as WhatsApp, with the worry that their phones may get confiscated at some point during their journey.[89] Others prefer WhatsApp specifically because of its end-to-end encryption feature.[90] Others still only trust informal channels and networks because of fears of government surveillance online. [91] Interestingly, researchers remark that selectivity of applications was usually based on individual perceptions of which application gave more privacy protections, and not necessarily based in fact: Answers given by different refugees interviewed were not always the same, even contradictory.[92]

Fourthly, refugees also make selective choices on when or whether to use their phones at all, sometimes choosing to disconnect entirely at certain points of the journey. It is worth highlighting that when it comes to staying anonymous and undetected by authorities, smugglers and refugees are aligned in their interests. Refugees recount how the smugglers they encountered would instruct them on particular strategies to avoid detection, for example telling them to turn off their phones when crossing borders or even to sell their phones.[93] These strategies exemplify how attuned refugees are to privacy considerations. Even when it comes to refugees who question the effectiveness of strategies to avoid detection,[94] there remains a strong recognition that there *are* privacy implications (which they simply cannot overcome).

Still, a number of factors contextualize refugees' sensitivity to privacy issues. One of the primary factors is a refugee's level of digital literacy, which is closely linked to their country of origin,

---

[89] See *ibid* at 4.

[90] See Mancini et al, *supra* note 61 at 10.

[91] See *ibid* at 11.

[92] See Steinbrink et al, *supra* note 16 at 14.

[93] See *ibid* at 12.

[94] See *ibid* at 14.

as well as their reasons for fleeing.[95] In Steinbrink et al's interviews, they observed for example that the refugees from Afghanistan did not seem to have a strong understanding of digital privacy, though they also pointed to the difficulties of explaining this term in languages (such as Dari, Pashtu, or Urdu) without a specific corresponding word.[96] Researchers contrast those fleeing political persecution, such as many from Syria,[97] from those fleeing other forms of violence, underscoring that the former are usually more familiar with privacy concerns. The second tactic of adapting communication can also be considered self-censorship, which is a common practice amongst political refugees, and they may have been circumscribing their digital activity already, even prior to flight.[98] All these factors contribute to refugees' understandings and valuing of "digital privacy." A distinctive feature of many displacement journeys, especially those attempting to reach Europe, is that asylum seekers often travel in groups. Within the group, smartphones are then used by multiple different people, meaning the smartphones are subject to collaborative ownership.[99] This complicates the straightforward privacy risks along the journey, as authorities who may be tracking the activity of one phone or one social media account may not realize the device is being shared, or that multiple people are accessing and using one person's profile to say, gather information and make plans. By extension, this challenges the digital border infrastructure logic, explored in more detail in Part IV, that "the data does not lie," in the sense that the data collected here does not actually pinpoint the identity of *one* individual, but that of many, and the data itself cannot reveal that fact.[100] In light of this reality of the displacement journey, it may be more

[95] See *ibid* at 10.

[96] See *ibid* at 9.

[97] See Gillespie, Osseiran & Cheesman, *supra* note 60 at 5.

[98] See Steinbrink et al, *supra* note 16 at 9.

[99] See Syed Ishtiaque Ahmed et al, "Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh" (2017) 1:CSCW Proceedings of the ACM on Human-Computer Interaction 1.

[100] See Jumbert, Bellanova & Gellert, *supra* note 58 at 4.

accurate to conceptualize privacy as a relational construct, where privacy resides in the context of a network of actors and data.[101]

As this section shows, refugees make choices on how to use their phone and to adapt their online behaviors based on personal perceptions about risk and privacy. Yet, just as this technology supports them on their journey, it is also part and parcel of the broader digital infrastructure of control, containment, and surveillance. Once on the move, refugees become deeply embedded in this digital border.

IV. The Digital Border

A. *An Overview*

In recent years, critical border scholars have been particularly attentive to the ways in which borders are no longer simply clearcut territorial markings. The EU border in particular, is a complex set of infrastructures which are not only digital but also "smart." In an attempt to capture this phenomenon, the border has been alternatively described as the "smart border," [102] "iBorder," [103] "high-tech fortress," [104] and "cyberfortress." [105] Descriptive as these terms may sound, they fail to adequately illustrate the fact that the border is constituted of a *network*, which includes the European Asylum Dactyloscopy Database (Eurodac), the European Union Visa Information System, the Schengen Information System, the European Travel Information and

[101] See Witteborn, *supra* note 40 at 887.

[102] Leurs, *supra* note 10.

[103] Philippa Metcalfe & Lina Dencik, "The politics of big borders: Data (in)justice and the governance of refugees" (2019) 24:4 First Monday.

[104] Luisa Marin, "Is Europe Turning into a 'Technological Fortress'? Innovation and Technology for the Management of EU's External Borders: Reflections on FRONTEX and EUROSUR" in Michiel A Heldeweg & Evisa Kica, eds, *Regulating Technological Innovation: A Multidisciplinary Approach* (London: Palgrave Macmillan, 2011) 131.

[105] Elspeth Guild, Sergio Carrera & Florian Geyer, "The Commission's New Border Package: Does It Take Us One Step Closer to a 'Cyber-Fortress Europe'?" (2008) CEPS Policy Brief No 154, online (pdf): <cdn.ceps.eu/wp-content/uploads/2009/08/1622.pdf>.

Authorisation System, the Entry/Exit System,[106] the European Criminal Record Information System for Third Country Nationals, and the European Border Surveillance system (Eurosur). This vast assemblage of infrastructures is established in the EU Area of Freedom, Security and Justice, and aside from Eurosur, each system is now interoperable with each other,[107] even though these systems were built with different mandates in mind.[108]

It is in this assemblage that refugees and their smartphones are embedded, and where privacy concerns abound. This section hones in on two of the systems in particular: Eurodac and Eurosur. Eurodac and Eurosur represent two of the most critical nodes of the "burgeoning trans-border cybersecurity apparatus" and the continued evolution and sophistication "of digitally adept and computer-networked gatekeepers" of the EU border.[109] The final part of the section will examine another component of the border: The practice of border agents searching and confiscating asylum seekers' phones. This practice further underscores how privacy negotiations during the journey continue at the more official checkpoints of the border.

Before delving into the privacy implications of these technologies for refugees and asylum seekers, it is necessary to foreground the legal framework for privacy and personal data protection in the EU. As mentioned in the Introduction, the EU remains the global standard in terms of privacy and data protection, and the GDPR presents the most comprehensive legal framework on data protection to date. Per the GDPR, every data processing activity must adhere to the principles of fairness, lawfulness, and transparency. The protection of personal data is based on the principles of consent, explicit and legitimate purpose

---

[106] This system is expected to be operational in May 2023. See "Entry-Exit System" (last visited 23 September 2023), online: *European Commission* <home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/smart-borders/entry-exit-system_en>.

[107] See "Interoperability" (last visited 23 September 2023), online: *eu-LISA* <eulisa.europa.eu/Activities/Interoperability>.

[108] See Cristina Blasi Casagran, "Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU" (2021) 21:2 HRLR 433 at 435.

[109] MI Franklin, "Refugees and the (Digital) Gatekeepers of 'Fortress Europe'" (2018) 7:1 State Crime J 77 at 78.

(and no further processing is allowed if it is not related to that purpose), the right to access the data, and the right to rectify the data.[110] The GDPR also guarantees that the data collected will not be kept for longer than needed for the processing of the specific purpose.[111] These principles – or rather, the suspension of these principles – will all come into play with EU border technologies, as will later be explored.

It is critical to add that the GDPR tempers the reach of its privacy protections with Article 23, which allows for restrictions to the aforementioned principles if they are "a necessary measure to safeguard national security and public security."[112] Of note too is the GDPR's brief mention of humanitarian action – the first to do so out of all the data protection laws in the world, though here its primary contextual consideration is public health rather than situations of conflict, which would be most relevant for refugees.[113]

B. Digital Border Systems vs Privacy

i) Eurodac

The Eurodac regulation was introduced in December 2001, and its original purpose was to enforce the Dublin Convention, which stipulated that asylum seekers to the EU had to make their application in their first country of arrival.[114] Fully operational since 2003, Eurodac represents the EU's first experiment with biometric border controls,[115] and remains the most widely used information system.[116] Initially it was tasked with collecting and storing the fingerprint data of people who arrived at the EU border, who would then be classified into three categories:

---

[110] See Forti, *supra* note 69 at 245.

[111] See *ibid*.

[112] Abomhara et al, *supra* note 50 at 265.

[113] See Hayes, *supra* note 13 at 195.

[114] See Latonero & Kift, *supra* note 78 at 6.

[115] See Niovi Vavoula, "Transforming Eurodac from 2016 to the New Pact: From the Dublin System's Sidekick to a Database in Support of EU Policies on Asylum, Resettlement and Irregular Migration" (2020) European Council on Refugees and Exile Working Paper No 13 at 3.

[116] See *ibid* at 6.

category 1, person as an applicant for international protection; category 2, person as having crossed, or attempted to cross, a border illegally; and category 3, person as being a potential illegal immigrant, who has been unsuccessful at gaining asylum status, is without papers, and has been found within a member state.[117] In 2016 and then again in 2020, Eurodac's mandate was significantly expanded and the system itself repurposed "for wider immigration purposes."[118] Under the new regulation, Eurodac is now interoperable with all five of the other EU information databases, meaning the data stored in each will be mutually accessible. [119] With this change, Eurodac became firmly embedded within the EU's turn towards more stringent border practices based on security and criminalization, and presents heightened privacy concerns for refugees and asylum seekers.

Through Eurodac, biometric data from fingerprints, as well as information about sex and state of origin, are entered into the database with the reference numbers of refugees and asylum seekers, who are thus tagged, categorized, and tracked with this information. Magdalena König contends that this kind of social categorization or social sorting is in fact "a disempowering form of surveillance,"[120] enhanced by the use of Big Data.[121] Taking risk management as its rationale, Eurodac translates biometric data into categories of risk, but it also establishes a hierarchy of risk categories where irregular migrants and asylum seekers are all considered suspicious. Gloria González Fuster and Serge

---

[117] See Metcalfe & Dencik, *supra* note 103.

[118] Vavoula, *supra* note 115 at 11.

[119] See Blasi Casagran, *supra* note 108 at 434. Although the interoperability of the systems has not been challenged in court, for more insights into the concerns over its legality, see e.g. Didier Bigo, Lina Ewert & Elif Mendos Kuşkonmaz, "The interoperability controversy or how to fail successfully: lessons from Europe" (2020) 6:1/2 Intl J Migration Border Stud 93; Valsamis Mitsilegas, "Interoperability as a Rule of Law Challenge" (29 January 2020), online: *Migration Policy Centre* <migrationpolicycentre.eu/interoperability-as-a-rule-of-law-challenge/>.

[120] Magdalena König, "The Borders, They are A-Changin'! The Emergence of Socio-Digital Borders in the EU" (2016) 5:1 Internet Pol Rev 1 at 2.

[121] See *ibid* at 8.

Gutwirth call this practice "the implicit stigmatization of people on the move."[122]

The general specter of surveillance raises privacy implications. More concretely, however, biometric data collection directly engages with issues of informed consent.[123] During the journey, refugees are able to make more informed choices due to access to translation applications, circumventing significant barriers presented by language. At border checkpoints where refugees must confront Eurodac's demand of their biometric information, technology provides no assistance, nor do humans. Despite the fact that the legal framework requires the informed consent of their data subjects, particularly for the collection of "sensitive data" (like biometrics), interpretation for refugees is either nonexistent or inaccurate.[124] The result of this loophole is that refugees often do not understand what kinds of information they have given the system (and now given the interoperability of the systems, *all* EU authorities), but they also provide this information without knowing they had rights of privacy and data protection to begin with.[125] As an example, refugees have the right to rectify inaccurate data, but because they are usually unaware this right exists, there is often no opportunity to correct the data – this data may then fundamentally impact their asylum claim.

Though biometrics are often touted as "accurate" and used to bolster arguments about reducing identity fraud[126] and the infallibility of human agents, there remains many questions over the proportionate and necessity calculus of infringing on privacy and data collection rights. These systems raise concerns about their contraventions of the GDPR's principle of data minimization,

---

[122] Gloria González Fuster & Serge Gutwirth, "When 'Digital Borders' Meet 'Surveilled Geographical Borders': Why the Future of EU Border Management is a Problem" in J Peter Burgess & Serge Gutwirth, eds, *Threat Against Europe? : Security, Migration and Integration* (Brussels: VUBPRESS Brussels University Press, 2011) 171 at 184.

[123] See Molnar, *supra* note 14 at 136; Elspeth Guild, "The Right to Dignity of Refugees: A Response to Fleur Johns" (2017) 111 AJIL Unbound 193 at 195.

[124] See Dragana Kaurin, "Data Protection and Digital Agency for Refugees" (2019) World Refugee Council Research Paper No 12 at 41.

[125] See *ibid* at 43.

[126] See Jumbert, Bellanova & Gellert, *supra* note 58 at 3.

because of the serious issue of function creep:[127] Where one system originally designed for a particular purpose is now being refashioned for a different use. Here we take particular note of the broadening of Eurodac's mandate without the consent of or notice to refugees and asylum seekers, those of whom are most vulnerable to this transition.[128]

Eurodac demonstrates how the border, rather than capturing spatial territory demarcating the boundaries between one nation-state and another, now captures the *bodies* that move through those spaces.[129] By relying on biometric identification and surveillance broadly in the context of mobility decisions, Eurodac has the ultimate effect of inscribing territorial determinations of insiders and outsiders onto bodies. As König concludes, "biometrics and big data surveillance enable rebordering."[130] Elspeth Guild illuminates in detail what it means for "the body [to be] transformed into a site of data collection": When all engagements with the "border" is mediated by technology, the refugee loses human contact, and she is deprived of her agency not only because her narrative and identity becomes secondary to her data, but also because the data collected then corresponds immediately to "immutable" categories.[131] In these impersonal, distant, and automated border crossing processes, individual asylum seekers become part of the "masses" of migrants, which does not enjoy privacy or data protections; "its component parts," who, in exercising their right to leave their country of origin to seek asylum under international law,[132] are expected to give up their individual rights to privacy.[133]

Guild emphasizes further, that the danger of the "individual disappear[ing] into data"[134] also entails the destruction of legal

---

[127] See Abomhara et al, *supra* note 50 at 265.

[128] See Kaurin, *supra* note 124 at 47.

[129] See Georgios Glouftsios & Stephan Scheel, "An inquiry into the digitisation of border and migration management: performativity, contestation and heterogeneous engineering" (2021) 42:1 Third World Q 123 at 131.

[130] König, *supra* note 120 at 8.

[131] Guild, *supra* note 123 at 194.

[132] Kaurin, *supra* note 124 at 44.

[133] See Guild, *supra* note 123 at 194.

[134] *Ibid*.

personality,[135] which is not only a core right in and of itself, but is also captured by the right to privacy (recall the fifth conception of privacy in Solove's taxonomy).

Even if these practices of biometric border processes come with the new reality for all travelers, its coercive control manifests most starkly on refugees and asylum seekers.[136] For one, Eurodac regulations allow for the personal information of refugees and asylum seekers stored in the database to also be shared with third countries (non-EU countries) in cases of return. This policy has been roundly criticized by the United Nations High Commissioner for Refugees for minimizing the principle of ensuring international protection of refugees,[137] particularly for those fleeing political persecution and those who had made specific choices regarding technological use *in order to* stay undetected by their home authorities.

What is particularly striking is the fact that human rights concerns, like the right to privacy, were not properly considered before their implementation of these databases.[138] Given the inherent fluidity of technology, these systems were designed as solutions to nonexistent problems or not-yet existent problems.[139] As such, Petra Molnar argues that the lack of regulation has been deliberate. Migrants, and their bodies, serve as the "testing ground for new technologies."[140] At the same time, scholars have continued to stress the necessity for increased regulation of these technologies, as one of the only tangible mechanisms to address the privacy issues laid out in this section.[141]

---

[135] See *ibid* at 195.

[136] See Hayes, *supra* note 13 at 185.

[137] See Kaurin, *supra* note 124 at 48.

[138] See Giray Sadik & Ceren Kaya, "The Role of Surveillance Technologies in the Securitization of EU Migration Policies and Border Management" (2020) 17:68 Uluslararası İlişkiler 145 at 9.

[139] See *ibid* at 7.

[140] Petra Molnar, "Technology on the margins: AI and global migration management from a human rights perspective" (2019) 8:2 Cambridge Int' LJ 305 at 306 [Molnar, "Technology on the margins"].

[141] See *ibid* at 318; Hayes, *supra* note 13 at 182.

ii) Eurosur

Let us now turn to Eurosur. Eurosur is managed and operated by Frontex, facilitating information exchanges to fulfill Frontex's mission of the "safe and well-functioning [of] external borders [and] providing security."[142] Eurosur's mandate is to gather information and to strengthen intelligence and risk management at borders, in service of a preventative approach to border management.[143] To achieve this, Eurosur functions on a different scale to Eurodac. While Eurodac is concerned with individual identification through biometrics, Eurosur gathers big picture information to manage EU's external borders. This information is gathered under the programs "European Situational Picture" and common pre-frontier intelligence picture, through a combination of satellite, ship-board monitoring systems, unmanned aerial vehicles or remotely piloted aircraft systems (also known as drones), and ground sensors, just to name a few.[144]

The main technology of concern for its privacy implications is the use of drone technology. It is significant to note that the body tasked with operating this technology, Frontex, has been faced with criticism over its operational transparency.[145] Some have dismissed the privacy concerns of Eurosur, pointing to the "exceptional" nature of the border regarding privacy rights and its limitations. Even so, Luisa Marin and Kamila Krajčíková maintain that Eurosur and its operations through Frontex are tied

---

[142] "Who We Are" (last visited 23 September 2023), online: *Frontex* <frontex.europa.eu/about-frontex/who-we-are/tasks-mission/>.

[143] See Luisa Marin, "The deployment of drone technology in border surveillance: Between techno-securitization and challenges to privacy and data protection" in Michael Friedewald et al, eds, *Surveillance, Privacy and Security: Citizens' Perspectives* (London: Routledge, 2017) at 5.

[144] See Luisa Marin & Kamila Krajčíková, "Deploying Drones in Policing Southern European Borders: Constraints and Challenges for Data Protection and Human Rights" in Aleš Završnik, ed, *Drones and Unmanned Aerial Systems: Legal and Social Implications for Security and Surveillance* (Cham: Springer International Publishing, 2016) 101 at 109.

[145] See "Frontex, secrecy and story-telling: control of information as super-strategy" (29 July 2021), online: *Statewatch* <statewatch.org/analyses/2021/frontex-secrecy-and-story-telling-control-of-information-as-super-strategy/>.

to European and national frameworks for data protection,[146] and that as an EU agency, Frontex is subject to all the EU regulations on privacy and the GDPR.

Some others excuse the information gathering and privacy concerns by explaining that Eurosur identifies boats, not the people on them.[147] However, this argument ignores the reality that drones collect visual data without the consent and knowledge of the refugees and asylum seekers on these boats (again, going up against a core principle of data collection) – but further, information is gathered on other people also sharing the space, also without their consent and knowledge.[148] Moreover, Paula Kift pushes back on this assumption, arguing that personal anonymity in this case may protect against identifiability, but it does not protect against reachability.[149] In fact, in light of rapid technological advances, privacy scholars consider anonymity and the concept of "personally identifiable information" effectively meaningless. The right to privacy, in its full extent, is meant to protect "lawful processing of personal data, but also the freedom of not having any data processed to begin with"[150] (as in conception four of Solove's taxonomy, where control also means the ability to *not* provide information). This protection is particularly relevant for asylum seekers who have, throughout their journey, taken measures to reduce their digital trace and minimize their digital identity. Solon Barocas and Helen Nissenbaum note that "even when individuals are not 'identifiable', they may still be 'reachable:' they may still be comprehensibly represented in records that detail their attributes and activities, and they may be subject to consequential inferences and predictions taken on that basis."[151] Extending this

---

[146] See Marin & Krajčíková, *supra* note 144 at 119.

[147] See Paula Kift, "In Search of Safe Harbors: Privacy and Surveillance of Refugees in Europe" (Paper delivered at The 17th Annual Conference of the Association of Internet Researchers, Berlin, 31 October 2016) at 1.

[148] See Marin, *supra* note 143 at 8.

[149] See Kift, *supra* note 147 at 1.

[150] *Ibid* at 4.

[151] Solon Barocas & Helen Nissenbaum, "Big Data's End Run around Anonymity and Consent" in Helen Nissenbaum et al, eds, *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge: Cambridge University Press, 2014) 44 at 45.

argument, some scholars have raised a corollary fundamental rights concern. Eurosur's refusal to register the personal information of the passengers on the boats contravenes the fundamental right to seek asylum, wherein all asylum seekers have the right to be assessed individually. In this way, "the logic of surveillance allows EU authorities to strategically prevent contested refugees from becoming legible to the state, thus avoiding potential conditions of accountability."[152]

Lastly, what is especially striking about Eurosur is that its activities are considered humanitarian.[153] As a result, the increasing turn to the use of drone technology, an asset originally intended for the military, has been justified through humanitarian rationales.[154] While the irony of this narrative is clear, it also raises the privacy stakes of Eurosur's policy of third-country data sharing, similar to that of Eurodac's.

iii) Smartphone Searches

Finally, I return to the smartphone, which remains a key player in the border infrastructure even beyond the refugee journey itself. At the border, there has been contentious debate in many countries over whether or to what extent border guards can search people's digital devices. In the US, the Supreme Court created a "border search exception," granting such powers to border guards for the specific purpose of enforcing immigration and customs laws.[155] In Canada, Bill S-7 was recently brought to the Senate to concretize powers granted to border guards to search digital devices at the Canadian border. Both these measures have been subject to criticism by privacy rights advocates[156] and are examples in a global trend, of which many European countries are also at the forefront. In Europe, Belgium

---

[152] Latonero & Kift, *supra* note 78 at 6.

[153] See Marin & Krajčíková, *supra* note 144 at 104.

[154] See *ibid* at 105; Molnar, "Technology on the margins", *supra* note 140 at 307.

[155] See Sophia Cope, "Law Enforcement Uses Border Search Exception as Fourth Amendment Loophole | Electronic Frontier Foundation" (8 December 2016), online: *EFF* <eff.org/deeplinks/2016/12/law-enforcement-uses-border-search-exception-fourth-amendment-loophole>.

[156] See Brenda McPhail, "Phone Searches at the Border: Bill S-7 Fails to Protect Privacy - CCLA" (16 May 2022), online: *CCLA* <ccla.org/privacy/phone-searches-at-the-border-bill-s-7-fails-to-protect-privacy/>.

passed legislation in 2017 allowing immigration authorities to search the digital devices of asylum seekers.[157] Germany, Denmark, and Norway are among the other EU countries to follow suit.[158] The legal framework allowing for this invasion of privacy further illustrates how refugees are "embedded into infrastructures that expose them to surveillance"[159] even as digital devices also serve to facilitate their mobility. At the same time that smartphones are vital tools during refugees' journey, the information contained therein may lead to severe consequences for them if it is leaked.

Another privacy concern relates to the principle of proportionality. Even if this practice, like the collection of biometric data, impacts everyone's travel regardless of citizenship or status, the asylum seeker's context is especially sensitive and almost exclusively characterized by an "inherent power asymmetry between a European immigration official and the individual or family seeking to make a claim for international protection."[160] Further, it is not even clear that these legislations adhere to GDPR.[161]

The confiscation and search of digital devices operates on a similar logic to the collection of biometric data. The assumption is that smartphones (and social media profiles) can verify identity, especially in situations where passports and national IDs are not available, thereby preventing identity fraud and false information in an asylum seekers file, as well as guarding against security threats.[162] In the same way biometrics ostensibly follow the truism that "the body does not lie," smartphones now point to the truism that "the digital devices does not lie."[163] However, as this paper has shown, the digital device does lie – or at the very least, it misleads, distorts, and hides a much more complicated story.

---

[157] See Forti, *supra* note 69 at 243.

[158] See Hayes, *supra* note 13 at 189.

[159] Jumbert, Bellanova & Gellert, *supra* note 58 at 3.

[160] *Ibid* at 4.

[161] See Forti, *supra* note 69 at 245.

[162] See *ibid* at 243.

[163] Jumbert, Bellanova & Gellert, *supra* note 58 at 4.

V. Conclusion

For refugees and asylum seekers, the journey to Europe is "sociotechnical, embodied, and imaginative." [164] As such, refugees continuously and consciously negotiate the vulnerabilities[165] within their fundamental right to privacy, moving between physical and online visibility and invisibility, depending on the border context. Technology, in the form of smartphones, exhibits the "twin dynamics of empowerment and surveillance"[166] for refugees: supporting refugees' mobility, on their own terms, but also implicating them into an ever-expanding border infrastructure of digital systems and engagements with digital devices, where they have no choice but to operate within as they make use of technologies on their passage. There are many unresolved and unaddressed privacy issues relating to the individual systems as well as the digital border infrastructure writ large, yet ultimately, these refugee stories remind us that migrants continue on in whatever way they can, no matter in the physical, or the digital context.

[164] Gillespie, Osseiran & Cheesman, *supra* note 60 at 1.

[165] See *ibid* at 5.

[166] Frouws et al, *supra* note 61 at 12.

Bibliography

Abomhara, Mohamed et al, "Border Control and Use of Biometrics: Reasons Why the Right to Privacy Can Not Be Absolute" in Michael Friedewald et al, eds, *Privacy and Identity Management Data for Better Living: AI and Privacy* (Cham: Springer International Publishing, 2020) 259.

Ahmed, Syed Ishtiaque et al, "Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh" (2017) 1:CSCW Proceedings of the ACM on Human-Computer Interaction 1.

Aizeki, Mizue et al, "Smart Borders or A Humane World?" (October 2021), online: *Immigrant Defense Project's Surveillance, Tech & Immigration Policing Project, and the Transnational Institute* <tni.org/en/publication/smart-borders-or-a-humane-world>.

Aleaziz, Hamed, "ICE accidentally released the identities of 6,252 immigrants who sought protection in the U.S.", *Los Angeles Times* (30 November 2022), online: <latimes.com/california/story/2022-11-30/ice-released-names-6252-immigrants-persecution>.

Alencar, Amanda, "Mobile communication and refugees: An analytical review of academic literature" (2020) 14:8 Soc Compass 1.

Awad, Isabel & Jonathan Tossell, "Is the smartphone always a smart choice? Against the utilitarian view of the 'connected migrant'" (2021) 24:4 Inf Comm & Soc 611.

Barocas, Solon & Helen Nissenbaum, "Big Data's End Run around Anonymity and Consent" in Helen Nissenbaum et al, eds, *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge: Cambridge University Press, 2014) 44.

Bernal, Rafael & Rebecca Beitsch, "Biden budget accelerates shift from Trump policies on immigration", *The Hill* (28 March 2022), online: <thehill.com/latino/600074-biden-budget-accelerates-shift-from-trump-policies-on-immigration/>.

Bigo, Didier, Lina Ewert & Elif Mendos Kuşkonmaz, "The interoperability controversy or how to fail successfully: lessons from Europe" (2020) 6:1/2 Intl J Migration Border Stud 93.

Blasi Casagran, Cristina, "Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU" (2021) 21:2 HRLR 433.

Cope, Sophia, "Law Enforcement Uses Border Search Exception as Fourth Amendment Loophole | Electronic Frontier Foundation" (8 December 2016), online: *EFF* <eff.org/deeplinks/2016/12/law-enforcement-uses-border-search-exception-fourth-amendment-loophole>.

Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953).

Dehm, Sara, "Transnational Migration Law: Authority, Contestation, Decolonization" in Peer Zumbansen, ed, *The Oxford Handbook of Transnational Law* (Oxford: Oxford University Press, 2021) 682.

Diggelmann, Oliver & Maria Nicole Cleis, "How the Right to Privacy Became a Human Right" (2014) 14:3 HRLR 441.

"Entry-Exit System" (last visited 23 September 2023), online: *European Commission* <home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/smart-borders/entry-exit-system_en>.

Evans, Marcus & Anna Rudawski, "EDPB clarifies territorial scope of the GDPR | Data Protection Report" (6 December 2018), online: *Data Protection Report* <dataprotectionreport.com/2018/12/edpb-clarifies-territorial-scope-of-the-gdpr/>.

Fabbrini, Federico & Edoardo Celeste, "The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders" (2020) 21:S1 German LJ 55.

Finn, Rachel L, David Wright & Michael Friedewald, "Seven Types of Privacy" in Serge Gutwirth et al, eds, *European Data Protection: Coming of Age* (Dordrecht: Springer Netherlands, 2013) 3.

Forti, Mirko, "Migrants and refugees in the cyberspace environment: privacy concerns in the European approach" (2020) 2020:2 Eur J Privacy L & Tech 241.

Franklin, MI, "Refugees and the (Digital) Gatekeepers of 'Fortress Europe'" (2018) 7:1 State Crime J 77.

"Frontex, secrecy and story-telling: control of information as super-strategy" (29 July 2021), online: *Statewatch* <statewatch.org/analyses/2021/frontex-secrecy-and-story-telling-control-of-information-as-super-strategy/>.

Frouws, Bram et al, "Getting to Europe the Whatsapp Way: The Use of ICT in Contemporary Mixed Migration Flows to Europe" (2016), online (pdf): <mixedmigration.org/wp-content/uploads/2018/05/015_getting-to-europe.pdf>.

Fuster, Gloria González & Serge Gutwirth, "When 'Digital Borders' Meet 'Surveilled Geographical Borders': Why the Future of EU Border Management is a Problem" in J Peter Burgess & Serge Gutwirth, eds, *Threat Against Europe? : Security, Migration and Integration* (Brussels: VUBPRESS Brussels University Press, 2011) 171.

Gillespie, Marie, Souad Osseiran & Margie Cheesman, "Syrian Refugees and the Digital Passage to Europe: Smartphone Infrastructures and Affordances" (2018) 4:1 Social Media + Society 1.

Glouftsios, Georgios & Stephan Scheel, "An inquiry into the digitisation of border and migration management: performativity, contestation and heterogeneous engineering" (2021) 42:1 Third World Q 123.

Guild, Elspeth, "The Right to Dignity of Refugees: A Response to Fleur Johns" (2017) 111 AJIL Unbound 193.

Guild, Elspeth, Sergio Carrera & Florian Geyer, "The Commission's New Border Package: Does It Take Us One Step Closer to a 'Cyber-Fortress Europe'?" (2008) CEPS Policy Brief No 154, online (pdf): <cdn.ceps.eu/wp-content/uploads/2009/08/1622.pdf>.

Hamelink, Cees J & Maria Hagan, "Communication Rights for Migrants" in Kevin Smets et al, eds, *The SAGE Handbook of Media and Migration* (London: SAGE Publications Ltd, 2020) 373.

Hayes, Ben, "Migration and data protection: Doing no harm in an age of mass displacement, mass surveillance and 'big data'" (2017) 99:904 Intl Rev Red Cross 179.

Higgins, Claire, "Budget 2022: What it means for Australia's refugee system" (30 March 2022), online: *Kaldor Centre*

<kaldorcentre.unsw.edu.au/news/budget-2022-what-it-means-australias-refugee-system>.

Hoang, Khanh, "Asylum seekers and refugees in Australia's 2018-2019 Budget" (9 May 2018), online: *Kaldor Centre* <kaldorcentre.unsw.edu.au/news/asylum-seekers-and-refugees-australia%E2%80%99s-2018-2019-budget-0>.

International Covenant on Civil and Political Rights, 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976).

"Interoperability" (last visited 23 September 2023), online: *eu-LISA* <eulisa.europa.eu/Activities/Interoperability>.

Jones, Chris, Jane Kilpatrick & Yasha Maccanico, "At what cost? Funding the EU's security, defence, and border policies, 2021–2027" (April 2022), online (pdf): *Statewatch and the Transnational Institute* <eubudgets.tni.org/wp-content/uploads/2022/05/At-what-cost-Statewatch-TNI.pdf>.

Jørgensen, Martin Bak & Leandros Fischer, "Impossible Research? Ethical Challenges in the (Digital) Study of Deportable Populations Within the European Border Regime" in Marie Sandberg, Luca Rossi & Vasilis Galis, eds, *Research Methodologies and Ethical Challenges in Digital Migration Studies: Caring For (Big) Data?* (Cham: Springer International Publishing, 2022).

Jumbert, Maria Gabrielsen, Rocco Bellanova & Raphaël Gellert, "Smart Phones for Refugees. Tools for Survival, or Surveillance?" (April 2018), online: *Peace Research Institute Oslo Policy Brief* <repository.ubn.ru.nl/bitstream/handle/2066/221131/221131.pdf?sequence=1>.

Kaurin, Dragana, "Data Protection and Digital Agency for Refugees" (2019) World Refugee Council Research Paper No 12.

Kift, Paula, "In Search of Safe Harbors: Privacy and Surveillance of Refugees in Europe" (Paper delivered at The 17th Annual Conference of the Association of Internet Researchers, Berlin, 31 October 2016).

König, Magdalena, "The Borders, They are A-Changin'! The Emergence of Socio-Digital Borders in the EU" (2016) 5:1 Internet Pol Rev 1.

Ktistakis, Yannis, *Protecting migrants under the European Convention on Human Rights and the European Social Charter: A handbook for legal practitioners* (Strasbourg: Council of Europe, 2013).

Latonero, Mark & Paula Kift, "On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control" (2018) 4:1 Social Media + Society 1.

Leese, Matthias, "Privacy and Security – On the Evolution of a European Conflict" in Serge Gutwirth, Ronald Leenes & Paul de Hert, eds, *Reforming European Data Protection Law* (Dordrecht: Springer Netherlands, 2015) 271.

Leurs, Koen, "Communication rights from the margins: politicising young refugees' smartphone pocket archives" (2017) 79:6–7 Intl Comm Gazette 674.

Leurs, Koen & Jeffrey Patterson, "Smartphones: Digital Infrastructures of the Displaced" in Peter Adey et al, eds, *The Handbook of Displacement* (Cham: Springer International Publishing, 2020) 583.

Lind, Samantha, "Refugees need phone credit almost as much as food and water" (7 October 2018), online: *The Independent* <independent.co.uk/happylist/refugees-need-phone-credit-almost-as-much-as-food-and-water-a8572611.html>.

Mancini, Tiziana et al, "The opportunities and risks of mobile phones for refugees' experience: A scoping review" (2019) 14:12 PLoS ONE 1.

Marin, Luisa, "Is Europe Turning into a 'Technological Fortress'? Innovation and Technology for the Management of EU's External Borders: Reflections on FRONTEX and EUROSUR" in Michiel A Heldeweg & Evisa Kica, eds, *Regulating Technological Innovation: A Multidisciplinary Approach* (London: Palgrave Macmillan, 2011) 131.

——, "The deployment of drone technology in border surveillance: Between techno-securitization and challenges to privacy and data protection" in Michael Friedewald et al, eds, *Surveillance, Privacy and Security: Citizens' Perspectives* (London: Routledge, 2017).

Marin, Luisa & Kamila Krajčíková, "Deploying Drones in Policing Southern European Borders: Constraints and Challenges for Data Protection and Human Rights" in Aleš Završnik, ed,

Drones and Unmanned Aerial Systems: Legal and Social Implications for Security and Surveillance (Cham: Springer International Publishing, 2016) 101.

McDonald, Nora et al, "Privacy and Power: Acknowledging the Importance of Privacy Research and Design for Vulnerable Populations" (Paper delivered at CHI '20: CHI Conference on Human Factors in Computing Systems, Honolulu, 25 April 2020).

McPhail, Brenda, "Phone Searches at the Border: Bill S-7 Fails to Protect Privacy - CCLA" (16 May 2022), online: *CCLA* <ccla.org/privacy/phone-searches-at-the-border-bill-s-7-fails-to-protect-privacy/>.

Metcalfe, Philippa & Lina Dencik, "The politics of big borders: Data (in)justice and the governance of refugees" (2019) 24:4 First Monday.

Milanovic, Marko, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age" (2015) 56:1 Harv Intl LJ 81.

Mitsilegas, Valsamis, "Interoperability as a Rule of Law Challenge" (29 January 2020), online: *Migration Policy Centre* <migrationpolicycentre.eu/interoperability-as-a-rule-of-law-challenge/>.

Molnar, Petra, "Robots and refugees: the human rights impacts of artificial intelligence and automated decision-making in migration" in Marie McAuliffe, ed, *Research Handbook on International Migration and Digital Technology* (Cheltenham: Edward Elgar Publishing Limited, 2021) 134.

——, "Technology on the margins: AI and global migration management from a human rights perspective" (2019) 8:2 Cambridge Int' LJ 305.

O'Hara, Kieron, "The Seven Veils of Privacy" (2016) 20:2 IEEE Internet Computing 86.

"OHCHR | The right to privacy in the digital age: report (2021)" (15 September 2021), online: *OHCHR* <ohchr.org/en/calls-for-input/2021/right-privacy-digital-age-report-2021>.

"Privacy International at the 62nd Session of the African Commission on Human and People's Rights (ACHPR)" (28 April 2018), online: *Privacy International* <privacyinternational.org/news-analysis/2227/privacy-

international-62nd-session-african-commission-human-and-peoples-rights>.

Rachovitsa, Adamantia, "Engineering and lawyering privacy by design: understanding online privacy both as a technical and an international human rights issue" (2016) 24:4 Intl JL Info Tech 374.

Refugees, United Nations High Commissioner for, "UNHCR - Refugee Statistics" (last visited 23 September 2023), online: *UNHCR* <unhcr.org/refugee-statistics/>.

Rengel, Alexandra, "Privacy as an International Human Right and the Right to Obscurity in Cyberspace" (2014) 2:2 GroJIL 33.

Sadik, Giray & Ceren Kaya, "The Role of Surveillance Technologies in the Securitization of EU Migration Policies and Border Management" (2020) 17:68 Uluslararası İlişkiler 145.

Schrock, Andrew Richard, "Communicative Affordances of Mobile Media: Portability, Availability, Locatability, and Multimediality" (2015) 9 Intl J Comm 1229.

"Special Rapporteur on the right to privacy" (last visited 23 September 2023), online: *OHCHR* <ohchr.org/en/special-procedures/sr-privacy>.

Steinbrink, Enno et al, "Digital Privacy Perceptions of Asylum Seekers in Germany: An Empirical Study about Smartphone Usage during the Flight" (2021) 5:CSCW2 Proceedings of the ACM on Human-Computer Interaction 1.

Universal Declaration of Human Rights, GA Res 217A (III), UNGAOR, 3rd Sess, Supp No 13, UN Doc A/810 (1948) 71.

Vavoula, Niovi, "Transforming Eurodac from 2016 to the New Pact: From the Dublin System's Sidekick to a Database in Support of EU Policies on Asylum, Resettlement and Irregular Migration" (2020) European Council on Refugees and Exile Working Paper No 13.

"Who We Are" (last visited 23 September 2023), online: *Frontex* <frontex.europa.eu/about-frontex/who-we-are/tasks-mission/>.

Witteborn, Saskia, "Privacy in collapsed contexts of displacement" (2022) 22:4 Fem Media Stud 883.