SI: Forced Migrants and Digital Connectivity

SM+S
social media + society

Social Media + Society
January-March 2018: 1–11

DOI: 10.1177/2056305118764432
journals.sagepub.com/home/sms
SAGE

# On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control

**Mark Latonero[1] and Paula Kift[2]**

**Abstract**

Since 2014, millions of refugees and migrants have arrived at the borders of Europe. This article argues that, in making their way to safe spaces, refugees rely not only on a physical but increasingly also digital infrastructure of movement. Social media, mobile devices, and similar digitally networked technologies comprise this infrastructure of "digital passages"—sociotechnical spaces of flows in which refugees, smugglers, governments, and corporations interact with each other and with new technologies. At the same time, a digital infrastructure for movement can just as easily be leveraged for surveillance and control. European border policies, in particular, instantiate digital controls over refugee movement and identity. We review the actors, technologies, and policies of movement and control in the EU context and argue that scholars, policymakers, and the tech community alike should pay heed to the ethics of the use of new technologies in refugee and migration flows.

**Keywords**

refugees, migration, infrastructure, digital technologies, ethics, policy

## Navigating the Digital Passage

The world has changed dramatically since 1951, when the United Nation (UN) first set out legal protections for refugees in the Geneva Convention. Terrorism has become a global watchword, governments and economies both have toppled and soared, and the Internet and digital devices are accessible from all over the globe.

In Syria, a series of political protests in 2011 set off a wave of crises that have culminated in a years-long civil war; with casualty rates reported above 200,000 in 2015, more than 4 million refugees have since fled the country (BBC, 2016). These refugees, and the Syrian crisis as a whole, have become the focal point in contemporary debates around the movement, risks, and resettlement of refugees from numerous conflict zones.

The Syrian refugee crisis is often labeled as the largest since World War II (WWII) following which the first international policies and protections for refugees were developed. Refugees today face the same struggles to escape war-torn homes as previously; however, their experience differs in at least one dramatic way: refugees today not only depend on a physical but increasingly also on digital infrastructure to make their way across to safer places. It is the components of this "digital passage," and the actors that populate it, that we analyze in this article.

Focusing on the context of the highly mediatized arrival of refugees and migrants at the borders of Europe in 2015–2016, we will illustrate how refugees, human traffickers, governments, and the private sector interact in this new digital environment. Refugees are able to rely on digital networks to both communicate with distant family members and locate the resources they need. Yet, those same tools are increasingly also used to exploit their vulnerabilities. For instance, the movement of refugees is facilitated by digital platforms provided by multinational corporations. But the design of those platforms is rarely catered toward the specific needs and risks inherent to the refugee experience. Furthermore, refugees must contend with the fact that similar technologies are used by governments to increase their control over borders, migration, and the access to asylum.

The European Union (EU) and its member states have been at the forefront of this development. At the European

[1]Data & Society Research Institute, University of Southern California, USA
[2]New York University, USA

**Corresponding Author:**
Mark Latonero, Data & Society Research Institue, University of Southern California, 36 W. 20th St. New York, NY 10002, USA.
Email: latonero@usc.edu

level, two regulations are particularly noteworthy in this regard: Eurosur (mandating drone and satellite surveillance of the Mediterranean Sea) and Eurodac (biometric information collection at the border). Eurosur and Eurodac are both reflective of the EU's increasingly digitalized system of border controls, but the underlying logic of the use of drones and biometrics within that system differs greatly: while Eurosur reinforces external borders through the classification of *groups*, Eurodac reinforces internal boundaries through the identification of *individuals*. Moreover, whereas Eurosur pushes the physical border *outwards* as satellites and drones are designed to prevent populations of asylum seekers and "illegal" migrants from reaching the continent in the first place, Eurodac pushes the border *inwards* as biometric information technologies inscribe the border into the bodies of each and every individual asylum seeker in Europe. While the EU enforces its digital borders at the level of *infrastructure*, individual EU member states are mirroring the European approach at the level of *artifacts*, as they increasingly turn toward the confiscation of smartphones and the analysis of social media in an attempt to identify and classify individual migrants and asylum seekers.

Methodologically, we will provide an overview of the use of digital technologies by refugees and human smugglers, on one hand, as well as provide an in-depth analysis of relevant private and public sector initiatives, on the other hand, in order to demonstrate that the digital passage not only facilitates movement but could just as easily be exploited as a tool for surveillance and control. Note that the discussion of refugees and human traffickers will mostly focus on *artifacts*, whereas the discussion of corporations and governments will mostly focus on *infrastructure*. We argue that the digital passage is ultimately defined by both.

In sum, in this article, we will examine what we call the new digital passage for movement and explore the inherent tensions that are embedded in the sociotechnical relationships that it enables. We conclude with a discussion of the risks and benefits inherent to the digital passage and urge researchers, policymakers, and the tech community alike to pay heed to the ethical questions surrounding the use of digital technologies in modern migration and refugee flows.

## Migration, Globalization, and Modernity

The study of refugees and modern communication technologies lies at the intersection of the fields of migration, globalization, and modernity and draws upon a rich literature ranging from migration and media studies, anthropology and law. As Inda and Rosaldo (2008) point out, we are experiencing an "intensification of global interconnectedness, suggesting a world full of movement and mixture, contact and linkages, and persistent cultural interaction and exchange" (p. 4). This interconnectedness has facilitated the flow not only of information and goods but also of people; migration is, thus, an important part of globalization. At the same time, that information flow has not been even or symmetrical. Indeed, as Fassin (2011) cautions, "whereas the circulation of goods was progressively facilitated through international trade agreements, the transnational circulation of persons became increasingly restricted, at least for the majority of the population of the planet" (p. 214). This is confirmed by Balibar (2004), according to whom

> Nothing could be more wrong than the idea that globalization would be accompanied by a parallel growth of material, immaterial, and human circulatory flows. Whereas information has become practically "ubiquitous," and whereas the circulation of goods and currency conversions have [sic] been almost entirely "liberalized," the movements of men are the object of heavier and heavier limitations. (p. 113)

But regardless of whether it is encouraged or suppressed, "Migration, in its endless motion, surrounds and pervades almost all aspects of contemporary society" (Papastergiadis, 2000, p. 1).

In recent years, migration and media studies have joined forces. Of course, the media have always been a powerful tool for shaping national publics. As Anderson (2006) famously described, print capitalism significantly contributed to the formation of "imagined communities," which were vital to fostering a sense of national belonging. This sense of belonging has been complicated, however, by a marked increase in transnational flows of both people and information. As Appadurai (1996) points out, "new forms of electronically mediated communication are beginning to create virtual neighborhoods" (p. 195) that are no longer restricted to the geographical confines of the nation-state.

A number of scholars have explored the specific relationship between digital media and the migrant experience. Madianou (2014) argues that "media do not just add a new dimension to the phenomenon of migration—they transform it altogether" (p. 323). In her study of Filipina overseas workers living in the United Kingdom, the promise that communication technologies would help them stay connected with family back home encouraged their decision to migrate in the first place. In reality, however, connectivity was often not enough, and family structures could end up damaged and strained. Hegde (2016), by contrast, demonstrates that digital media can help create and sustain transnational diasporic public spheres. Similarly, Leurs (2015) examines how online technologies are used by migrant and diasporic youth to perform and negotiate identity. Finally, in the Anthology of Migration and Social Transformation (2016), Drüeke provides a useful overview of recent work in which media and migration studies intersect.

As Bauman (2012) suggests, "[m]odernity starts when space and time are separated from living practice and from each other" (p. 8). It is, hence, the seemingly antithetic intertwining of the instantaneous borderless fluidity of digital

media and the drudging constricted materiality of the migrant experience that this article intends to explore.

## Exploring the Digital Passage: Technologies, Actors, and Relationships

In the context of the Syrian refugee crisis, the attention of journalists, scholars, and humanitarian organizations has increasingly turned toward refugees' use of digital media and communication technologies. For instance, in August 2015, the *New York Times* published an article describing how asylum seekers rely on digital devices, such as smartphones, in order to navigate the external and internal borders of the EU (Brunwasser, 2015; see also Latonero, 2016a, 2016b). Yet, the focus on a single device obscures the bigger picture (Ram, 2015). Social media, mobile apps, online maps, instant messaging, translation websites, wire money transfers, cell phone charging stations, and Wi-Fi hotspots all constitute what we would define as a new digital infrastructure for global movement. According to Larkin (2013), "What distinguishes infrastructures from technologies is that they are objects that create the grounds on which other objects operate, and when they do so they operate as systems" (p. 329). Larkin (2013) further posits that infrastructures can be technological, financial, biological, and social (pp. 338–339). We embrace Larkin's definition but choose to rely on the word *passage* instead of infrastructure as this allows us to simultaneously refer to its meaning as a right, an act, and a temporal condition of movement, on one hand (see dictionary.com, 2017, which defines "passage," among others, as "an act or instance of passing from one place" and "the permission, right or freedom to pass") and also to architectural constraints upon the movement of people, goods, and information, on the other hand (see Larkin, 2013, also defining passage as "route or course by which a person or thing passes or travels" and "hall or corridor," respectively). Paraphrasing Benjamin (1999), the ambiguity of the passage is, thus, "an ambiguity of space" (p. 877; see also Leurs, 2015, p. 22). That said, the success of refugees in making it to safe spaces increasingly relies on access to not only a safe physical but also digital infrastructure. This digital infrastructure, and attempts by both public and private actors to control it, is, thus, just as important to our analysis as the impressive range of people and artifacts that it encompasses (Bowker, Baker, Millerand, & Ribes, 2010). In what follows, we will outline how the reliance on both infrastructure *and* artifacts affects the interplay of some of the major protagonists in this sociotechnical space: refugees, smugglers, corporations, and governments.

### *Refugees*

When refugees use social media and networked technologies, they both produce and rely on a digital infrastructure of information flows. Castells' definition of the "space of flows" suggests that it is "the material arrangements that allow for simultaneity of social practices without territorial contiguity" (Castells, 1999, p. 295). Access to this "space of flows" has proved crucial to refugees on their journeys. Not only does it allow refugees to stay in touch with friends and family at home but it also provides them with real-time information as they try to make their way to safer places (e.g., Frouws, Phillips, Hassan, & Twigt, 2016). The "Asylum and Immigration Without Smugglers" Facebook group founded by the Syrian refugee Abu Amar in 2013, for instance, proved to be a particularly valuable resource of information on borders, routes, weather conditions, and safe places to stay (e.g., Schmidle, 2015; Todtmann & Edlbe, 2015). The *New Yorker* has dubbed it a kind of TripAdvisor for refugees (Schmidle, 2015).

At the same time, an analysis of the impact of digital networks on the refugee experience must also consider the material conditions of that which is so often characterized as purely informational. Indeed, accessing crucial information on the Internet depends on an entire infrastructure and economy of Wi-Fi hotspots, shops that sell SIM cards, or the physical offices of wire transfer services.

For example, field observations for this project in Serbia in November 2015 occurred at a time when "irregular" migrants and refugees were allowed to travel across the country and exit for a period of 3 days. Without this grace period, many would have had to resort to unauthorized entry across the border and to obtaining illegal transportation often supplied by human smugglers.

While the majority of asylum seekers sought to move across Serbia to the next border as quickly as possible, some needed to stop in Belgrade in order to access critical resources—medical attention, food, shelter, or information. A park in the center of Belgrade became the de facto meeting place for refugees in need of obtaining these services. In one area of the park, the Red Cross provided free Wi-Fi, while in another area an International non-governmental organization (NGO) received and distributed free clothing.

Refugees discovered this park via word-of-mouth or through the various mobile tools at their disposal. These mobile devices were charged at solar charging stations near an infirmary. Indeed, images of packed mobile phone charging stations for refugees have become a familiar trope in the news media. Yet, an equally visited area was an information booth manned by aid workers with photocopies of bus schedules to the Croatian border tacked to the outside wall. Other refugees needed to stop in the capital in order to find a bank or financial center for electronic money transfers. Finding these places of financial access connectivity are essential in order to fund the various stages of the journey.

Based on these observations we note that refugees' movement within physical space is intrinsically connected

with information needs, flows, and access. Digital technologies allow for refugee movement across space and time, yet also require a material anchoring in the technical infrastructure.

## Traffickers

The dual use nature of technology is on display in the refugee context. The same technologies that afford refugees with many benefits today can just as easily be exploited to do them harm. Human smugglers and human traffickers rely on those technologies too; but they use them to profit from those who are desperately seeking a better life. Human trafficking and human smuggling are two distinct socio-legal constructs. Yet, the two blur in relation to the technologies used and the refugees and migrants who are vulnerable to various degrees of exploitation, and thus, both will be discussed in the same context for the purposes of this article. Research in other national contexts has demonstrated that human traffickers use online technologies and mobile phones to exploit more individuals across greater distances in shorter periods of time (Latonero, 2011, 2012). As nationally and internationally defined crimes, human trafficking tends to focus on exploitation, whereas human smuggling focuses on transportation (UN Office of Drugs Crime [UNODC]). Yet, in practice, the distinctions between the two phenomena can blur and the technologies facilitating the crimes are the same.

Previous descriptive research has demonstrated that human smugglers leverage sophisticated social networks and increasingly rely on new technologies to operate more effectively (Mavris, 2002). Reports have recently surfaced that social media are being used to connect smugglers with refugees from the Middle East and North Africa. For example, human smugglers in Libya and Egypt have used Facebook to advertise "trips to Italy" (Kingsley, 2015; Saleh, 2015). According to the Organization for Economic Co-operation and Development (Organisation for Economic Co-operation and Development [OECD], 2015),

> the arrivals of relatively wealthy Syrians migrants on this smuggling route, mostly transiting through Egypt to Libya, and the greater use of social media to reach out potential clients, have increased expected profits and the business for traffickers on the central Mediterranean route.

A report from Europol and Interpol (2016) on migrant smuggling networks further highlights that "social media is also an important tool widely used by migrants and recruiters alike to diffuse information about routes, services, and prices."

In addition to social media, mobile phones and messaging services like Viber have served as a primary means for smugglers to organize illicit boats, trucks, and lodging for refugees and migrants seeking such services. These illicit relationships are enabled by digital connectivity. Yet, due to the clandestine and illegal nature of these activities, increased connectivity, somewhat paradoxically, actually entails increased isolation from social structures in this case. For example, in some human-trafficking cases, an individual may have the digital means to communicate with traffickers but is unable to contact the authorities if he or she become victimized for fear of being arrested (Latonero, Wex, & Dank, 2015).

Despite the risks, refugees' use of mobile tools such as WhatsApp can also serve as a virtual lifeline (Kozlowska, 2015; Specia, 2015). In an interview conducted in November 2015, a Norwegian law enforcement officer working aboard a ship in the Mediterranean explained that smugglers forced refugees and migrants into dangerously unsafe boats, sometimes with the threat of physical violence. Once in the boat, the passengers hope to reach the coverage area where their cell phones can be used to send distress signals before their boats sink. It is a complicated array of phone devices, cell towers, service providers, applications, and national policies that enables scenarios such as these.

## Corporations

As mentioned earlier, many of the platforms and devices that refugees and other actors in the digital passage have come to rely upon are provided by private corporations. It probably comes as no surprise that refugees use social media platforms provided by the tech sector, just like everybody else, since they are intended to be used by consumers for myriad aspects of everyday life. Refugees are not everyday consumers, however. They have specific characteristics that make them a vulnerable population. Privacy concerns, for example, can be more sensitive for refugees who may be fleeing political persecution and violence in their home countries. Increased visibility on social media may put their remaining relatives back home at risk or potentially stigmatize them in their host countries.

Yet, a platform like Facebook, whose business model centers around collecting, analyzing, and selling its users' data, does not differentiate between refugees as a vulnerable group and the population at large. In essence, social media platforms provide much needed services for refugees, while surveilling and tracking them for commercial purposes. Every text message, money transfer, social media login, and Wi-Fi connection generates data on refugees and smugglers alike. Companies like Facebook, Vodafone, and Western Union currently collect and analyze such data for commercial purposes; but this raises the question of whether the private tech sector cannot also leverage the same technologies to benefit refugees more directly.

Yahoo, Google, and others have started to create programs to intentionally intervene in the refugee issue (Al Jazeera, 2015; Datta, 2015). For instance, Google has created apps that purport to provide refugees with helpful information along their journey and in host countries. The company has

also donated US$5.3 million in Chromebooks to children in refugee camps. Similarly, Facebook announced that it would provide "free" Wi-Fi in refugee camps in coordination with the UN Refugee Agency. As an indication of the growing interest in private tech sector involvement, in September, President Obama (2016), at the UN General Assembly, announced US$650 million of investments for refugee "solutions" from companies like Airbnb, HP, LinkedIn, Mastercard, Microsoft, TripAdvisor, and Western Union.

It remains to be seen whether a digital infrastructure that remains part of a global, privatized, and commercial space and is primarily geared toward making profit can, at the same time, be repurposed for the protection of fundamental rights. Labels such as "user" and "customer" might not as easily attach to refugees as they do to non-displaced populations. One possible way to incentivize companies to consider the special rights and concerns of refugee users is to appeal to user safety policies. For example, Facebook has previously come under fire for facilitating human (sex) trafficking (Mason, 2012) and responded by partnering with groups like the US-based Center on Missing and Exploited Children to identify child sex abuse images (Facebook, 2016). Facebook has also sought to apply its facial recognition technology to identify possible trafficking victims and offenders (Roberts, 2015). If similar interventions were developed in the refugee context, the benefits and risks for refugees are unclear, particularly when infrastructure for free movement is simultaneously deployed for surveillance and control.

More specifically, the prevalence of refugee use of these platforms casts a new light on the debates over data collection and privacy, particularly when such collection can be used for corporate profits, user surveillance, and identifying bad actors on proprietary networks. A major debate is government access to the online "intelligence" gathered by technology firms. While it may, thus, be right, historically, to claim that states have "monopolized the *authority* to restrict movement vis-à-vis other potential claimants, such as private economic or religious entities" (Torpey, 2000, p. 5), those states have increasingly come to rely on private sector infrastructure to do so *effectively* (e.g., Gammeltoft-Hansen, 2013; Gammeltoft-Hansen & Sørensen, 2013). The following section will explore the extent to which European governments have already exploited digital infrastructure and technology policy to reinforce their border controls.

## *Governments*

In order to make their way across to safe spaces, refugees have to navigate multiple borders. While borders were initially defined simply as "international boundaries between nation-states" (Alvarez, 1995, p. 449), political geographers and anthropologists are increasingly turning toward the study of borderlands as sites of investigations where not only issues related to nationality but also culture, values, and identity are challenged and renegotiated (Aas, 2011b; Alvarez, 1995; Heymann & Symons, 2012; Van Houtum & van Naerssen, 2002). Furthermore, in the context of migration control, the study of external (national) borders has recently been complemented by a study of internal (cultural) boundaries, and how the policing of the former can lead to the reinforcement of the latter (Fassin, 2011; see also Van Houtum & van Naerssen, 2002). Finally, several scholars have also turned their attention to how the introduction of new technologies, particularly in the digital realm, has led to a proliferation of borders both horizontally—beyond the sovereign territory of nation-states—and vertically—outsourcing migration control to private companies and platforms (Aas, 2006, 2007, 2011a, 2013; Amoore, Marmura, & Salter, 2008; Balibar, 1992; Broeders, 2007; Dijstelbloem, 2009; Dijstelbloem & Broeders, 2015; Epstein, 2008; Gammeltoft-Hansen, 2013; Gammeltoft-Hansen & Sørensen, 2013; Mitsilegas, 2012; Pötzsch, 2015). These questions call for a fundamental reconsideration of the nature of borders and boundaries in the digital age and more specifically how one can

> grapple, empirically, with the concept of a "border," when a border is no longer simply a "wall" around a nation-state territory but rather a distributed network of myriad checkpoints, technologies, and actors, which can be situated inside or outside a given state territory. (Aas, 2011a, p. 296)

The EU is a particularly complicated borderland. While the Schengen Agreement resulted in the abolition of the internal borders of the EU, it simultaneously encouraged the fortification of its external borders. This is because migration is no longer only framed as an economic but, in the aftermath of the 11 September 2001 terrorist attacks, increasingly also as a security concern. Consequently, there is a growing perception that the freedom of movement within the EU can only be protected by restricting movement into the EU (Huysmans, 2006; see also Aas, 2011b; Schwell, 2014). The instability of the Northern African border region following the Arab Spring and the ongoing conflicts in the Middle East further contributed to the sentiment that Europe was surrounded, if not enclosed, by sources of insecurity. This sentiment was aggravated as increasing numbers of migrants, displaced persons, and asylum seekers arrived at the borders of Europe.

In response to increased migratory pressures and perceived security threats, the EU reinforced its border controls, complementing the physical infrastructure of "natural" sea and land, as well as man-made borders such as checkpoints and fences, with a digital infrastructure for surveillance and control. Two EU regulations are particularly noteworthy in this regard: Eurodac (biometric information collection at the border) and Eurosur (drone and satellite surveillance of the Mediterranean Sea). Both regulations form part of an increasingly digitalized EU border surveillance system but the underlying logic of the use of drones and biometrics within

that system differs greatly: whereas the former facilities *classification*, the purpose of the latter is *identification*. Finally, we will demonstrate that individual EU member states have taken the desire to classify and identify one step further, as law enforcement officials are increasingly turning toward smartphone and social media analysis toward the same end. These are some of the clearest examples of how the digital passage is defined and constrained not only by people and artifacts but also by the infrastructure in which the two are embedded, and hence, warrant further examination by the authors below.

*Eurodac.* The Eurodac regulation (Council Regulation [EC] No 2725/2000) was introduced in the European parliament on 11 December 2001. The original purpose of the regulation was to allow for the effective enforcement of the Dublin Convention, which mandates that refugees have to apply for asylum in the first country of arrival in the EU. The establishment of a central European database comprised of the fingerprints of all asylum seekers above the age 14 was deemed necessary toward this end because it allowed each individual EU member state "to check whether an alien found illegally present on its territory has applied for asylum in another Member State" (Council Regulation [EC] No 2725/2000, p. 3) and, thus, to prevent asylum seekers from filing multiple asylum applications (Boehm, 2012, p. 305). But the Eurodac database also includes information about all other immigrants who have been arrested for illegal border crossings in the EU. In June 2013, the mandate of the Eurodac regulation was expanded to also allow European law enforcement agencies such as Europol, the European Police Office, access to the database, based on the argument that "the information contained in Eurodac is necessary for the prevention, detection or investigation of terrorist offenses" (Regulation [EU] No. 603/2013). Finally, in May 2016, the European Commission published a proposal to collect not only fingerprints but also facial recognition data under the Eurodac regulation (European Commission, 2016, pp. 12–13) to lower the minimum age for inclusion in the database from 14 to 6 (European Commission, 2016, p. 6) and to extend the data retention period from 18 months to 5 years (European Commission, 2016, p. 4).

*Eurosur.* The Eurosur regulation (Regulation [EU] No. 1052/2013) was adopted on 22 October 2013. The goal of the Eurosur regulation is to provide EU member states and Frontex, the EU's border management agency,

> with the infrastructure and tools needed to improve their situational awareness and reaction capability at the external borders of the Member States of the Union ("external borders") for the purpose of detecting, preventing and combating immigration and cross-border crime and contributing to ensuring the protection and saving the lives of migrants.

Toward this end, Eurosur proposes a comprehensive system of surveillance of the maritime and external land borders of the EU, including the establishment of so-called national coordination centers for the exchange of information and the use of sophisticated surveillance tools, such as satellite imagery and drones (Regulation (EU) No. 1052/2013, Article 12(3)c). Importantly, in order to maintain pre-frontier intelligence pictures, the EU not only monitors its own external land and maritime borders but also monitors the borders of neighboring third countries. Consequently, the Eurosur regulation also explicitly encourages information sharing and cooperation with those countries (Regulation [EU] No. 1052/2013, Article 20).

*From Massification to Individuation.* The Eurodac and Eurosur regulations both form part of the EU's comprehensive border surveillance system, but the respective purposes of Eurosur and Eurodac within that system greatly differ. The goal of Eurosur is to prevent illegal migration into the EU from happening in the first place, whereas Eurodac is concerned with controlling the movement of migrants and asylum seekers once they have already crossed the border. In order to achieve these goals—both of which rely on digitally networked technologies—each system employs a unique logic of control.

Eurosur's drone and satellite surveillance allow for a birds-eye view of the Mediterranean Sea. It allows for the detection of the movement of boats, but it does not allow for the identification of individual passengers on those boats. Nor is this necessary from the perspective of external border controls at least, as the concern is less with the *identity* of the passengers on those boats than with the *attribute* associated with them, namely that of clandestine and potentially illegal migration. Indeed, somewhat paradoxically, in this case it may actually be the *refusal* of EU authorities to collect personal information about the passengers on these boats that raises fundamental rights concerns, since each passenger should be processed individually in order to assess whether he or she has a claim to international protection. The logic of surveillance, thus, allows EU authorities to strategically prevent contested refugees from becoming legible to the state, thus avoiding potential conditions of accountability. Once migrants and refugees have successfully crossed a European border, on the other hand, the EU is no longer only interested in *what* these border crossers are—"illegal" migrants or refugees with claims to international protection—but also *who* they are, as reflected in the use of biometric technologies that are geared toward establishing and tracking the exact identity of each individual migrant and asylum seeker. While blanket surveillance, thus, attempts to "manage migration as a mass phenomenon," biometric data collection practices treat asylum seekers and refugees as "hyperindividualized entities" that need to be identified and controlled (Feldman, 2012, pp. 78–79; see also Epstein, 2008; Maguire, 2009)—and, as the recently proposed lowering of the minimum age for inclusion in the database as well as significant extension of

the retention period suggests, identified and controlled at an ever younger age and for ever increasing amounts of time.

*Social Media Surveillance.* Governments increasingly seek to exploit the affordances of digital infrastructure for the purposes of migration management and control. The European Commission's (EC's) European Migration Network (2016) details how social media is being used to facilitate human smuggling (and trafficking) and argues that monitoring social media sites can aid in prevention and criminal investigations. Proactive monitoring of social media for smuggling prevention involves counter-messaging in online sites, while smuggling investigation involves collecting electronic evidence for possible criminal prosecutions. The EC also states that a number of EU member states engage in direct monitoring of social media sites with the assistance of Europol and Frontex, but with a key distinction.

> Frontex primarily focuses on social media monitoring for preventive risk analysis purposes (e.g. performing analyses on irregular migration routes, to inform Member States who can then tailor responses to new phenomena). Europol on the other hand is involved in both the prevention and investigation aspects. (EC, European Migration Network, 2016)

According to a 2017 report by Europol's European Migrant Smuggling Center, social media accounts of suspected smugglers were "communicated to" Europol over the prior year's investigations.

For examples involving direct monitoring by EU member states, both the German and Belgium governments proposed measure that would allow "law enforcement authorities to access smartphones and social media accounts of asylum seekers, in order to 'make safety checks,' i.e. carrying out identification in the absence of ID documents and searching for security-relevant information" (Bellanova, Jumbert, & Gellert, 2016). The German Ministry of the Interior (BMI) initiated proposals in early 2017, which would allow officials to seize the data on the smartphones and laptops of asylum seekers—without their consent—who do not have proper identification.

Demanding access to social media accounts is not limited to the governments in Europe. In late 2016, during the Obama Administration, the US Customs and Border Protection (CPB) began to request the social media accounts of foreign visitors entering into the country (Romm, 2016). In 2017, the head of the Department of Homeland Security (DHS), under the new Trump Administration, stated that his agency is considering looking into the social media accounts of individuals seeking entry into the country from selected Muslim-majority countries (Naylor, 2017). At the same time, the Council on American–Islamic Relations (CAIR) filed an official complaint with the US CBP and DHS, claiming that the agencies were systematic targeting of Muslim-Americans. According to CAIR (2017), "the complaints reported increased scrutiny of American-Muslim's social media accounts and contents of their mobile phones along with invasive questions regarding their religious beliefs and political opinions about American Citizens." These examples further the notion that the digital platforms facilitating movement are simultaneously sites of surveillance that instantiate government border policies of control.

## The Ethics of the Digital Passage

As Bedoya (2014) points out, "the survival of our *most* vulnerable communities has often turned on their ability to avoid detection." It is important to interrogate, then, whether networks serve to proactively connect and aid refugees or whether they instead (or also) make them dangerously accessible to harmful systems, policies, or individuals. Bedoya argues that too often the critique of harmful data is focused on its use rather than its capture; the collection of data at every opportunity has become assumed in numerous spheres of life (including the handling of refugees and asylum). However, once collected, data on vulnerable populations can be abused at a later stage, after political winds have changed or public opinion has shifted. Thus, the submission to data collection at borders which might secure refugees a new life abroad might also leave them newly vulnerable to the prejudices that will ultimately limit or hurt their lives in the future.

This critique is of particular importance if refugee populations themselves become aware of the potential negative impact of data-emitting infrastructures. Such knowledge can spark "system avoidance" (Brayne, 2014), where individuals choose unofficial or non-monitored channels and services over those that are official and generate data. And while this can avoid the negative repercussions of unfettered data collection practices by central authorities, such off-the-grid alternatives can also expose refugees to new risks of exploitation and violence, far beyond the reach of law enforcement or relief services. Thus, in examining the realities of the new digital passage, it is important to focus on when data are captured, how data are captured, the purpose for which it is collected, and the (potentially harmful) ends to which it is eventually applied.

Yet, this is not to deny that some forms of government collection of individual data can also be legitimate and even helpful for refugees. According to Lerman (2013, p. 60), "Policymaking increasingly depend[s] on the accuracy of big data and advanced analytics. Exclusion or underrepresentation in government datasets, then, could mean losing out on important government services and public goods." The effective collection and analysis of data therefore also have the potential to significantly improve the fair allocation of goods and services, and hence, improve the overall wellbeing of a community. As Torpey (2000, p. 11) suggests, the functioning of modern states depends on infrastructural control; states "*must* embrace societies *in order to* penetrate them successfully. Individuals who remain beyond the embrace of

the state necessarily represent a limit on its penetration. The *reach* of the state, in other words, cannot exceed its *grasp*." This is also one of the reasons why it is problematic that the EU claims not to collect any personally identifiable information under the Eurosur regulation: registration always also means integration into a community. This is well understood by countries in the Southern European periphery who have repeatedly been chided by fellow EU member states for failing to register the fingerprints of refugees even when they are obliged to do so under Eurodac (Zalan, 2015). On one hand, these states might simply be unable to abide by the rules because their administrations are overwhelmed by the sheer number of arrivals at their borders; on the other hand, one could easily imagine that national authorities also actively neglect to register asylum seekers, precisely to absolve themselves of the responsibility of having to include them in their national bureaucratic apparatuses (e.g., BBC, 2016).

## Looking Ahead: Beyond Technological Solutionism

In February 2016, European government and border control officials met with representatives from a variety of tech companies to develop "technical solutions" to the refugee crisis. The proposals range from "a smartcard ID system" for the distribution of food and services to "tempt[ing] refugees to download tracking apps on their smartphones by offering helpful information about sea crossings and conditions in different EU countries" (Taylor & Graham-Harrison, 2016). At the same time, a group of well-meaning computer scientists, engineers, and startup representatives from across the world have joined forces to organize a series of "techfugee" conferences with a similar goal (Techfugees, 2016). The difference lies in how these actors define "the solution": European government and border control officials are incentivized to utilize digital infrastructures to reinforce physical borders and maximize control over refugees; "digital humanitarians," on the other hand, may seek to develop technologies to facilitate and support the freedom of movement.

There is no easy answer to the question of whether or not the digital passage ultimately benefits or harms vulnerable populations. However, we would urge academics, policymakers, and the tech community alike to grapple with this question *before* experimenting with new technologies in the context of refugee and migration flows. Most importantly, we have to remain mindful that there is not, in fact, "an app for everything" (Latonero, 2016a) and meaningfully addressing the current refugee crisis—one that extends far beyond the borders of Europe moreover—also, if not primarily, requires physical assistance on the ground. At the same time, for those cases in which digital technologies *can* facilitate (or impede upon) the movement of asylum seekers and migrants, the people and institutions demanding and developing those "solutions" need to be cognizant of the particular needs and risks inherent to the refugee experience.

This article has tried to map out the contours of a new digital infrastructure for movement and the ways in which it is navigated by government officials, tech representatives, human traffickers, and the refugees themselves. This focus on refugees exemplifies a broader research approach wherein the dual use nature of technologies can only be understood upon investigating how such technologies play out in specific social contexts—particularly in human rights and humanitarian contexts where vulnerable populations are concerned. As the tools that comprise new digital infrastructures expand in scope and usage in the near future, we should make sure to remain mindful of the ethics of the digital passage, with a particular focus on individual's fundamental rights to privacy, freedom of movement, asylum, and, above all, human dignity.

### Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

### Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

### References

Aas, K. F. (2006). "The body does not lie": Identity, risk and trust in technoculture. *Crime, Media, Culture*, *2*, 143–158.

Aas, K. F. (2007). Analyzing a world in motion: Global flows meet "criminology of the other." *Theoretical Criminology*, *11*, 283–303.

Aas, K. F. (2011a). "Crimmigrant" bodies and bona fide travelers: Surveillance, citizenship and global governance. *Theoretical Criminology*, *15*, 331–346.

Aas, K. F. (2011b). A borderless world? Cosmopolitanism, boundaries and frontiers. In C. M. Baillet & K. F. Aas (Eds.), *Cosmopolitan justice and its discontents* (pp. 134–150). New York, NY: Routledge.

Aas, K. F. (2013). The ordered and bordered society: Migration control, citizenship, and the northern penal state. In K. F. Aas & M. Bosworth (Eds.), *The borders of punishment: Migration, citizenship, and social exclusion* (pp. 20–36). Oxford, UK: Oxford University Press.

Al Jazeera. (2015, October 24). Google launches "crisis info hub" to help refugees. *Al Jazeera*. Retrieved from http://www.aljazeera.com/news/2015/10/google-crisis-info-hub-refugees-151024061606185.html

Alvarez, R. R.Jr. (1995). The Mexican-US border: The making of an anthropology of borderlands. *Annual Review of Anthropology*, *24*, 447–470.

Amoore, L., Marmura, S., & Salter, M. B. (2008). Editorial: Smart borders and mobilities: Spaces, zones, enclosures. *Surveillance & Society*, 5, 96–101.

Anderson, B. (2006). *Imagined communities* (rev. ed.). New York, NY: Verso Books.

Appadurai, A. (1996). *Modernity at large: Cultural dimensions of globalization*. Minneapolis: University of Minnesota Press.

Balibar, E. (1992). *Politics and the other scene*. New York, NY: Verso Books.

Balibar, E. (2004). *We, the people of Europe? Reflections on transnational citizenship*. Princeton, NJ: Princeton University Press.

Bauman, Z. (2012). *Liquid modernity*. Cambridge, MA: Polity Press.

BBC. (2016, March 11). Syria: The story of the conflict. *BBC*. Retrieved from http://www.bbc.com/news/world-middle-east-26116868

Bedoya, A. (2014, November 7). Big data and the underground railroad. *Slate*. Retrieved from http://www.slate.com/articles/technology/future_tense/2014/11/big_data_underground_railroad_history_says_unfettered_collection_of_data.html

Bellanova, R., Jumbert, M. G., & Gellert, R. (2016, October 17). Give us your phone and we may grant you asylum. *Peace Research Institute Oslo Blogs*. Retrieved from https://blogs.prio.org/2016/10/give-us-your-phone-and-we-may-grant-you-asylum/

Benjamin, W. (1999). *The arcades project*. Cambridge, MA: Harvard University Press.

Boehm, F. (2012). *Information sharing and data protection in the area of freedom, security: Towards harmonised data protection principles for information exchange at EU-level*. Berlin, Germany: Springer.

Bowker, G. C., Baker, K., Millerand, F., & Ribes, D. (2010). Toward information infrastructure studies: Ways of knowing in a networked environment. In J. Hunsinger, L. Klastrup, & M. M. Allen (Eds.), *International handbook of Internet research* (pp. 97–115). Berlin, Germany: Springer.

Brayne, S. (2014). Surveillance and system avoidance: Criminal justice contact and institutional attachment. *American Sociological Review*, *79*, 367–391.

Broeders, D. (2007, January). The new digital borders of Europe: EU databases and the surveillance of irregular migrants. *International Sociology*, *22*, 71–92.

Brunwasser, M. (2015, August 25). A 21st-century migrant's essentials: Food, shelter, smartphone. *The New York Times*. Retrieved from http://www.nytimes.com/2015/08/26/world/europe/a-21st-century-migrants-checklist-water-shelter-smartphone.html

Bundesministerium des Innern. (2017). Änderungen zur Erleichterung von Abschiebungen auf den Weg gebracht. Retrieved from http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2017/02/kabinettsbeschluss-ausreisepflicht.html

Castells, M. (1999). Grassrooting the space of flows. *Urban Geography*, *20*, 294–302.

Council on American-Islamic Relations. (2017, January 18). *CAIR-FL files 10 complaints with CBP after the agency targeted and questioned American-Muslims about religious and political views*. Retrieved from https://www.cairflorida.org/newsroom/press-releases/720-cair-fl-files-10-complaints-with-cbp-after-the-agency-targeted-and-questioned-american-muslims-about-religious-and-political-views.html

Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention.

Datta, D. (2015, November 23). Benetech and Yahoo for good discuss technology's role in the refugee crisis. *Benetech's Blog*. Retrieved from http://benetech.org/2015/11/23/benetech-and-yahoo-for-good-discuss-technologys-role-in-the-refugee-crisis/

Dijstelbloem, H. (2009). Europe's new technological gatekeepers: Debating the deployment of technology in migration policy. *Amsterdam Law Forum*, *1*, 11–18.

Dijstelbloem, H., & Broeders, D. (2015). Border surveillance, mobility management and the shaping of non-publics in Europe. *European Journal of Social Theory*, *18*, 21–38.

Drüeke, R. (2016). Mediated communication and migration in Europe: A contribution to the ongoing debate. In A. Amelina, K. Horvath, & B. Meeus (Eds.) An *anthology of migration and social transformation: European perspectives* (pp. 327–340). Berlin, Germany: Springer.

Epstein, C. (2008). Embodying risk: Using biometrics to protect the borders. In L. Amoore & M. de Goede (Eds.), *Risk and the war on terror* (pp. 178–193). New York, NY: Routledge.

European Commission. (2016). *Proposal for a regulation of the European parliament and of the council on the establishment of "Eurodac" for the comparison of fingerprints for the effective application of (Regulation [EU] No 604/2013 establishing the criteria and mechanisms for determining the member state responsible for examining an application for international protection lodged in one of the member states by a third-country national or a stateless person), for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by member states' law enforcement authorities and Europol for law enforcement purposes (recast)*. Retrieved from http://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-272-EN-F1-1.PDF

European Commission, European Migration Network. (2016). The Use of Social Media in the Fight Against Migrant Smuggling. Retrieved from http://www.emn.lv/wp-content/uploads/emn-informs00_emn_inform_on_social_media_in_migrant_smuggling.pdf

Europol European Migrant Smuggling Centre. (2017). *First year activity*. Retrieved from https://www.europol.europa.eu/sites/default/files/documents/european_migrant_smuggling_centre_emsc_-_first_year_activity_year_1.pdf

Europol and Interpol. (2016). *Migrant smuggling networks*. Retrieved from https://www.europol.europa.eu/sites/default/files/documents/ep-ip_report_executive_summary.pdf

Facebook. (2016). Safety resources. *Facebook*. Retrieved from https://www.facebook.com/safety/resources

Fassin, D. (2011). Policing borders, producing boundaries: The governmentality of immigration in dark times. *Annual Review of Anthropology*, *40*, 213–246.

Feldman, G. (2012). *The migration apparatus: Security, labor, and policymaking in the European Union*. Stanford, CA: Stanford University Press.

Frouws, B., Phillips, M., Hassan, A., & Twigt, M. (2016, June). Getting to Europe the "WhatsApp" way. *Regional Mixed Migration Secretariat*. Retrieved from http://reliefweb.int/report/world/briefing-paper-2-getting-europe-whatsapp-way-use-ict-contemporary-mixed-migration-flows

Gammeltoft-Hansen, T. (2013). *Access to asylum: International refugee law and the globalisation of migration control*. Cambridge, UK: Cambridge University Press.

Gammeltoft-Hansen, T., & Sørensen, N. N. (Eds.). (2013). *The migration industry and the commercialization of international migration*. New York, NY: Routledge.

Hegde, R. (2016). *Mediating migration*. Cambridge, UK: Polity Press.

Heymann, J. M., & Symons, J. (2012). Borders. In D. Fassin (Ed.), *A companion to moral anthropology* (pp. 540–557). West Sussex, UK: John Wiley.

Huysmans, J. (2006). *The politics of insecurity: Fear, migration and asylum in the EU* (New International Relations). New York, NY: Routledge.

Inda, J. X., & Rosaldo, R. (2008). Tracking global flows. In J. X. Inda & R. Rosaldo (Eds.), *The anthropology of globalization: A reader* (2nd ed., pp. 3–46). Malden, MA: Blackwell Publishing.

Kingsley, P. (2015, May 8). People smugglers using Facebook to lure migrants into "Italy trips." *The Guardian*. Retrieved from http://www.theguardian.com/world/2015/may/08/people-smugglers-using-facebook-to-lure-migrants-into-italy-trips

Kozlowska, H. (2015, September 14). The most crucial item that migrants and refugees carry is a smartphone. *Quartz*. Retrieved from http://qz.com/500062/the-most-crucial-item-that-migrants-and-refugees-carry-is-a-smartphone/

Larkin, B. (2013). The politics and poetics of infrastructure. *Annual Review of Anthropology*, *42*, 327–343.

Latonero, M. (2011). *Human trafficking online: The role of social networking sites and online classifieds*. Los Angeles, CA: USC Annenberg Center on Communication Leadership & Policy.

Latonero, M. (2012). *Technology and human trafficking report: The rise of mobile and the diffusion of technology-facilitated trafficking*. Los Angeles, CA: USC Annenberg Center on Communication Leadership & Policy.

Latonero, M. (2016a, May 23). An app to save Syria's lost generation? *Foreign Affairs*. Retrieved from https://www.foreignaffairs.com/articles/syria/2016-05-23/app-save-syrias-lost-generation

Latonero, M. (2016b, February 1). Refugees' new infrastructure for movement: A digital passage. *Data & Society*. Retrieved from https://points.datasociety.net/refugees-new-infrastructure-for-movement-d31c3ab53b20#.wxiltwxst

Latonero, M., Wex, B., & Dank, M. (2015). *Technology and labor trafficking in a network society: General overview, emerging innovations, and Philippine case study*. Los Angeles, CA: USC Annenberg Center on Communication Leadership & Policy.

Lerman, J. (2013, September 3). Big data and its exclusions. *Stanford Law Review Online*, *66*, 55–63.

Leurs, K. (2015). *Digital passages: Migrant youth 2.0: Diaspora, gender and youth cultural intersections*. Amsterdam, The Netherlands: Amsterdam University Press.

Madianou, M. (2014). Polymedia communication and mediatized migration: An ethnographic approach. In K. Lundby (Ed.), *Mediatization of communication* (pp. 323–248). Berlin, Germany: De Gruyter.

Maguire, M. (2009). The birth of biometric security. *Anthropology Today*, *25*(2), 9–14.

Mason, M. (2012, October 29). Facebook used to kidnap, traffic Indonesian girls. *USA Today*. Retrieved from http://www.usatoday.com/story/news/world/2012/10/29/facebook-used-to-kidnap-traffic-indonesian-girls/1665321/

Mavris, L. (2002, December). *Human smugglers and social networks: Transit migration through the states of former Yugoslavia. UNHCR*. Retrieved from http://www.unhcr.org/research/working/3e19aa494/human-smugglers-social-networks-transit-migration-states-former-yugoslavia.html

Mitsilegas, V. (2012). Immigration control in an era of globalization: Deflecting Foreigners, weakening citizens, strengthening the state. *Indiana Journal of Global Legal Studies*, *19*(1), 3–60.

Naylor, B. (2017, February 9). Homeland security secretary: Travel vetting could include passwords, Tweets. *National Public Radio*. Retrieved from http://www.npr.org/2017/02/09/514175464/homeland-security-secretary-travel-vetting-could-include-passwords-tweets

Obama, B. (2016). Remarks by President Obama at call to action CEO roundtable. *The White House*. Retrieved from https://www.whitehouse.gov/the-press-office/2016/09/20/remarks-president-obama-call-action-ceo-roundtable

Organization for Economic Co-operation and Development. (2015). *Can we put an end to human smuggling? OECD*. Retrieved from https://www.oecd.org/migration/Can%20we%20put%20an%20end%20to%20human%20smuggling.pdf

Papastergiadis, N. (2000). *The turbulence of migration*. Cambridge, UK: Polity Press.

Pötzsch, H. (2015). The emergence of iBorder: Bordering bodies, networks, and machines. *Environment and Planning D: Society and Space*, *33*, 101–118.

Ram, A. (2015, December 15). Smartphones bring solace and aid to desperate refugees. *Wired*. Retrieved from http://www.wired.com/2015/12/smartphone-syrian-refugee-crisis/

Regulation (EU) No. 1052/2013 of the European Parliament and the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur).

Regulation (EU) No. 603/2013 of the European Parliament and the Council of 26 June 2013 on the establishment of "Eurodac" for the comparison of fingerprints for the effective application of Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the member state responsible for examining an application for international protection lodged in one of the member states by a third-country national or a stateless person and on requests for the comparison with Eurodac data by member states' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No. 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security, and justice (recast).

Roberts, J. (2015, October 8). How Facebook will fight sex trafficking. *Fortune*. Retrieved from http://fortune.com/2015/10/08/facebook-sex-trafficking

Romm, T. (2016, December 22). US government begins asking foreign travelers about social media. *Politico*. Retrieved from http://www.politico.com/story/2016/12/foreign-travelers-social-media-232930

Saleh, H. (2015, April 24). Human traffickers advertise their trade on Facebook. *Financial Times*. Retrieved from http://www.ft.com/intl/cms/s/0/b1a55608-ea79-11e4-a701-00144feab7de.html

Schmidle, N. (2015, October 26). Ten borders: A Syrian refugee's epic escape from Syria. *The New Yorker*. Retrieved from http://www.newyorker.com/magazine/2015/10/26/ten-borders

Schwell, A. (2014). Compensating (In)security: Anthropological perspectives on internal security. In M. Maguire, C. Frois, & N.

Zurawski (Eds.), *Anthropology of security: Perspectives from the frontline of policing, counter-terrorism and border control* (pp. 83–103). London, England: Pluto Press.

Specia, M. (2015, July 3). WhatsApp offers lifeline for Syrian refugees on journey across Europe. *Mashable*. Retrieved from http://mashable.com/2015/07/03/syrians-europe-whatsapp-refugees/#anXMyaVlxsqJ

Taylor, D., & Graham-Harrison, E. (2016, February 18). EU asks tech firms to pitch refugee-tracking systems. *The Guardian*. Retrieved from http://www.theguardian.com/world/2016/feb/18/eu-asks-tech-firms-to-pitch-refugee-tracking-systems

Techfugees. (2016). About Techfugees. Retrieved from http://techfugees.com/about/

Todtmann, F., & Edlbe, B. (2015, December 7). How a paraplegic Syrian man became an emergency lifeline for thousands of refugees. *Vice*. Retrieved from http://www.vice.com/read/how-a-paraplegic-syrian-became-an-emergency-life-line-for-thousands-of-refugees-876

Torpey, J. (2000). *The invention of the passport: Surveillance, citizenship and the state*. Cambridge, UK: Cambridge University Press.

UN Office of Drugs Crime. *On human trafficking and migrant smuggling.* Retrieved from https://www.unodc.org/unodc/human-trafficking/(accessed March 1 2018)

Van Houtum, H., & van Naerssen, T. (2002). Bordering ordering, and othering. *Tijdschrift Voor Economische En Sociale Geografie*, *93*, 125–136.

Zalan, E. (2015, December 10). EU launches migration cases against Croatia, Greece, Hungary, and Italy. *EU Observer*. Retrieved from https://euobserver.com/migration/131479

## Author Biographies

Mark Latonero (PhD, University of Southern California [USC]), is the lead researcher on Human Rights at the Data and Society Research Institute and a senior fellow at the USC Annenberg School and Leiden University. His research investigates the development and application of data-driven technologies in human rights and humanitarian contexts.

Paula Kift (MA, New York University [NYU], MPP, Hertie School of Governance), began working on privacy, transborder data flows and the ethics of migration in the context of the doctoral program in Media, Culture, and Communication at NYU, which she since left with a master's degree in the fall of 2016. She currently works as a Privacy and Civil Liberties Engineer at Palantir Technologies, and plans to finish writing her dissertation in Europe. All views expressed are her own.