Selected Papers of AoIR 2016:
The 17th Annual Conference of the
Association of Internet Researchers
Berlin, Germany / 5-8 October 2016

IN SEARCH OF SAFE HARBORS – PRIVACY AND SURVEILLANCE OF REFUGEES AT THE BORDERS OF EUROPE

Paula Kift
New York University

Introduction

Over the course of 2015, more than a million refugees and migrants arrived at the borders of Europe. One of the ways in which the European Union (EU) attempted to manage the continuous inflow of people was through the collection of vast amounts of personal information; information that is not only used to assess and process asylum claims but also to prevent irregular migration and to alleviate national security concerns. Two EU regulations are particularly noteworthy in this regard: Eurosur (mandating drone and satellite surveillance of the Mediterranean Sea)[1] and Eurodac (biometric information collection at the border).[2] While biometric data collection under Eurodac clearly raises both privacy and data protection concerns, as defined in European law, Eurosur is said to raise neither because drone and satellite surveillance of the Mediterranean Sea only involves the collection of information about boats, but not the collection of any personally identifiable information (PII) of the passengers on those boats. The following paper questions the soundness of this argument. More specifically, it argues that while anonymity in this case protects against *identifiability*, it does not protect against *reachability*; the latter arguably being a much more important privacy concern in the age of big data.

Eurodac and Eurosur

The Eurodac regulation was introduced in the European Parliament on December 11, 2001.[3] 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

1. Regulation (EU) No. 1052/2013 of the European Parliament and the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur) [hereinafter: Eurosur Regulation].
2. Regulation (EU) No. 603/2013 of the European Parliament and the Council of 26 June 2013 on the establishment of 'Eurodac' [hereinafter: 2013 Eurodac Regulation].
3. 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 [hereinafter: 2000 Eurodac Regulation].

Suggested Citation (APA): Kift, P. (2016, October 5-8). *In Search of Safe Harbors: Privacy and Surveillance of Refugees at the Borders of Europe.* Paper presented at AoIR 2016: The 17th Annual Conference of the Association of Internet Researchers. Berlin, Germany: AoIR. Retrieved from http://spir.aoir.org.

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 towards 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"[4] and thus to prevent asylum seekers from filing multiple asylum applications.[5] In June 2013, the mandate of the Eurodac regulation was expanded to also allow European law enforcement agencies access to the database.[6] Finally, in May 2016,[7] the European Commission published a proposal to collect not only fingerprints but also facial recognition data under the Eurodac regulation,[8] to lower the minimum age for inclusion in the database from 14 to 6[9] and to extend the data retention period from 18 months to five years.[10] Finally, in May 2016, the European Commission published a proposal to collect not only fingerprints but also facial recognition data under the Eurodac regulation, to lower the minimum age for inclusion in the database from 14 to 6 and to extend the data retention period from 18 months to five years.

The Eurosur regulation, on the other hand, was adopted on October 22, 2013.[11] 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 illegal immigration and cross-border crime and contributing to ensuring the protection and saving the lives of migrants."[12] Towards 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 (NCCs) and the use of sophisticated surveillance tools, such as satellite imagery and drones.[13] Importantly, in order to maintain pre-frontier intelligence pictures, the EU not only monitors its own external land and maritime borders, but also the borders of neighboring third countries. Towards this end, the Eurosur regulation explicitly encourages information sharing and cooperation with those countries.[14]

---

4. *Id.* at para. 3.
5. See Franziska Boehm, INFORMATION SHARING AND DATA PROTECTION IN THE AREA OF FREEDOM, SECURITY: TOWARDS HARMONISED DATA PROTECTION PRINCIPLES FOR INFORMATION EXCHANGE AT EU-LEVEL 305 (2012).
6. *See* 2013 Eurodac Regulation *supra* note 2.
7. European Commission, *Proposal for a Regulation of the European Parliament and 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)*, EUROPEAN COMMISSION 2 (May 4, 2016), http://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-272-EN-F1-1.PDF.
8. *Id.* at 12-13.
9. *Id.* at 6.
10. *Id.* at 4.
11. *See* Eurosur Regulation *supra* note 1.
12. *Id.* para 1.
13. *Id.* Article 12(3)c.
14. *Id.* Article 20.

The Rights to Privacy and Data Protection as Applied to Eurodac and Eurosur

The fundamental right to *privacy* is anchored in Article 8 of the European Convention on Human Rights (ECHR), which is closely mirrored by Article 7 of the Charter of Fundamental Rights of the European Union (CFREU). It stipulates that "Everyone has the right to respect for his private and family life, his home and his correspondence." The CFREU, moreover, also includes a separate right to *data protection* according to which "Everyone has the right to the protection of personal data concerning him or her." The applicability of the right to privacy in European law, then, is defined by whether a government's actions impinge on a person's "private life" whereas the applicability of the right to data protection depends upon the presence of "personal data" which is defined as "any information relating to an identified or identifiable natural person" in Art. 2 Directive 95/46/EC (the EU Data Protection Directive).

While biometric data collection under Eurodac clearly raises both privacy and data protection concerns, as defined in European law, Eurosur is said to raise neither because drone and satellite surveillance of the Mediterranean Sea only involves the collection of information about boats, but not the collection of any personally identifiable information (PII) of the passengers on those boats. The continued reliance of the right to data protection on the presence of "personal data" is thus a serious limitation in this case.

A person's private life, by contrast, can be affected by a public authority's data collection practices*, even when no PII is being collected*. In the case of Eurosur, even if drones and satellites do not enable the EU to identify *who* these passengers are, they do enable the EU to identify *what* they are, namely, irregular migrants and possibly refugees in need of international protection. While anonymity in this case protects against *identifiability*, it does not protect against *reachability*.[15] Indeed, somewhat paradoxically, in this case it may actually be the *refusal* of EU authorities to collect PII about the passengers on these boats that raises fundamental rights concerns since they are collectively classified as "illegal" migrants and potentially sent back to their ports of origin without first establishing whether there are refugees with international protection claims among them.

Privacy and Data Protection in an Age of Big Data

The implications of these findings are not limited to the applicability of the rights to privacy and data protection to migrants and asylum seekers at the borders of Europe. Rather, they encourage us to look ahead and to reflect on the continued viability of the rights to privacy and data protection in an age of big data more generally. As notable

15. For a discussion of anonymity as unreachability, *see* Helen Nissenbaum, *The Meaning of Anonymity in an Information Age*, 15 INFO. SOC. 141, 142 (1999) (arguing that "the value of anonymity lies not in the capacity to be unnamed, but in the possibility of acting or participating while remaining out of reach, remaining unreachable"). *See also* Solon Barocas and Helen Nissenbaum*, Big Data's End Run Around Anonymity and Consent*, in PRIVACY, BIG DATA AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 45 (Julia Lane et al. eds., 2015) (arguing that "[e]ven when individuals are not 'identifiable', they may still be 'reachable', may still be comprehensibly represented in records that detail their attributes and activities, and may be subject to consequential inferences and predictions taken on that basis").

privacy scholars have pointed out, rapid technological advances in the areas of data collection and processing have rendered the concepts of PII and anonymity mostly meaningless, as even the most innocuous seemingly unconnected bits and pieces of data might be recombined to constitute "personal data" and thus raise significant privacy concerns.[16] Furthermore, as public and private actors increasingly make profiles about us, they could easily argue that their practices do not raise any privacy or data protection concerns because their profiles are not concerned with the *identity* of the people they are targeting, but only their *characteristics*. This may suggest that the right to privacy is ultimately better suited to protect us against both private and public sector intrusions in the future. This is because, unlike the right to data protection, the right to privacy not only regulates the lawful processing of personal data, but it also provides us with the freedom of not having any data about us processed to begin with – regardless of whether that information is ultimately accurate or "personally identifiable."

References

Barocas, Solon and Helen Nissenbaum*, Big Data's End Run Around Anonymity and Consent*, in PRIVACY, BIG DATA AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 44-75 (Julia Lane et al. eds., 2015).

Boehm, Franziska. INFORMATION SHARING AND DATA PROTECTION IN THE AREA OF FREEDOM, SECURITY: TOWARDS HARMONISED DATA PROTECTION PRINCIPLES FOR INFORMATION EXCHANGE AT EU-LEVEL (2012).

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.

Narayanan, Arvind and Vitaly Shmatikov, *Myths and Fallacies of 'Personally Identifiable Information'*, 53 Comm. of the ACM 24 (2010).

Nissenbaum, Helen, *The Meaning of Anonymity in an Information Age*, 15 INFO. SOC. 141 (1999).

Ohm, Paul, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

Rubinstein, Ira and Woodrow Hartzog, *Anonymization and Risk*, 91 WASHINGTON L. REV. (forthcoming 2016).

16. On the failures of anonymization, *see* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010); and Ira Rubinstein and Woodrow Hartzog, *Anonymization and Risk*, 91 WASHINGTON L. REV. (forthcoming 2016). On the increasing difficulty to define what constitutes PII, *see* Paul M. Schwartz and Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814 (2011); and Arvind Narayanan and Vitaly Shmatikov, *Myths and Fallacies of 'Personally Identifiable Information'*, 53 COMM. OF THE ACM 24 (2010).

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'.

Schwartz, Paul M. and Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814 (2011).