Prioritizing Fair Information Practice Principles Based on Islamic Privacy Law

Ayesha Rasheed*

All global privacy law is, to varying degrees, based upon the Organization for Economic Cooperation and Development's Fair Information Practice Principles (FIPPs). Though first developed in 1973, few have questioned the extent to which the FIPPs and subsequent regulations operationalizing them account for non-Western (i.e. non-neoliberal) legal and cultural systems. But given the increasingly international character of data flows and the number of non-European countries now enacting national data privacy laws for the first time, that oversight should be remedied. In particular, nations that observe some form of Islamic law or culture have rich histories of discourse that speak directly to definitions of privacy interests and methods of privacy protections. Those studying data privacy in these nations or looking to move information to and from them should be mindful of Islamic perspectives on privacy and encourage greater examination of such perspectives' intersection with extant data privacy regimes.

DOI: https://doi.org/10.15779/Z38P843W74

*. J.D., University of California, Berkeley, School of Law; M.Sc., University of Oxford; B.S. with Honors, Stanford University. Many thanks to Talha Aziz Mirza (J. D. Candidate, University of California, Berkeley, School of Law '21) for his patience and thoughtful edits, to Sabreen Ahsan (University of Oxford, '16) for guiding me through a maze of hadith, Adil Tobaa (University of Chicago, '16) for helping me parse words in Arabic and English, and the vibrant Muslim community of the Bay Area. Errors and oversights are my own.

INTRODUCTION

For decades, the Organization for Economic Cooperation and Development's (OECD) Fair Information Practices (FIPPs) have formed the bedrock of global data privacy law.[1] However, by their nature and stated purpose, the FIPPs reflect primarily – if not exclusively – Eurocentric beliefs about what data privacy means and how it should be used to order society.

First formed to administer American and Canadian aid for the post-World War II reconstruction of Europe,[2] the OECD included just six non-European countries at the time the FIPPs were promulgated.[3] And, of those six geographically non-European nations, at least four were heavily influenced by European values and norms. Now, almost a half-century later, only Mexico, South Korea, Israel, and Chile have joined those ranks.[4] Notably missing from the OECD's membership list (except for Turkey) are nations that observe some form of Islamic law, Islamic culture, or both. This raises a question: to what degree are the FIPPs that undergird modern privacy laws representative of non-European data privacy values?

Because the European Union's data protection laws follow its citizens internationally, are hugely influential globally,[5] and appear to be inspiring look-alike laws in predominantly Muslim countries such as the United Arab Emirates and Bahrain,[6] such a question is worth asking. To date,

---

1. *See* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L. J. 115, 128 (2017)(observing that the FIPPs are "found in the EU at the constitutional level as well as in statutory law," most notably within both the General Data Protection Regulation (GDPR) and its predecessor, the European Directive on Data Protection); *see also* Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771 (2019)(exploring the EU's leading role in influencing global data protection standards and the global diffusion of its philosophical approach to data privacy).

2. *See* Warren Christopher, IN THE STREAM OF HISTORY: FOREIGN POLICY FOR A NEW ERA 165 (1998).

3. The six OECD countries not located on the European continent were Australia, Canada, Japan, New Zealand, Turkey, and the United States. *See List of OECD Member Countries*, OECD, https://www.oecd.org/about/document/list-oecd-member-countries.htm (last visited Mar. 15, 2020).

4. *See id*.

5. *See generally* Schwartz, *Global Data Privacy*, *supra* note 1.

6. *See* Naushad K. Cherrayil, *UAE Data Protection Law, Similar to GDPR, Likely Landing This Year*, TECHRADAR (June 24, 2019), https://www.techradar.com/news/uae-data-protection-law-similar-to-gdpr-likely-landing-this-year.

while some effort has been made to smooth adoption of the European Union's General Data Protection Regulation (GDPR) in Gulf countries with close economic ties to Europe,[7] little attention has been given to first principles regarding data privacy in Islam or, more generally, how the increasingly "narrow, legalistic"[8] FIPPs may be utilized with greater cultural sensitivity.

This Note observes that the European data protection laws now being used to fill the void of specific data protection laws in Muslim majority nations were largely informed by a set of specific goals related to administrative and economic efficiency. In contrast, by the letter of its primary texts, Islam values privacy as a fundamental human right. It would be wrong, therefore, to imply via juxtaposition that the European Union's legal system stands alone (or even foremost) in treating privacy as a human right.[9]

This Note highlights an underdeveloped field of study that is of value to Muslim nations and those seeking to move data to and from them. Islamic jurisprudence and philosophy contain centuries-worth of rich sources of scholarly dialogue on privacy topics, though much of it is overlooked in the West due to the lack of English-language translations and ready access to source materials.[10] The scope and difficulty in defining the "Muslim world" also contribute to this gap in academic exchange, as

---

7. *See, e.g.*, *Data Privacy Frameworks in MENA: Emerging Approaches and Common Principles*, GSM ASSOCIATION (June 2019); *see also* Mireille M. Caruana & Joseph A. Cannataci, *European Union Privacy and Data Protection Principles: Compatibility with Culture and Legal Frameworks in Islamic States*, 16 INFO. & COMM. TECH. L. 99, 111 (2007) (comparing, broadly, data protection laws in Jordan and Tunisia against those of the EU).

8. *See* Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY (Jane K. Winn, ed., 2006).

9. *See, e.g.*, Christopher G. Weeramantry, JUSTICE WITHOUT FRONTIERS: FURTHERING HUMAN RIGHTS 132-33 (1997) (noting that Islamic jurisprudence advanced the legal principle of a right of privacy almost from Islam's inception, while most modern legal systems such as English common law evolved the right much later and largely in the context of modern electronics).

10. *See* Intisar A. Rabb & Sharon Tai, *Digital Islamic Law: Purpose and Prospects*, 50 CAMBRIDGE U. PRESS 113 (2018) (describing a "persistent problem of access and ease of use" in Islamic law). Notably, English is also the *lingua franca* of modern Internet and computing technology. Arabic is well-documented as losing significant context and nuance when translated to English, as several common word categories require deep knowledge of custom and culture and/or represent concepts that have no equivalent in English. *See, e.g.*, Oukab Chahrour, *Cultural Difficulties in Translations from English Into Arabic*, TRANS. J. (April 2017).

does the misconception that Islamic law is monolithic.[11] For these reasons alone, this Note hopes to serve primarily as a small spark for further study in Islamic data privacy law, and as a call for more cross-cultural studies in data privacy laws generally. The latter are woefully few, despite both the global nature of data flows and possible future risks to privacy and cybersecurity arising from forms of technological colonialism.[12]

This Note proceeds in three parts. Part I briefly describes the origins of the FIPPs in an American federal advisory committee report and the FIPPs' subsequent influence on major data protection laws. It also states what the principles are. Part II then details core concepts from Islamic law relating to privacy protection, such as prohibitions on eavesdropping and spying, and protection of individuals' personal dignity and reputation. Finally, Part III evaluates how FIPPs might be best weighted to ensure better conformity to the values observed in Part II, should they be further incorporated into future data protection laws in Islamic countries.

I. ADMINISTRATIVE AND ECONOMIC MOTIVES BEHIND THE OECD'S FAIR INFORMATION PRACTICES

The FIPPs are broad guidelines frequently used as model rules for laws governing the collection and use of personal data.[13] Their influence is hard to understate: the guidelines recommended by the OECD in 1980 have gone on to become the foundation for most national and international laws governing data protection.[14]

Yet for all their success in creating a global language of privacy, the

11. There are over 1.5 billion Muslims worldwide, and they also represent the majority of populations from Southeast Asia to Sub-Saharan Africa. The Organization of the Islamic Conference alone comprises fifty-seven states across four continents. *See History*, ORG. OF ISLAMIC COOPERATION, https://www.oic-oci.org/page/?p_id=52&p_ref=26&lan=en (last visited Mar. 29, 2020). For a review of constitutional structures and legal systems in the modern Middle East, *see generally* Nathan J. Brown, CONSTITUTIONS IN A NONCONSTITUTIONAL WORLD: ARAB BASIC LAWS & THE PROSPECTS FOR ACCOUNTABLE GOVERNMENT (2001).

12. *See, e.g.*, Michael Kwet, *Digital Colonialism is Threatening the Global South*, AL JAZEERA NEWS (Mar. 13, 2019), https://www.aljazeera.com/indepth/opinion/digital-colonialism-threatening-global-south-190129140828809.html.

13. *A Review of the Fair Information Principles: The Foundation of Privacy Public Policy*, PRIVACY RTS. CLEARINGHOUSE (Oct. 1, 1997), https://privacyrights.org/resources/review-fair-information-principles-foundation-privacy-public-policy.

14. *See* Fred H. Cate, Peter Cullen & Viktor Mayer-Schönberger, *Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines*, OXFORD INTERNET INST. 2 (2013).

FIPPs are deficient in many ways. Scholars have repeatedly shown that the FIPPs are imperfect as both a normative framework and as a set of ready-made data privacy rules.[15] For purposes of this Note, the FIPPs' American origins, institutional economic policy goals, and correspondingly restricted underlying philosophy merit special scrutiny because they cast doubt upon the appropriateness of using the FIPPs for crafting data privacy laws in non-European legal systems when unchanged from the form in which Western privacy laws have operationalized them.[16]

The FIPPs' limited perspective on privacy is apparent from its inception. The committee that prepared the 1973 advisory report for the U.S. Department of Health, Education and Welfare from which the FIPPs originated was comprised entirely of Americans, all of whom were charged with a specific task of domestic scope. Concerned by the growing computerization of personal record-keeping practices in the context of "large-scale government information collection programs that were essential for the delivery of some social good,"[17] such as food stamp distribution and accurate census counts, the committee's duty was to identify the likely consequences of increased automation amongst federal agencies and recommend safeguards and remedies for potentially harmful consequences.[18]

The committee's five-point "Code of Fair Information Practice" necessarily reflects its narrow scope. First, committee members appear to have never lost sight of the political nature of their task. For example,

---

15. *See, e.g.*, Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952 (2017); Graham Greenleaf, *It's Nearly 2020, So What Fate Awaits the 1980 OECD Privacy Guidelines?,* 159 PRIVACY LAWS & BUS. INT'L REP. 18 (2019); Hon. Michael Kirby, *The History, Achievement and Future of the 1980 OECD Guidelines On Privacy*, 1 INT'L DATA PRIVACY L. 6 (2011).

16. Much ink has been spilled comparing and contrasting American privacy law and EU data protection regimes. *See, e.g.*, Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the U.S. and EU*, 102 CALIF. L. REV. 877 (2014). This Essay acknowledges that European-based or "Western" privacy law is by no means homogenous, but assumes for the sake of limiting the Essay's scope that the FIPPs represent an upstream point of overlap between American and European privacy approaches.

17. *See* Hoofnagle, *The Origin of Fair Information Practices: Archive of the Meetings of the Secretary's Advisory Committee on Automated Personal Data Systems* (SACAPDS), BERKELEY CTR. FOR L. & TECH. (Jan. 1, 2016, 11:28 AM), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2466418.

18. *See Preface*, U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf (stating that the Report was made to the United States Secretary of Health, Education, and Welfare in response to concerns "about the harmful consequences that may result from uncontrolled application of computer and telecommunications technology to the collection, storage, and use of data about individual citizens").

because the Report's development (1971-73) coincided with the Watergate scandal (1972-74), the committee chose to limit travel to liberal states like California when gathering information on industry practices, so as to prevent news coverage from painting privacy as a partisan issue.[19] Second, committee talks fixated on issues of importance to the American administrative state, including the collection of census records, use of Social Security numbers, credit reporting practices under the Fair Credit Reporting Act, and court record disclosure issues raised by Watergate.[20] Unsurprisingly, the Report therefore emphasized measures that would promote transparency in data collection practices and thereby foster public trust in government.[21] Other countries' burgeoning privacy laws (in Sweden, Britain, Canada, and Hessen) went unmentioned until the fifth of the committee's nine planning meetings, and even then, only efforts in Canada were discussed in detail.[22] From the group's first meeting, it was also apparent that the committee was both guided by the American federal "amorphous, constitutional sense of privacy" described to them by law professor Arthur Miller, and concerned almost exclusively with how their recommendations might conform to it.[23]

The OECD later used the committee's recommendations to create the FIPPs in 1980, and it is that version that has substantially influenced global data protection laws.[24] Yet, just as the U.S. advisory committee's

---

19. *See* Hoofnagle, *supra* note 17.

20. *See id*.

21. *See The Code of Fair Information Practices*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/consumer/code_fair_info.html (last visited Dec. 18, 2019).

22. *See* Hoofnagle, *supra* note 17. Administrative control of the central German lands of Hesse was divided between France and the United States after World War II: the committee's references to "Hessen" likely refer to the portion of Hesse administered by the latter.

23. *See id*. (describing an influential lecture by Professor Miller on the United States Constitution at the group's first meeting, his reminders of constitutional rights of privacy throughout, and "powerful testimony" by attorneys from the American Civil Liberties Union regarding infringement of individuals' First, Fourth, and Fifth Amendment rights as a result of government surveillance). *See also* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, *supra* note 18, at 4, 20 (discussing the importance of accurate record-keeping to the promotion of American democracy). Though primarily a professor of civil procedure and copyright law, Miller had published a book, *Assault on Privacy*, in 1971 that identified privacy threats from computerization for a public audience. *See Faculty Profile: Arthur Miller*, N.Y.U. SCHOOL OF LAW, (accessed Apr. 14, 2020) https://its.law.nyu.edu/facultyprofiles/index.cfm?fuseaction=profile.biography&personid=20130.

24. *See* Pam Dixon, *A Brief Introduction to Fair Information Practices*, WORLD PRIVACY FORUM (Dec. 19, 2007), https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/. However, the FIPPs have been restated

American members and particular policy goals colored their recommendations, so too are the FIPPs reflective of the OECD's tightly cabined membership and institutional raison d'être. As was noted in the Introduction, though the OECD purports to be a truly "international" organization, only a third of its members are not geographically located in Europe.[25] And, from that subset, just one has a Muslim-majority population.[26] In fact, Justice Kirby, the Australian chairman of the OECD committee that formulated the FIPPs, has himself speculated that he was only appointed to his post as a compromise between member states because "the Europeans could not tolerate the idea of a non-European chair for the expert group."[27]

More telling is the economic focus of the OECD's stated mission, both in general and in promulgating the FIPPs. Indeed, as Justice Kirby pointed out, "One normally thinks of the OECD as a body of sober economists, statisticians, and technologists. . . Ordinarily, the OECD is not concerned with human rights protection."[28] Rather, it is "an organization concerned with economic efficiency. . . [and] the proper operation of democratic governance and free market economies."[29] In the 1970s, the OECD worried that, should different countries (particularly those on either side of the North Atlantic) institute substantially dissimilar laws governing transborder data flows, those laws' "restrictions, regulations, and even treaties. . . [would] impose 'barriers' on the free flow of data."[30] That flow of data, at the time, fueled a growing sector of its member states' economies in industries like banking and insurance.[31] Thus, the FIPPs were developed to harmonize national privacy legislation to stimulate commerce in (almost entirely) Western countries – upholding human rights was important insofar as it stymied more stringent legal

several times, and there seems to be no enumeration of them that all parties agree upon. Even so, about a hundred countries worldwide have a data privacy law that includes some version of the FIPPS. *See* Graham Greenleaf, *Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories*, 23 J.L. INFO & SCI. 4 (2014); GRAHAM GREENLEAF, GLOBAL TABLES OF DATA PRIVACY LAWS AND BILLS (3d ed. 2013), http://ssrn.com/abstract=2280875.

25. *See List of OECD Member Countries*, *supra* note 3.

26. *See id*.

27. Kirby, *supra* note 15, at 7.

28. *Id*. at 6-7.

29. *Id*. at 8.

30. *See id*.

31. *See OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD (1980), http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

interruptions in international data flows.[32]

In this way, the FIPPs are rooted in the assumption that free flow of information is necessary and good, and are structured predominantly to foster globalization and easy access to the data trade rather than protection of personal privacy or accommodation of different cultures of privacy. As Professor Woodrow Hartzog observes, there are "many different possible conceptions of privacy: control, secrecy, intimacy, dignity, autonomy, trust, the right to be let alone, limited access to the self, personhood, and more. Data protection laws could revolve around any of them."[33] Yet, not only do the FIPPs frame privacy almost exclusively in terms of control, they leave little room for other conceptions of privacy to breathe. That choice cannot be accidental: while it is easy to pick out an intellectual lineage between the FIPPs' control conceptualization of privacy and classic Enlightenment philosophies regarding autonomy and democracy,[34] a control model wherein "users are given control when they are given notice of a company's information practices [and] once that permission is granted. . . the data spigot keeps pouring"[35] powerfully serves free market economic interests.

As articulated in the OECD's Guidelines from 1980, the eight FIPPs are as follows:[36]

- **Collection Limitation Principle**: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data Quality Principle**: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary . . . should be accurate, complete and kept up-to-date.
- **Purpose Specification Principle**: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not

32. *See id*.

33. *See* Hartzog, *supra* note 15, at 959-60.

34. *See e.g.*, Marco De Boni & Martyn Prigmore, *Cultural Aspects of Internet Privacy*, (2002). Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.14.6032&rep=rep1&type=pdf. (describing how "the right to privacy. . . derives from the empiricist and liberal philosophy of thinkers such as Hobbes and Locke. . . [and how] this tradition cannot claim to be universal, as even in the context of "Western" [philosophy]").

35. *See* Hartzog, *supra* note 15, at 959-60.

36. *See OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, *available at* https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm)(1980, expanded in 2013).

incompatible with those purposes and as are specified on each occasion of change of purpose.

- **Use Limitation Principle**: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified . . . except: a) with the consent of the data subject; or b) by the authority of law.
- **Security Safeguards Principle**: Personal data should be protected by reasonable security safeguards.
- **Openness Principle**: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
- **Individual Participation Principle**: An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
- **Accountability Principle**: A data controller should be accountable for complying with measures that give effect to [these] principles.

II. PRIVACY PRINCIPLES FROM ISLAMIC LAW

Islamic texts and jurisprudence[37] leave no doubt that privacy was expected and required in numerous contexts. Chief among Islamic privacy values was privacy of the home and of personal affairs, and those values were operationalized through mechanisms such as prohibitions on eavesdropping and espionage. Additionally, Islamic privacy laws sought to protect individuals' personal dignity and reputation beyond the home by, for instance, prohibiting the opening of another's personal correspondence and discouraging the spread of suspicion and gossip.

37. This Essay cannot do justice to the myriad sources here implied. For those unfamiliar with Islamic law, the Qur'an and Sunnah form its primary sources. Where those texts were silent on a matter, jurists engaged in interpretation and reasoning (i.e. *qiyas*, and *ijma*) via different methodologies. Countless differences amongst scholars resulted in the creation of numerous schools of legal thought, of which four Sunni schools (Hanafi, Maliki, Shafi'i, and Hanbali) and two Shi'a schools (Ja'fari and Zaidi) today dominate. For a fuller history and greater detail about various methodologies of Islamic jurisprudence, *see generally* Wael B. Hallaq, SHARI'A: THEORY, PRACTICE, TRANSFORMATIONS (2009).

As a general matter, the "directives of the Qur'an and *Sunnah* on privacy . . . tend to lay down the basis of a right, but not specify the scope."[38] Though Islamic primary texts outline a generic right of privacy, the unspecified contours of Islamic privacy rights do not translate into diminished privacy protections. Instead, the standards of Sharia set all issues and meetings between people as private by default, "unless and until they [were] proved to belong to the public sphere."[39] In fact, the Prophet Muhammad is quoted as saying that all meetings are confidential except three kinds: "those for the purpose of shedding blood unlawfully, or committing fornication, or acquiring property unjustly."[40]

In Islamic law, nowhere is the default assumption of privacy stronger than within an individual's home. Many admonitions, both in the Qur'an and the hadith as well as throughout subsequent legal writings, recognize the sanctity of the private domain by forbidding encroachment into such spaces and related affairs. Foremost, the Qur'an explicitly prohibits intrusions into personal living areas without clear, affirmative consent.[41] And, that proscription applies not only to entries into a home occupied by its owner, but also to "entry onto the owner's property in the absence of the owner."[42] Moreover, should government agents "unlawfully enter, or even spy into one's home. . . most scholars agree that the evidence obtained through this violation is inadmissible as proof of criminal wrongdoing."[43]

A story from the hadith illustrates the intensity with which such directives were interpreted, and the notion that privacy could be violated by both physical and constructive acts. According to Bukhari, when a man peeped through a hole into the Prophet's "dwelling place" whilst the

---

38. *See* Mohammad Hashim Kamali, THE RIGHT TO LIFE, SECURITY, PRIVACY AND OWNERSHIP IN ISLAM 160-61 (2008). Future scholars should, nevertheless, be encouraged to scrutinize early case rulings in their original Arabic in order to supplement limited secondary source literature.

39. *See* Kadivar *supra* note 60, at 663.

40. SUNAN ABU-DAUD, bk. 43, no. 97, *available at* https://sunnah.com/abudawud/43/97 ("Narrated Jabir ibn Abdullah: The Prophet (peace be upon him) said: Meetings are confidential except three: those for the purpose of shedding blood unlawfully, or committing fornication, or acquiring property unjustly.").

41. *See e.g.*, THE HOLY QUR'AN 24:27-28 (Marmaduke Pickthall, trans., 1930) ("Enter not houses other than your own without first announcing your presence . . . And if ye find no-one therein, still enter not until permission hath been given. And if it be said unto you: Go away again, then go away, for it is purer for you").

42. *See* Saima Saifee, Note, *Penumbras, Privacy, and the Death of Morals-Based Legislation: Comparing U.S. Constitutional Law with the Inherent Right of Privacy in Islamic Jurisprudence*, 27 FORDHAM INT'L L.J. 370, 417 (2003).

43. *See id*. at 417-18.

Prophet was inside, the Prophet later implied he would have been justified in using force (i.e. poking through the peephole at the voyeur with his comb) as a form of self-defense.[44] In this way, it is suggested that individuals have substantial immunity when protecting themselves from spying and prying in their personal spaces (and to some degree, also in activities that have a reasonable expectation of privacy attached, such as maintenance of personal hygiene). Notably, this hadith also suggests something akin to strict liability for privacy violations: the motive for the stranger's peeping appears irrelevant to the determination of whether the act itself constituted a privacy violation.

Injunctions on spying and eavesdropping extended the protections afforded to individuals within their living spaces to the informational substance of their private affairs, even when discussed outside the home. The Qur'an contains unqualified prohibitions on espionage, gossip, and slander,[45] and the hadith likewise emphasizes a respect for others' privacy and lawfulness in the acquisition of information and ideas.[46] Notably, spying or eavesdropping – even when done to further a good cause – is disallowed unless it falls within a proscribed exception.[47] The reasons for such a bright-line rule regarding informational privacy appears to be founded in Islam's "integral. . . fraternity between Muslims,"[48] which was believed to be eroded by the decrease in interpersonal trust that accompanies gossip, spying, eavesdropping, etc.

A number of legal disputes regarding urban housing design (e.g. the installation of new windows, upper floors, and doors) further demonstrate

---

44. *See* SAHIH BUKHARI, vol. 8, bk. 74, no. 258 (M. Muhsin Khan, trans., Imam Bukhari ed.), *available at* http://theonlyquran.com/hadith/Sahih-Bukhari/?volume=8&chapter=74&hadith=258 ("Narrated by Sahl bin Sa'd: A man peeped through a round hole into the dwelling place of the Prophet, while the Prophet had a Midray (an iron comb) with which he was scratching his head. the Prophet said, " Had known you were looking (through the hole), I would have pierced your eye with it (i.e., the comb)." Verily! The order of taking permission to enter has been enjoined because of that sight, (that one should not look unlawfully at the state of others)").

45. *See, e.g.*, THE HOLY QUR'AN 49:12 (Abdullah Yusuf Ali, trans., 1934)("And spy not on each other. . .behind their backs"); THE HOLY QUR'AN 24:19 (Marmaduke Pickthall, trans., 1930)("Those who love that slander should be spread concerning those who believe, theirs will be a painful punishment in the world and the Hereafter"). Interestingly, whether eavesdropping is a form of espionage, and to what extent the prohibitions on each differ, vary by and within schools of fiqh. *See, e.g.*, Kamali, *supra* note 38, at 183-84.

46. *See* Mohamed Ali Ahdash, COPYRIGHT IN ISLAMIC LAW 56, 69 (2016); Kamali *supra* note 38, at 183-85, 193.

47. *See* Kamali, *supra* note 38, at 183, 210-11 (discussing the use of surveillance and espionage by public officers such as customs inspectors).

48. *See id*. at 200.

that Islamic jurists thought often and unambiguously about privacy concerns. For example, in a case asking whether a small window opening recessed in a wall caused more or less harm to a neighbor's privacy than a large opening, medieval Maliki jurist Ibn al-Rami held that the small opening posed greater harm because "a small opening can be used to look out without being seen or warned, and this is not acceptable unless the opening is built in a manner without causing harm."[49] The case illustrates how consent and forewarning about potential privacy invasions were critical means for preventing or lessening privacy injuries. In addition, individuals appear to have had a duty to structure their buildings in such a manner as to anticipate others' reasonable expectations of privacy.

Secondary literature on urban design cases also suggests that in cases "involving a breach of privacy or the proximity of one dwelling to another, the intervention of the jurist-consult was also used to control reciprocal harm and to maintain order."[50] Privacy concerns were thus clearly attached to legal remedies, and courts and jurists played a central role in balancing individuals' privacy interests against each other.

That courts featured prominently in privacy disputes also reveals how privacy maintenance in Islamic societies was seen as an essential means of structuring a peaceful and just society. Early Islamic societies tended to keep "disputes involving intimate and private matters . . .away from the public eye and scrutiny. For every case that went to court – and these were countless – many more were informally resolved at the local level, with the intervention of the elders, the imam, the household matriarch, or others."[51] But, where privacy claims were heard and adjudicated by a neutral decision-maker, that decision-maker's duty was to balance individual interests against broader the social context, in order to ensure "an absolute equality and a complete mutual responsibility . . . of all men alike in the spiritual and in the political sphere."[52] It makes sense, then, that opportunities to hear privacy claims on record, or in public fora separate from informal dispute resolution spaces, were important features of early Islamic societies.

---

49. *See* Akel Isma'il Kahera, READING THE ISLAMIC CITY: DISCURSIVE PRACTICES AND LEGAL JUDGMENT 92 (2011).

50. *See id*. at 42 (analyzing a variety of cases regarding public harms and private/public spaces by Maliki jurists).

51. *See* Hallaq, *supra* note 37, at 163.

52. *See* SAYED KOTB, 'ADĀLAH AL-IJTIMĀ'IYAH FĪ AL-ISLĀM [SOCIAL JUSTICE IN ISLAM] 93 (trans. John B. Hardie, 1970).

III. WEIGHTING FIPPS ACCORDING TO ISLAMIC PRIVACY VALUES

Because the FIPPs are nonbinding guidelines, national and international privacy laws are required to operationalize them. Thus, the form the FIPPs take in any given privacy law has important ramifications for how a country conceptualizes privacy, and, broadly, for laying down the building blocks of future regulation.[53] For this reason, lawmakers and scholars have praised the FIPPs for providing a common cross-border language of privacy law and providing legislatures with principles they can mix-and-match according to their unique national needs. That said, scholars and experts have long observed that privacy is "an inherently contextual, culturally dependent concept" that is not easily imposed by lawmakers across cultures and individuals.[54] While the FIPPs may be able to accommodate greater cultural sensitivity because of their malleability, scholars appear to have failed to notice that the FIPPs are inherently limited in their perspective on privacy by merit of why they were created and by whom. As nonbinding guidelines, national and international privacy laws are needed to operationalize the FIPPs. Therefore, while FIPPs do provide "the closest thing the world has to a universal privacy touchstone,"[55] that touchstone at best fails to consider non-Anglo-European models of privacy that do not center on personal control over information, and at worst, might be entirely incongruous with them.

Creating an entirely new set of FIPPs based on Islamic primary texts and/or a specific school of *fiqh*, and then examining its compatibility with extant privacy laws like the GDPR, cannot be accomplished by a single Note. Instead, as a conversation starter, Part III of this Note uses the Islamic privacy values highlighted in Part II to roughly configure the 1980 OECD FIPPs for a nation that ascribes to Islamic law or Islamic culture. The result is a different ordering and weighting of FIPPs than what is seen in American- or European-based privacy laws, and that could inform policymakers and professionals looking to increase data flow to and from Islamic nations.

Before examining each of the 1980 FIPPs in turn, it is worth noting two major differences between Islamic approaches to privacy and existing secular legal ones. First, it would be extremely difficult to create a standalone set of Islamic privacy laws akin to sectoral privacy laws in the United States because Muslim jurists aspired to create a combined moral and legal system that attempted to develop rules concerning *all* human

53. *See* Hartzog, *supra* note 15, at 959-63.

54. *Id*. at 959.

55. *Id*.

acts.[56] Though Islamic law has "great jural variety. . . [that variety] existed within *a structural and systemic unity*"[57] because it "has an all-encompassing interest in human acts. . . In fact, there are no words in Arabic, the lingua franca of the law, for the contrastive notions of moral/legal."[58] Legal principles in Islam are thus not intended to control or discipline society in the way that the modern state does, but rather, to lay out a comprehensive set of social rules, based in "the performative force of the five pillars," that promote peaceful living "with oneself. . . with and in society. . . and third, with and in the world."[59]

Second, Islamic jurisprudence does not actually appear to explicitly recognize the terms "private" and "public."[60] Instead, the literature ascribes three different meanings for what is "private": "first, that which is personal or exclusive to the individual; second, that which one would rather keep concealed and protected from others; third, that over which the individual should exercise exclusive authority and control."[61] As a threshold matter then, FIPPs operationalized in Islamic societies ought to clarify which of the three meanings of privacy is closest to their intended aims. Islamic principles would seem to emphasize the second meaning of the word – personal protection – rather than the control model that the FIPPs are exclusively built upon.

But because the FIPPs are so enmeshed with leading privacy laws, it is more pragmatic to interrogate how they might be used in accordance with Islamic privacy values rather than replaced altogether. To that end, a weighting of the FIPPs informed by Islam would prioritize principles that enable data accuracy, traceable data flows, preservation of source confidentiality, collection of unambiguous, affirmative consent to data collection, and provide for legal resolutions for privacy violations.

Beginning with the three most foundational FIPPs for Western privacy law (the purpose specification principle, individual participation principle, and use limitation principle), it seems clear that Islamic privacy values align best with a default "opt-in" consent system for data collection. These three FIPPs require that the purpose of data use be specified at the

---

56. *See generally* MUHAMMAD B'QIR AL-SADR (Roy Parviz Mottahedeh, trans., intro. by, 2003)) DURUS FI 'ILM AL-USUL [LESSONS IN ISLAMIC JURISPRUDENCE].

57. *See* Wael B. Hallaq, SHARI'A: THEORY, PRACTICE, TRANSFORMATIONS 16 (2009)(emphasis in original).

58. *Id*. at 84.

59. *Id*. at 84, 226.

60. *See* Mohsen Kadivar, *An Introduction to the Public and Private Debate in Islam*, 70 SOCIAL RESEARCH 659, 661 (2003).

61. *Id*.

time or in advance of data collection and that subsequent data use be limited to those purposes unless further notice is given to the data subject. Crucially, both rely on a strong control model of data privacy: consent is stressed as the primary means of giving individuals control over their data.

In an opt-in system, an individual must affirmatively grant the right to access his data before collection may begin. By contrast, most data collection in the United States operates via an "opt-out" consent mechanism wherein data is automatically collected unless an individual explicitly withdraws their consent.[62] However, apart from the default status of the vast majority of interpersonal interactions as confidential in Islam, the Qur'an and hadith explicitly require affirmative consent before physical or constructive entry into personal areas.[63] Moreover, because the Qur'an suggests that consent should be obtained upon any re-entry[64] and bans on physical entry and observation remain in force even when the owner or occupant is absent,[65] Islamic privacy laws might want to require consent more often than the purpose specification and use limitation principles require. An Islamically-informed system may therefore make data transfers less efficient by requiring consent at every data collection, putting it at odds with the OECD's general ethos, but the trade-off is perhaps preferred by Islam's primary texts.

On the other hand, two related FIPPs – the collection limitation principle and transparency principle – might occupy less relative space in Islamic data privacy laws precisely because of the strong focus on consent and confidentiality abovementioned. These FIPPs require the lawful collection of personal data and transparency in the processing of it and features prominently in both E.U. data protection laws and American consumer protection regulations.[66] However, the emphasis that Western

62. This may be of particular interest to transatlantic privacy scholars, who have long contrasted the American preference for opt-out consent to surveillance with opt-in approaches in Europe. *See, e.g.*, Paul M. Schwartz & Daniel J. Solove, *ALI Data Privacy: Overview and Black Letter Text*, 68 UCLA L. REV. (forthcoming 2020)(declining to embrace either an opt-in or opt-out position in the American Legal Institute's novel privacy law project because of the radical disruptions such a clean sweep would cause to American privacy laws).

63. *See* QUR'AN *supra* note 41; *see also* SAHIH BUKHARI, *supra* note 44.

64. *See* QUR'AN *supra* note 41. The rest of the verse quoted enjoins people to ask permission at three times of day that are considered especially private (i.e. before the dawn prayer, during afternoon rest, and after the night prayer). There is no indication that consent obtained at one of those times suffices for the other–if anything, the forcefulness of the Qur'an's defense of private spaces suggests that consent even for the same time of day should be obtained upon each separate entry.

65. *See* Saifee *supra* note 42.

66. *See* Frederik Zuiderveen Borgesius, Jonathan Gray & Mireille van Eechoud, *Open*

privacy laws have on informing individuals of the purpose for which their data is collected becomes relatively less important if consent is obtained for every data use. Presumably, the form obtaining consent would make collection limitation measures redundant and transparency far easier to achieve. But, if Islamic primary texts are found *not* to require consent at every data collection,[67] then these two FIPPs should be given almost the same importance as the purpose specification and use limitation principles.

What is unassailable, however, is that the data quality principle is a FIPP that would be of paramount importance in an Islamic system. This FIPP requires accuracy and completeness of personal data, because decisions made on incorrect data can have serious negative consequences for both individuals and organizations. The data quality principle also requires that data be relevant to the purposes for which it is gathered. This FIPP could be the primary way to operationalize the Qur'an's and Sunnah's bans on gossip, slander, and suspicion, all of which are forbidden because they promote inaccurate information and increase distrust between individuals.[68] A more robust focus on this FIPP that is tailored to Islamic societies could limit the number of parties to whom data can be transferred, but is not out of line with current concerns amongst technologists regarding cybersecurity and the spread of misinformation. Likewise, to the extent that it ensures data accuracy and authenticity within data flows, the security safeguards principles could be more robust in Islamic data privacy law than, for instance, the current "reasonableness" standards present in Western cybersecurity laws.[69]

Finally, the accountability principle requires that a data controller be accountable for compliance with the laws used to operationalize the FIPPs, and would likely be important to an Islamic privacy system if modified. While this principle did not exist until the OECD's 1980 version of the FIPPs and its exhortation to identify a duty-bearer remains weak,[70] the close relationship between early Islamic privacy laws and the availability of various forms of legal redress strongly suggests that there should be a readily accessible avenue for dispute resolution that could be based in this FIPP. A specialized or otherwise reliable space where neutral

---

Data, Privacy, and Fair Information Principles: Towards a Balancing Framework,

67. This question of consent frequency might be resolved by privacy scholarship involving those with expert knowledge of Qur'anic Arabic – perhaps there are clear, relevant connotations of the words used for "entry" and "permission," or at very least, Islamic jurists have likely confronted the question before in materials as yet not translated.

68. *See* Kamali, *supra* note 38, at 200.

69. *See* Schwartz, *supra* note 62.

70. *See* Kirby, *supra* note 15, at 10.

decisionmakers could balance the interests of parties would enable precise identification of who the duty-bearer should be in a privacy conflict and limit the number of people privy to sensitive information that could arise in much the same way as early Islamic jurists heard and resolved privacy claims. To this end, Islamic teachings suggest that invasions of privacy cause harm in and of themselves that can later be adjudicated upon, thereby lessening the difficulties in proving standing in privacy suits under much of American (and to a lesser extent, European) privacy laws.

CONCLUSION

Data transfers have an undisputedly global character. But, such transfers are largely rooted in the OECD's FIPPs, which were designed to serve specific "countries committed to democracy and the market economy."[71] Though Islam's holistic approach to privacy [72] echoes the omnibus nature of new data protection laws such as the GDPR, Islamic privacy values are not wholly served by extant data privacy laws based on the OECD's FIPPs. Given burgeoning privacy laws in and data transfers with Muslim countries, further investigation into the extent to which the FIPPs are compatible or best used by non-Western legal and cultural models of data privacy is worthwhile. While this Note only scratches the surface of Islamic perspectives on data privacy laws, importing Western privacy laws into Muslim nations without modification risks raising the specter of colonialism and raises worries about how Western intellectual traditions can distort, erase, or misread the histories and experiences of non-Western cultures.

71. *See OECD Privacy Principles*, http://oecdprivacy.org/.

72. *See* Kamali, *supra* note 38, at 234 ("The fact that the Qur'an and Sunnah contain moral advice and religious guidance side by side with legal injunctions makes respect for the privacy of others an integral part of the social and cultural ethos of the Muslim community").