American University Law Review

Volume 38 | Issue 3 Article 13

2023

Stars, Stripes, and Surveillance: The United States' Failure to Regulate Data Privacy

Sam Begland

Follow this and additional works at: https://digitalcommons.wcl.american.edu/aulr

 Part of the Comparative and Foreign Law Commons, Human Rights Law Commons, International Humanitarian Law Commons, International Law Commons, National Security Law Commons, and the Privacy Law Commons

Recommended Citation

Sam Begland (2023) "Stars, Stripes, and Surveillance: The United States' Failure to Regulate Data Privacy," *American University Law Review*: Vol. 38: Iss. 3, Article 13.
Available at: https://digitalcommons.wcl.american.edu/aulr/vol38/iss3/13

This Comment is brought to you for free and open access by the Washington College of Law Journals & Law Reviews at Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in American University Law Review by an authorized editor of Digital Commons @ American University Washington College of Law. For more information, please contact kclay@wcl.american.edu.

Stars, Stripes, and Surveillance: The United States' Failure to Regulate Data Privacy

Abstract

In the wake of the United States Supreme Court's devastating decision to strip Americans of their constitutional right to abortion in Dobbs v. Jackson Women's Health Organization, data privacy is more salient than ever. Without adequate data regulations, state governments and anti-abortion activists alike can harass and prosecute pregnant people attempting to exercise their bodily autonomy. This comment argues that the United States has violated its obligations under the International Covenant on Civil and Political Rights (ICCPR) Article 17 by failing to protect against interference with the use and collection of reproductive health data. Further, this comment analyzes interpretations of Article 17 to show that the United States is allowing arbitrary intrusions of privacy. Because the United States must act to comply with the ICCPR, this comment recommends that (1) the United States create and enter into regional data privacy regulations, (2) the United Nations Human Rights Committee update General Comment 16 to Article 17 to reflect technological advancements in data collection, and (3) the United States enact domestic legislation addressing reproductive health data and data privacy generally.

Keywords

International Law, International Human Rights, Human Rights, United Nations, United Nations Human Rights Committee, Privacy, National Security, Privacy and Data

This comment is available in American University Law Review: https://digitalcommons.wcl.american.edu/aulr/vol38/iss3/13

COMMENT

STARS, STRIPES, AND SURVEILLANCE: THE UNITED STATES' FAILURE TO REGULATE DATA PRIVACY

SAM BEGLAND*

In the wake of the United States Supreme Court's devastating decision to strip Americans of their constitutional right to abortion in Dobbs v. Jackson Women's Health Organization*, data privacy is more salient than ever. Without adequate data regulations, state governments and anti-abortion activists alike can harass and prosecute pregnant people attempting to exercise their bodily autonomy. This comment argues that the United States has violated its obligations under the International Covenant on Civil and Political Rights (ICCPR) Article 17 by failing to protect against interference with the use and collection of reproductive health data. Further, this comment analyzes interpretations of Article 17 to show that the United States is allowing arbitrary intrusions of privacy. Because the United States must act to comply with the ICCPR, this comment recommends that (1) the United States create and enter into regional data privacy regulations, (2) the United Nations Human Rights Committee update General Comment 16 to Article 17 to reflect technological advancements in data collection, and (3) the United States enact domestic legislation addressing reproductive health data and data privacy generally.*

* Samantha Begland is a J.D. Candidate, American University Washington College of Law (2024); B.A. English & B.A. Political Science, Tulane University (2021). I would like to thank Michelina Partipilo and Professor William Snape for their thoughtful guidance. Thank you to my family for their life-long support and inspiration. Dedicated to Kate Foley, Sarah Benjamin, Ali Ruvolis, Megan Meissner, and Kevin Botros for being the most wonderful friends and colleagues.

I. INTRODUCTION

Since the United States Supreme Court stripped Americans of their constitutional right to abortion, there have been increased concerns that private, personal health data from apps, internet searches, geolocation technology, and other sources may be used to prosecute and harass individuals for having or performing abortions. Meanwhile, the technology that allows private citizens and public entities to collect and use private data has advanced rapidly and the government has lagged in its duty to enact timely regulations.

This Comment asserts that as a party to the International Covenant on Civil and Political Rights (ICCPR), the United States of America is bound to protect against the arbitrary and unlawful violation of privacy. By failing to regulate the collection and use of reproductive health data, the United States has violated its obligations under the ICCPR. Doing so has left providers and seekers of abortion care particularly vulnerable to discrimination, violence, and prosecution following the *Dobbs v. Jackson Women's Health Organization* decision.

Part II of this Comment describes technological advancements, like femtech, and illustrates how their data collection methods often leave reproductive health data vulnerable to hostile third parties. This Part further defines the United States' duty to protect individuals' privacy rights under Article 17 of the International Covenant on Civil and Political Rights. Part III delves into the Human Rights Committee's interpretation of Article 17 to show that the United States' failure to regulate the use and collection of reproductive health data violates its

obligation to prevent interference with individuals' reproductive health privacy from both public and private actors. Part IV proposes several recommendations to help the United States comply with its ICCPR obligations moving forward.

II. BACKGROUND

A. FEMTECH AND REPRODUCTIVE HEALTH DATA PRIVACY CONCERNS

Since the term femtech was first coined in 2016, the international "Female Technology" market has seen incredible growth.[1] In anticipation of continued growth, the government and multiple private corporations have begun to invest heavily in femtech, hoping it will yield lucrative financial opportunities.[2]

But what exactly is "femtech"? The market itself includes a multitude of technologies aimed at addressing women's health issues across the spectrum.[3] Most prominent, however, are applications geared toward menstruation and fertility.[4] Such apps collect data on intimate details of the user's life, such as their sex life and reproductive cycle, to provide insights into their health.[5] The value of this technology has been widely recognized, with studies estimating that over a third of women in the United States have used femtech apps.[6]

---

1. Allysan Scatterday, *This Is No Ovary-Action: Femtech Apps Need Stronger Regulations to Protect Data and Advance Public Health Goals*, 23 N.C. J.L. & TECH. 636, 639 (2022) (stating that while currently valued at almost $19 billion USD, the industry is expected to reach between $50 and $60 billion by 2027).

2. *Femtech Market by Type (Devices, Software, Services), by End-Use (Direct-to-Consumer, Hospitals, Fertility Clinics, Surgical Centers, Diagnostic Centers), by Application (Reproductive Health, Pregnancy & Nursing Care, Pelvic & Uterine Healthcare), by Region, Forecasts to 2027*, EMERGEN RESEARCH (June 2021), https://www.emergenresearch.com industry-report/femtech-market [hereinafter *Femtech Market*](explaining that the rapid growth of the femtech market has attracted a swarm of startups and investors).

3. Scatterday, *supra* note 1, at 640; *Femtech Market*, *supra* note 2 (explaining that, in addition to fertility and menstruation, femtech aims to develop solutions for diagnosis and treatment of infectious diseases and gynecological disorders).

4. Scatterday, *supra* note 1, at 640.

5. *Id.* at 641.

6. Donna Rosatio, *What Your Period Tracker App Knows About You*,

1. What Risks Does Femtech Pose?

Despite the rosy possibilities touted by the femtech industry, the reality is that these apps pose substantial data privacy concerns that undermine their utility as platforms for studying women's health.[7] Unlike medical records held by doctors, the sensitive health information collected by femtech apps is not protected by the Health Insurance Portability and Accountability Act (HIPAA), meaning that the apps are relatively free to collect, hold, and share user data.[8] Apps may share information with advertising and marketing companies or with entities like data brokers, which aggregate data to create profiles on individuals for a profit.[9] This personal information is often traceable and users have little to no control over who may access it.[10]

Beyond the inherent privacy concerns associated with data sharing, femtech apps are troubling because users are often unaware that this seemingly innocuous technology is collecting and sending information to third parties.[11] A review of the most popular femtech apps revealed that many had poor data privacy standards.[12] Many apps exceeded the scope of their advertised health monitoring function by collecting behavioral and location data in addition to the personal-health data users provided.[13] Despite the sensitive nature of health

CONSUMER REPORTS (2020), https://www.consumerreports.org/health-privacy/what-your-period-tracker-app-knows-about-you-a8701683935 (reporting on a recent Kaiser Family Foundation study).

7. Scatterday, *supra* note 1, at 642.

8. Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936; Rosatio, *supra* note 6 (noting that HIPAA is a 1996 federal law that limits where healthcare providers can share individual's health information).

9. Rosatio, *supra* note 6 (describing how data brokers often sell user profiles to unknown sources).

10. *Id.* (explaining that even when data is de-identified by removing obviously identifiable information, research suggests it may still be traced back to the user by combining it with other information, such as location).

11. *See* Joseph Cox, *Data Broker is Selling Location Data of People Who Visit Abortion Clinics*, VICE (May 3, 2022), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood (describing how app developers can install code into their apps that sends users' data to companies in exchange for payment).

12. Najd Alfawzan et al., *Privacy, Data Sharing, and Data Security Policies of Women's mHealth Apps: Scoping Review and Content Analysis*, JMIR MHEALTH UHEALTH 187, 197–200 (June 5, 2022), https://mhealth.jmir.org/2022/5/e33735.

13. *Id.*

information, nearly all of the apps shared user data with third parties.[14] Often, these apps did not communicate to users that their data was being collected or shared.[15] As the femtech market booms, it is clear that data privacy protections are not adequate, leaving users' health data vulnerable to third-party use without their knowledge or consent.

2. Digital Data Collection Concerns Generally

Unfortunately, femtech is not the only means through which private data is collected, distributed, and analyzed. Digital data trails are formed constantly through online searches, purchasing history, location history, and more.[16] Data points that are innocent enough independently can be amassed to create telling profiles.[17] Because companies are aware that expecting parents are valuable customers, advertisers have dedicated extensive research to discerning the online habits of pregnant people, making them easy to identify.[18] This information could simply allow companies to send individuals targeted ads or, more disturbingly, allow individuals to be targeted or harassed.

While this may sound alarmist, personal digital data has already been weaponized to harm individuals. For example, in 2016, an anti-abortion group used geofencing technology, which allows companies to advertise products based on a consumer's location, to harass people visiting Planned Parenthood clinics by sending anti-abortion advertisements to their phones.[19]

What's more, these data violations can be used for purposes beyond sending unsavory advertisements. In several instances, personal data was used to prosecute or undermine women in court. In one case from

14. *Id.*; *see also* Rosatio, *supra* note 6 (noting that a study of 10 popular femtech apps found that the apps were collectively sharing information with at least 135 companies).

15. Alfawzan et al., *supra* note 12 (stating that of the twenty-three apps studied, only seventy percent displayed a privacy policy, only fifty-two percent requested consent from users, and only fifty-seven percent provided users with information regarding data security).

16. Cynthia Conti-Cook, *Surveilling the Digital Abortion Diary*, 50 U. BALT. L. REV. 1, 7 (2020).

17. Rosatio, *supra* note 6.

18. *See* Conti-Cook, *supra* note 16, at 24–25.

19. Cox, *supra* note 11; Conti-Cook, *supra* note 16, at 51.

2017, Mississippi woman Latice Fisher was prosecuted for second-degree murder after experiencing pregnancy loss at home.[20] The prosecution offered her web search history, which showed a search for the abortion drug misoprostol, as evidence to prove she had intentionally killed her fetus.[21] Despite no proof that Fisher had received or taken abortion-inducing medication, a grand jury indicted her.[22] Fisher's case demonstrates how search histories may be used to prosecute women for their reproductive health choices and foreshadows how other forms of data may be used against women in the future.[23]

While the concerns associated with digital data collection are not limited to reproductive health privacy, data may continue to be weaponized as the legal conversation surrounding reproductive rights becomes more contentious.

B. THE INCREASED IMPORTANCE OF DATA PRIVACY AFTER THE DOBBS DECISION

On June 24, 2022, the United States Supreme Court overturned the constitutional right to abortion in *Dobbs v. Jackson Women's Health Organization*.[24] The Court's decision to take away this fundamental right allowed many states to heavily restrict abortion or ban abortion altogether, leaving pregnant people in these areas with few reproductive health options.[25]

Naturally, many pregnant people who are confronted with barriers to abortion care will turn to the internet to independently manage their

20. Conti-Cook, *supra* note 16, at 3-5.

21. *Id.*

22. *Id.* at 4.

23. *See* Cat Zakrezewski et al., *Texts, Web Searches About Abortion have been Used to Prosecute Women*, WASH. POST (July 3, 2022), https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution (suggesting that simple search histories and data maintained in period tracker apps may pose huge risks in a post-*Roe* world).

24. 142 S. Ct. 2228 (2022) (holding that the Constitution does not confer a right to abortion and overruling the precedent set in both *Roe v. Wade*, 410 U.S. 113 (1973), and *Planned Parenthood v. Casey*, 505 U.S. 833 (1992)).

25. *See generally* Oriana Gonzalez & Jacob Knutson, *Where Abortion Has Been Banned Now that* Roe v. Wade *is Overturned*, AXIOS, https://www.axios.com/2022/06/25/abortion-illegal-7-states-more-bans-coming (last updated Jan. 6, 2023).

condition.[26] Many will use their devices to contact healthcare providers, order abortion medication, research clinics, arrange transportation, consult their health apps, and more.[27] Unfortunately, these activities are traceable through their digital data. With law enforcement and anti-abortion activists using data trails to prosecute, harass, and spread misinformation, experts in both reproductive rights and surveillance worry that personal data will be used as ammunition in the war on abortion.[28]

In the wake of *Dobbs*, many took comfort in the possibility of continued access to abortion by mail. Even before *Dobbs*, medicated abortions had become increasingly popular among patients and practitioners.[29] Now more than ever, medicated abortion is often the only option for those who cannot afford to travel.[30] Unsurprisingly, however, the states that have enacted harsh abortion restrictions also wish to outlaw telemedicine for abortion, meaning that simply exploring this option could lead to harassment and legal penalties.[31]

Further, the abortion ban means that those living in anti-abortion states who can afford to travel will begin to cross state lines for treatment. However, even these individuals are not safe. Such travel can be documented through location data, which some companies specialize in collecting from common smartphone apps and selling to

26. *See* Conti-Cook, *supra* note 16, at 22 (explaining that using the internet to seek medical advice was already a prevalent and growing practice for pregnant people before the *Dobbs* decision).

27. *Id.*

28. Lil Kalish, *Meet Abortion Ban's New Best Friend—Your Phone*, MOTHER JONES (Feb. 16, 2022), https://www.motherjones.com/politics/2022/02/meet-abortion-bans-new-best-friend-your-phone.

29. *See* Conti-Cook, *supra* note 16, at 21 (reporting that in 2017, "an estimated 60 percent of women who were early enough in their pregnancy [to choose] abortion pills" did so); Kalish, *supra* note 28 (explaining that during the COVID-19 pandemic, the FDA lifted its requirement for in-person visits for mifepristone prescriptions, the hormone blocker used in abortion medication, and in doing so greatly expanded access to abortion medication); *id.* (describing that mail order abortion medication is critical now that many abortion clinics have either been forced to close or are overwhelmed by an influx of patients from nearby states).

30. Kalish, *supra* note 28.

31. *Id.*

third parties.[32]

Throughout American history, women have been punished for terminating a pregnancy, and cases like Latice Fisher's make clear that prosecutors will use digital data to do so.[33] Now that states have criminalized abortion in the wake of *Dobbs v. Jackson Women's Health Organization*, reproductive health data is more vulnerable than ever as prosecutors and anti-abortion activists alike may weaponize digital data.[34]

C. THE UNITED STATES' OBLIGATIONS UNDER THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS

Since entering into force in 1976, the International Covenant on Civil and Political Rights (ICCPR) has guaranteed a broad array of civil and political rights to all individuals under the jurisdictions of State Parties.[35] The ICCPR obligates Parties to respect the rights outlined in the treaty.[36] More specifically, governments are compelled to take administrative, judicial, and legislative action to give effect to these rights and to provide remedies if rights are violated.[37] To oversee compliance with the ICCPR, the U.N. established the United Nations Human Rights Committee (HRC).[38] The HRC is tasked with

32. *See* Cox, *supra* note 11 (identifying SafeGraph as one of the companies collecting location data from apps without users knowing and aggregating information into trackable "brands"); *id.* (noting that Planned Parenthood is one of the trackable brands SafeGraph has identified and that location data for Planned Parenthood visitors was sold for under $200).

33. Zakrzewski et al., *supra* note 23 ("[Ms. Fisher's case is] one of a handful in which American prosecutors have used text messages and online research as evidence against women facing criminal charges related to the end of their pregnancies.").

34. *See* Conti-Cook, *supra* note 16, at 6 (stating that even pregnant people's decisions not regarding their pregnancy, such as seeking substance abuse treatment, could be digitally surveilled).

35. International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.

36. *See* S. EXEC. REP. NO. 102-23, pt. 1 (1992) (U.S. Senate Report on Ratification of the International Covenant on Civil and Political Rights).

37. *FAQ: The Covenant on Civil and Political Rights*, AM. C.L. UNION, https://www.aclu.org/other/faq-covenant-civil-political-rights-iccpr (last updated Apr. 2019).

38. S. EXEC. REP. NO. 102-23, *supra* note 36, pt. 1.

monitoring the implementation of the ICCPR.[39] It hears individual complaints and releases decisions that illustrate how the ICCPR should be interpreted and applied.[40] Though State Parties are not obligated to acknowledge the competency of the HRC, Parties that ratify the additional Optional Protocol allow victims of ICCPR violations to present claims before the HRC.[41] Altogether, the Covenant aims to afford democratic freedoms to all.[42]

1. An Explanation of the United States' Ratification of the ICCPR

When the United States ratified the ICCPR in 1992, it became the supreme law of the land, superior to state law and equal to federal law.[43] During ratification, the Senate articulated comments and conditions that help shape how the United States specifically is expected to behave under the ICCPR.

To begin, compliance with the ICCPR is subject to the reservations, understandings, and declarations (RUDs) made upon ratification.[44] RUDs allow a country to become party to a treaty contingent on certain terms or interpretations of the treaty language.[45] One of the most notable of these RUDs is the Senate's fifth understanding: Federalism.[46] This understanding acknowledges the United States' federal system of government and clarifies that the ICCPR applies to state and local governments as well as the federal government and its entities.[47] Here, the federal government pledged to ensure compliance with the ICCPR through its relevant legislative and judicial powers

39. *Id.* pt. 4.
40. *Id.* pts. 4, 5.
41. G.A. Res. 2200A (XXI) Optional Protocol to the International Covenant on Civil and Political Rights (Dec. 16, 1966).
42. S. EXEC. REP. NO. 102-23, *supra* note 36.
43. *FAQ: The Covenant on Civil and Political Rights*, *supra* note 37.
44. *Id.*
45. Eric Neumayer, *Qualified Ratification: Explaining Reservations to International Human Rights Treaties*, 36 J. LEGAL STUD. 397, 397-98 (explaining that states may exempt themselves from certain obligations); *id.* (explaining that RUDs are common for international human rights treaties as they are a means to account for cultural, religious, and political diversity).
46. S. EXEC. REP. NO. 102-23, *supra* note 36, pt. 2.
47. *Id.*; *see also FAQ: The Covenant on Civil and Political Rights*, *supra* note 37 (stating that the ICCPR applies to all government entities, including state and local governments).

while obligating state and local governments to comply through their relevant powers.[48]

Further, in the ICCPR's ratification document, the Senate Committee on Foreign Relations acknowledged the Covenant's importance.[49] The Committee additionally acknowledged that they hoped ratifying the ICCPR would allow the United States to participate in monitoring compliance with the Covenant.[50]

Despite the Committee's advice that the United States should accept the competence of the HRC to hear complaints, the United States has yet to become a party to the Optional Protocol.[51] Acknowledging competence is crucial to the HRC's ability to monitor and enforce compliance, so the failure to do so allows the United States to escape accountability.[52]

2. Article 17: The Right to Privacy

In an age of rapid technological advancements that often surpass our understanding and intrude on our personal information, privacy rights are more salient than ever. ICCPR Article 17 aims to protect privacy rights and states:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such

48. *FAQ: The Covenant on Civil and Political Rights*, *supra* note 37.

49. S. EXEC. REP. NO. 102-23, *supra* note 36, pt. 4 (stating that it was one of the "fundamental instruments created by the international community for the global promotion and protection of human rights").

50. *Id.*

51. *Status of Ratification Interactive Dashboard*, U.N. HUM. RTS. OFF. HIGH COMM'R, https://indicators.ohchr.org (last updated Jan. 27, 2023).

52. *See generally* Optional Protocol to the ICCPR, *supra* note 41, art. 1 (explaining the function of the Optional Protocol as an enforcement mechanism and acknowledging that the HRC cannot hear communications concerning States not Party to the Protocol); *see* David Kaye, State *Execution of the International Covenant on Civil and Political Rights*, 3 U.C. IRVINE L. REV. 94, 96 (2013) (highlighting that the Senate ratification documents also included an understanding that the Covenant is non-self-executing, meaning it is unenforceable in U.S. courts and unavailable to litigants as a basis for legal action without legislation); *id.* (noting that such legislation has not yet been introduced at the state or federal level).

interference or attacks.[53]

Article 17 is noticeably broad, referring to privacy interferences generally, rather than specifying exact violations. This is useful because it accounts for violations not yet envisioned and allows victims of privacy interference to construe the article broadly to suit their situation.

3. Explanation and Interpretation of General Comment 16

To guide the interpretation of the ICCPR, the HRC publishes general comments which serve to elaborate and develop the language of articles and clarify how they should be applied.[54] *General Comment 16* expands on the right to privacy articulated in Article 17, providing State Parties with guidance on how to ensure compliance.[55] *General Comment 16* is useful for analyzing Article 17 for several reasons.

First, *General Comment 16* outlines where relevant privacy interferences originate. The HRC writes that State Parties must guarantee the right to privacy against all interferences and attacks, "whether they emanate from State authorities or from natural or legal persons."[56] This clarification shows that the State Parties must not only refrain from interfering with an individual's privacy but must also prohibit interference from private parties through legislation.[57]

Second, the Comment provides an interpretation of the terms

53. ICCPR, *supra* note 35, art. 17.

54. AM. C.L. UNION, THE HUMAN RIGHT TO PRIVACY IN THE DIGITAL AGE (2015), https://www.aclu.org/sites/default/files/field_document/informational_privacy_in_the_digital_age_final.pdf (explaining that general comments also work to ensure that treaty monitoring bodies correctly and consistently interpret the right at issue when reviewing complaints).

55. *See* AM. C.L. UNION, INFORMATIONAL PRIVACY IN THE DIGITAL AGE: A PROPOSAL TO UPDATE *GENERAL COMMENT 16* [RIGHT TO PRIVACY] TO THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS 1 (2015) (stating that in 1988, the HRC issued *General Comment 16* which noted that the right to privacy encompasses a diverse range of important interests, such as bodily privacy).

56. U.N. Hum. Rts. Comm., *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, ¶ 1 (Apr. 8, 1988), https://www.refworld.org/docid/453883f922.html [hereinafter *General Comment 16*].

57. *Id.*

"arbitrary" and "unlawful" so that State Parties and the HRC can better identify when a particular privacy interference violates the ICCPR. The HRC writes that, "no interference can take place except in cases envisaged by the law," and that any lawful interference must, "comply with the provisions, aims, and objectives of the Covenant."[58] For privacy interference to be lawful, the interference must be authorized by specific domestic legislation which conforms to the ICCPR's goals.[59] Then, even when an interference is determined to be lawful, it may still violate Article 17 if it is arbitrary.[60] *General Comment 16* emphasizes that arbitrariness protects individuals from lawful interferences that are unreasonable under the circumstances.[61]

Third, the General Comment explains the scope of privacy rights by describing situations that would constitute violations. Beyond well-established privacy interests, like privacy in one's domicile, of their person, or concerning family life, the Comment includes more modern privacy interests applicable to modern technology.[62] For example, it asserts that the right to confidential correspondence should be guaranteed. It goes on to say that surveillance, including interference with electronic communication, should be prohibited. Perhaps the most salient for privacy in our current technological environment is the clause that states, "[t]he gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law."[63] The Comment emphasizes a State's responsibility to protect personal information from reaching the hands of those not authorized to have it and to allow individuals to ascertain which entities may control or collect their data.[64]

Finally, *General Comment 16* lays out States' obligations to protect and provide for privacy rights. While the Comment acknowledges that instances may arise where a government's interest in protecting

58. *Id.* ¶¶ 3, 4.
59. INFORMATIONAL PRIVACY IN THE DIGITAL AGE, *supra* note 55, at ii.
60. *General Comment 16*, *supra* note 56, ¶ 4 (stating that an arbitrary interference "can also extend to interferences provided for under the law").
61. *Id.*
62. *Id.* ¶¶ 8, 10.
63. *Id.* ¶¶ 8, 10.
64. *Id.* ¶¶ 8, 10.

society outweighs individuals' privacy interests, the Committee states that any interference should be necessary under the aims of the ICCPR.[65] To that end, the Comment commands State Parties to specify in detailed legislation any circumstances where interferences may be permitted.[66] Further, states are obligated to refrain from unauthorized interferences and must legislate to ensure private entities refrain from interferences altogether.[67] Any privacy interference must be a narrow exception rather than a broadly applied practice.

4. Human Rights Committee Decisions Interpreting Article 17

The Human Rights Committee hears complaints against State Parties and publishes decisions that interpret the ICCPR and determine how it should be applied. Several ICCPR decisions specifically address privacy concerns under Article 17.

Collectively, the reports on these individual cases reveal that the HRC believes restricting abortion is a violation of Article 17.[68] In *K.L. v. Peru*, a hospital prevented Karen Noelia Llantoy Huamán (K.L.) from receiving an abortion for her non-viable pregnancy, despite the fact she met the legal requirements to receive treatment.[69] The HRC considered this interference with an abortion a violation of K.L.'s rights under Article 17.[70]

---

65. *Id.* ¶ 8.

66. *See id.* ¶ 8 ("A decision to make use of such authorized interference must be made only by the authority designated under the law, and on a case-by-case basis.").

67. *Id.* ¶¶ 1, 9.

68. *See* Llantoy Huamán v. Peru [*K.L. v. Peru*], Communication No. 1153/2003, U.N. Human Rights. Committee [HRC], ¶ 6.4., U.N. Doc. CCPR/C/85/D/1153/2003 (Oct. 24, 2005) (stating that "the refusal to act in accordance with author's decision to terminate her pregnancy was not justified and amounted to a violation of Article 17 of the covenant"); Mellet v. Ireland, Communication No. 2324/2013, HRC, ¶¶ 7.7, 7.8, U.N. Doc. CCPR/C/116/D/2324/2013 (Mar. 31, 2016) (concluding that interference with author's decision was unreasonable and arbitrary in violation of article 17); Whelan v. Ireland, Communication No. 2425/2014, HRC, ¶¶ 7.8, 7.9, U.N. Doc. CCPR/C/119/D/2425/2014 (Mar. 17, 2017) (finding the State party's interference in the author's decision unreasonable and an arbitrary interference in the author's right to privacy).

69. *K.L. v. Peru*, Communication No. 1153/2003, HRC, ¶¶ 2.2–2.5, 3.1 (explaining that while Peru's criminal code prohibited therapeutic abortions unless the health of the mother was at risk, K.L. had presented sufficient medical evidence to show this condition had been met).

70. *Id.* ¶ 6.4.

Likewise, in both *Whelan v. Ireland* and *Mellet v. Ireland*, Irish law prevented the complainants from receiving abortions, even after learning that their fetuses were suffering from fatal defects.[71] The HRC found that the bodily autonomy and privacy of the women seeking abortions outweighed the government's interest in the fetus, and recommended Ireland change its law to comply with Article 17.[72]

These cases also demonstrate that the HRC believes failing to protect an individual's personal data is a violation of Article 17.[73] In *G. v. Australia*, a transgender woman was told that, due to Australian law, she would not be allowed to change her sex on her birth certificate unless she divorced her spouse.[74] The HRC found that Australia's requirement interfered with G.'s rights under Article 17 because it revealed private health information and interfered with her family life.[75]

The HRC again took issue with personal data violations in *N.K. v. Netherlands*.[76] In this case, a DNA sample was mistakenly taken from an innocent minor and retained in a database used for criminal investigations.[77] The HRC found that the Netherlands' collection of such data to analyze and use in future prosecutions interfered with N.K.'s privacy under Article 17.[78]

Finally, in *Vandom v. Republic of Korea*, Vandom was subjected to mandatory HIV testing to renew her work visa.[79] The HRC found that Vandom's interest in her private health information outweighed the negligible public health benefits of HIV testing, thus violating

71. *Mellet*, Communication No. 2324/2013, HRC, ¶¶ 2.1, 2.2; *Whelan*, Communication No. 2425/2014, HRC, ¶¶ 2.1, 3.1.

72. *Mellet*, Communication No. 2324/2013, HRC, ¶ 7.8; *Whelan*, Communication No. 2425/2014, HRC, ¶ 7.9.

73. *See generally* G. v. Australia, Communication No. 2172/2012, HRC, U.N. Doc. CCPR/C/119/D/2172/2012 (Mar. 17, 2017); N.K. v. Netherlands, Communication No. 2326/2013, HRC, U.N. Doc. CCPR/C/120/D/2326/2013 (July 18, 2017); Vandom v. Republic of Korea, Communication No. 2273/2013, HRC, U.N. Doc. CCPR/C/123/D/2273/2013 (July 12, 2018).

74. G. v. Australia, Communication No. 2172/2012, HRC, ¶ 7.2.

75. *Id.* ¶ 7.10.

76. N.K. v. Netherlands, Communication No. 2326/2013, HRC, ¶ 9.3.

77. *Id.* ¶ 3.1.

78. *Id.* ¶ 9.3.

79. Vandom v. Republic of Korea, Communication No. 2273/2013, HRC, ¶ 8.6, U.N. Doc. CCPR/C/123/D/2273/2013 (July 12, 2018).

Vandom's privacy under Article 17.[80]

Though the HRC has yet to address the lack of reproductive health data protections in the United States and globally, these decisions should be used to analyze the degree of protection the ICCPR prescribes for reproductive health data.

III. ANALYSIS

A. THE UNITED STATES' FAILURE TO PROTECT WOMEN'S HEALTH DATA HAS VIOLATED ITS OBLIGATIONS UNDER ICCPR ARTICLE 17

As a State Party to the International Covenant on Civil and Political Rights, the United States has a duty to protect and provide for the privacy rights of those within its territory. Not only must the government refrain from engaging in privacy interferences, but it must also prohibit such acts from private entities or individuals.[81] This means that both a negative and a positive right to privacy exist.[82] For the negative right, the government itself cannot interfere arbitrarily or unlawfully with someone's privacy. For the positive right, the government must act through legislation to prevent entities and individuals from interfering with others' privacy rights. At present, the United States has neglected to provide this positive right to privacy through its failure to regulate the collection and use of reproductive health data. Under the ICCPR, the United States is committing a widespread Article 17 privacy rights violation.

1. Analysis of an Interference Under Article 17

Article 17, in relevant part, provides that each person should be free from arbitrary or unlawful interferences with their privacy, family, home, or correspondence.[83] Jurisprudence from the Human Rights Committee (HRC) helps apply Article 17 to the privacy violations

80. *Id.* ¶ 8.9.

81. *General Comment 16*, *supra* note 56, ¶¶ 1, 9.

82. S. EXEC. REP. NO. 102-23, *supra* note 36, pt. 5 ("The Covenant obligates each State Party to respect and ensure these rights, to adopt legislative or other necessary measures to give effect to these rights, and to provide an effective remedy to those whose rights are violated.").

83. ICCPR, *supra* note 35, art. 17.

happening currently in the United States.

i. What Falls Under "Privacy, Family, Home, or Correspondence"?

The first step when analyzing an Article 17 claim is to ensure that the interference in question is an invasion of one's privacy. Privacy under Article 17 may be broadly construed.[84] To fall within the scope of Article 17, the interference must infringe on one's privacy, family, home, or correspondence.[85]

General Comment 16 advocates for a broad interpretation of each of these terms. Family should include, "all those comprising the family as understood in the society of the State party concerned."[86] For example, in the United States, family is now understood to take a variety of complex forms. In recent years, there has been a large departure from the traditional two-parent household.[87] Today, families are more diverse and complex than ever in terms of the marital status of parents, the number of parents cohabitating, the declining fertility rates, and a wealth of other factors.[88] Similarly, home refers to both one's domicile or the place where they carry out their usual activities.[89] Correspondence, as discussed above, should be read to include both electronic forms, such as email and instant messages, and other traditional forms.[90] In the cases below, the HRC shows that privacy with respect to these categories is a broad concept, determined by the circumstances.

ii. What Is an "Arbitrary or Unlawful" Interference?

Once an interference is determined to fall within the scope of

84. *General Comment 16*, *supra* note 56, pts. 1, 4, 8, 10.0.
85. *Id.* pt. 1.
86. *Id.* pt. 1, 5.
87. PEW RSCH. CTR., PARENTING IN AMERICA: OUTLOOK, WORRIES, ASPIRATIONS ARE STRONGLY LINKED TO FINANCIAL SITUATION, 15–16 (2015) https://www.pewresearch.org/social-trends/2015/12/17/1-the-american-family-today.
88. *See id.* (stating that there is no longer one dominant family form); *id.* (stating that compared to the 1960s, increasingly more children are born outside of marriage and to single women).
89. *General Comment 16*, *supra* note 56.
90. *Id.* ¶¶ 1, 8.

Article 17, the next step of the analysis is to determine whether the interference is unlawful or arbitrary.

When a dispute arises and the injured party claims the government or a private party has interfered with their rights under Article 17, the first question in analyzing the claim must be whether the interference was lawful. As stated above, unlawful interferences are those not "envisaged by the law."[91] Therefore, any interference must be made on the basis of law, not simply in the absence of law.[92] Accordingly, specific legislation that is clear and accessible to citizens must outline how interferences may occur in detail.[93]

Next, if a restriction is determined to be lawful, it must also be determined to be non-arbitrary to be acceptable. *General Comment 16* states that arbitrariness should be judged in light of the objectives of the ICCPR and in light of the particular circumstances.[94]

In the cases discussed below, the HRC analyzes claims on a case-by-case basis to determine whether privacy interferences are unlawful and or arbitrary.

2. ICCPR Article 17 as a Protection for Access to Safe Abortions in the United States

An array of decisions from the HRC demonstrate that the Committee believes restricting or interfering with access to abortions is a violation of ICCPR Article 17.[95] Even when abortion restrictions are lawful according to domestic laws, the HRC consistently finds such restrictions arbitrary. After *Dobbs*, abortion restrictions have been lawfully enacted in many states but, under the HRC's analysis, these restrictions are arbitrary. Likewise, surveilling private reproductive health data to interfere, directly or indirectly, with abortion access violates Article 17.

---

91. *Id.* ¶ 3.
92. *Id.* ¶¶ 1, 3, 9.
93. *Id.*
94. *Id.* ¶ 4.
95. *K.L. v. Peru*, Communication No. 1153/2003, HRC, ¶¶ 2.2–2.5, 3.1, U.N. Doc. CCPR/C/85/D/1153/2003 (Oct. 24, 2005); Mellet v. Ireland, Communication No. 2324/2013, HRC, ¶ 7.8, U.N. Doc. CCPR/C/116/D/2324/2013 (Mar. 31, 2016); Whelan v. Ireland, Communication No. 2425/2014, HRC, ¶ 7.9, U.N. Doc. CCPR/C/119/D/2425/2014 (Mar. 17, 2017).

i. Abortion Access Interferences in the United States Fall Within the Scope of Article 17 as Interferences with One's Privacy

To apply the HRC's Article 17 analysis, the first step is to show that the alleged violation falls within the scope of the Article as an interference with one's privacy, family, home, or correspondence.[96] The following cases demonstrate that interference with abortion access falls within the scope of Article 17.

As stated above, *K.L. v. Peru* is a critically important case because it established that a person's decision to request an abortion is an issue within the scope of Article 17.[97] After K.L., a minor, was informed of a fetal abnormality and advised by a doctor to seek an abortion, she sought treatment at the hospital.[98] There, she was told that termination could not be carried out because it was prohibited under Peru's criminal code and "therapeutic abortion was permitted only when termination of the pregnancy was the only way of saving the life of the pregnant woman or avoiding serious and permanent damage to her health."[99] Despite reports by social workers and psychologists advising that making K.L. bring the pregnancy to term would cause extreme anguish due to the eventual fatal outcome, she was not permitted to have an abortion.[100] K.L. claimed that by denying access to an abortion, Peru arbitrarily interfered in her private life and the HRC agreed.[101]

In deciding that Peru had violated K.L.'s Article 17 right to privacy, the HRC acknowledged that State Parties have a duty to act, even when the state itself is not inflicting the harm. Under *General Comment 16*, State Parties should enact legislation to prevent private parties from interfering and provide victims an avenue for redress.[102]

The right to abortion access established in *K.L. v. Peru* is analogous to abortion access in the United States as women in each case are being denied a right to abortion access. Consequently, the various forms of

96. ICCPR, *supra* note 35, art. 17.
97. *K.L. v. Peru*, Communication No. 1153/2003, HRC, ¶ 6.4.
98. *Id.* ¶¶ 2.2, 2.3.
99. *Id.* ¶ 2.3.
100. *Id.* ¶¶ 2.4–2.6.
101. *Id.* ¶¶ 3.6, 6.4.
102. *General Comment 16*, *supra* note 56, ¶¶ 9, 11.

prosecution, harassment, and deterrence taking place in the United States, such as the use of Planned Parenthood visitor's location data to send them anti-abortion advertisements, is interference with abortion that violates pregnant people's privacy rights under Article 17.[103] Additionally, non-governmental interference by entities such as hospitals or doctors is comparable to interference by private parties in the United States, such as anti-abortion groups that weaponize data, femtech apps that collect and sell personal data without consent, and other technologies that overreach.

Finally, while *K.L. v. Peru* established that interference with abortion access falls within the scope of Article 17, *Whelan v. Ireland* expanded on this notion to include protections for healthcare providers.[104] Though the *Whelan* case dealt with a woman who was denied access to abortion after learning her fetus had a fatal defect, the HRC also acknowledged that healthcare providers should not fear criminal sanctions when delivering medical advice.[105] The HRC suggested that Ireland, "take measures to ensure that health-care providers are in a position to supply full information on safe abortion services without fearing being subjected to criminal sanctions."[106]

Similarly, in the United States, femtech apps, telehealth platforms, and practitioners who communicate with patients virtually all allow individuals to seek healthcare advice. Consequently, these entities are effectively healthcare providers. In the eyes of the HRC, these entities should not be prevented from supplying advice by the threat of prosecution, yet many providers in the United States face the same threats that pregnant people do under current abortion restrictions.[107]

103. Cox, *supra* note 11 ("A location data firm is selling information related to visits to clinics that provide abortions including Planned Parenthood facilities, showing where groups of people visiting the locations came from, how long they stayed there, and where they then went afterwards, according to sets of the data purchased by Motherboard.").

104. Whelan v. Ireland, Communication No. 2425/2014, HRC, ¶ 9, U.N. Doc. CCPR/C/119/D/2425/2014 (Mar. 17, 2017).

105. *Id.*

106. *Id.*

107. Conti-Cook, *supra* note 16, at 10 ("[D]igital trails will lead to investigations and prosecutions of medical providers and those who assist with abortions.").

ii. Abortion Access Interferences in the United States are Arbitrary Interferences Under Article 17

In finding that interferences with abortion access fall under the scope of Article 17, the next step in the HRC analysis is to determine whether such interferences are unlawful or arbitrary. Recall that even if interferences are lawful, they may still be deemed violations of Article 17 if they are found to be arbitrary.[108] In both *Whelan v. Ireland* and *Mellet v. Ireland*, the Irish Constitution clearly stated that abortion restrictions were lawful.[109] However, in both cases, the HRC engaged in a balancing test to show that individuals' privacy interests are arbitrarily violated when their reproductive autonomy is impeded.[110]

As mentioned above, Whelan's fetus was diagnosed with a fatal birth defect and Whelan was forced to travel out of the country to receive an abortion.[111] As a result, she suffered mental anguish and suffered great emotional and financial costs. Whelan argued that the interference with abortion access arbitrarily violated her right to privacy under Article 17.[112]

Finding that a woman's reproductive autonomy is included in their right to privacy and may be at risk when the state interferes with a woman's reproductive decision-making, the HRC then engaged in a balancing test between the state's interest in protecting the fetus and an individual's interest in their reproductive privacy.[113] The HRC stated that limitations to privacy must be proportional to the interest the state is aiming to protect.[114] Here, the Committee found that Whelan's interest in her autonomy was greater than the state's interest in protecting the fetus and recommended that Ireland amend its law to allow for voluntary abortion.[115]

---

108. *General Comment 16*, *supra* note 56, ¶¶ 3, 4.
109. *Whelan*, Communication No. 2425/2014, HRC, ¶¶ 7.8, 7.9; Mellet v. Ireland, Communication No. 2324/2013, HRC, ¶¶ 3.6, 3.22, U.N. Doc. CCPR/C/116/D/2324/2013 (Mar. 31, 2016).
110. *Whelan*, Communication No. 2425/2014, HRC, ¶¶ 7.8, 7.9; *Mellet*, Communication No. 2324/2013, HRC, ¶ 7.8.
111. *Whelan*, Communication No. 2425/2014, HRC, ¶ 2.4.
112. *Id.* ¶¶ 2.4–2.6.
113. *Id.* ¶¶ 7.8, 7.9.
114. *Id.*
115. *Id.* ¶¶ 7.8, 7.9, 9.

Mellet v. Ireland is similarly valuable because it again demonstrates the HRC's analysis of arbitrary interferences that are lawful under a state's domestic law.[116] When Mellet was informed that her fetus was not viable, she was forced to leave the country to procure an abortion.[117] As noted above, Ireland's Constitution prohibits abortions in all cases except when the mother's life is in danger.[118] As such, denying Mellet's request for an abortion was legal under domestic law. However, the HRC found that Ireland's decision to uphold the "right to the life of the unborn" infringed on Mellet's autonomy and privacy at the expense of her well-being.[119] Because Mellet had to endure intense suffering and the negative consequences of traveling for medical care, the HRC found that Ireland arbitrarily violated Article 17.[120]

Engaging in the balancing test described above, the HRC described that the arbitrariness requirement is intended to ensure that the interference is reasonable under particular circumstances.[121] Further, the interference must be proportionate to the aims of the ICCPR.[122] The HRC found that Ireland's law limited Mellet's right to privacy to protect the fetus, which was neither reasonable nor proportionate.[123]

Arguably, the now-legal abortion restrictions imposed by individual states after *Dobbs*[124] inflict similar unreasonable and disproportionate consequences on pregnant people seeking an abortion. For some people living in anti-abortion states, travel is not an option and their bodily autonomy is completely impaired. Or conversely, those who must travel for care, like Mellet and Whelan, incur significant costs, are often not able to be accompanied by family and friends, may have

116. Mellet v. Ireland, Communication No. 2324/2013, HRC, ¶¶ 7.7, 7.8, U.N. Doc. CCPR/C/116/D/2324/2013 (Mar. 31, 2016).
117. *Id.* ¶¶ 2.1, 2.4.
118. *Id.* ¶ 7.2.
119. *Id.* ¶¶ 7.7, 7.8.
120. *Id.* ¶ 7.8.
121. *Id.*
122. *Id.* ¶¶ 7.7, 7.8.
123. *Id.*
124. *See Dobbs v. Jackson Women's Health Org.*, 142 S. Ct. 2228 (2022) (overturning the constitutional right to abortion and paving the way for individual states to enact abortion restrictions at any stage of pregnancy, regardless of the circumstances).

to wait extended periods of time for treatment, and expose themselves to harassment.[125] All of these barriers cause suffering, stress, and inconvenience. Even if abortion restrictions in the United States are now lawful, they would likely be considered arbitrary by HRC standards because they interfere significantly with an individual's right to exercise privacy regarding their health and family when choosing how to cope with pregnancy.

Additionally, *Whelan* and *Mellet* reiterate the decision in *K.L. v. Peru*, bolstering the assertion that a pregnant person's interest in their bodily autonomy is a legitimate privacy interest.[126] Applying this to the United States' lack of privacy regulations, it is necessary to weigh the state's interest in allowing apps, companies, and other entities to collect data against an individual's interest in their reproductive privacy. So far, the HRC has not found that any state interest outweighs an individual's interest in their reproductive privacy when choosing whether or not to pursue an abortion, so it is unlikely the HRC would find a compelling state interest in the United States' lack of regulations.

3. ICCPR Article 17 as a Protection for Reproductive Health Data in the United States

In addition to bodily autonomy being an established form of privacy under Article 17, the HRC has interpreted the ICCPR to provide that personal data must also be protected. The following HRC decisions establish that failure to protect personal data is a violation of Article 17. Because the United States does not adequately regulate the collection and use of reproductive health data, a form of personal data, the government has violated its obligations under Article 17.

125. *See Mellet*, Communication No. 2324/2013, HRC, ¶¶ 2.4, 2.5, 3.3; *see* Cox, *supra* note 11.

126. *See K.L. v. Peru*, Communication No. 1153/2003, HRC, ¶¶ 3.6, 6.4, U.N. Doc. CCPR/C/85/D/1153/2003 (Oct. 24, 2005); *Mellet*, Communication No. 2324/2013, HRC, ¶ 7.8; Whelan v. Ireland, Communication No. 2425/2014, HRC, ¶ 7.9, U.N. Doc. CCPR/C/119/D/2425/2014 (Mar. 17, 2017).

i. Reproductive Health Data Interferences in the United States Fall Within the Scope of Article 17 as Interferences with One's Privacy

Once again, the first step in applying the HRC's Article 17 analysis is determining that the alleged violation falls within the scope of the Article as an interference with one's privacy, family, home, or correspondence.[127] The following cases demonstrate that personal data, and particularly data pertaining to health, is a privacy interest within the scope of Article 17.

In *N.K. v. Netherlands*, the HRC discussed the implications of storing an individual's private health information in a database.[128] When N.K. was still a minor, a public prosecutor mistakenly sent her a DNA testing kit even though she had not been convicted.[129] Despite the mistake, her DNA was analyzed and stored in a police database, accessible for future criminal investigations.[130] N.K. argued that she was subjected to arbitrary interference with her private life, in violation of Article 17.[131] The HRC found that the collection of DNA material to analyze and store the collected material in a database that could be used in the future for criminal investigation is sufficiently intrusive and constituted an interference with the N.K.'s privacy under Article 17.[132] This was true even when the information could later be deleted or destroyed.[133]

Likewise, in *Vandom v. Republic of Korea*, the HRC similarly found that Korea violated the complainant's health data privacy under Article 17.[134] Here, a national of the United States was teaching English in Korea when the Ministry of Justice of the Republic of Korea instituted a policy requiring teachers who were not nationals of

127. ICCPR, *supra* note 35, art. 17.
128. N.K. v. Netherlands, Communication No. 2326/2013, HRC, ¶ 9.3, U.N. Doc. CCPR/C/120/D/2326/2013 (July 18, 2017).
129. *Id.* ¶¶ 3.1, 3.2.
130. *Id.* ¶¶ 2.1, 2.2, 9.3.
131. *Id.* ¶ 3.1.
132. *Id.* ¶¶ 9.3, 9.5, 9.6, 9.11.
133. *Id.* ¶¶ 9.3, 9.11.
134. Vandom v. Republic of Korea, Communication No. 2273/2013, HRC, ¶ 8.9, U.N. Doc. CCPR/C/123/D/2273/2013 (July 12, 2018).

Korea to complete mandatory HIV testing to obtain a visa.[135] Noting that even lawful interferences with privacy must comply with the aims and objectives of the ICCPR, the HRC found that the HIV testing requirement was not reasonable because any benefits deriving from testing visa applicants for HIV were negligible in comparison to the privacy interest such a test violated.[136] The HRC's decision in *Vandom* confirms that one's privacy interest in their health data is significant.[137]

Applying the HRC's rationale in *N.K. v. Netherlands* and *Vandom v. Republic of Korea* to the present situation in the United States, it becomes clear that the government's failure to regulate the use and collection of reproductive health data is a violation of Article 17. First, collecting health data falls within the privacy concerns, or scope, of Article 17. In *N.K. v. Netherlands*, the HRC condemned unreasonably collecting personal health data to analyze and store in a database that could later be used in criminal investigations.[138] Further, the HRC persisted in this belief even in situations where the data could be deleted.[139] Similarly, collecting, holding, and selling individuals' private reproductive health data, especially without their knowledge or consent, exposes private data that could be used to harass or prosecute people. Even though some femtech apps and similar entities allow users to delete their data, the HRC acknowledges that the simple act of collecting unauthorized data was sufficiently intrusive.[140] As such, the United States' failure to act falls within the scope of Article 17.

ii. Reproductive Health Data Interferences in the United States are Unlawful and or Arbitrary Interferences Under Article 17

In finding that interferences with health data fall within the scope of Article 17, the next step in the HRC analysis is to determine whether such interferences are unlawful or arbitrary. As discussed above, if the HRC determines that an interference is lawful, it applies a balancing

135. *Id.* ¶¶ 2.1, 2.2.
136. *Id.* ¶¶ 8.8, 8.9.
137. *Id.* ¶¶ 8.9, 9.
138. N.K. v. Netherlands, Communication No. 2326/2013, HRC, ¶ 9.3.
139. *Id.* ¶ 9.3 (wherein the DNA samples collected could be deleted from the database after they were entered).
140. *Id.* ¶¶ 9.3, 9.11.

test to determine whether it is arbitrary and therefore a violation of Article 17.[141]

The case *G. v. Australia* illustrates a situation where lawful interference with informational and familial privacy was found to be arbitrary.[142] In this case, G. was a transgender woman seeking to change her sex on her birth certificate from male to female.[143] While seeking to amend her birth certificate, she was told she could not change her sex unless she was divorced from her spouse.[144] Under Australian law, an explicit requirement dictated that a person be unmarried if they wished to change their sex on their birth certificate.[145] G. argued that Australia invaded her privacy for several reasons.[146] First, her birth certificate revealed private information about the fact that she was transgender, and her privacy includes the right to control information about her sex and her medical history.[147] Second, she argued that an interference with privacy arises when information is revealed to the public without an individual's consent.[148] Finally, G. contended that requiring her to divorce her spouse to change her sex on her birth certificate interfered with her

141. *General Comment 16*, *supra* note 56, ¶¶ 3, 4 ("The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.").

142. G. v. Australia, Communication No. 2172/2012, HRC, ¶¶ 7.3, 7.10, U.N. Doc. CCPR/C/119/D/2172/2012 (Mar. 17, 2017) ("[T]he Committee is of the view that the interference with the author's privacy and family is not necessary and proportionate to a legitimate interest, and is therefore arbitrary within the meaning of article 17.").

143. *Id.* ¶¶ 2.1, 2.6.

144. *See id.* ¶ 2.6 ("In a letter dated 30 July 2010, the New South Wales Registry stated that under section 32B(1)(c) of the Births, Deaths and Marriages Registration Act 1995, a person must be unmarried at the time of their application to register a change of sex.").

145. *See id.* ¶ 2.6 (citing sections 32B(1)(c) and 32D (3) of the Births, Deaths, and Marriages Registration Act 1995).

146. *Id.* ¶¶ 3.1–3.3 (arguing that her birth certificate reveals private information, her privacy includes the right to control this information, the relevance of this information to the public without consent is an interference, and the requirement that she divorce her spouse in order to change her sex on her birth certificate interfered with her family).

147. *Id.* ¶ 3.2.

148. *Id.*

family.[149]

In reviewing this case, the HRC acknowledged that "an interference with privacy or family under Article 17 must not be arbitrary or unlawful."[150] Because an official act specifically requires that a person be unmarried to register a change in sex on their birth certificate, the interference was envisaged by law and therefore deemed lawful.[151] However, the HRC then considered whether the law was arbitrary.[152] At the time of this conflict, Australia had already allowed G. to change her sex on her passport while staying married, yet would not allow the change on her birth certificate under the same circumstances.[153] The HRC found the law unreasonable under the circumstances, claiming that the necessity and proportionality of the interference were questionable.[154]

The case *N.K. v. Netherlands* also provides an analysis of the lawfulness and arbitrariness of a claimed interference. As described above, N.K. was mistakenly instructed to provide a DNA sample and then the sample was stored for potential use in future criminal prosecutions.[155] The HRC noted that the Netherlands' law regulating DNA collection, the Dutch DNA Testing Act, served a legitimate purpose in investigating and prosecuting serious criminal offenses and seeking justice for victims.[156] Likewise, the law is proportional because it is the best tool to achieve this purpose.[157] However, the HRC cautioned that permissible interference should not be unlimited.[158] The government's interest in fighting crime through this DNA database should be balanced against an individual's interest in privacy.[159]

149. *Id.* ¶ 3.3.
150. *Id.* ¶ 7.4.
151. *See id.* ¶ 2.10 ("[S]ince the New South Wales Registry's decision to refuse the author's application was made in order to comply with the requirement under section 32B(1)(c) of the Births, Deaths and Marriages Registration Act 1995, that decision was lawful.").
152. *Id.* ¶¶ 7.4, 7.10.
153. *Id.* ¶¶ 2.1, 2.3, 2.6.
154. *Id.* ¶ 7.14.
155. N.K. v. Netherlands, Communication No. 2326/2013, HRC, ¶ 9.3, U.N. Doc. CCPR/C/120/D/2326/2013 (July 18, 2017).
156. *Id.* ¶ 9.4.
157. *Id.* ¶¶ 9.4, 9.5.
158. *Id.* ¶ 9.5.
159. *Id.*

Accordingly, the HRC held that the government should only be allowed to obtain information related to an individual's private life if it is absolutely necessary to achieve society's interest.[160] Then, even when an interference works to achieve a legitimate interest, the ICCPR prescribes that detailed legislation must specify the precise circumstances in which an interference could be permitted and designate an authority to authorize interference on a case-by-case basis.[161] Regarding N.K., the HRC found that the lawful procedure was arbitrary because it was neither proportionate nor legitimate to achieve the government's interest due to the fact she was both a child and presumptively innocent when her DNA was collected and stored.[162]

Finally, in *Vandom v. Republic of Korea*, an American teacher living in Korea claimed that the mandatory HIV testing policy for a visa renewal was an arbitrary interference with her right to privacy under Article 17 of the ICCPR.[163] The HRC applied the balancing test and contemplated whether Vandom's privacy interest in her health information outweighed the government's interest in protecting public health.[164]

The HRC began its analysis of the interference by first examining whether it was lawful.[165] Again, the HRC cited *General Comment 16*, which notes that to be lawful, an interference must be "envisaged" by law.[166] In the present case, Vandom was forced to take the HIV test when it was recommended under "mere internal guidelines which had no legal effect," two months before it was officially introduced into

160. *Id.* ¶¶ 9.5, 9.11.

161. *Id.* ¶ 9.5.

162. *Id.* ¶¶ 9.7, 9.9–9.11 (noting that children differ significantly from adults both physically and psychologically, and State parties have a heightened obligation to protect them and their privacy in criminal trials).

163. Vandom v. Republic of Korea, Communication No. 2273/2013, HRC, ¶¶ 8.6, 8.9, U.N. Doc. CCPR/C/123/D/2273/2013 (July 12, 2018).

164. *Id.* ¶ 8.9 (noting that no evidence demonstrates that these kinds of HIV restrictions alone protect public health, evidence actually demonstrates that such restrictions may harm public health, and that the State party has not explained how imposing the policy on E-2 visa holders and applicants – and exempting Korean teaches – were in furtherance of protecting public health, maintaining public order, or are reasonably justifiable).

165. *Id.* ¶¶ 8.6, 8.7.

166. *General Comment 16*, *supra* note 56, ¶ 3.

domestic law.[167] The HRC provision was thus not initially lawful.[168]

Next, the HRC looked at whether, even if the HIV testing was lawful, it was arbitrary. For an interference to be considered non-arbitrary, the HRC once again noted that the interference must (1) comply with the objectives of the ICCPR and (2) be reasonable under the circumstances.[169] Based on the findings of the International Task Team, no evidence was found that HIV restrictions on entry and residence to a country based on positive HIV status alone served the government's interest in protecting public health.[170] While Vandom had a strong interest in her privacy, the Korean government did not demonstrate that a strong interest was being fulfilled through the HIV testing requirement.[171] As such, the HRC found the policy unreasonable under the circumstances and therefore a violation of Article 17.[172]

The cases described above show that time and time again, personal data violations are found to be arbitrary, if not also unlawful when domestic law does not "envisage" such data collection and use.[173] The outcomes in each of these cases are analogous to the reproductive health data violations occurring in the United States currently. For instance, in *G. v Australia*, the HRC determined the government interfered with G.'s privacy because the Australian law at issue both revealed private health information and invaded G.'s private family life.[174] Similarly, femtech apps interfere with individuals' private information and family life by collecting and selling reproductive health information that is used by third parties to learn when a person is pregnant, target individuals who visit abortion clinics, and prosecute

167. *Vandom*, Communication No. 2273/2013, HRC, ¶¶ 8.6, 8.7.

168. *Id.* ¶ 8.7.

169. *Id.* ¶ 8.8 ("The Committee further recalls that the law itself 'must comply with the provisions, aims and objectives of the Covenant, and should be, in any event, reasonable in the particular circumstances.").

170. *Id.* ¶ 8.9.

171. *Id.* ¶¶ 8.6, 8.9.

172. *Id.* ¶ 8.9.

173. *General Comment 16*, *supra* note 56, ¶¶ 3, 4 ("[N]o interference can take place except in cases envisaged by law").

174. G. v. Australia, Communication No. 2172/2012, HRC, ¶ 7.10, U.N. Doc. CCPR/C/119/D/2172/2012 (Mar. 17, 2017).

people who miscarry, to name a few examples.[175] Collecting and selling this data without consent gives third parties access to sensitive information, just as G.'s assigned sex was revealed through her birth certificate. Additionally, making reproductive health data easily accessible enables anti-abortion activists and prosecutors to influence individuals' private decisions about their reproductive health.[176] Just as it would have been arbitrary to force G. to divorce her spouse, it is arbitrary to force individuals to make certain decisions regarding their reproductive health care. Even if the United States' laws do not prevent companies from collecting private health information, this is an arbitrary interference with one's private data and family life just as in *G. v. Australia*.

Similar parallels may be drawn between the arbitrary collection of N.K.'s DNA and the interferences occurring in the United States. When N.K.'s DNA was collected, she had not been convicted so her data did not serve the government's interest in solving and prosecuting criminal cases.[177] Similarly, the users whose data is taken from femtech apps and technologies are also presumptively innocent of any crime.[178] Collecting their data cannot be said to serve a governmental interest that outweighs their privacy concerns. Such data should not be stored for future retaliatory purposes.

Finally, the private health information Vandom was forced to share is comparable to reproductive health data. Vandom's HIV status could have cost her job and visa or had other social consequences.[179]

175. Conti-Cook, *supra* note 16, at 48-58 (discussing femtech apps' practice of covertly collecting data and selling it to advertising agencies and data brokers, the Planned Parenthood hack, and the prosecution of Latice Fisher using her search history).

176. *Id.* at 7 (referencing the Planned Parenthood hack).

177. N.K. v. Netherlands, Communication No. 2326/2013, HRC, ¶¶ 9.6, 9.7, 9.11, U.N. Doc. CCPR/C/120/D/2326/2013 (July 18, 2017).

178. *Compare* Zakrzewski et al., *supra* note 23 (describing how prosecutors used Latice Fisher's previously collected data history to convict her of murdering her fetus), *with* N.K. v. Netherlands, Communication No. 2326/2013, HRC, ¶ 9.3 (holding that past data cannot be stored to potentially use for prosecuting a crime that has yet to be committed).

179. Vandom v. Republic of Korea, Communication No. 2273/2013, HRC, ¶¶ 2.1, 2.2, 2.6, U.N. Doc. CCPR/C/123/D/2273/2013 (July 12, 2018) (describing that those who failed the HIV and drug tests had their E-2 visas cancelled and were

Likewise, reproductive health data that is collected without consent and often distributed among third parties similarly invades one's privacy and exposes individuals to harassment as well as potential social and legal consequences.[180] In *Vandom*, the Korean government attempted to justify its interference by claiming it had an interest in protecting the public from HIV, which was discredited by the HRC. The United States government cannot claim to be providing for public health by allowing apps and private parties access sensitive health information. The anguish and persecution caused by reproductive health data violations work against public health interests altogether.

B. SUMMARY OF APPLYING HRC ANALYSIS TO THE UNITED STATES' APPROACH TO DATA PRIVACY

In sum, the HRC decisions demonstrate that Article 17 protects against interferences with one's ability to obtain an abortion and interferences with an individual's reproductive health data.

First, the HRC determined that Article 17 acts as a protection for safe abortions. The HRC established that a person's decision to pursue an abortion is a private decision about their health and family within the scope of Article 17.[181] Further, the HRC repeatedly held that even lawful abortion restrictions are arbitrary violations of Article 17 because individuals' privacy interests in their bodily autonomy outweigh any governmental interest in restricting abortion.[182]

---

deported); *id.* (describing how immigration authorities warned Vandom that she would face the cancellation of her visa, arrest and loss of employment if she refused to undergo the tests).

180. *See* Conti-Cook, *supra* note 16, at 7-8 (explaining that digital data can be used to surveil "bad behavior" by pregnant people and individuals could be potentially criminalized for being pregnant).

181. *K.L. v. Peru*, Communication No. 1153/2003, HRC, ¶¶ 3.6, 6.4, U.N. Doc. CCPR/C/85/D/1153/2003 (Oct. 24, 2005) (finding that the State party's refusal to act in accordance with the author's decision to terminate her pregnancy was unjustifiable and amounted to a violation of article 17 of the Covenant).

182. Mellet v. Ireland, Communication No. 2324/2013, HRC, ¶ 7.8, U.N. Doc. CCPR/C/116/D/2324/2013 (Mar. 31, 2016) (finding that interfering with the author's decision as to how to best cope with her non-viable pregnancy was unreasonable and arbitrary in violation of Article 17 of the Covenant); Whelan v. Ireland, Communication No. 2425/2014, HRC, ¶ 7.9, U.N. Doc. CCPR/C/119/D/2425/2014 (Mar. 17, 2017) (suggesting even lawful abortion

Accordingly, the abortion restrictions implemented by individual states after *Dobbs* likely violate Article 17. [183]

Next, the HRC also determined that Article 17 acts as a protection for reproductive health data. The HRC decisions established that a person's health data falls within the scope of Article 17.[184] Additionally, the HRC found that lawful interferences with informational privacy were arbitrary when the interference exposed an individual's private information or interfered with their family life.[185] Even when balanced against government interests like public health and criminal justice, personal data privacy interests prevailed.[186] Similarly, the United States' failure to regulate the use and collection of reproductive health data arbitrarily exposes private health information and leaves people vulnerable to harassment and prosecution.

Overall, these HRC decisions illustrate how the ICCPR specifically protects the right to abortions and the right to data privacy. Even in a variety of situations, these privacy interests outweighed government interests every time, making even lawful interferences with privacy

---

restrictions may be arbitrary violations of Article 17 if the pregnant individual suffers or is inconvenienced as a result).

183. S. EXEC. REP. NO. 102-23, *supra* note 36, pt. 2 (acknowledging the United States federal system of government and clarifying that the ICCPR applies to state and local governments as well as the federal government).

184. N.K. v. Netherlands, Communication No. 2326/2013, HRC, ¶ 9.3, U.N. Doc. CCPR/C/120/D/2326/2013 (July 18, 2017); *Vandom*, Communication No. 2273/2013, HRC, ¶ 8.9.

185. *See generally* G. v. Australia, Communication No. 2172/2012, HRC, ¶ 7.10, U.N. Doc. CCPR/C/119/D/2172/2012 (Mar. 17, 2017) (finding law requiring author divorce her spouse to change her sex on birth certificate arbitrary interference); N.K. v. Netherlands, Communication No. 2326/2013, HRC, ¶¶ 9.3, 9.11 (finding lawful collection of DNA material to analyze and storing the collected material in a database that could be used in the future for the purposes of criminal investigation is arbitrary interference); *Vandom*, Communication No. 2273/2013, HRC, ¶¶ 8.6, 8.8 (finding lawful HIV/AIDS and drug testing policies on the specific group of E-2 visa holders and applicants to be arbitrary interference).

186. *See* N.K. v. Netherlands, Communication No. 2326/2013, HRC, ¶¶ 9.3, 9.4, 9.11 (holding that DNA databases that serve a legitimate government interest in furthering criminal investigations cannot justify holding data collected from individuals who had not been convicted at the time the data was collected); *Vandom*, Communication No. 2273/2013, HRC, ¶ 8.9 (holding that mandatory HIV testing did not serve a sufficiently compelling public health interest).

arbitrary violations of Article 17. Under the ICCPR, the government has a duty to prevent unlawful or arbitrary interferences with reproductive health data.

IV. RECOMMENDATIONS

A. CREATE REGIONAL REGULATIONS THAT PROTECT HEALTH DATA

In 2018, the European Union enacted the General Data Protection Regulation (GDPR).[187] The GDPR aims to protect individuals' fundamental freedoms and rights by creating rules on the processing and free movement of personal data.[188] The European Union's approach to data privacy is markedly different from that of the United States. While the United States regards privacy rights broadly, the European Union explicitly aims to protect citizens' digital data by requiring companies to obtain clear consent before consumer data is collected and creating remedial rights if violations occur.[189] What's more, the European Union actively responded to changes in technology and data collection through the GDPR.[190] Rather than mirror the United States' practice of letting companies dictate data policy, the European Union prioritized individual data rights. Under the GDPR's extraterritorial framework, individuals within the European Union are protected against data violations from entities originating in the European Union and those whose business reached into the European Union.[191]

Compared to the GDPR, the United States data policy leaves much

187. Commission Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119/1).

188. *Id.*

189. Matthew Humerick, *The Tortoise and the Hare of International Data Privacy Law: Can the United States Catch Up to Rising Global Standards*, 27 CATH. UNIV. J.L. & TECH. 76, 99, 105–06 (2018) (citing the Charter of Fundamental rights of the European Union).

190. *See id.* at 100, 105 (explaining that the GDPR replaced the European Union's former data privacy regulation, the Data Protection Directive (DPD), in order to create a stronger data protection scheme).

191. *Id.* at 111 (positing that as the European Union privacy rights surpasses those the United States, European Union member states will grow increasingly wary of conducting business with unregulated American companies).

to be desired. To re-establish itself as a worthy player in international data transactions, the United States should look to emulate the GDPR by collaborating with international allies to formulate and enact its own regional or multinational agreement. Adopting an agreement like the GDPR would strengthen the United States' data privacy protections by holding the government to more specific and heightened standards that comply with Article 17 obligations.

B. CREATE AMENDMENTS TO *GENERAL COMMENT 16*

General Comment 16 is incredibly useful in interpreting Article 17 and articulating the breadth of privacy rights individuals should have. However, this Comment was drafted in the 1980s and fails to reflect modern technological advances.[192] *General Comment 16* could not possibly have envisioned the capabilities of contemporary data interference methods.

A 2015 proposal from the American Civil Liberties Union (ACLU) advocated for an update to *General Comment 16* that would incorporate developments in technology and the law.[193] While the ACLU acknowledged that many of the Comment's key principles remain applicable in today's world, other areas need urgent revamping.[194]

To make *General Comment 16* more applicable, the ACLU suggests updates to redefine the scope of privacy, the extent of obligations accruing under the ICCPR, and the meaning of interference.[195] Privacy rights must be redefined to include personal information rights in electronic form and otherwise.[196] Additionally, given the global structure of digital networks, updates should include a clause

192. *The Human Right to Privacy in the Digital Age*, *supra* note 54 ("[T]he committee's original General Comment on privacy, published in 1988, did not anticipate the development of new forms of communication like email and texting, the emergence of government capacities to intercept and process large quantities of electronic data, or the explosion of social media websites.").

193. *Id.*

194. INFORMATIONAL PRIVACY IN THE DIGITAL AGE, *supra* note 55, at 1.

195. *Id.* at i.

196. *Id.* at 8–9 (suggesting Article 17's use of the word "home" should be construed to include personal spaces online and the term "communications" should extend beyond letters and phone calls to include emails, direct messages, and other electronic communication).

explaining that a State Party's obligations must extend extraterritorially.[197] Finally, an updated General Comment should consider that modern interference is often accomplished through the collection, analysis, and use of information data.[198] Infringement of personal privacy or activities that dissuade an individual from engaging in otherwise protected acts should be considered violations under this article.

Though one single document cannot possibly account for the innumerable technological advancements capable of interfering with digital data privacy, *General Comment 16* should be a living document that attempts to address the most prominent modern concerns while preparing for others.

C. ENACT DOMESTIC LEGISLATION

Despite attempts to introduce legislation that addresses reproductive health data post-*Dobbs*, there are presently no federal laws or practices that adequately regulate reproductive data security. To provide for digital data security, Congress should prioritize and pass two bills currently on the floor and additionally urge states to enact privacy legislation.

First, the *American Data and Privacy Protection Act* (ADPPA) is a bipartisan bill that was introduced in the House of Representatives in June of 2022.[199] The bill establishes protections that allow consumers to access, correct, and delete their data. ADPPA would additionally require data collection to be minimally intrusive, which coincides with the aims of Article 17.[200] If companies fail to implement the security

197. *Id.* at 6("It should also address emerging issues by affirming the inherent illegality of mass surveillance and the nature and extent of a State's extraterritorial obligations to protect the right to privacy.").

198. *Id.* at v ("The interpretation of 'interference' under Article 17 must account for recent advances in information technology, the now-artificial distinction between metadata and content, the erosion of boundaries between the public and private sphere, and the modern day capacities of States Parties to infringe persons' rights to privacy by tracking Internet and other electronic activities, and collecting, storing, and synthesizing electronic data.").

199. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2021).

200. *Id.*; *see also General Comment 16*, *supra* note 56, ¶¶ 7, 8, 11 (stating that interferences with informational privacy should be minimally intrusive and never invasive enough to impair the right).

measures created by this bill, the Federal Trade Commission (FTC) is empowered to hold them accountable.[201] Though more work must certainly be done to ensure complete data privacy, scholars consider passing the ADPPA necessary to fill the void in the United States' data privacy law.[202]

The *My Body, My Data Act* is a bill more narrowly focused on establishing protections for personal reproductive or sexual health information.[203] The proposed restrictions specifically target platforms that collect personal data without being subject to existing health-related privacy regulations.[204] This includes fertility apps, entities that provide reproductive health services, and entities that engage with pregnancy, menstruation, contraception, sexual health, and more.[205] Echoing the language of *General Comment 16*, the bill requires such entities to provide users with a mechanism to delete their reproductive or sexual health information.[206] It additionally obligates entities to publish a privacy policy to inform individuals about how their data will be used and obtain consent before disclosing any data.[207] Finally,

201. American Data Privacy and Protection Act, *supra* note 199.

202. Anne Toomey McKenna, *A New U.S. Data Privacy Bill Aims to Give You More Control Over Information Collected About You – And Make Businesses Change How They Handle Data*, CONVERSATION (Aug. 23, 2022), https://theconversation.com/a-new-us-data-privacy-bill-aims-to-give-you-more-control-over-information-collected-about-you-and-make-businesses-change-how-they-handle-data-188279 (acknowledging that the ADPPA has potential shortcomings, like failing to include deidentified data, which can often still be traced to individuals).

203. My Body, My Data Act, H.R. 8111, 117th Cong. (2021) (showing this bill was introduced in the House of Representatives in June of 2022, one day before the *Dobbs* decision was released).

204. *Id.* §§ 2, 3.

205. Hayley Tsukayama & India McKinney, *Pass the "My Body, My Data" Act*, ELEC. FRONTIER FOUND. (June 21, 2022), https://www.eff.org/deeplinks/2022/06/pass-my-body-my-data-act.

206. My Body, My Data Act, *supra* note 203, § 3 ("A regulated entity shall make available a reasonable mechanism by which an individual, upon a verified request, may request the deletion of any personal reproductive or sexual health information."); *see also General Comment 16*, *supra* note 56, ¶ 10 (suggesting that individuals should have the right to know which public authorities or private individuals can access their data); *id.* (maintaining that States must ensure that information regarding an individual's private life cannot be obtained by those not authorized to have it).

207. My Body, My Data Act, *supra* note 203, § 4.

this bill prohibits any unnecessary data collection, meaning that apps would be unable to collect data not directly related to its stated purpose.[208] If enacted, this bill could remedy femtech apps' laissez-faire approach to privacy.

As previously articulated, Article 17 obligates State Parties to provide a legislative framework to prohibit interference by private entities.[209] To fulfill these obligations, Congress must enact legislation like the *American Data and Privacy Protection Act* and the *My Body, My Data Act* which responds to reproductive health data violations from individuals, organizations, and commercial entities. If Congress fails to enact this crucial legislation, individual states should fulfill their obligations under the ICCPR by enacting their own legislation and giving individuals enforceable privacy protections.[210]

V. CONCLUSION

While technological advances and the rise of femtech have left reproductive health data vulnerable for years, the *Dobbs* decision highlighted the lack of data privacy regulations in the United States. As a State Party to the International Covenant on Civil and Political Rights, the United States is bound by Article 17, which protects against arbitrary and unlawful interferences with one's privacy. A series of decisions by the Human Rights Committee illustrate how Article 17 specifically protects both the right to abortion and health data privacy. Accordingly, by failing to protect against interferences with the use and protection of reproductive health data, the United States violates its obligations under the ICCPR Article 17 and must act quickly to remedy this human rights crisis.

208. *Id.* § 2.

209. *General Comment 16*, *supra* note 56, ¶¶ 1, 9–11.

210. S. EXEC. REP. NO. 102-23, *supra* note 36, pt. 2 (noting that the Senate ratification documents bind individual states to ICCPR obligations); Kaye, *supra* note 52, at 96 (noting that the federal government has failed to give legal effect to the ICCPR domestically and suggesting that states may be the principal institutions for enforcing human rights law).

* * *