DATING DATA: LGBT DATING APPS, DATA PRIVACY, AND DATA SECURITY

Nivedita Sriram[*]

TABLE OF CONTENTS

I. INTRODUCTION

With the advent of the Internet and mobile phones, an increasing number of American adults are using online dating as a way to meet people. A 2016 study from the Pew Research Center reported that 15% of adults in the United States have used online dating sites or mobile apps.[1] Dating apps originated for the gay community[2] and same-sex attracted individuals are using these services at a higher rate than their opposite-sex attracted counterparts.[3] This is in part because of the unique opportunities the Internet affords LGBT people who may

* J.D. Candidate, University of Illinois College of Law Class of 2021. I would like to thank Sriram, Kripa, and Abhinav for supporting me through everything, and Emily Muerhoff for always having a listening ear. I would also like to thank Professor Faye E. Jones for her feedback and guidance. A special thank you to all the JLTP editors, and members for their contributions in editing this Note.

1. Aaron Smith & Monica Anderson, *5 Facts About Online Dating*, PEW RSCH. CTR. (Feb. 29, 2016), https://www.pewresearch.org/fact-tank/2016/02/29/5-facts-about-online-dating.

2. Ashley Fetters, *How Tinder Changed Dating for a Generation*, THE ATLANTIC (Dec. 21, 2018), https://www.theatlantic.com/family/archive/2018/12/tinder-changed-dating/578698.

3. Michael Rosenfeld, *Disintermediating Your Friends: How Online Dating in the United States Displaces Other Ways of Meeting*, 116 PNAS 17753 (finding that in 2017, 65% of same sex couples met on online dating apps, where 39% of heterosexual couples did so).

face stigma, discrimination, difficulty finding other local LGBT singles, or other roadblocks to dating offline.[4] Popular examples of these dating apps—like Tinder or Grindr—are location-based or geosocial, suggesting and connecting users to other users within a specific geographic radius depending on users' relative distance from one another.[5]

Privacy and security risks of all kinds exist for users of geosocial apps that are targeted toward the general public, such as Tinder, including problems in the way the apps are coded that make users' locations easily visible.[6] Adding active location broadcasts to apps has made it "theoretically possible to determine a user's address, track their movements, and even stalk a user throughout the day."[7] Revealing a user's location is considered a significant privacy breach.[8] As illustrated later in this Note, it is frighteningly common for users of dating apps to have their privacy and security breached.[9] The number of times researchers have demonstrated this illustrates that there is a particularly high risk to the members of the LGBT community who use these apps.[10]

The Privacy International Network, in emphasizing why issues related to gender and privacy are so important, noted, "[e]very human being is to a degree subject to corporate and government surveillance. But…there is a uniqueness to the surveillance faced by women, trans and gender queer people. Understanding this experience means shedding light on the inextricable ties between surveillance, patriarchy and other systems of oppression, which rely on surveillance to retain control and power."[11] Many researchers who look at the security failings of apps like Grindr choose to study these apps because of the vulnerability of the LGBT community to online surveillance.[12] The unique risks of being LGBT in any society compound the need for privacy for LGBT users online.[13] The need for privacy and the need for security are intertwined.

In the years since the apps have been launched, the leaking of location data has become clear to the developers of these apps, but little has been done to

4. Fetters, *supra* note 2; Ari Ezra Waldman, *Opinion: Queer Dating Apps Are Unsafe by Design*, N.Y. TIMES (June 20, 2019), https://www.nytimes.com/2019/06/20/opinion/queer-dating-apps.html.

5. Fetters, *supra* note 2.

6. *See, e.g.*, Bree Fowler, *Flaws in Tinder's App Put Users' Privacy at Risk, Researchers Say*, CONSUMER REP. (Jan. 23, 2018), https://www.consumerreports.org/privacy/tinder-app-security-flaws-put-users-privacy-at-risk (explaining how Tinder allowed hackers to see how users used the app); *see also How Tinder Keeps Your Exact Location (A Bit) Private*, ROBERT HEATON (July 9, 2018), https://robertheaton.com/2018/07/09/how-tinder-keeps-your-location-a-bit-private (explaining flaws in Tinder's location function that left users' locations exposed).

7. Jody Farnden et al., *Privacy Risks in Mobile Dating Apps*, *in* PROC. OF THE TWENTY-FIRST AMERICAS CONF. ON INFO. SYS. 2 (2015).

8. Iasonas Polakis et al., *Where's Wally? Precise User Discovery Attacks in Location Proximity Services*, *in* PROC. 22ND ACM SIGSAC CONF. ON COMPUT. AND COMMC'NS. SEC. 817, 817 (2015).

9. *Infra* Section II.B.

10. *Data Privacy is Crucial for the LGBT Community*, STOP. THINK. CONNECT (Feb. 20, 2018), https://www.stopthinkconnect.org/blog/data-privacy-is-crucial-for-the-lgbt-community [hereinafter *Privacy is Crucial*].

11. *Gender*, PRIV. INT'L, https://privacyinternational.org/topics/gender (last visited Oct. 21, 2020).

12. *See, e.g.*, Andy Greenberg, *Gay Dating Apps Promise Privacy, But Leak Your Exact Location*, WIRED (May 20, 2016, 7:00 AM), https://www.wired.com/2016/05/grindr-promises-privacy-still-leaks-exact-location ("But Hoang says the Kyoto team focused on gay dating apps in part because of the vulnerability of the LGBT population to online surveillance.").

13. *Id.*

change the apps and protect users.[14] The problem is that the law permits the development of apps that are unsafe by design,[15] and there is no easy solution.

Part II of this Note discusses the history and use of geolocative dating apps in the LGBT community, and it presents a timeline of the security and privacy breaches of users of these apps, particularly on the popular app Grindr. Part III discusses the recognition of need for extra protection of the LGBT community—even in modern American society, the steps geolocative dating apps for same-sex attracted men have taken to protect their users, the failures of these apps to adopt readily available fixes to make their platforms safer, and the reactions to and implications of these failures. Part IV discusses why it is possible, but unfair and unfeasible, to ask users of these apps to protect themselves and their own locations while using the apps, the reasons why external enforcement of safety features is necessary, and what should be done to ensure the security and privacy of users of LGBT dating apps is uncompromised and secure.

II. BACKGROUND

A. A History of Dating Apps and Their Uses in the LGBT Community

The LGBT community is said to have invented and innovated online dating, with an overwhelming number of same-sex couples having met online.[16] Grindr was one of the first dating apps geared toward same-sex attracted people[17] and is an exceptionally popular dating app geared toward gay and bisexual men. It has users in more than 234 countries and territories all around the world,[18] with 3.8 million daily users and 27 million users worldwide.[19]

The history of dating apps having a greater use in the LGBT community, particularly for men who seek to date other men, because of its root in the invisibility of same-sex attraction.[20] Actively choosing to be present on an app for same-sex attracted people helps members of the LGBT community identify each other, and allows users control over if, how, and with whom they present their LGBT identity.[21] Users who are LGBT might also find apps that are aimed broadly toward the general population to be unfriendly in their user interface and

14. *Infra* Section III.A.

15. Waldman, *supra* note 4.

16. Jon Shadel, *A Queer User's Guide to the Wild and Terrifying World of LGBTQ Dating Apps*, WASH. POST (Oct. 8, 2019, 6:00 AM), https://www.washingtonpost.com/lifestyle/2019/10/08/queer-users-guide-wild-terrifying-world-lgbt-dating-apps.

17. Nguyen Phong Hoang, et al., *Your Neighbors are My Spies: Location and Other Privacy Concerns in GLBT-focused Location-based Dating Applications*, 5 ICACT TRANSACTIONS ON ADVANCED COMMC'NS. TECH. 851, 855 (2016).

18. Brian Latimer, Grindr Security Flaw Exposes Users' Location Data, NBC NEWS (Mar. 28, 2018, 6:52 AM), https://www.nbcnews.com/feature/nbc-out/security-flaws-gay-dating-app-grindr-expose-users-location-data-n858446.

19. Jon Shadel, *Grindr Was the First Big Dating App for Gay Men. Now It's Falling Out of Favor*, WASH. POST (Dec. 6, 2018), https://www.washingtonpost.com/lifestyle/2018/12/06/grindr-was-first-big-dating-app-gay-men-now-its-falling-out-favor.

20. Jeremy Birnholtz et al., *Identity, Identification and Identifiability: The Language of Self-Presentation on a Location-Based Mobile Dating App*, SOC. NETWORKS & INPUT & INTERACTION 3, 3 (2014).

21. *Id.*

would feel more comfortable using an app that is meant to cater more specifically to LGBT identities.[22] A study from 2013 shows that compared to heterosexual populations, gay men tended to open their dating apps more and spend more time on them when the apps were open.[23]

While this Note refers broadly to the security and privacy needs of the LGBT community, and the recommendations apply to the needs of the community as a whole, this Note focuses on apps used by men and nonbinary individuals who are attracted to men. This is primarily because there has not been a popular dating app geared toward women and nonbinary individuals who are looking for women.[24] The app HER, used by five million users in 113 countries,[25] and the more recent Lex, which was downloaded by six thousand users when it launched in November 2019, are the only apps geared toward women that have sizable followings.[26] Tinder has reported itself as the most used app for LBTQ women,[27] although Tinder is by no means a perfect environment for women looking to date without facing harassment from other users not in their dating pool.[28] Additionally, there are simply more apps geared toward men seeking men,[29] and these apps are the ones that have faced the security and privacy breaches on which this Note focuses.

Geolocation information plays a crucial role in dating apps.[30] Revealing a user's location is considered a significant privacy breach, and services are adopting the more privacy-preserving approach of location proximity: identifying users who are nearby, and at what distance.[31] When the exact distance to a user is revealed, trilateration attacks become possible.[32] Trilateration, which is also colloquially referred to as triangulation, is a process that uses at least three measures to a target from a known distance (or "station") to determine that target's "absolute location."[33] This functionality is effectively similar to GPS and cell phone location services.[34] It is easy to exploit geosocial

22. *See, e.g.*, Chris Riotta, *Tinder Still Banning Transgender People Despite Pledge of Inclusivity*, THE INDEP. (July 17, 2019, 3:58 PM), https://www.independent.co.uk/news/world/americas/tinder-ban-trans-account-block-report-lawsuit-pride-gender-identity-a9007721.html ("Tinder has dealt with accusations of banning transgender and non-binary users from the platform for years, with little controversy or backlash resulting among its estimated 50 million users.").

23. Christian Grov et al., *Gay and Bisexual Men's Use of the Internet: Research from the 1990s through 2013*, 51 J. SEX RES. 390, 404 (2014).

24. Lane Moore, *Why Do So Few Lesbians Use Dating Apps?*, COSMOPOLITAN (Nov. 17, 2015), https://www.cosmopolitan.com/sex-love/news/a44476/lesbian-dating-apps-why-they-suck.

25. Trish Bendix, *A New App Wants to Revolutionize Dating as a Queer Person. Can It?*, THE CUT (Nov. 11, 2019), https://www.thecut.com/2019/11/lex-is-a-dating-app-for-queer-people-but-will-they-use-it.html.

26. *Id.*

27. Mary Emily O'Hara, *Looking for Love on Tinder? Lesbians Must First Swipe Past a Parade of Straight Men*, NBC NEWS (Sept. 2, 2019), https://www.nbcnews.com/think/opinion/looking-love-tinder-lesbians-must-first-swipe-past-parade-straight-ncna1047721.

28. *Id.*

29. Shadel, *supra* note 16.

30. *Sensitive Information Vulnerable on Dating Apps, Say Privacy, Security Experts*, WASH. INTERNET DAILY (Apr. 20, 2015) [hereinafter *Sensitive Information*].

31. Polakis, *supra* note 8, at 817–18.

32. *Id.* at 817.

33. Max Veytsman, *How I was Able to Track the Location of Any Tinder User*, INCLUDE SEC. (Feb. 2014), https://blog.includesecurity.com/2014/02/how-i-was-able-to-track-location-of-any.html.

34. *Id.*

apps that use trilateration techniques to sort users by location and proximity to one another.[35] These vulnerabilities can be used for potentially manipulative and nefarious purposes and can create dangers for all users.

B. A Timeline of Dating App Location Leaks

Grindr's security woes have existed for many years. One early incident related to its location-based services took place in 2014 when a security flaw was discovered in the app that revealed the exact location of every user who had location services enabled.[36] An anonymous user on PasteBin, a website that allows users to store plain text and share it publicly for a period of time, laid out how Grindr sent detailed distance information without requiring any authentication or security keys to access, using trilateration.[37] Using this process, anyone could use the app to find the location, names, and photos of its nearest 50 users.[38] This flaw affected the security of almost every user of the app, since, according to Grindr, more than 90% of its users at the time had location services enabled.[39]

The original PasteBin article claimed that Grindr had knowledge of the flaw, saying, "I know officials at [G]rindr have been informed several times within the past months about these issues, which would seem to imply that the concept of 'social responsibility' is lost upon Grindr."[40] Grindr downplayed the concerns, essentially saying that the ability to share distance was a feature, not a bug, and that any users who did not want to share their location could disable it in the app's settings at any time.[41] However, after being contacted by media about the security flaw, Grindr sent an alert out to its users, warning them that they might want to hide their location on the app.[42]

Tech company Synack looked into "dating services [that] are heavily location aware and possibly insecure" after Tinder was discovered to reveal users' exact GPS coordinates.[43] After being called "basically a stalker's dream,"[44] Tinder quickly patched the bugs.[45] Grindr had been audited in the past and cited for its range of security vulnerabilities, but not for its location-sharing capabilities.[46] Synack found that "Grindr willingly shares location-based data about its users down to [an] incredibl[y] high level of accuracy," allowing any

35. *Id.*

36. James Cook, *Security Flaw in Gay Dating App Grindr Reveals Precise Location of 90% of Users*, BUS. INSIDER (Aug. 29, 2014), https://www.businessinsider.com/exploit-reveals-location-of-grindr-users-2014-8.

37. *[Grindr] Errors and Omissions 2014*, PASTEBIN (Aug. 16, 2014), https://pastebin.com/fRa1s6yQ.

38. Cook, *supra* note 36.

39. *Id.*

40. *[Grindr] Errors and Omissions 2014*, *supra* note 37.

41. Cook, *supra* note 36.

42. *Id.*

43. Patrick Wardle, *The Dos and Don'ts of Location Aware Apps: A Case Study*, SYNACK (Sept. 11, 2014), https://www.synack.com/blog/the-dos-and-donts-of-location-aware-apps-a-case-study.

44. *Sensitive Information*, *supra* note 30.

45. *Id.*

46. Wardle, *supra* note 43.

user or even anonymous non-user of the application to gather information about any Grindr user in the area.[47]

Synack also discovered an important vulnerability in Grindr's existing user-protections regarding location: though Grindr users could restrict their location being shared with other users in the area, the user's location was still sent to the Grindr server, which resulted in it being accessible to *anyone*.[48] Synack also reverse engineered Grindr's Application Programming Interface (API) which allowed it to "spoof" its coordinates on the app, allowing anyone with access to pretend to be in a location where they are not.[49] Because there is no rate limit on the app's API, Synack researchers were able to do this "as many times as [they] want[ed], as fast as [they] want[ed], to any location that [they] want[ed]."[50] This allowed Synack to find and create a map of every single Grindr user in San Francisco.[51]

In 2016, Wired Magazine reporter Andy Greenberg worked with Nguyen Phong Hoang's security research team from Kyoto University to demonstrate how easy it was to find Grindr users, "pinpointing their location down to a few feet" by finding Greenberg's dummy account on Grindr down to the exact intersection where Greenberg lived in New York City.[52] This method worked even when users took the precaution of not sharing their location on the Grindr app itself.[53] Even when users disabled their distance and prevented the app from listing the exact distance they were from a particular user, the users were still displayed on the app in order of how far they were from one another, which allowed their location to be discovered through multiple trilateration tests using the known locations of others on the app who were geographically close to them.[54] Although Greenberg and Hoang used Grindr as their application of choice for this test, Hoang said this method of tracking other users worked with "other gay dating apps like Hornet and Jack'd, too" and successfully demonstrated the location-tracking tactic for Greenberg using those two apps as well.[55]

The issue that allowed this breach was the app's use of trilateration to show other Grindr users nearby in order of proximity to the searching Grindr user.[56] Despite Hornet and Jack'd "adding noise" to their trilateration services to obscure the *exact* distance between users' phones, nearby users were still visible in order, from nearest to furthest from a particular user's phone, which allowed for a colluding trilateration attack.[57] The researchers created two fake Grindr

47. *Id.*
48. *Id.*
49. *Id.*
50. *Id.*
51. *Id.*
52. Greenberg, *supra* note 12.
53. *Id.*
54. @Seppevdpll, *It is Still Possible to Obtain the Exact Location of Millions of Cruising Men on Grindr*, QUEER EUROPE (Sept. 13, 2018), https://www.queereurope.com/it-is-still-possible-to-obtain-the-exact-location-of-cruising-men-on-grindr.
55. Greenberg, *supra* note 12.
56. *Id.*
57. *Id.*

accounts and used their combined trilateration abilities through the app to pinpoint where a particular user would be.[58] They did this by "spoofing" their location from Kyoto, exploiting a weakness in the app's API, similar to what the Synack researchers did.[59] Grindr's responded that it takes user safety "extremely seriously" and was "working to develop increased security features for the app."[60] Hornet and Jack'd responded similarly.[61] There was no indication, to either Hoang or Greenberg, that any of the apps used any of the information they were given to make changes to the way the apps handled location.[62]

A few years later, in March 2018, a startup CEO created a third-party website where Grindr users voluntarily entered their usernames and passwords to see which users had blocked them on the app.[63] The website, C*ckblocked, was able to access information that was collected by the app but not available on people's public profiles, such as the location data of users that had opted through the settings of the app not to make their locations public.[64] It was even easier to find the exact location of users who had opted to make their location public: in a test run by NBC News, the website was able to find the profile "pinpointed down to the area of the building in which the user was located, in a matter of minutes."[65] Any Grindr user who accessed the website could pinpoint other Grindr users, without any sort of verification or authentication.[66] This kind of access would make it easy to pinpoint a user's location, potentially putting peoples' lives at risk.[67] When Grindr learned of this security flaw, it changed its policy on access to data regarding which users had blocked other users, but changed nothing else about its user security.[68] Instead, Grindr warned users to avoid sharing information with third parties to avoid putting their accounts at risk.[69]

In September 2018, security researchers found another instance in which "Grindr [was] still exposing the precise location of its more than 3.6 million users although it has long been aware of the issue."[70] A free app called Fuckr was built in 2015 on top of unauthorized access to Grindr's API and exploited the extremely precise information Grindr collected about its users' locations in order to pinpoint their exact whereabouts using trilateration techniques.[71] Using this app, it was possible to pinpoint which house or even room a user is in[72]—

58. *Id.*
59. *Id.*; Wardle, *supra* note 43.
60. Greenberg, *supra* note 12.
61. *Id.*
62. *Id.*
63. Latimer, *supra* note 18.
64. *Id*.
65. *Id*.
66. *Id*.
67. *Id*.
68. *Id*.
69. *Id*.
70. Nicole Nguyen, *There's a Simple Fix, But Grindr is Still Exposing the Location of Its Users*, BUZZFEED NEWS (Sept. 14, 2018, 5:36 PM), https://www.buzzfeednews.com/article/nicolenguyen/grindr-location-data-exposed.
71. *Id.*
72. @Seppevdpll, *supra* note 54.

one user was able to see that Grindr displayed exactly which corner of his garden he was sitting in.[73] Until Fuckr was publicized in the media and the repository was taken down because of its unauthorized access to the Grindr API, anyone could use the app to find where Grindr users were,[74] "within a few minutes, and without any coding experience."[75]

Grindr's response was to emphasize the importance of geolocation to the app and user experience and at the same time acknowledge the inherent "challenges" to geolocative applications.[76] Grindr also argued that it uses a "geohash" system, which ostensibly obscures the precise location of users by only approximating users' distance from one another.[77] However, as one user tested, Grindr's "approximation" was more precise than it claimed—users could still be located within a few feet of their location, and their locations could be nailed down even more precisely using multiple trilateration tests.[78]

One feature of Grindr, as a "relatively unique place for openness about H.I.V. status," is the ability of users to share H.I.V. data, such as their status or their last time tested, on their profiles.[79] Grindr, without making it clear to their userbase, shared that data with two third-party firms.[80] Although Grindr encrypted the H.I.V. data shared by users and placed the outside firms under strict contractual obligations to keep the data confidential,[81] SINTEF, an independent researcher, found that because the H.I.V. information was sent linked with "users' GPS data, phone ID, and email," it was able to identify specific users and those users' HIV status.[82] SINTEF's research also showed that other sensitive information, such as GPS location, was also being shared out with third-party advertising companies, but this data, unlike the H.I.V. data, was not encrypted and therefore easily hackable.[83]

Grindr responded that this data was shared with two outside companies as "a standard industry practice for rolling out and debugging software."[84] It restricted the data shared to whatever was "appropriate for the services" that the vendors were providing—in this case, to test and support development of features like the app's HIV Test Reminders.[85] Grindr said the services it

73. Nguyen, *supra* note 70.
74. *Id*.
75. @Seppevdpll, *supra* note 54.
76. Nguyen, *supra* note 70.
77. *Id*.; @Seppevdpll, *supra* note 54.
78. @Seppevdpll, *supra* note 54.
79. Azeen Ghorayshi & Sri Ray, *Grindr is Letting Other Companies See User HIV Status and Location Data*, BUZZFEED NEWS (Apr. 2, 2018, 11:45 AM), https://www.buzzfeednews.com/article/azeenghorayshi/grindr-hiv-status-privacy#.knOVOgLLA.
80. *Id*.
81. *Grindr Shared Information About Users' HIV Status With Third Parties*, THE GUARDIAN (Apr. 3, 2018, 12:28 AM), https://www.theguardian.com/technology/2018/apr/03/grindr-shared-information-about-users-hiv-status-with-third-parties.
82. Ghorayshi & Ray, *supra* note 79.
83. *Id*.
84. Mike Sorrentino, *Grindr Dating App to Stop Sharing HIV Status with Third Parties*, CNET (Apr. 2, 2018, 10:15 PM), https://www.cnet.com/news/grindr-dating-app-to-stop-sharing-hiv-status-with-third-parties.
85. Grindr, *Here's What You Should Know Regarding Your HIV Status Data*, TUMBLR (Apr. 2, 2018), https://grindr.tumblr.com/post/172528912083/heres-what-you-should-know-regarding-your-hiv.

received from the outside firms would only make the app experience better,[86] and that the company's internal policies would protect the userbase.[87] The company emphasized that it had never and would never "sell personally identifiable user information—especially information regarding HIV status or last test date—to third parties or advertisers."[88] Grindr subsequently announced that it would no longer share the HIV status of their users with outside companies.[89]

However, it also turned the blame around to its userbase, reminding Grindr users that "Grindr is a public forum" and users should not have had a high expectation of privacy for information they put on their public profiles.[90] Grindr was criticized by both its userbase and major media publications for this lapse in data security, as well as the way it handled the breach.[91]

III. ANALYSIS

A. What Have Dating Apps Done to Protect LGBT Users?

The danger that dating apps have addressed the most clearly and concisely is the issue of LGBT safety in countries that are hostile to LGBT identities.[92] Companies like Tinder and Grindr have been vigilant about addressing this issue on the worldwide stage, in light of dangers faced by LGBT individuals living in or traveling to oppressive nations.[93] Particularly, apps meant for gay and bisexual men (Grindr, as well as Scruff and Hornet) have instituted special features meant to protect their userbase.[94] Grindr, at one point, disabled a feature in Egypt that showed users' precise distances from one another that Egyptian authorities were using to trilaterate users' locations, although it still did rank other users from closest to farthest from the user.[95]

Starting in July 2019, Tinder began offering a "Traveler Alert" feature, which gives users the choice to keep their location private, instead of automatically appearing on Tinder when they arrive in an "oppressive state," or a nation that criminalizes same-sex acts or relationships.[96] If users still opt-in to

86. Ghorayshi & Ray, *supra* note 79.

87. Natasha Singer, *Grindr Sets Off Privacy Firestorm After Sharing Users' H.I.V-Status Data*, N.Y. TIMES (Apr. 3, 2018), https://www.nytimes.com/2018/04/03/technology/grindr-sets-off-privacy-firestorm-after-sharing-users-hiv-status-data.html.

88. Scott Neuman, *Grindr Admits It Shared HIV Status of Users*, NPR (Apr. 3, 2018, 3:47 AM), https://www.npr.org/sections/thetwo-way/2018/04/03/599069424/grindr-admits-it-shared-hiv-status-of-users.

89. *Id.*

90. *Id.*

91. *See, e.g.*, @Seppevdpll, *supra* note 54 (criticizing Grindr's location collecting methods).

92. Mike Miksche, *Gay Dating Apps Are Protecting Users Amid Egypt's LGBTQ Crackdown*, VICE (Oct. 25, 2017, 4:15 PM), https://www.vice.com/en_us/article/pa3pxg/gay-dating-apps-are-protecting-users-amid-egypts-lgbtq-crackdown; Russell Brandom, *Designing for the Crackdown*, THE VERGE (Apr. 25, 2018, 10:42 AM), https://www.theverge.com/2018/4/25/17279270/lgbtq-dating-apps-egypt-illegal-human-rights.

93. Zack Whittaker, *Tinder's New Personal Security Feature Can Protect LGBTQ+ Users in Hostile Nations*, TECHCRUNCH (July 24, 2019, 10:41 AM), https://techcrunch.com/2019/07/24/tinder-security-travel-lgbtq; Miksche, *supra* note 92.

94. Miksche, *supra* note 92.

95. *Id.*

96. Whittaker, *supra* note 93.

make their profile public, their sexual orientation and/or gender identity is hidden from their profile.[97] Tinder uses the user's location data based on their wireless connection and phone network to determine when to offer this option to users who are in 69 countries that the app determined the most dangerous for LGBT users, usually because same-sex relationships are punished under law there.[98] This update is offered to protect LGBT users from law enforcement as well as "others who may target them."[99]

After several LGBT people were arrested for "promoting sexual deviancy" in Egypt in 2014, Grindr offered an update in "Middle Eastern, Gulf, and North African areas" which allowed users to change the appearance of the Grindr app on their smartphones to something "less conspicuous," and to password protect the app and the information contained inside.[100] Grindr made these changes preventing users in oppressive nations' locations from being determined "via trilateration or any other method, keeping [users'] position[s] private and secure" in response to news that authorities in Egypt were using the location functionality to target and arrest gay men.[101] Hornet and Grindr also used the app to send safety tips to users, encouraging them to take care when meeting people users connected with on the app.[102]

However, these efforts did not have perfect results.[103] After a security glitch in 2014 exposed the locations of hundreds of thousands of Grindr users, it repeated its usual statement that the leaking of location is not a security flaw, but shortly after, turned the location-functionality completely off for users in several countries with anti-gay legislation.[104] However, a blog noted that a short while later, the location functionality was re-enabled, and Grindr had not made any other actual substantive changes to the way the app collected and shared location data.[105]

Grindr and Hornet, which had taken a similar tack to allow users to protect their location data, still did not resolve the issue: researchers were still able to locate users using triangulation techniques.[106] In 2018, Grindr was hiding location by default in some countries where LGBT people face persecution, but

97. *Id*.

98. *Id*.

99. Whittaker, *supra* note 93; Nadia Suleman, *Tinder's Newest Feature Aims to Keep LGBTQ People Safer Across the World*, TIME (July 24, 2019, 6:14 PM), https://time.com/5633974/tinder-lgbtq-safety-feature.

100. *Id*.; Whittaker, *supra* note 93; Suleman, *supra* note 99.

101. Sarah Kaufman, *Grindr Makes Big Change After App is Used to Track, Arrest Gay Men*, VOCATIV (Sept. 8, 2014), https://www.vocativ.com/culture/lgbt/grindr-egypt/index.html.

102. *Id*.

103. *Id*.

104. *Id*.; John Aravosis, *"Grindr" Gay Smartphone App Turns Off "Distance" Option in the Face of Privacy Concerns*, AMERICABLOG (Sept. 1, 2014, 7:40 PM), http://gay.americablog.com/2014/09/gay-grindr-smartphone-app-turns-distance-option-privacy-complaints.html.

105. Aravosis, *supra* note 104 ("UPDATE: Grindr has turned the location functionality back on, and there's no indication that they've made any other changes to their system."); *Sensitive Information*, *supra* note 30 ("Synack…found in those countries that had distance information turned on, including the U.S., it was still possible to track users in real time.").

106. Norman Shamas, *Queer Dating Apps Need to Protect Their Users Better*, SLATE (Feb. 28, 2018, 9:00 AM), https://slate.com/technology/2018/02/queer-dating-apps-need-to-protect-their-users-better.html.

location was still enabled by default for other countries that are legally dangerous for the LGBT community.[107]

LGBT dating apps were built amid "thriving, sex-positive gay culture[s]," and the design and designated usage of these apps demonstrate that.[108] As writer Russell Brandom noted: "For Americans, it's hard to imagine being afraid to show your face on such an app. It's not just a technological challenge, but a cultural one: how do you design software knowing that simple interface decisions like watermarking a screenshot could result in someone being arrested or deported?"[109]

This sense of attention to safety and protection is not felt in countries which are "friendlier" to LGBT identities, due to a combination of factors. One is that there is less of a perceived need for such protections.[110] For example, in the United States, most LGBT individuals do not expect regularly to cross security checkpoints where government officials can look at the apps they have on their phones and possibly take action against them based on the presence of those apps.[111] However, the intersection of privacy and security demonstrates how important protecting LGBT user data on apps like this can be.

B. Why is it Important to Protect LGBT Users of Dating Apps?

The failure of geolocative dating apps to protect the data of LGBT users in countries like the United States demonstrates a lack of recognition of the necessity of protecting user data.[112] Even worse, it demonstrates that in a country that may not seem overtly hostile to LGBT identities, which has many communities and families where out LGBT individuals can feel safe to express their identities, there are still special risks LGBT people face that others do not.[113] These factors combined lead to a reasonably heightened desire for privacy.[114] For instance, there is a risk of being LGBT and living in a rural area, where communities can be small and close-knit, and individuals may not want everyone they know to know about their sexual orientation.[115] There are many individual communities and families, even in ostensibly LGBT-friendly countries like the United States, that are hostile toward LGBT individuals.[116] There is an individualized risk of outing an LGBT individual who may not be ready or able to come out, for any number of personal, political, or professional

107. Nguyen, *supra* note 70 ("[L]ocation is still enabled by default in other places where the LGBT community faces discrimination: Algeria, Turkey, Belarus, Ethiopia, Qatar, Abu Dhabi, Oman, Azerbaijan, China, Malaysia, and Indonesia.").

108. Brandom, *supra* note 92.

109. *Id.*

110. *Id.*

111. *Id.*

112. INSIKT GROUP, ONLINE SURVEILLANCE, CENSORSHIP, AND DISCRIMINATION FOR LGBTQIA+ COMMUNITY WORLDWIDE 5 (2020).

113. *Id.*

114. *Privacy is Crucial*, *supra* note 10.

115. *See generally* MOVEMENT ADVANCEMENT PROJECT, WHERE WE CALL HOME: LGBT PEOPLE IN RURAL AMERICA (2019) (outlining the risks of being LGBT in rural areas).

116. *See generally* JACOB POUSHTER & NICHOLAS KENT, THE GLOBAL DIVIDE ON HOMOSEXUALITY PERSISTS (2020) (describing hostility towards LGBT people in individual communities and families).

reasons.[117] There is a particularly high risk when an LGBT individual is living in a location that is legally and politically hostile toward LGBT individuals, where a person could face severe legal and social consequences for their identity.[118]

For example, despite a landmark ruling from the Supreme Court in June 2020 that prevents employers from firing workers for being gay or transgender,[119] there are still existing contexts in which LGBT workers are left vulnerable.[120] In addition, many states do not have laws which explicitly and affirmatively prohibit discrimination based on sexual orientation and transgender identity in housing, public accommodations, and education, despite evidence of ongoing discrimination in these areas.[121] The Equality Act, introduced in 2015 and passed by the U.S. House of Representatives in 2019, is an acknowledgment of the gaps that still exist in discrimination law when trying to protect LGBT individuals.[122] The bill would explicitly prohibit discrimination on the basis of sexual orientation and gender identity in housing, public accommodations, public education, federal funding, and the jury system, as well as other areas.[123] Although the bill clearly arises out of a recognized need for codification of these protections for the LGBT community, it faces an uphill battle to enaction,[124] leaving LGBT individuals open to discrimination in their daily lives.[125]

---

117. *See* Rachel Moss, *The 'Devastating' Impact Being Outed Can Have on LGBT+ People,* HUFFINGTON POST UK (Mar. 28, 2018), https://www.huffingtonpost.co.uk/entry/the-devastating-impact-being-outed-can-have-on-lgbt-people_uk_5aba3587e4b008c9e5fb5e49 ("Outing someone ignores the many valid reasons a person may have for not choosing to be open about their sexuality to every person in their life. …Some LGBT people are not out because of a real need to protect themselves. We do not live in a world that is accepting of everyone's sexual orientation or gender identity.").

118. INSIKT GROUP, *supra* note 110, at 5.

119. Tucker Higgins, *Supreme Court Rules Workers Can't be Fired for Being Gay or Transgender,* CNBC (June 15, 2020), https://www.cnbc.com/2020/06/15/supreme-court-rules-workers-cant-be-fired-for-being-gay-or-transgender.html.

120. *See, e.g.*, Jon Webb, *Despite Supreme Court Ruling, You Can Still Get Fired for Being Gay, Transgender*, EVANSVILLE COURIER & PRESS (June 16, 2020), https://www.courierpress.com/story/opinion/columnists/jon-webb/2020/06/16/despite-supreme-court-you-can-still-get-fired-being-gay-trans/3197494001 (discussing the ministerial exception to certain protections under the Civil Rights Act, which would mean that some LGBT employees of religious organizations could possibly still be fired for their identity despite the June 2020 Supreme Court ruling); Sarah Jones, *To Truly Protect LGBTQ Workers, Get Rid of At-Will Employment*, INTELLIGENCER (June 15, 2020), https://nymag.com/intelligencer/2020/06/at-will-employment-leaves-lgbtq-workers-vulnerable.html (explaining how at-will employment, and specifically the absence of just-cause employment, allows employers to fire employees for a generic reason, forcing the now unemployed worker to spend time and money to meet a legal burden of proving they were fired for being transgender or gay).

121. *LGBTQ Americans Aren't Fully Protected from Discrimination in 29 States*, FREEDOM FOR ALL AMERICANS, https://www.freedomforallamericans.org/states (last visited Oct. 21, 2020).

122. German Lopez, *The House Just Passed a Sweeping LGBTQ Rights Bill*, VOX (May 17, 2019), https://www.vox.com/policy-and-politics/2019/5/17/18627771/equality-act-house-congress-lgbtq-rights-discrimination.

123. Nonnie L. Shivers, *5 FAQs on the Equality Act and Employment Nondiscrimination*, OGLETREE DEAKINS (May 22, 2019), https://ogletree.com/insights/5-faqs-on-the-equality-act-and-employment-nondiscrimination.

124. *Id*.; *House Passes Sweeping Anti-Discrimination Bill to Expand Protections of LGBT People*, CBS NEWS (last updated May 17, 2019, 4:28 PM), https://www.cbsnews.com/news/house-passes-sweeping-anti-discrimination-bill-to-expand-protections-of-lgbt-people [hereinafter *House Passes Sweeping Anti-Discrimination Bill*].

125. *House Passes Sweeping Anti-discrimination Bill*, *supra* note 124.

There has also been an increase in LGBT hate crimes.[126] The FBI's Annual Hate Crimes Statistics Report, which covers 2018, states that hate crimes targeting lesbians, gays, and bisexuals increased by 6% in 2018, and the number of hate crimes against transgender individuals over the same period increased by 41%.[127] There were more than 1300 hate crime incidents in 2018 alone targeting individuals for their sexual orientation or gender identity.[128]

Law professor Anita L. Allen argues that for LGBT plaintiffs, recovery under tort for invasion of privacy is unlikely when the plaintiff's sexual orientation comes into play, because of the gap between the expectation of the "reasonable person" and the "reasonable LGBT person."[129] LGBT people's need for "secrecy and selective self-disclosure" arose in times of persecution and discrimination.[130] So long as there is still intolerance of LGBT people in society, "the need for seclusion, secrecy, and selective self-disclosure will remain as well."[131]

These increased real-life dangers show that LGBT privacy online, where LGBT users may go to find a community when they cannot find one in person, is incredibly important.[132]

C. What are the Consequences of Dating Apps' Failure to Protect LGBT Users?

In recent years, Grindr has lost favor with some members of the gay community.[133] This is in light of both the data and security problems discussed throughout this Note; other cultural problems with users of the app, such as racism; and, especially recently, the widespread availability of other apps for members of the LGBT community.[134] The culture on Grindr has even led to whispers of a class-action lawsuit, because of Grindr's failure to meaningfully address the racism of its users.[135] In addition, Grindr was early to the game of geolocative dating apps, meaning that now it looks and feels "dated" to some younger users.[136] Grindr's competitors have been quick to jump on the backlash against Grindr, attempting to grow their own userbases as a consequence.[137]

However, even moving away from Grindr to other, newer LGBT apps does not protect LGBT users from data security breaches. Other geosocial apps come

126. Lou Chibbaro, Jr., *FBI Report Shows Increase in Anti-LGBT Hate Crimes,* WASH. BLADE (Nov. 20, 2019, 1:47 PM), https://www.washingtonblade.com/2019/11/20/fbi-report-shows-increase-in-anti-lgbt-hate-crimes.
127. *Id.*
128. *Id.*
129. Anita L. Allen, *Privacy Torts: Unreliable Remedies for LGBT Plaintiffs*, 98 CAL. L. REV. 1711, 1764 (2010).
130. *Id.*
131. *Id.*
132. *Privacy is Crucial*, *supra* note 10.
133. Shadel, *supra* note 19.
134. *Id.*
135. *Id.*
136. Shadel, *supra* note 16.
137. *Id.*; Shadel, *supra* note 19.

with their own problems, often the same problems, as Grindr, including the same location-based data issues.[138]

Researchers in 2019 demonstrated that apps like Grindr, Romeo, and Recon (all apps for gay men), did not secure their programming interface, allowing researchers to generate a map of users, revealing their precise locations through trilateration.[139] Because all of these apps show how far away potential matches are relative to the person using the app, it is easy to determine the exact locations of the identified matches.[140] The researchers also noted the previously cited problem with Grindr's unsecured API—a problem shared by Recon and Romeo—which allowed them "to generate maps of thousands of users at a time."[141]

Grindr and Romeo, although acknowledging that they took these location concerns seriously, pointed only to existing settings concerned users could turn on to hide their location data on their apps.[142] After being confronted by the researchers with the problems with their app's location services, only the app Recon switched to "grid-snapping," a location-tracking technique where a user's location is "snapped" to a line on a grid, obscuring their exact longitudinal and latitudinal location.[143] Two apps for gay and bisexual men not included in the study were already using measures to protect the location of their users—Scruff uses a "location-scrambling algorithm" enabled automatically in regions where same-sex acts are criminalized and available in the settings menu for all users, and Hornet uses grid-snapping.[144]

Grindr's cavalier lack of accountability is frustrating to its users.[145] One user summarized the controversies succinctly: "[a]fter 5 years of controversies, and in contrast to what Grindr claims, it is still possible to obtain the exact location of millions of cruising men on Grindr.…To protect the LGBTQ+ community, Grindr needs to step up its game."[146]

There are potential long-term consequences with these breaches, as well. The researchers from Kyoto University and Synack both noted that people are "creatures of habit," often returning to the same places—gym, work, school, home—over and over again.[147] If someone tracked a particular user on an app like Grindr for even a week at a time, that person might discover, for example, where a particular Grindr user lived.[148] A bad actor could then use that information to put the user in danger.[149]

138. Chris Fox, *Gay Dating Apps Still Leaking Location Data,* BBC NEWS (Aug. 8, 2019), https://www.bbc.com/news/technology-49265245.
139. *Id.*
140. *Id.*
141. *Id.*
142. *Id.*
143. *Id.*
144. *Id.*
145. Shadel, *supra* note 16.
146. @Seppevdpll, *supra* note 54.
147. Greenberg, *supra* note 12.
148. Fox, *supra* note 138.
149. Wardle, *supra* note 43; Greenberg, *supra* note 12.

These breaches are not unique to LGBT dating apps.[150] There will always be risks to using location-based dating apps, whether security, privacy, or other safety concerns.[151] The difference is that some apps have fixed these flaws to protect their users, while others have continually failed to do so, despite being given opportunities, knowledge, and instruction as to how to do so.[152]

IV. RECOMMENDATION

Grindr's ongoing leaking of location data combines security and privacy issues.[153] Although users should always be careful about the personal information they share with strangers, the issues with dating apps for gay and bisexual men take the issue of personal privacy to another level by improperly protecting data that the app has access to, but users have *not* made public.[154] Just because users feel comfortable using a dating app to share their location with a particular person or set of people does not place the burden on the user to ensure that sensitive identifying information is not accessible to the public at large.

Grindr, when confronted with the many breaches to the security and privacy of its users, has routinely asserted that users should take matters into their own hands and turn off location-sharing features or share less information on the application.[155]

There is some merit to this privacy argument. Professor Allen argues that individuals have a moral and ethical responsibility to "respect not only other people's privacy but also their own,"[156] and that "duties to self of self-care and self-respect entail reservation and circumspection when it comes to sharing potentially sensitive information…."[157] There are many safety tips pertaining to being safe online while being LGBT,[158] including tips for users of dating apps specifically to protect themselves.[159] However, this only covers the issue of privacy.[160] There are, as Allen continues, serious practical limits to protecting our own privacy, and in the "Big Data era," the "content of any moral responsibility to protect one's own privacy…looks empty."[161] With regard to

150. *See, e.g.*, Sam Frizell, *Tinder Security Flaw Exposed Users' Locations*, TIME (Feb. 19, 2014), https://time.com/8604/tinder-app-user-location-security-flaw/ (detailing how users were able to use trilateration to pinpoint users' locations, which Tinder addressed by making its locations in increments of a mile, making "triangulation less precise"); *see also* Stephanie M. Lee, *An HIV-Positive Dating App Leaked 5000 Users' Data*, BUZZFEED NEWS (Dec. 16, 2015, 8:32 PM), https://www.buzzfeednews.com/article/stephaniemlee/a-dating-app-for-hiv-positive-people-leaked-sensitive-data (discussing how personal user data leaked from Hzone, a dating app geared toward people living with H.I.V.).

151. Lee, *supra* note 151.

152. *Id.*

153. Nguyen, *supra* note 70.

154. *Id.*

155. *See, e.g.*, Fox, *supra* note 138 ("Grindr told BBC News users had the option to 'hide their distance information from their profiles.'").

156. Anita L. Allen, *Protecting One's Own Privacy in a Big Data Economy*, 130 HARV. L. REV. F. 71, 72 (2016).

157. *Id.* at 73.

158. *Privacy is Crucial*, *supra* note 116.

159. Nguyen, *supra* note 70; @Seppevdpll, *supra* note 54.

160. Allen, *supra* note 156, at 73.

161. *Id.*

security, users are not always able to protect themselves if they do not know how much information platforms are gathering about them, and if the platforms are in turn sharing information with outside parties.[162] For instance, Grindr's argument that users can turn off the public display of their locations has little merit when users cannot limit the app's own private access to their location, allowing the app to collect that precise information and continue to make users vulnerable to those with malicious intent.[163]

Grindr and similar geolocative dating apps are aware of the problems that plague their apps and threaten their userbases.[164] Researchers, after identifying breaches, have reached out to companies such as Grindr, offering potential fixes to code to make the apps safer.[165] For instance, Grindr and similar apps have been told to disable location sharing by default;[166] limit the accuracy of location sharing,[167] such as by adopting grid-snapping locative techniques;[168] and secure their APIs.[169] Security experts have suggested that geolocative apps should have, and even do have, a responsibility to use informed consent practices to allow users to enable access to their data only after being reminded of the risks of sharing personal information with strangers and the platform, and being clearly told how the app will use their data.[170] Users should be aware of specific security risks that may result and steps the platform is actively taking to mitigate those technological risks.[171]

Though there are potential solutions, a troubling lack of action[172] and a complete lack of enforcement exist.[173] LGBT dating apps can, and some even have, adopted these changes, but there is no authoritative external pressure for these apps to protect their users.[174] Researchers have noted with frustration that "there is no industry standard for ensuring the locational privacy of users; attempts are based on ad-hoc approaches that often exhibit a lack of understanding of the technical intricacies of localization attacks."[175]

Because dating apps geared toward gay and bisexual men like Grindr have recognized the necessity of taking steps to protect users in countries that punish

162. *Id.*
163. Nguyen, *supra* note 70.
164. Fox, *supra* note 138; Greenberg, *supra* note 12; Wardle, *supra* note 43.
165. Fox, *supra* note 138.
166. @Seppevdpll, *supra* note 54.
167. *Id.*; Fox, *supra* note 138.
168. Fox, *supra* note 139.
169. @Seppevdpll, *supra* note 54.
170. Fox, *supra* note 139 ("Location sharing should be 'always something the user enables voluntarily after being reminded what the risks are'"); Ghorayshi & Ray, *supra* note 79 ("Some experts argue that Grindr should be more specific in its user agreements about how it's using their data."); PASTEBIN, *supra* note 37.
171. PASTEBIN, *supra* note 37.
172. Polakis, *supra* note 8, at 825. Researchers contacted four location-based services they studied and provided them with an outline of the attacks they had tested on the apps' privacy guarantees; guidelines for preventing privacy breaches through spatial cloaking; and the tradeoffs of switching from location proximity to spatial cloaking for geolocative purposes. Two of the services, Facebook and Foursquare, made changes to their location-based services based on the researchers' suggestions. The other two services, Grindr and Skout (another location-based dating app) never informed the researchers of any changes they had made.
173. *Id.* at 818.
174. *Id.*
175. *Id.*

and persecute LGBT individuals, change is not impossible for these apps when there is a demonstrated need.[176] After years of data breaches and minimal action, it seems clear that legal or legislative penalties are required to force companies to make needed fixes and take necessary steps to protect user data. They must do more than "papering over" security breaches.[177] LGBT users of these apps deserve more than flimsy, ineffective "fixes" that only arise as a reaction to data security scandals.[178] No legal action has been taken against Grindr due to harm from leaking of location data,[179] but there is no reason to wait until harm occurs to take proactive steps to protect vulnerable individuals from the violation of their personal and private information.

In general, despite public perception of security and privacy regulations, the law lags behind technology.[180] Although different laws cover different types of data, there is no "overarching powerful law protecting you," as Electronic Frontier Foundation (EFF) Activism Director Rainey Reitman pointed out.[181] Agencies and others in positions of power in government do not respond quickly technological threats nor to the implications of those threats.[182] They fail to discern how they could and should act to protect consumers.[183]

This partially explains why there has been no legal or legislative action addressing the security and privacy concerns of Grindr users, but the federal government has shown that it *can* act when Grindr seems like a threat to national security.

In 2016, Grindr was sold to Beijing Kunlun Tech Co., Ltd., a Chinese company, with the acquisition completing in 2018.[184] The ownership of a Chinese company by an American dating app for, by Grindr's own description, "gay, bisexual, transgender, and queer people"[185] raised some concerns in the federal government, with two United States senators sending a letter to Grindr in 2018 asking how it would protect user privacy under the new ownership.[186] In March 2019, a U.S. government security panel chaired by the U.S. Department of the Treasury, called the Committee on Foreign Investment in the United States (CFIUS), forced the company to sell off Grindr.[187] Although CFIUS's concerns with Kunlun's ownership were not specified, the committee

176. Shamas, *supra* note 106.

177. *Id*.

178. *Id*.

179. Suhauna Hussain et. al., *Grindr, Tinder and OkCupid Apps Share Personal Data, Group Finds*, L.A. TIMES (Jan. 14, 2020, 5:20 PM), https://www.latimes.com/world-nation/story/2020-01-14/dating-apps-leak-personal-data-norwegian-group-says.

180. *Sensitive Information*, *supra* note 30.

181. *Id*.

182. *Id*.

183. Ingrid Lunden, *Report: Grindr's Chinese Owner Kunlun is Selling the Dating App After CFIUS Raised Personal Data Concerns*, TECHCRUNCH (Mar. 27, 2019, 9:30 AM), https://techcrunch.com/2019/03/27/report-grindrs-chinese-owner-kunlun-is-selling-the-dating-app-after-cfius-raised-personal-data-concerns.

184. Casey Newton, *How Grindr Became a National Security Issue*, VERGE (Mar. 28, 2019, 9:20 AM), https://www.theverge.com/interface/2019/3/28/18285274/grindr-national-security-cfius-china-kunlun-military.

185. Carl O'Donnell et al., *Exclusive: Told U.S. Security at Risk, Chinese Firm Seeks to Sell Grindr Dating App*, REUTERS (Mar. 27, 2019, 12:02 AM), https://www.reuters.com/article/us-grindr-m-a-exclusive/ exclusive-u-s-pushes-chinese-owner-of-grindr-to-divest-the-dating-app-sources-idUSKCN1R809L.

186. *Id*.

187. *Id*.

informed Kunlun that its ownership of Grindr was a "national security risk."[188] The decision coincided with the U.S. government's increased focus on the safety of personal data of U.S. military members and intelligence personnel.[189]

The government's action through CFIUS and inaction on every other front seems to demonstrate an unwillingness on behalf of not only Grindr but the United States federal government to protect LGBT people for any reason lesser than national security.[190] As Privacy International states:

> "…when it comes to how much governments care about our privacy, some are more equal than others. Our privacy matters to them when we are top civil servants, in the military or the intelligence services. When our private lives and who we date blur with national security, this is when governments start caring. But what about the millions of users, whose lives may still be affected by Grindr's practice? What about those who may be paying more for their health insurance because their HIV status has been shared or those who will be targeted by the government where Grindr users may face repression?"[191]

However, there is a path forward. Federal and state proposals, plus advocacy from independent organizations, show what the federal government could do to comprehensively protect everyone's data security and privacy.

A. Creating Comprehensive Federal Data Protection Laws

One broad recommendation is that the United States implement a model like the European Union's General Data Protection Regulation (GDPR).

The European Union's approach to personal data is "overarching and comprehensive."[192] The United States' lack of an overarching and comprehensive federal law protecting personal data means personal data protection in the United States is "patchwork," allowing businesses to self-regulate, and protecting consumers only when businesses violate their own privacy policies.[193] This leaves much of the burden on the consumer for their own data protection.[194] As the issues with Grindr and similar apps have shown, this is not an effective strategy for protecting information and may lead to harm.

A demonstration of how this could work is unfolding in the European Union: in January 2020, the Norwegian Consumer Council filed formal complaints against Grindr under the GDPR to their Norwegian Data Protection Authority, because of concerns that Grindr users' information was potentially

188. *Id.*

189. James Wellemeyer, *U.S. Designates Grindr a National Security Risk*, WASH. BLADE (Apr. 2, 2019, 11:40 AM), https://www.washingtonblade.com/2019/04/02/us-designates-grindr-a-national-security-risk.

190. *Grindr and U.S. National Security: Why It is Time We Start Caring for the Privacy of All Users*, PRIV. INT'L (Apr. 2, 2019), https://privacyinternational.org/news-analysis/2775/grindr-and-us-national-security-why-it-time-we-start-caring-privacy-all-users; Newton, *supra* note 185.

191. *Id.*

192. Constance Gustke, *Which Countries Are Better at Protecting Privacy?*, BBC WORKLIFE (June 25, 2013), https://www.bbc.com/worklife/article/20130625-your-private-data-is-showing.

193. *Id.*

194. *Id.*

improperly sold to advertising agencies.[195] The Norwegian Consumer Council notes that it was necessary to take action in this way because of the "very few actions" available to consumers to ensure that their personal data is not being exploited.[196]

Certain states, like California, Maine, and Nevada, have privacy laws or bills in the model of the GDPR.[197] These are important protections for the residents of these states and can help provide a model for how an American data protection law could function practically on a federal level. However, leaving these state-level laws to function on their own without a federal baseline for data protection[198] only furthers the patchwork problems with American data protection laws.[199]

United States consumer rights groups are utilizing these laws to ask federal and state governments to investigate Grindr and other apps for this same violation of informed consent.[200] The issue of data privacy and security is important enough that the federal government should take notice and apply a uniform standard for how companies that run dating apps treat user data. Pointing to the Norwegian Consumer Council's report, several consumer protection agencies in the United States have said that Congress should take action to demonstrate that "such flagrant violations of privacy found in the EU are not acceptable in the U.S."[201]

An effort to allow Americans more control over how companies collect data from users and how the companies use their data, the Consumer Online Privacy Rights Act (COPRA), was introduced in the U.S. Senate in late 2019.[202] COPRA would focus on establishing individual privacy rights, including giving individuals the right to be free from deceptive and harmful data practices; the

195. *New Study: The Advertising Industry is Systematically Breaking the Law*, FORBRUKERRÅDET (Jan. 14, 2020), https://www.forbrukerradet.no/side/new-study-the-advertising-industry-is-systematically-breaking-the-law.

196. *Id.*

197. *Dating Apps Leak Personal Data, Norwegian Group Says*, AP NEWS (Jan. 31, 2020), https://apnews.com/8f3318e83e91275ebf227fd3fd36ef18; Mitchell Noordyke, *US State Comprehensive Privacy Law Comparison*, INT'L ASS'N OF PRIV. PROS. (last updated July 6, 2020), https://iapp.org/resources/article/state-comparison-table.

198. Letter from Electronic Privacy Information Center (EPIC) to Senator Roger Wicker and Senator Maria Cantwell (Apr. 29, 2019), *accessed at* https://epic.org/testimony/congress/EPIC-SCOM-ConsumerPerspectives-Apr2019.pdf ("We call for federal baseline legislation that ensures a basic level of protection for all individuals in the United States. We oppose the preemption of stronger state laws. U.S. privacy laws typically establish a floor and not a ceiling so that states can afford protections they deem appropriate for their citizens and be 'laboratories of democracy,' innovating protections to keep up with rapidly changing technology.") [hereinafter *Letter from EPIC*].

199. Noordyke, *supra* note 197. After the California Consumer Privacy Act was passed in 2018, many other states introduced measures covering how personal information is used. Although the laws and bills from different states have some similar provisions, there are differences in consumer rights and business obligations in each bill.

200. *Popular Dating, Health Apps Violate Privacy*, CTR. FOR DIGIT. DEMOCRACY (Jan. 14, 2020), https://www.democraticmedia.org/article/popular-dating-health-apps-violate-privacy.

201. *Dating Apps Leak Personal Data, Norwegian Group Says*, *supra* note 198.

202. Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019); Jessica Corbett, *Expert Says Senate Democrats' Sweeping Online Privacy Bill Answers Public Demand for 'Transformative Shift,'* COMMON DREAMS (Nov. 26, 2019), https://www.commondreams.org/news/2019/11/26/expert-says-senate-democrats-sweeping-online-privacy-bill-answers-public-demand.

right to clear and detailed information on how user data is used and shared; the right to control the movement of data, which would allow users to prevent their data from being shared with unknown third parties; and the right to delete or correct user data.[203] The bill sets out a private right of action for individuals to sue companies that break data privacy rules and gives state attorneys general the right to bring privacy cases under federal law.[204]

COPRA also establishes accountability measures for companies that handle user data.[205] It creates an affirmative "duty of loyalty," which would prohibit companies from using data in ways harmful to consumers, institute higher fines for companies that mishandle user data, and require companies to conduct internal assessments about potentially discriminatory effects of their internal algorithms.[206] Most important for issues like LGBT dating app location leaks, COPRA would require companies to get "special permission" to collect certain types of sensitive data, such as precise location information.[207]

However, the framework of COPRA is only a beginning. The EFF called it a "strong step forward," but that the organization would seek "strengthening amendments."[208] Relevantly, COPRA calls for a bar on entities covered by the law from "processing or transferring data 'beyond what is reasonably necessary, proportionate, and limited' to certain kinds of purposes,"[209] meaning companies covered by the law would be asked to limit the amount of information they process from users. EFF approved of the presence of a data minimization provision that would be applied not only to the way an entity *processes* data, not only data collection and sharing of data, but said data privacy legislation should go further than what COPRA asks for, barring companies from "processing data except as reasonably necessary *to give the consumer what they asked for*, or for a few narrow purposes."[210]

B. Creating a Federal Data Protection Agency

Another broad recommendation is that the federal government create a federal agency that handles issues related to technological privacy and security. While the Federal Trade Commission (FTC) has been the chief federal agency on privacy policy and enforcement since the 1970s,[211] the FTC only steps in to

203. Corbett, *supra* note 202.

204. Tony Romm, *Top Senate Democrats Unveil New Online Privacy Bill, Promising Tough Penalties for Data Abuse*, WASH. POST (Nov. 26, 2019, 6:45 AM), https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2019/11/26/the-technology-202-top-senate-democrat-s-new-privacy-bill-likely-to-spark-gop-protests/5ddc3680602ff1181f2640e3.

205. Corbett, *supra* note 202.

206. *Id.*

207. *Id.*

208. Adam Schwartz, *Sen. Cantwell Leads with New Consumer Privacy Bill*, ELEC. FRONTIER FOUND. (Dec. 3, 2019), https://www.eff.org/deeplinks/2019/12/sen-cantwell-leads-new-consumer-data-privacy-bill.

209. *Id.*

210. *Id.*

211. *Protecting Consumer Privacy and Security*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security (last visited Oct. 21, 2020).

protect consumers in cases where the company has already violated its privacy policy,[212] levying fines in cases of certain privacy violations.[213]

In April 2019, the Electronic Privacy Information Center (EPIC) sent a letter to the U.S. Senate Committee on Commerce, Science, and Transportation, pointing out the failures of the FTC in both arriving at and enforcing consent-agreements with companies that violate data privacy[214] and asking for:

> a federal agency focused on privacy protection, compliance with data protection obligations, and emerging privacy challenges. The agency should also examine the social, ethical, and economic impacts of high-risk data processing and oversee impact-assessment obligations. Federal law must establish a data protection agency with resources, rulemaking authority and effective enforcement powers.[215]

There are clear gaps in federal protections of individual privacy and security rights that need to be addressed in a uniform, proactive, and clear manner. Even if federal privacy legislation existed, there would need to be a federal agency capable of enforcing that legislation to back up its effectiveness. Creating an agency would ensure that all users of dating applications are protected, including LGBT users, and ensure that at least one part of the notoriously tech-averse government was paying attention to and had some knowledge of important issues of safety when using technology, which most Americans encounter nearly every day.[216]

Two legislators in the U.S. House of Representatives introduced a bill in 2019, the Online Privacy Act,[217] that would establish a new federal agency to "place significant restrictions on the kinds and amount of personal data companies can collect and what they can do with that information while they have it."[218] This agency would centralize privacy regulation in the United States,[219] a necessary step needed to mitigate the current patchwork of privacy regulation. This is still not a perfect law. It is not proactive, nor does it incentivize companies not to have exploitative policies. Instead it gives the agency and state attorneys general mitigatory powers in the event a company violates privacy regulations.[220] The bill requires more transparency from companies when writing privacy policies and user consent processes,[221] which might give consumers who read the policies more understanding of how the company plans to use their data and allow potential users the chance to consider whether they want the app to use their data in that proposed way.

---

212. Gustke, *supra* note 192.

213. Dennis Fisher, *Online Privacy Act Would Create Federal Privacy Agency*, DECIPHER (Nov. 6, 2019), https://duo.com/decipher/online-privacy-act-would-create-federal-privacy-agency.

214. *Letter from EPIC*, *supra* note 198.

215. *Id.*

216. Lunden, *supra* note 183.

217. Online Privacy Act of 2019, H.R. 4978, 116th Congress (2019).

218. Fisher, *supra* note 213.

219. *Id.*

220. *Id.*

221. *Id.*

Legislators proposed the Online Privacy Act because of a lack of federal laws that focus on individual privacy rights.[222] In a slate of laws proposing a federal data privacy protection framework, this was the only bill (including COPRA, which only creates a "privacy-focused bureau" under the FTC[223]) which proposed a new agency for enforcement of data protection issues.[224]

V. CONCLUSION

It is unfair to ask the LGBT community to regulate their actions and change their behavior because of concerns about their privacy, security, and safety. Companies like Grindr have shown that they cannot be expected to hold themselves accountable, even in the face of years of sustained criticism. The government is notoriously slow on issues relating to data, but the issue of privacy and security relating to location data and the vulnerabilities that can be exposed by the revelation of that data, are important for the safety of the LGBT users of these apps and more generally for all Americans. While there have been illustrated paths toward the protection of user data privacy and security in the United States, these are only proposals. What has been done so far is not enough. The federal government needs to take privacy and security concerns seriously and take deliberate, concrete steps to enact and enforce unified protection of user data privacy and security.

222. *Id.*
223. Romm, *supra* note 204.
224. Fisher, *supra* note 213.