

Grindr and Privacy Concerns of LGBTQ+ People in the United States and the European Union

By Zane McNeill and Riley Clare Valentine **

INTRODUCTION

In 2016, the European Union (EU) instituted the General Data Protection Regulation (“GDPR”) which has greatly expanded the privacy rights of European internet users.³ Under the GDPR, the processing of data concerning a person’s sexual orientation or sex life is a special category of data which is required to have a higher standard of protection.⁴ The GDPR recognizes that LGBTQ+ people are at a higher risk of discrimination and violence if their personal information is revealed; therefore, data relating to this community must be under a heightened standard of privacy protection.⁵

In 2020, the Norwegian Consumer Council (“NCC”) filed a series of GDPR complaints against the LGBTQ+ social networking app, Grindr, alleging that the company violated the regulation by engaging in the unlawful sharing of personal data with third parties for marketing purposes.⁶ The NCC complaints claimed that Grindr shared sensitive personal data, including the

**Zane McNeill has a MA in political science from Central European University and is a J.D. candidate at University of Denver Sturm College of Law. Riley Clare Valentine is an independent scholar with a PhD in Political Science from Louisiana State University. Their work centers on political rhetoric, care ethics, and neoliberalism.*

**We would like to thank Bernard Cho, John Acevedo, and Michael Drake for their thoughtful comments on this article.*

¹ E.g., Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance (Art. 9). European Commission, Guidance note on the collection and use of data for LGBTIQ equality, https://commission.europa.eu/system/files/2023-07/202307_JUST_Guidance_note_on_the_collection_and_use_of_data_for_LGBTIQ_equality.pdf (last visited Nov 26, 2023).

² *Id.*

³ European Commission, *Guidance note on the collection and use of data for LGBTIQ equality*, https://commission.europa.eu/system/files/202307/JUST_Guidance_note_on_the_collection_and_use_of_data_for_LGBTIQ_equality.pdf (last visited Nov 26, 2023).

⁴ EUROPEAN DATA PROTECTION BOARD, NORWEGIAN DPA IMPOSES FINE AGAINST GRINDR LLC NORWEGIAN DPA IMPOSES FINE AGAINST GRINDR, LLC (2021), available at <https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-imposes-fine-against-grindr-llc>; en#:~:text=Summary%20of%20the%20Decision&text=In%202020%2C%20the%20Norwegian%20Consumer,in%20question%20was%20on%20Grindr (last visited Nov 26, 2023).

GPS locations, IP addresses, Advertising IDs, ages, and genders of its users to outside marketing companies.⁷ A year later, on January 26, 2021, Grindr was fined 10 million Euros, which was later adjusted to a 5.3 million Euro fine.⁸

In the wake of the NCC complaint against Grindr, the Council, alongside the cybersecurity company, Mnemonic, released a report titled “Out of Control,” which highlighted how advertising technology companies receive personal data about app users and profile them for targeted advertising.⁹ Specifically, the NCC found that Grindr shared detailed user data with major advertising companies, which reserved the right to share the data they collected with their large number of partner companies.¹⁰

In response to requests from the NCC and Mnemonic, Grindr said that the company collected numerous data points on its users, including: chat messages and images (that may be sexually explicit); email addresses; display names; age; height; weight; body type; favored sexual position; ethnicity; relationship status; “tribes” (bear, twink, jock, trans, etc); “looking for” (chat, friends, right now, etc); gender, preferred pronouns (he, they, etc); HIV status and testing details; linked Facebook, Instagram; and Facebook data; in addition to user’s profile pictures; location data; IP address; and device ID such as Google Advertising ID.¹¹

The NCC not only found that the large amount of user data that Grindr was collecting, sharing, and processing, often without their specified consent, was illegal under the GDPR, but also emphasized that the collection of this vast amount of sensitive data could be used for discriminatory purposes and put the app users at risk of harm.¹²

This Article addresses the importance of LGBTQ+ privacy online and compares the protection offered to the LGBTQ+ community in Europe to the U.S. As such, Part I discusses the importance of data privacy for vulnerable groups. Part II introduces the privacy landscape in the U.S. and in the EU and how it affects LGBTQ+ users. Concluding, Part III delves deeper into Grindr’s privacy concerns and compliance issues in the U.S. and the EU.

5 *Out of control: Complaints and follow up*, FORBRUKERRÅDET (Jan. 14, 2020), <https://www.forbrukerradet.no/side/complaints-against-grindr-and-five-third-party-companies/>.

6 Terje Solsvik, *Grindr fine cut to \$7 mln in Norway Data Privacy Case*, REUTERS (Dec. 15, 2021), <https://www.reuters.com/technology/grindr-fine-cut-7-mln-norway-data-privacy-case-2021-12-15/>.

7 *Out of control*, *supra* note 6.

8 *Id.*

9 Alex Scroxton, *LGBTQ+ social app Grindr accused of breaching GDPR*, COMPUTER-WEEKLY.COM (Jan. 15, 2020), <https://www.computerweekly.com/news/252476780/LGBTQ-social-app-Grindr-accused-of-breaching-GDPR>.

10 *Out of control*, *supra* note 6.

I. The Landscape of Data Privacy Concerns for LGBTQ Populations: The Importance of Strong Data Privacy Protections for LGBTQ People

For LGBTQ+ people, a data breach that could expose, or “out,” their sexual orientation could have far-reaching consequences, including loss of employment, loss of familial relationships, and the potential for physical harm or even death.¹³ In “Outed by Advertisements: How LGBTQ Internet Users Present a Case for Federal Data Privacy Legislation,” Noah Ashman details how advertisements targeting LGBTQ+ people in the U.S. can create safety concerns and my ‘out’ individuals in a country which lacks federal protection for sexual orientation and can create numerous possibilities for discrimination.¹⁴ Although the vulnerabilities the LGBTQ+ community experiences are shared across marginalized communities, for example gender discrimination, the confluence of gender, sex, and sexuality raises particular and unique concerns pertaining to data security.

The U.S. has lagged behind other countries when it comes to privacy rights for its citizens; other countries have recognized that LGBTQ+ people are a vulnerable group whose require a higher level of data protection and privacy rights.¹⁵ Some jurisdictions have even established a general prohibition against processing sensitive information, including information relating to an individual’s sex life or sexual orientation include sexual practices, sexual attraction, sexual orientation, gender identity, stages of gender transition, and consumption habits, except in limited circumstances, because of potential discrimination risks.¹⁶

When intimate data is leaked or disclosed to hackers and criminals, individuals have an increased risk of reputational ruin, blackmail, and extortion...These risks are not evenly distributed across society. Women and marginalized communities disproportionately bear the burden of private-sector surveillance of intimate life,” Danielle Keats Citron explains in “A New Compact for Sexual Privacy.”¹⁷

¹¹ I am focusing largely on sexuality and mostly excluding privacy concerns gender identity in this analysis.

¹² Noah Ashman, *Outed by Advertisements: How LGBTQ Internet Users Present a Case for Federal Data Privacy Legislation*, 99 OR. L. REV. 523, 524 (2021).

¹³ European Commission, *Guidance note on the collection and use of data for LGBTIQ equality*, https://commission.europa.eu/system/files/202307/JUST_Guidance%20note%20on%20the%20collection%20and%20use%20of%20data%20for%20LGBTIQ%20equality%20%E2%80%93%202023.pdf.pdf (last visited Nov 26, 2023).

¹⁴ Such as Brazil (General Personal Data Protection Law), the European Union (General Data Protection Regulation), and China (Personal Information Protection Law).

These higher standards of privacy protections for LGBTQ+ people are necessary because in the European Union and the United States being “outed” can lead to LGBTQ+ people being fired from their jobs or denied housing. In countries where being LGBTQ+ is illegal, proxy attributes such as location data and interests, which are often used for behavioral advertising, could also reveal sensitive information related to topics such as sexual preferences. This information could be used for surveillance or criminalization of LGBTQ+ people in those countries.¹⁵

According to Carlos Gutierrez, the deputy director of legal and policy affairs at the LGBT Technology Partnership & Institute, in addition to the heightened risks that LGBTQ+ people face from a data privacy breach, this population also tends to be heavier users of the internet and online services than their heterosexual counterparts, which can intensify potential harms.¹⁹ “Mobile devices play a particularly vital role in the lives of LGBT-identifying adults across jurisdictions because of their unique need to find resources and places that will be welcoming and supportive of them.”²⁰ Specifically, the LGBT Technology Institute has found that 81% of LGBTQ+ youth have searched for health information online, compared to just 46% of non-LGBTQ+ youth and 80% of LGBTQ+ respondents participated in a social networking site, compared to only 58% of the general public.²¹

The high usage of the internet and social media by LGBTQ+ people, coupled with the risks of employment discrimination, loss of liberty, housing discrimination, and healthcare discrimination, makes this population particu-

15 Danielle Citron, *A New Compact for Sexual Privacy*, 62 WM. & MARY L. REV. 1763, 1768-1769 (2021).

16 Matt Payton, *Egyptian Police “Are Using Grindr to Find and Arrest LGBT people”*, INDEPENDENT (Aug. 27, 2016), <https://www.independent.co.uk/news/world/africa/egyptian-police-grindr-dating-app-arrest-lgbt-gay-antigay-lesbian-homophobia-a7211881.html>. In a report by the cybersecurity organization Recorded Future, they found that the LGBTQ+ community in Russia and Eastern European were targeted by cyberattacks, censorship, and surveillance. Recorded Future found that law enforcement and, very likely, intelligence agencies in the Middle East, Asia, and Africa “have deployed the use entrapment to expose members of the LGBTQIA+ community for imprisonment and torture,” through LGBTQ dating apps. INSIKT GROUP, *Online Surveillance, Censorship, and Discrimination for LGBTQIA+ Community Worldwide*, RECORDED FUTURE (July 14, 2020), <https://www.recordedfuture.com/lgbtqia-community-cyber-threats>.

17 National Cybersecurity Alliance, *Data Privacy is Crucial for the LGBT Community*, (Feb. 28, 2018), <https://staysafeonline.org/online-safety-privacy-basics/data-privacy-crucial-lgbt-community/#:~:text=A%20privacy%20data%20breach%20that,for%20physical%20harm%20or%20death>.

18 *Id.*

19 CHRIS WOOD ET AL., *THE ROLE OF DATA PROTECTION IN SAFEGUARDING SEXUAL ORIENTATION AND GENDER IDENTITY INFORMATION* 7 (2022), available at https://www.lgbttech.org/_files/ugd/1b643a_21883c316e1547c99c6a1d997688f975.pdf.

larly vulnerable.²² Because of this, “data privacy is a special concern for the LGBT community. Our heightened use of the internet, coupled with the potentially catastrophic consequences of a data breach, makes our community especially vulnerable.”²³

II. A Comparative Look at Data Protection Legislation in the U.S. and Europe

While an investigation into the landscape of data protection laws across the world is necessary to determine how different legal regimes protect and process the sensitive data of LGBTQ+ users, this Article specifically surveys the U.S. and European approaches to privacy concerns.²⁴ Regulations in the U.S. and the EU could possibly eliminate the concerns we have raised, due to the U.S. and the EU as predominantly the origins of these apps. Usually in countries without data protection legislation, the LGBTQ+ population faces higher levels of persecution than in countries with data protection laws.²⁵ In the 162 countries with data protection laws, the protected status of LGBTQ+ people under the law determines what protection is established for data regarding an individual’s sexual orientation or gender identity.²⁶

A. Data Protection and Concerns for LGBTQ+ People in the United States

In the United States, there is an absence of a uniform data privacy scheme. The right to privacy was explicitly applied to the LGBTQ+ community in *Lawrence v. Texas*.²⁷ Although the Texas’ laws against sodomy were at issue in the case, the holding itself was more narrow and applied strictly to consensual sexual acts between adults in private spaces.²⁸ Nonetheless, these protections have been called in question by the Supreme Court’s recent ruling in *Dobbs v. Jackson*.²⁹ Privacy scholars have con-

²⁰ *Id.*

²¹ National Cybersecurity Alliance, *supra* note 18.

²² This Article focuses on regulations in the U.S. and E.U. because these are predominately the countries of origin of apps like Grindr.

²³ STONEWALL, DO ASK, DO TELL CAPTURING DATA ON SEXUAL ORIENTATION AND GENDER IDENTITY GLOBALLY (2016), available at, https://www.stonewall.org.uk/sites/default/files/do_ask_do_tell_guide_2016.pdf.

²⁴ Importantly, not all of these nations have protected status for LGBTQ+ persons. For example, Abu Dhabi has data privacy laws, but no protections for LGBTQ+ persons. Graham Greenleaf, *Global Data Privacy Laws 2023: 162 National Laws and 20 Bills*, 181 PRIVACY LAWS AND BUSINESS INTERNATIONAL REPORT (PLIBR) 1, 2-4 (2023), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4426146.

²⁵ See *Lawrence v. Texas*, 539 U.S. 558 (2003).

²⁶ See *id.*

²⁷ In landmark Supreme Court decisions, including *Griswold v. Connecticut*, 381 U.S. 479 (1965), *Lawrence v. Texas*, 539 U.S. 558 (2003), and *Whalen v. Roe*, 429 U.S. 589 (1977),

tended that the “constellation” of constitutional privacy rights that have been discussed in cases like *Obergefell v. Hodges* may be imperiled³⁰ by the *Dobbs* decision.³¹ The *Dobbs* ruling has also recently been used by conservative lawyers and judges to support their arguments that gender-affirming care bans for transgender youth are constitutional.³²

Instead of a uniform privacy law framework, the U.S. has a loose mix of federal privacy laws that protects health-related data (The Health Insurance Portability and Accountability Act of 1996), the data of children under 13-years old (Children’s Online Privacy Protection Rule), sensitive data of the clients of financial companies (Gramm-Leach-Bliley Act), the accuracy and fairness of consumer information assembled by Credit Reporting Agencies (The Fair Credit Reporting Act), and other privacy laws designed to target only specific types of data in special, often outdated, circumstances.³³

Some federal statutes in the U.S. require that before collecting personally identifiable information from an individual, a company collecting the data must provide the individual with notice of what information it will collect and how it expects to use that information.³⁴ Often, this notice is accomplished by providing a link to the companies’ privacy policy or is hidden at the bottom of an agreement or otherwise not visible or consciously engaged

the Court has recognized the right of privacy for citizens, including personal matters. In the Third Circuit decision of *Sterling v. Borough of Minersville*, 232 F.3d 190 (3rd Cir. 2000), the Third Circuit held that sexual orientation specifically falls within the “zone of privacy.” However, after the Supreme Court ruling in *Dobbs v. Jackson Women’s Health Org.*, 142 S. Ct. 2228 (2022), the case that overruled *Roe v. Wade*, 410 U.S. 113 (1973), privacy advocates are concerned that the court may be signaling that long-standing federal recognition of rights directly or indirectly concerning sexual orientation and gender identity (“SOGI” information) may be at risk.

28 The Court’s holding in *Roe v. Dobbs* that “a right of personal privacy, or a guarantee of certain areas or zones of privacy [existed] under the Constitution” (specifically in matters relating to marriage, procreation, contraception, family relationships, child rearing and education,) led to “other rights giving individuals control over their bodies and their most personal and intimate associations.” The minority in the *Dobbs* decision attested that the privacy rights protected by *Roe* may be eroded by the *Dobbs* decision. Maya Manian, *The Ripple Effects of Dobbs on Health Care Beyond Wanted Abortion*, 76 SMU L. REV. 77, 78 (2023).

29 E.g., Rona Kaufman, *New Supreme Court Cases: Duquesne Law Faculty Explains: Privacy: Pre- and Post-Dobbs*, 61 DUQ. L. REV. 62 (2023).

30 Erin Reed, *6th Circuit judges cite Dobbs Abortion ruling to uphold TN Trans Care Ban* 6th Circuit Judges Cite Dobbs Abortion Ruling To Uphold TN Trans Care Ban, (July 8, 2023), <https://www.erininthemorning.com/p/6th-circuit-judges-cite-dobbs-abortion>.

31 Mike Davis, Opinion, *US must catch up with rest of the world on Data Privacy*, ROLL CALL (Oct. 14, 2021), <https://rollcall.com/2021/10/14/us-must-catch-up-with-rest-of-the-world-on-data-privacy/>.

32 John Rothchild, *Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (Or Anywhere Else)*, 66 CLEV. ST. L. REV. 559, 607 (2018).

with by the user.³⁵ The individual, being notified of what information will be collected and how it will be used, then is given a choice about whether to consent to that collection of data or not.³⁶ As Daniel Citron explains in *A New Compact for Sexual Privacy*: “American privacy law generally does not curtail data collection. Instead, it focuses on procedural protections, such as ensuring the transparency of corporate data practices (referred to as notice) and securing certain rights over personal data (referred to as choice).”³⁷

Consent in the U.S. evolved from tort and contract law.³⁸ In contract law, consent is not necessarily consent to just one activity.³⁹ For example, a contract of adhesion, while it can be challenged as unfair in court, can render consent applicable to all potential uses.⁴⁰ Additionally, if an individual does not consent to the collection of their data, they may not be able to use the product that would otherwise be provided to them if they had consented.⁴¹ While “consent is the primary mechanism for legally permitting collection and use of personal information, a functional proxy for choice,” the U.S. theory of consent is less strict than “consent” under the GDPR.⁴²

In the United States, a primary mechanism for federal enforcement of the right to privacy is the Federal Trade Commission Act (FTC Act).⁴³ Under Section 5 of the FTC Act, “unfair or deceptive acts or practices in or affecting commerce” are prohibited.⁴⁴ Unfair acts or practices include acts that causes or is likely to cause substantial injury to consumers, acts that cannot be reasonably avoided by consumers, and acts that are not outweighed by countervailing benefits to consumers or to competition.⁴⁵ Deceptive acts are a representation, omission, or practice that misleads or is likely to mislead the consumer.⁴⁶ The consumer’s interpretation of the representation, omission, or practice must be considered reasonable under the circumstances and the misleading representation, omission, or practice must be material.⁴⁷ “The FTC’s emphasis on transparency enables a system (commonly called “notice-

33 *Id.*

34 *Id.*

35 Citron, *supra* note 16, at 1804.

36 Charlotte A. Tschide, *Meaningful Choice: A History of Consent and Alternatives to the Consent Myth*, 22 N.C. J.L. & TECH. 617, 623 (2021).

37 *Id.*

38 *Id.*

39 *Id.*

40 *Id.* at 650.

41 See 15 USCS § 57a.

42 FEDERAL TRADE COMMISSION, A BRIEF OVERVIEW OF THE FEDERAL TRADE COMMISSION’S INVESTIGATIVE, LAW ENFORCEMENT, AND RULEMAKING AUTHORITY (2021), available at, <https://www.ftc.gov/about-ftc/mission/enforcement-authority>.

43 *Id.*

44 *Id.*

45 *Id.*

and-choice”) that leaves dating apps largely free to set their own privacy policies,” Caitlin Chin, explained in 2020.⁴⁸ In the U.S., the Federal Trade Commission (FTC) has stepped into the role of policing consumer privacy and data security. The FTC carries out its Section 5(a) mission through formal rulemaking and case-by-case litigation.⁴⁹ While the FTC has gone after BetterHelp, Inc.,⁵⁰ a mental health platform that hosts a counseling service called “Pride Counseling” that targets the LGBTQ+ community, for sharing consumer’s data with Facebook and Snapchat for advertising, advocacy groups in the U.S. have alleged that the FTC has remained disinterested in investigating LGBTQ+ dating apps for similarly violating users’ privacy.⁵¹

Between 2012 and 2018, dozens of consumer complaints against Grindr were filed with the FTC, alleging deceptive trade practices and misrepresentation, but the agency has not publicly opened an investigation into the company.⁵² The FTC’s role is limited to stopping unfair and deceptive practices, which means if Grindr, or other LGBTQ+ dating apps, disclose their privacy practices truthfully, even if they are bad practices, those apps are not engaging in prohibited conduct.⁵³ As Danielle Citron explains: “So long as companies post privacy policies and offer opt-out rights under state law, they can largely collect, use, and sell intimate information without limitation. It should therefore not be a surprise that Grindr’s privacy policy warns that its advertising partners may also collect information directly from you.”⁵⁴

Federal policies in the United States are significantly more substantive than those of private organizations. Due to this, self-regulatory initiatives have an important role in terms of data collection. The Network Advertising Initiative (NAI) develops and enforces self-regulatory policies surrounding data collection and its usage for digital advertising.⁵⁵ NAI’s Code of Conduct

46 Caitlin Chin & Mishaela Robison, *This Cuffing Season, It’s Time to Consider the Privacy of Dating Apps*, BROOKINGS (Nov. 20, 2020), <https://www.brookings.edu/articles/this-cuffing-season-its-time-to-consider-the-privacy-of-dating-apps/>.

47 FEDERAL TRADE COMMISSION, *supra* note 43.

48 *FTC to Ban BetterHelp from Revealing Consumers’ Data*, FEDERAL TRADE COMMISSION (Mar. 2, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook>.

49 *Historic Grindr Fine Shows Need for FTC Enforcement Action*, PUBLIC CITIZEN, <https://www.citizen.org/news/historic-grindr-fine-shows-need-for-ftc-enforcement-action/> (last visited Dec. 9, 2023).

50 Federal Trade Commission, <https://www.ftc.gov/legal-library/browse/frequently-requested-foia-records/online-dating/foia-2018-00259-grindr-consumer-complaints-december-1-2012-through-december-1-2017> (last visited Aug 1, 2023).

51 While there has been some evidence that the FTC expects sensitive information to require enhanced notice to users, there is not remedy for the user to seek if an entity misuses their sensitive information. Daniel J. Solove & Woodrow Hartzog, *THE FTC AND THE NEW COMMON LAW OF PRIVACY*, 114 COLUM. L. REV. 583, 585 (2014).

52 Citron, *supra* note 16, at 1804.

53 *Id.*

requires individual businesses to seek for opt-in consent for targeted advertising based upon a person's known or inferred sexual orientation.⁵⁶ A report from the Future of Privacy Forum notes, "In contrast, the Digital Advertising Alliance (DAA), a larger self-regulatory organization that is made up of a number of industry advertising trade groups, does not consider sexual orientation to be sensitive except in the context of health conditions derived from medical records."⁵⁷

In 2021, forty members of Congress sent a letter⁵⁸ to Lina Khan, Chair of the Federal Trade Commission, and Jessica Rosenworcel, chair of the Federal Communications Commission, urging the agencies to develop new rules against the collection and sale of consumers' location data after a Catholic media site used commercially available app data to out a Catholic church official, which resulted in his resignation.⁵⁹ Despite pressure from members of Congress, the privacy concerns and endangerment of the LGBTQ+ community have persisted. "Experts have warned for years that data collected by advertising companies from Americans' phones could be used to track them and reveal the most personal details of their lives," Senator Ron Wyden (D-Oregon) told *Recode* in 2021. "Unfortunately, they were right. Data brokers and advertising companies have lied to the public, assuring them that the information they collected was anonymous. As this awful episode demonstrates, those claims were bogus — individuals can be tracked and identified."⁶⁰

In addition to having to comply with the Federal Trade Act, Grindr, which is a California company, is also subject to the California Consumer Privacy Act of 2018 (CCPA).⁶¹ The CCPA greatly expands privacy rights for Californians, including a right to know about the personal information collected, the right to delete the personal information collected, the right to out-

54 Marc Groman, *No One Should be Outed By an Ad*, IAPP, <https://iapp.org/news/a/nai-takes-lgbt-stand/> (last visited Dec. 9, 2023); see also NETWORK ADVERTISING INITIATIVE, 2020 NAI CODE OF CONDUCT (2020), available at, https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf.

55 Wood, *supra* note 20.

56 JOEL REARDON ET AL., 50 WAYS TO LEAK YOUR DATA: AN EXPLORATION OF APPS' CIRCUMVENTION OF THE ANDROID PERMISSIONS SYSTEM (2019), available at, https://www.ftc.gov/system/files/documents/public_events/1415032/privacycon2019_serge_egelman.pdf.

57 Michelle Boorstein, Marisa Iati & Annys Shin, *Top U.S. Catholic Church official resigns after cellphone data used to track him on Grindr and to gay bars*, WASH. POST (July 21, 2021), <https://www.washingtonpost.com/religion/2021/07/20/bishop-misconduct-resign-burrill/>.

58 Sara Morrison, *This Outed Priest's Story is a Warning for Everyone About the Need for Data Privacy Laws*, Vox (July 21, 2021), <https://www.vox.com/recode/22587248/grindr-app-location-data-outed-priest-jeffrey-burrill-pillar-data-harvesting>.

59 Some states, including California, Colorado, Connecticut, Iowa, Virginia, and Utah, have taken it upon themselves to pass state privacy protection laws in the absence of federal protections. *E.g.*, Anokhy Desai, *US State Privacy Legislation Tracker*, <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/> (last updated Dec. 8, 2023).

out of sharing personal data, and the right to non-discrimination for exercising their CCPA rights.⁶² While the CCPA has been celebrated as the strongest data protection law in the country, it encompasses less rights and protections than the GDPR and is limited to residents of only one state.⁶³ While other states have enacted or have considered enacting state-level privacy protections, none have approached the level of protection offered by the GDPR.

B. Data Protections and Concerns for LGBTQ+ People in the European Union

Unlike the U.S., which has a loose patchwork of privacy laws, the EU has an uniform data privacy scheme, the GDPR, which sets a minimum standard of data protection for each member state.⁶⁴ The GDPR centers the overarching principles of “lawfulness, fairness, and transparency,” to guide the way personal data is collected, processed, and stored.⁶⁵ Specifically, in order to be compliant with the GDPR, data must be “collected for specified, explicit and legitimate purposes,” and thus be limited to those specific purposes; stored for only as long as necessary to fulfil those purposes; be accurate and kept up to date; and, be processed in a way that guarantees the “integrity and confidentiality” of data subjects.⁶⁶ To ensure compliance with these principles, the GDPR holds data controllers liable for any violations.⁶⁷

The GDPR also provides data subject with an explicit set of rights that can be employed to protect their privacy, including: the right to access their personal data from data controllers;⁶⁸ the right to rectify any inaccurate data concerning them;⁶⁹ the right to have their personal data erased;⁷⁰ and the right of explanation regarding how certain algorithms process and make

60 State of California - Department of Justice - Office of the Attorney General, *California Consumer Privacy Act (CCPA)*, <https://oag.ca.gov/privacy/ccpa> (last visited Aug 1, 2023).

61 Salomé Viljoen, *The Promise and Pitfalls of the California Consumer Privacy Act*, (Apr. 11, 2020), <https://www.dli.tech.cornell.edu/post/the-promise-and-pitfalls-of-the-california-consumer-privacy-act>.

62 Ashman, *supra* Note 13.

63 Regulation 2016/679 (Art 5 (1)(a).

64 A legitimate purpose, under the GDPR, is the usage of data to prevent fraud, ensure network and information security, or protection from possible criminal acts or threats to public security. Regulation 2016/679 (Art 5(1)(a) – Art 5(1)(e).

65 A data controller is a body that determines the purposes of any personal data and the means of processing it. A data processor is a body who processes personal data on behalf of a data controller. The data controller is liable for GDBR compliance violations.

66 Art 15 – data subjects may also access additional information, such as the purposes of the data processing, the categories of the data processing, the recipients in which the data will be disclosed, and right to lodge a complaint with a supervisory authority in regards to the data being collected and processed.

67 Regulation 2016/679 Art 16.

68 Regulation 2016/679 Art 17.

decisions based on the processing of their data.⁷¹ The GDPR creates a private right of action for data subjects whose privacy rights were violated.⁷²

As mentioned earlier in this Article, the GDPR also explicitly prohibits the processing of data pertaining to a person's sex life or sexual orientation. This prohibition can be circumvented if the data subject gives explicit consent or if other requirements are met.⁷³ This circumvention gives significant power to the individual and their right to privacy.

Under the GDPR, consent is subject to a heightened standard than in the U.S. and must be "freely given," meaning that the data subject must freely give a "specific, informed and unambiguous indication" that they agree to have their data collected, processed, and stored.⁷⁴ Individuals can thereby withdraw their consent at any time. An individual's consent must also be in the form of a "clear affirmative action," which means that "opt-in" consent, such as a pre-checked box, is not sufficient to show consent under the GDPR.⁷⁵ Additionally, freely given consent must be given by the data subject for every type of data collection and processing being done by the data controller—in other words, consent for one type of processing cannot be used for consent of another type of processing.⁷⁶

The GDPR outlines specific enforcement provisions that give data subjects the right to file complaints with supervisory authorities and includes a private right of action to hold data controller's accountable.⁷⁷ These specific enforcement provisions allow individuals who pursue claims to be compensated for their damages.⁷⁸ Under this enforcement scheme, privacy advocates have celebrated the EU for achieving effective and uniform privacy standards.⁷⁹

LGBTQ+ dating apps, which use vast amounts of personal data – including name, email, age, and location – have struggled to comply with the GDPR heightened privacy protections for vulnerable groups.⁸⁰ Because LGBTQ+ people are under a higher risk of harm if their privacy rights are

69 Regulation 2016/679 Art 22.

70 TrueVault, *The GDPR's private right of action* TrueVault, <https://www.truevault.com/learn/gdpr/gdpr-private-right-of-action#:~:text=It's%20a%20big%20question%20for,whose%20privacy%20rights%20were%20violated>. (last visited Nov 26, 2023).

71 Regulation 2016/679 Art 9(2).

72 Regulation 2016/679 Art 4(11).

73 Regulation 2016/679 Art 7,

74 A provided box at the end of a catchall policy, therefore, is also not sufficient to illustrate consent under this standard.

75 Regulation 2016/679 Art 77 – Art 79.

76 TrueVault, *supra* Note 71.

77 Dana Leigh, *5 Years Of GDPR, What Do The Experts Say?*, TECHROUND (May 25, 2023), <https://techround.co.uk/news/5-years-of-gdpr-what-do-the-experts-say/>.

78 Regulation 2016/679 Art 9.

violated, apps like Grindr face a higher scrutiny when it comes to privacy protections for app users. Grindr necessitates some data collection to connect users. Location being one such important piece of data for the app. The purposes of Grindr and other LGBTQ+ dating apps necessitate the sharing of some data; however, there is significant concern over what data ought to be retained.

Warwick International Higher Education Academy's (WIHEA) resource on best practices for gender and LGBTQ+ data collection under the GDPR privacy scheme highlights that apps must be conscious specifically about data minimization.⁸¹ Data minimization requires that data controllers only process data that is "adequate, relevant and limited to what is necessary in relation to your processing purpose."⁸² Many apps in the U.S. collect and process as much data as possible, often outside the scope of what is necessary, in order to sell it to advertisers.⁸³ Under the GDPR, this practice, which can have harmful consequences, is unlawful.⁸⁴

As the "Out of Control" report shows, LGBTQ+ apps also have struggled with complying with the needed consent for data processing under the GDPR. None of the apps investigated in the report, including Grindr, OkCupid, and Tinder, "provide[d] any meaningful ways of giving or refusing consent to the sharing of personal data with third parties."⁸⁵ The report argues that the advertising technology system in its current form "is deprived of any meaningful individual choice and transparency, and personal data is transmitted to an enormous amount of actors who each operate with their own privacy policies," and that, therefore, the industry as a whole is unlikely to be complying with GDPR consent responsibilities.⁸⁶ The Norwegian complaint against Grindr highlights these concerns. Grindr unlawfully shared GPS data, IP address, age, and gender data. Alongside this, Grindr's former chief privacy officer, Ron De Jesus, in a lawsuit against Grindr alleges the companies stored personal data such as nude photos, which violates privacy law.⁸⁷

79 Warwick International Higher Academy, https://warwick.ac.uk/fac/cross_fac/academy/activities/learningcircles/transqueerpedagogies/datacollection/ (last visited Dec. 9, 2023).

80 Regulation 2016/679 Art 5.

81 Jason Cohen, *These Apps Collect the Most Personal Data*, PCMag (Jan. 11, 2022), <https://www.pcmag.com/news/sick-of-data-collection-try-these-apps-instead>.

82 Matt O'Brien & Frank Bajak, *Priest Outed via Grindr App Highlights Rampant Data Tracking*, AP News (July 22, 2021), <https://apnews.com/article/technology-europe-business-religion-data-privacy-97334ed1aca5bd363263c92f6de2caa2>.

83 Out of Control, *supra* Note 6.

84 *Id.* at 171.

85 Epic, *In re grindr, LLC*, <https://epic.org/documents/in-re-grindr-llc/#:~:text=In%20June%202023%2C%20Grindr's%20former,to%20correct%20its%20privacy%20practices>. (last visited Nov 26, 2023).

III. Grindr and Privacy Concerns in the U.S. and the European Union

Grindr has been in hot water multiple times in the past few years. In 2018, an investigation by the Norwegian nonprofit SINTE found that Grindr shared user's HIV status and "last tested date" with two companies.⁸⁸ Because the HIV information was provided to the companies along with users' GPS data, phone ID, and email, researchers at SINTE could identify specific users and their HIV status.⁸⁹

While Grindr contended that information provided to vendors was encrypted, SINTEF's analysis found that some information shared with third-party advertisers was sometimes shared via "plain text," which can be easily hacked.⁹⁰ In the same year, Grindr also suffered from a security issue which had the potential to expose the information of its users.⁹¹ In 2019, security researchers exposed how Grindr could be used to pinpoint the location of its users.⁹²

The 2020 NCC investigation into Grindr revealed multiple potential GDPR violations by the company. Particularly, privacy advocates were concerned about 1) "vagueness of which legal basis Grindr is using for processing personal data;" 2) the company attempting to "shift accountability for the advertising technologies that it is using away from itself;" 3) whether users are given "sufficient information about how data may be shared during the registration process in the app."⁹³ Specifically, the Norwegian Data Protection Authority (NDPA) found that the company breached articles 6(1) and 9(1) of the GDPR.⁹⁴

Art 6(1) of the GDPR relates to the lawfulness of processing.⁹⁵ It was found that Grindr was providing advertisers with personal data without a

86 Jenna Payesko, *Grindr found to be sharing users' HIV status with other companies*, CONTAGIONLIVE (Apr. 3, 2018), <https://www.contagionlive.com/view/grindr-found-to-be-sharing-users-hiv-status-with-other-companies>.

87 Azeen Ghorayshi & Sri Ray, *Grindr Is Letting Other Companies See User HIV Status And Location Data*, BUZZFEED NEWS (Apr. 2, 2018), <https://www.buzzfeednews.com/article/azeenghorayshi/grindr-hiv-status-privacy#.yp0J48W0N>.

88 *Id.*

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

90 Chris Fox, *Gay Dating Apps Still Leaking Location Data*, BBC (Aug. 8, 2019), <https://www.bbc.com/news/technology-49265245>.

91 Out of Control, *supra* Note 6, at 72-74; 131.

92 Natasha Lomas, *Grindr Hit With \$7M Fine for GDPR Consent Breaches*, TECHCRUNCH (Dec. 15, 2021), <https://techcrunch.com/2021/12/15/grindr-final-gdpr-fine/>.

93 Regulation 2016/679 Art. 6(1).

legal basis—and that, specifically, the company was found to have disclosed special category personal data without receiving proper consent or another valid exemption via Art 9(1).⁹⁶ The NDPA's conclusion that Grindr had violated the GDPR sparked interest in the U.S., where privacy advocates were concerned about whether Grindr's privacy policy also failed to comply with the CCPA.⁹⁷ A group of civil rights and consumer groups in response to the NCC's investigation of Grindr urged federal and state regulators to use the finding to pass a federal law similar to GDPR and investigate any potential violations of the CCPA by Grindr.⁹⁸

While Grindr made changes “to remedy the deficiencies in their previous consent-management platform,” leading to a drop in NDPA fines, an ex-employee recently blew the whistle on other privacy concerns at the company.⁹⁹ According to the company's former chief privacy officer, Ron De Jesus, who is engaged in a wrongful termination suit with Grindr, the company has repeatedly violated the CCPA.¹⁰⁰

De Jesus has alleged that he was terminated in retaliation for raising concern regarding data privacy practices at the company, which allegedly included the retention of users' personal data, including sexually explicit images and HIV status, that were accessible by third parties and staff even after the user deleted their account.¹⁰¹ In addition to violating state privacy laws, De Jesus has accused Grindr of contradicting its own privacy policy, which may constitute deceptive trade practices under the FTCA and open the company up to an investigation by the FTC.¹⁰² However, at this time, there is no evidence that the FTC or the California's Office of the Attorney General, which is responsible for enforcing the CCPA, has opened an investigation

94 Administrative Fine - Grindr LLC, <https://www.datatilsynet.no/contentassets/8ad827efefcb489ab1c7ba129609edb5/administrative-fine---grindr-llc.pdf> (last visited Aug 1, 2023).

95 Bobby Allyn, *Study: Tinder, Grindr And Other Apps Share Sensitive Personal Data With Advertisers*, NPR (Jan. 14, 2020), <https://www.npr.org/2020/01/14/796427696/study-grindr-tindr-and-other-apps-share-sensitive-personal-data-with-advertisers#:~:text=Tiny%20Desk->.

96 *Leading Consumer and Privacy Groups Urge Congress, the FTC, State AGS in California, Texas, Oregon to Investigate Several Popular Dating Apps*, PUBLIC CITIZEN (Jan. 14, 2020), <https://www.citizen.org/article/popular-dating-health-apps-violate-privacy/>.

97 Terje Solsvik, *Grindr fine cut to \$7 mln in Norway Data Privacy Case*, REUTERS (Dec. 15, 2021), <https://www.reuters.com/technology/grindr-fine-cut-7-mln-norway-data-privacy-case-2021-12-15/>.

98 Skye Witley, *Fired Grindr Executive says App Places “profit over privacy”*, YAHOO! FINANCE (June 15, 2023), <https://finance.yahoo.com/news/fired-grindr-executive-says-app-182812301.html>.

99 Epic, *In re grindr, LLC*, <https://epic.org/documents/in-re-grindr-llc/#:~:text=In%20June%202023%2C%20Grindr's%20former,to%20correct%20its%20privacy%20practices>. (last visited Nov 26, 2023).

100 *Id.*

into the company.¹⁰³

In the U.S., privacy advocates have demanded that the U.S. implement a federal data privacy scheme, similar to the EU's GDPR, and recognize the importance of enacting special protections for sensitive information and vulnerable groups. However, European privacy advocates have alleged that the EU's approach may in fact be failing¹⁰⁴ because of a lack of enforcement.¹⁰⁵ Despite challenges implementing and enforcing a data privacy scheme, it is imperative for privacy experts and legislators to consider how data privacy and civil rights interact. As De Jesus' case illustrates, data privacy is largely determined by the companies. If the companies lack an adherence to data privacy laws, which vary significantly, it is difficult to maintain a level of protections for at-risk groups, such as LGBTQ+ people. For marginalized groups, particularly LGBTQ+ people, who face a high level of discrimination, it is imperative that there is a higher level of data protection and privacy rights.

101 *Id.*

102 Vincent Manancourt, *EU Privacy Chief Bashes Lack of GDPR Enforcement Against Big Tech*, POLITICO (June 17, 2022), <https://www.politico.eu/article/gdpr-europe-wojciech-wiewiorowski-privacy-chief-lack-enforcement-big-tech/>.

103 The low number of GDPR compliance violation cases have led WIRED writer, Matt Burgess, to allege that GDPR is, in fact, failing and European Data Protection Supervisor Wojciech Wiewiórowski has remarked that there has not yet been sufficient enforcement of the data privacy scheme. Matt Burgess, *How GDPR Is Failing*, WIRED (May 23, 2022), <https://www.wired.com/story/gdpr-2022/>.