Ask App Not to Track: Data Privacy Concerns Posed by Gender Transition Tracking Applications

*Noa Batlan**

"Gender Transition Tracking applications" are newly emerging platforms that provide transgender individuals extraordinary access to each other and information about gender-affirming healthcare. However, the use of these apps leaves transgender individuals vulnerable, especially amidst an increasingly broad and fervent campaign to criminalize gender affirming care. These apps collect uniquely identifiable and incriminating information that, if collected by law enforcement through existing warrant processes, may pose risk to the transgender community and their healthcare providers.

This Note offers several novel contributions to this important contemporary issue. First, this Note explores how law enforcement officials may leverage existing data surveillance infrastructures to gather often detailed information stored on gender tracking apps. Second, this Note investigates existing efforts to limit these vulnerabilities through privacy protections by government entities. Finally, the Note concludes by offering proposals to protect transgender gender tracking app users.

* JD Candidate, University of California, Davis School of Law, '25; BA, University of Chicago, '20. Thank you to Professor Courtney G. Joslin for her immensely generous support and guidance in writing this Note. Thank you to Clayton and the editors of the Texas Journal on Civil Liberties & Civil Rights for engaging so thoughtfully throughout the editing process. Lastly, thank you to the wisdom and strength of my fellow trans law students.

INTRODUCTION[1]

The trans[2] community's unique use of the Internet makes their digital information distinctively vulnerable to abuse. Many trans

[1] My experience being transgender and nonbinary has greatly impacted the way I approach this research. I have navigated the medical institutions discussed herein and underwent the process of coming to understand my own gender and the medical interventions necessary to feel aligned and euphoric in my expression. While this experience is in no way definitive of the extraordinarily diverse transgender community, I hope to include my own impressions of these systems as credible and meaningful sources to describe how real trans people experience these hurdles day-to-day.

[2] I use the term "trans" as short for "transgender." "Trans" for the purposes of this Note will serve as an umbrella term for those who are transgender, gender non-conforming, or non-

individuals, particularly those living in isolated or politically unwelcoming areas, use the Internet to connect with other trans people.[3] In communicating online with each other on social media and other outlets, trans users leverage the internet to gather and share information, find trans-friendly medical providers, and explore gender identity.[4] In seeking community and advice, some trans people share personal details of their identity online that they may not otherwise share with others in person. As such, some may expose more personal information online than their cis peers in order to meet their personal and medical needs. Their reliance and prevalent presence on internet platforms, as well as the politicized nature of their identity, make trans people particularly vulnerable to invasions of privacy.

The proliferation of trans-targeted tech contributes to this vulnerability. In recent years, companies have developed "Gender Transition Tracking Applications"[5] to help trans users document and archive milestones of their transition. These apps "track" the user's gender identity as it evolves over time and help facilitate the social and medical mechanisms of their transitions. The emergence of these apps fit within a larger social context of increased numbers of individuals transitioning and the wide cultural practice of using social media to mark transition. In recent history, users have documented their transitions on platforms such as YouTube or TikTok, synthesizing months of physiological changes in succinct short-form videos shared publicly.[6] Some may be familiar with the "*Hi, my name is [insert], and this is my voice [insert] months on T*" model, where individuals share physical changes to their appearance and voice over the course of their initial transition.[7] Increasingly, trans individuals are able to use gender-tracking apps on their phones like TRACE and For Them, rather than YouTube and TikTok, to track their gender transition progress.[8]

---

binary. Gender and its "transness" are deeply personal but can broadly refer to those whose gender identity is different from their gender assigned at birth.

[3] *See* Yolanda N. Evans et al., *Understanding Online Resource Use by Transgender Youth and Caregivers: A Qualitative Study*, 2 TRANSGENDER HEALTH 129, 131 (2017).

[4] *Id.*

[5] Hereinafter referred to as "gender-tracking apps" or "the apps."

[6] Beatrice Rothbaum et al., *Transgender Community Resilience on YouTube: Constructing an Informational, Emotional, and Sociorelational Support Exchange*, 50 J. CMTY. PSYCH. 2366, 2367 (2022).

[7] *See, e.g.*, Gayety, *6 Trans Folks Show Off Their Voice Changes on Testosterone*, YOUTUBE (Feb. 26, 2023), https://www.youtube.com/watch?v=NRDrB_hLUlc [https://perma.cc/9ADU-HNEQ].

[8] Other apps serve similar purposes, including Solace, Euphoria, TransTracks, and Transcapsule. All of these apps provide similar platforms and services to the ones above.

These platforms share the same general features of logging journal entries, either for exclusively personal use or onto a shared social media feed, and uploading photos, with some distinguishing elements. For example, For Them is "an online community" originating out of a company selling chest binders.[9] Customers pay $15 a month to opt into the subscription-based platform called "The Playground," which features daily mood and identity check-ins in addition to discounts on binder purchases.[10] Users can upload photos and descriptions that track progress in one's physical transition.[11] This kind of subscription service and purchasing tie-in is unique amongst other transition tracking apps.

Simultaneous to the emergence of gender-tracking apps, U.S. states have become increasingly hostile towards the trans community, passing laws that target and attack trans civil rights. Since 2017, nearly four out of five U.S. states—39 in total—have passed laws restricting how patients, including adults and youth, access gender-affirming care.[12] More imminently, the *Mandate for Leadership*, more commonly known as *Project 2025*, laid out the second Trump Administration's policy goals to directly attack access to trans healthcare, including eliminating coverage for the prescription of gender affirming care regardless of a patient's age.[13] Amidst a growing political and cultural animus against gender non-conforming individuals, it is understandable that the trans community is seeking safety and connection, particularly online and through these apps. Simultaneously, this anti-trans political climate increases the risk of information stored and shared online by individuals on these platforms being used against them.

---

[9] Chest or breast binders are anything used to flatten one's breast tissue so as to minimize their appearance under clothes. *See How to Bind Your Chest Safely*, CLEV. CLINIC (July 26, 2021), https://health.clevelandclinic.org/safe-chest-binding [https://perma.cc/5Q24-62T9]. For Them's product works as a compression shirt or bra that constricts the user's breasts tight against their chest.

[10] Mb (@mb), X (Aug. 25, 2023, 2:46PM), https://threadreaderapp.com/thread/1695160767056597184.html [https://perma.cc/4FKS-EZ44] (describing features in-depth in the initial tweet and subsequent thread on the same topic). The Playground no longer seems to be ForThem's social platform, instead merging with their subsidiary publication, Autostraddle, to form AF+. *See aF+ Membership*, FORTHEM, https://www.forthem.com/product/af-plus-toki [https://perma.cc/74H4-VDT6]. This flux highlights the ever-shifting nature of transition support networks in the current political climate.

[11] @mb, *supra* note 10.

[12] *See* MOVEMENT ADVANCEMENT PROJECT, UNDER FIRE SERIES #5: BANNING MEDICAL CARE AND LEGAL RECOGNITION FOR TRANSGENDER PEOPLE 3 (2023), https://www.mapresearch.org/file/MAP-2023-Under-Fire-Report-5.pdf [https://perma.cc/6RAG-EZHN].

[13] *See* THE HERITAGE FOUNDATION, MANDATE FOR LEADERSHIP: THE CONSERVATIVE PROMISE 485, 495 (2023), https://www.documentcloud.org/documents/24088042-project-2025s-mandate-for-leadership-the-conservative-promise [https://perma.cc/LK2B-CTQA].

This Note will explore how gender-tracking apps may jeopardize trans users' digital privacy in the midst of the criminalization of transgender healthcare across many states. Part I illustrates how gender-tracking apps fit into the broader digital surveillance ecosystem. In addition, it details the rising criminalization of trans healthcare seekers and providers. Part II explores the specific risks posed by the digital ecosystem to the private information of those seeking this care. Particularly, this Part discusses the potential harms to trans communities should the information gathered by these apps be leveraged in a criminal investigation. Part III outlines ongoing legislative efforts to protect the data privacy of those seeking recently-criminalized healthcare and provides recommendations for more effective regulations.

Ultimately, this Note will demonstrate that, while offering the benefits of peer-to-peer information-sharing, gender-tracking apps pose a new risk to their trans users because their data can be accessed for criminal prosecution. In particular, geofence warrants and data brokers allow law enforcement to identify and catalog large numbers of trans individuals and their healthcare providers.[14] To be sure, these vulnerabilities are neither created by nor unique to these apps; they are already present aspects of the digital surveillance ecosystem and law enforcement practices.[15] Nevertheless, gender-tracking apps do represent a new threat in that they compile uniquely incriminating information in large quantities that could lead to the elimination of available gender-affirming care options.

While there are no reported cases of law enforcement seeking warrants for these apps' information yet, existing legislation fails to adequately protect the trans community's privacy interests. As such, there is opportunity for law enforcement to abuse these apps' user information. Therefore, I argue that local legislators invested in developing stronger systems of protection must turn their attention to putting in place greater regulation of the opaque and unruly data broker market, including limitations on police participation in these markets. I close this Note by offering recommendations that address these identified legal risks and better protect trans people using the internet to improve their care and build community.

---

[14] *See infra* notes 90–94 and accompanying text.

[15] *See, e.g.*, SHARON BRADFORD FRANKLIN ET AL., CTR. FOR DEMOCRACY & TECH., LEGAL LOOPHOLES AND DATA FOR DOLLARS: HOW LAW ENFORCEMENT AND INTELLIGENCE AGENCIES ARE BUYING YOUR DATA FROM BROKERS 7(Dec. 2021), https://cdt.org/insights/report-legal-loopholes-and-data-for-dollars-how-law-enforcement-and-intelligence-agencies-are-buying-your-data-from-brokers [https://perma.cc/UME4-WQDC] ("law enforcement and intelligence agencies are among the customers of some data brokers, spending millions of dollars to gain access to private sector databases which often contain very sensitive and very personal information on individuals.").

I. RELEVANT HEALTH, DIGITAL, AND LEGAL LANDSCAPES

This Part surveys the relevant health, digital, and legal contexts in which gender-tracking apps exist. First, this Part describes what gender-affirming care can look like. Then, it examines the harm that can result from not receiving this care and the barriers that exist to care. In addition, this Part discusses developments and implications of the fervent anti-trans campaign that has restricted access to gender-affirming care in a majority of states. Next, this Part provides more context for the functions of gender-tracking apps and how, through peer-to-peer information sharing, they can fill gaps created by an inaccessible healthcare system and anti-trans culture. Finally, this Part describes the digital surveillance ecosystem and identifies some of the ways in which law enforcement plays an active role in the data economy, such as purchasing information from data brokers and obtaining warrants that target vulnerable populations.

A. A Bit on Trans Health Care

While not all trans and non-binary individuals incorporate medical care into their transition, some seek out the assistance of doctors in achieving their gender goals.[16] Gender-affirming care can include a range of medical and social interventions, and the choices patients make in adapting their physical presentation to that which more accurately aligns with their identity are deeply personal.[17] Patients may choose to undergo hormone replacement therapies (HRT), surgical procedures, or voice training, amongst others.[18] A critical intervention for trans minors is puberty blockers, which use certain types of hormones to "pause" pubertal development that does not align with their gender identity.[19] HRT leads to slow hormonal changes over time that can alter one's physical appearance, voice, and internal endocrine system.[20] Patients may select the dosage of

[16] *See generally*, Jaclyn M. W. Hughto et al., *Social and Medical Gender Affirmation Experiences Are Inversely Associated with Mental Health Problems in a U.S. Non-Probability Sample of Transgender Adults*, 49 ARCH SEX BEHAV. 2635 (2020) (describing the significant benefits of both social and medical transition on mental health outcomes).

[17] *See* Juanita K. Hodax & Sara DiVall, *Gender-Affirming Endocrine Care for Youth with a Nonbinary Gender Identity*, 14 THERAPEUTIC ADV. ENDOCRINOL. METAB. 3, 10 (2023) (summarizing various forms of both hormonal and non-hormonal treatment and their effects.)

[18] U.S. DEP'T HEALTH & HUM. SERVS., OFFICE POPULATION AFFS., GENDER-AFFIRMING CARE AND YOUNG PEOPLE, at 2 (2023).

[19] *Id.*

[20] *Id.*; *Information on Testosterone Hormone Therapy*, UCSF HEALTH SYS. (July 2020), https://transcare.ucsf.edu/article/information-testosterone-hormone-therapy [https://perma.cc/Q2GR-5RAV].

HRT to align with the desired physical outcomes that best align with their identity.[21]

The provision of gender-affirming care is associated with increased mental-health outcomes among patients.[22] A recent study found that "receipt of gender-affirming care, including puberty blockers and gender-affirming hormones, was associated with 60% lower odds of moderate or severe depression and 73% lower odds of suicidality" amongst trans young adults.[23] Gender-affirming surgeries have been shown to have similar benefits in increasing mental health outcomes and reducing suicidality of patients.[24] If individuals pursuing gender-affirming medical care are forced to stop treatment suddenly, due to legal interventions that revoke the legality of either medical provision of care or insurance coverage, there can be medical repercussions. For example, patients who stop taking HRT can experience endocrine withdrawal symptoms, including extreme mood swings and hot flashes.[25]

The largest reported barrier trans individuals experience to receiving gender-affirming care is the general lack of sufficiently trained, knowledgeable, and compassionate providers.[26] The limited prevalence of doctors who competently and compassionately provide gender-affirming care contributes to severe waitlists or total unavailability of services.[27] Furthermore, nearly one-in-two trans patients have experienced forms of discrimination and mistreatment when attempting to access healthcare, ranging from care refusal and misgendering to verbal or physical abuse.[28] While HRT has been prescribed since the 1960s to cis-women to manage their menopause symptoms medically, some doctors are less comfortable prescribing HRT to their trans patients than their cis-gender counterparts

---

[21] Hodax & DiVall, *supra* note 17, at 3–4.

[22] Diana M. Tordoff et al., *Mental Health Outcomes in Transgender and Nonbinary Youths Receiving Gender-Affirming Care*, JAMA, Feb. 2022, at 2–3.

[23] *Id*. at 1.

[24] *See* Anthony N. Almazan & Alex S. Keuroghlian, *Association Between Gender-Affirming Surgeries and Mental Health Outcomes*, 156 JAMA SURG. 611, 612–13 (2021).

[25] Ze'ev Hochberg et al., *Endocrine Withdrawal Syndromes*, 24 ENDOCRINE REVS. 523, 529 (2003).

[26] *See* Joshua D. Safer et al., *Barriers to Health Care for Transgender Individuals*, 23 CURRENT OP. IN ENDOCRINOLOGY, DIABETES & OBESITY 168, 169 (2016) (collecting studies).

[27] *See* Sarah Dahlgren Allen et al., *A Waitlist Intervention for Transgender Young People and Psychosocial Outcomes*, 148 PEDIATRICS 1, 2 (2021).

[28] Caroline Medina, *Fact Sheet: Protecting and Advancing Health Care for Transgender Adult Communities*, CTR. FOR AM. PROGRESS (Aug. 25, 2021), https://www.americanprogress.org/article/fact-sheet-protecting-advancing-health-care-transgender-adult-communities [https://perma.cc/6KBA-PZS3].

due to a lack of training and stigma.[29] Furthermore, trans patients have reported a need to "teach" their doctor about transgender people in order to receive appropriate care.[30] As a result, there is notable distrust of the medical field among the trans community, which further contributes to the existing hurdles in accessing healthcare.[31]

Structural barriers to accessing insurance coverage also inhibit access to gender-affirming care. Transgender individuals are more likely to be uninsured than their cis-gendered counterparts due to intersecting factors including poverty, race, and age.[32] For those who are insured, many health insurance plans exclude coverage of transgender healthcare, procedures, and gender-affirming care.[33] Furthermore, transgender healthcare and procedures, even if covered, may be cost-prohibitive.[34] While insurance may cover part of a surgery or prescription co-pay, there are additional costs for medications, procedures, and everyday supplies that may be unaffordable to some trans individuals.[35]

In part due to barriers accessing medical treatment and navigating health institutions, many trans people turn to online resources and communities to help manage their transition. Peer-to-peer information sharing may fill the gaps when medical and insurance institutions fail to provide information, respect, or affordable resources.[36] Online communities are also often sought to celebrate and affirm the small

---

[29] *See generally* Angelo Cagnacci & Martina Venier, *The Controversial History of Hormone Replacement Therapy*, 55 MEDICINA (KAUNAS) 602 (2019); Safer, *supra* note 26, at 170.

[30] Medina, *supra* note 28.

[31] *See id*.

[32] Wyatt Koma et al., *Demographics, Insurance Coverage, and Access to Care Among Transgender Adults*, KFF (Oct. 21, 2020), https://www.kff.org/health-reform/issue-brief/demographics-insurance-coverage-and-access-to-care-among-transgender-adults [https://perma.cc/WY9V-XUGS].

[33] Medina, *supra* note 28.

[34] I am a trans-masculine person who has fantastic insurance that covers my gender-related healthcare. Insurance covered my top surgery, but I still paid several thousand dollars out of pocket. This did not cover the cost of recovery supplies and taking time off of work. Each month I pay $25-30 dollars to fill prescriptions, including testosterone, needles, and syringes for my weekly prescriptions. I also visit my doctor two to four times a year, paying co-pays for the visit and subsequent blood tests to monitor my hormone levels and health. All of this adds up! For a discussion of the economic insecurities many transgender folks experience, see Movement Advancement Project & Center for American Progress, *Paying an Unfair Price: The Financial Penalty for Being Transgender in America*, MOVEMENT ADVANCEMENT PROJECT (Feb. 2015), https://www.lgbtmap.org/unfair-price-transgender [https://perma.cc/AJK8-QQLV] (outlining the financial penalties experienced by transgender individuals in day-to-day life, including high costs of healthcare, housing, and education, resulting from discrimination).

[35] *Id*.

[36] Vern Harner, *Trans Intracommunity Support & Knowledge Sharing in the United States & Canada: A Scoping Literature Review*, 29 HEALTH & SOC. CARE CMTY. 1715, 1725 (2021).

victories of transition, such as winning a bureaucratic battle navigating health institutions or recovering from surgery.[37]

B. Current Developments in the Political Campaign Against Trans Healthcare

In the last nine years there has been a major increase in the quantity and severity of anti-trans legislation across the United States.[38] Anti-trans legislation has targeted individuals' ability to update legal identification documents, weakened workplace anti-discrimination laws, restricted speech related to pronouns and identity, prevented trans youths' participation and learning in school, and prohibited access to public accommodations such as bathrooms.[39]

One-third of anti-trans laws introduced in 2023 attacked trans individuals' access to gender-affirming healthcare, including interventions such as HRT and reconstructive surgeries.[40] Many of the trans-medical care bans specifically impact minors, but nine states currently prohibit access to care regardless of age: Arizona, Texas, Nebraska, Missouri, Tennessee, Kentucky, Ohio, South Carolina, and Florida.[41]

Laws across states target different access points for healthcare. Some refuse coverage of necessary medical care by state insurance plans, including Medicaid, while others focus on private insurance coverage.[42] Five states currently make it a felony to provide best practice medical care (as endorsed by the American Academy of Pediatrics and the American Medical Association) to transgender youth, meaning doctors and individuals who choose to defy state law and prescribe transgender healthcare face criminal penalties.[43] Other bills authorize state licensing

---

[37] *Id.*; *see also* Hannah Kia et al., *"It Saves Lives": Peer Support and Resilience in Transgender and Gender Diverse Communities*, 3 SSM - QUALITATIVE RSCH. HEALTH 5 (2023) ("participants often remarked on the power and significance of sharing lived experience with trans peers, particularly after enduring explicit, enacted, and intersecting forms of stigma and discrimination").

[38] *See Mapping Attacks on LGBTQ Rights in U.S. State Legislatures*, ACLU, https://www.aclu.org/legislative-attacks-on-lgbtq-rights [https://perma.cc/FR7T-4WY3].

[39] *Id.*

[40] MOVEMENT ADVANCEMENT PROJECT, *supra* note 12.

[41] *Id.* ("As a result of this rapid shift in state policy, this means that now over one in three (35%) transgender youth live in states that ban or severely restrict medically necessary health care—up from 4% at the beginning of [2023].").

[42] *Id.* For example, "The Arizona's Children Deserve Help Not Harm Act went into effect in March 2022, cutting off access to care for the state's estimated 7,300 transgender youth under 18." ELANA REDFIELD ET AL., PROHIBITING GENDER-AFFIRMING CARE FOR YOUTH 7 (2023). The bill "ban[s] treatments and referrals for treatment, the use of public funds, and Medicaid coverage, [and] a ban on tax reimbursements for gender-affirming care expenses for young people." *Id.*

[43] *See* MOVEMENT ADVANCEMENT PROJECT, *supra* note 12, at 3.

boards to discipline medical providers who prescribe gender-affirming care and allow private individuals to file civil lawsuits against medical providers who violate these laws.[44]

A primary example of a state law banning best practice medical care to trans minors is Idaho's HB 71, which was signed into law by the governor in April 2023.[45] Also known as "The Vulnerable Child Protective Act," HB 71 prohibits doctors from providing puberty blockers, hormone replacement therapy, and surgeries as gender-affirming care to patients under the age of 18.[46] Providing such care carries a penalty of up to ten years in prison.[47] While other states commonly use this policy and penalty,[48] Florida has taken a much more extreme approach. Florida's SB 254 takes an all-of-the-above approach, penalizing healthcare providers by inflicting felony penalties, revoking doctor licenses, prohibiting state Medicare coverage, and forbidding the use of public funds to finance gender-affirming care.[49] Not only that, this law also grants the state power to remove trans children from their transition-supporting parents on the grounds that they are being "subjected to or threatened with mistreatment or abuse."[50]

As described, many of the laws currently in motion target the provision of care to children. However, state legislatures and the federal government are expanding their sights to adults. For example, Oklahoma's proposed S.B. 129, which died in committee in 2023, "prohibits any physician from providing gender transition procedures or referral services relating to gender transition to any individual under 26 years of age."[51] While most states banning gender transition-related care limit their regulations to those under age eighteen, there is a growing trend of restricting access to care for young adults.[52] As new legislation is introduced, legislators may become increasingly emboldened to raise the age at which they ban healthcare. This may be more and more likely, particularly as this cause is possibly supported by Trump's second administration. *Project 2025*, which provides a speculative glimpse into Trump's future policy initiatives, calls for the prohibition of Medicare

---

[44] *See* REDFIELD, *supra* note 42, at 12.

[45] *See* H.R. 71, 67th Leg., Reg. Sess. (Idaho 2024).

[46] *Id.*

[47] *Id.*

[48] *See, e.g.,* Alabama's Vulnerable Child Compassion and Protection Act of 2022, ALA. CODE § 26-26-4.

[49] *See* S.B. 254, 2023 Leg., Reg. Sess. (Fla. 2023).

[50] *Id.*

[51] S.B. 129, 59th Leg., Reg. Sess. (Okla. 2023); *see also* H.R. 3730, 125th Gen. Assemb., Reg. Sess. (S.C. 2023) (introducing a similar law under the same name in South Carolina).

[52] MOVEMENT ADVANCEMENT PROJECT, *supra* note 12, at 5.

coverage of gender affirming care and trans-positive initiatives by the Department of Health and Human Services.[53]

Meanwhile, other newly passed legislation extends liability to those who merely assist trans individuals in receiving care. Over one-third of all anti-trans healthcare bills between 2020 and 2023 authorize penalties against non-medical professionals such as parents, teachers, friends, or neighbors of transgender children.[54] For instance, Iowa passed a law in March 2023 that "prohibit[s] conduct which 'aids or abets' youth access to gender-affirming care."[55] In response, some families who have the means to do so are leaving states that have passed anti-trans legislation to protect not only their child, but their entire family unit.[56]

To be clear, a majority of anti-trans healthcare laws create criminal liability only for *medical providers* prescribing gender-affirming care.[57] Trans individuals, as the laws are currently written, are unlikely to face criminal charges for *receiving* gender-affirming care.[58] However, as this Note discusses, the State may still seek penalties against trans families, gravely affecting trans individuals' ability to access necessary healthcare in such instances.[59]

Given these legal and medical circumstances, it is a dangerous time to be a trans person seeking access to necessary gender-affirming care. The nationally expanding criminalization of trans healthcare not only endangers trans people, but also their family members and care providers. The existing shortage of adequate healthcare providers to meet trans patients' needs is exacerbated by the severe penalties for providers that have been enacted across the country. While transgender patients are not

---

[53] THE HERITAGE FOUNDATION, *supra* note 13, at 284, 474.

[54] *See* MOVEMENT ADVANCEMENT PROJECT, *supra* note 12, at 10.

[55] *See* REDFIELD, *supra* note 42, at 7.

[56] *See, e.g.*, Kiara Alfonseca, *"Genocidal": Transgender People Begin to Flee States with Anti-LGBTQ Laws*, ABC NEWS (June 11, 2023), https://abcnews.go.com/US/genocidal-transgender-people-begin-flee-states-anti-lgbtq/story?id=99909913 [https://perma.cc/KAG4-YJJ7]; Arleigh Rodgers & Michael Goldberg, *New State Laws Force Families with Trans Kids to Seek Gender-Affirming Care Elsewhere*, PBS NEWS (July 10, 2023), https://www.pbs.org/newshour/nation/new-state-laws-force-families-with-trans-kids-to-seek-gender-affirming-care-elsewhere [https://perma.cc/X9N2-QMVM]; Tracee Wilkins et al., *'He Is a Gift': Trans Child's Family Talks about Fleeing Texas for Maryland*, NBC4 WASHINGTON (June 13, 2023), https://www.nbcwashington.com/investigations/he-is-a-gift-trans-childs-family-talks-about-fleeing-texas-for-maryland/3366679 [https://perma.cc/PG66-BTAE].

[57] *See* MOVEMENT ADVANCEMENT PROJECT, *supra* note 12, at 9.

[58] *See* Annette Choi & Will Mullery, *19 States Have Laws Restricting Gender-Affirming Care, Some With the Possibility of a Felony Charge*, CNN (June 6, 2023), https://www.cnn.com/2023/06/06/politics/states-banned-medical-transitioning-for-transgender-youth-dg/index.html [https://perma.cc/C8CA-ZGWN] (describing anti-trans laws, none of which allow criminal charges against patients).

[59] *Id.*

always the immediate target of healthcare criminalization at the moment, they acutely feel those laws' effects.

C. Gender Transition Tracking Applications

Amidst this healthcare setting, tracking apps have emerged to support peer-to-peer processes. There are several gender-tracking apps on the market, and this Note highlights two in particular: TRACE[60] and For Them's "The Playground," because they demonstrate the more typical services these types of apps provide to users, while still exhibiting some distinctive features.

Both TRACE and the "The Playground," like all other apps on the market, offer a journaling or reflective component where users can share their emotions, levels of dysphoria, and shifts in their gender expression at that given time.[61] Users of "The Playground" can record "daily mood and identity check-ins" through a sliding scale indicator to represent the user's quantity of joy, euphoria, and confidence felt when they log an entry.[62] On TRACE, the app's users, or "TRACERs," can share these updates with their "community" of "Allies," followers on the app, who engage with updates, milestones, and anniversaries.[63] Both TRACERs and members of

---

[60] Since this Note's initial writing, TRACE announced that it would shut down and no longer be available to users, as of October 30, 2024. thetrace.app (@thetrace.app), INSTAGRAM, (Sept. 29, 2024), https://www.instagram.com/thetrace.app/p/DAhXJs9P0l5 [https://perma.cc/9KPS-V7J8]. In making this decision, the app's leadership cited the need to "prioritize the well-being of our users" and assured users that they would delete all data associated with accounts within 30 days of the app's closure. Email from Aydian Dowling to TRACE Account Holders (Sep 29, 2024) (on file with publisher). It seems that concerns surrounding the app's collection of important, private information ultimately played a role in pressuring the company to close the app. TRACE stood out because it appeared the most publicly accessible and visible; one of its founders is a trans TikTok influencer and unlike other apps, it had a website to attract downloads and explain its mission. *Our Team*, TRACE, https://web.archive.org/web/20240726074744/https://www.thetrace.app/our-team. Now, it is possible that this publicity ultimately grabbed the attention of critics, who brought to their attention the possible vulnerabilities the app created for their trans users. While this application is no longer live and collecting information, we can still learn from it. The ways that TRACE collects trans users' information is not unique within the gender-tracking application market and can still serve as an example of how these apps operate.

[61] *See, e.g.*, Solace App, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.solace_10636&hl=en_US&pli=1 [https://perma.cc/9YEY-K7YE]; Trans Memo App, GOOGLEPLAY, https://play.google.com/store/apps/details?id=chrysalide.testomemo&hl=en_US [https://perma.cc/VHJ5-9FTZ]; TRANSTRACKS, https://transtracks.app [https://perma.cc/YD8N-ACNL].

[62] @mb, *supra* note 10.

[63] TRACE, https://web.archive.org/web/20240726075534/https://www.thetrace.app (July 26, 2024).

For Them's platform can chat with app users, upload photos, and save voice recordings.[64]

Limited research has been conducted on who uses gender-tracking apps. Per the apps' user agreements, these apps can be accessed by youth 13 years old or, in some cases, younger. For Them does not set an age minimum for its membership but does set restrictions for purchases.[65] TRACE limits use to those thirteen years or older.[66] The Google App Store reports tens of thousands of downloads of various gender-tracking apps,[67] but the age and demographics of these downloaders are unclear. For Them is members-only and requires a subscription for use.[68] Because many anti-trans bills are passed in certain states that target minors' access to care, a closer understanding of the percentage of users that are minors or the regions the users are based in would help identify the risks posed by gender-tracking apps to specific populations.

D. The Digital Surveillance Ecosystem

Gender-tracking apps are part of a larger data ecosystem, which allows law enforcement to interact with and access users' information. Data ecosystems are "complex networks of organizations and individuals that exchange and use data as [the] main resource" and create, manage, and sustain data sharing.[69] The exchange of this data has three different realms, Platform Economies, Sensing Nets, and Data Brokers—all of which implicate gender-tracking apps.

First, "Platform Economies" replicate markets, connect people in social and cultural spaces, and establish a "democratic public sphere."[70] Platform economies include large companies that facilitate the exchange of commodities and information on their platforms like Amazon, Google, or Facebook.[71] Gender-tracking apps also fall within this category. They can serve as social and personal media sites where users compile

---

[64] *Features*, TRACE, https://web.archive.org/web/20220901002634/https://www.thetrace.app/features-1 (Sept. 1, 2022); @mb, *supra* note 10.

[65] *See Terms of Use*, TRACE, https://web.archive.org/web/20240726075534/https://www.thetrace.app/terms-of-use (July 26, 2024)("By agreeing to these Terms of Service . . . you are at least the age of majority in your state or province of residence, or that you are the age of majority . . . residence and you have given us your consent to allow any of your minor dependents to use this site.").

[66] *Id.*

[67] *See supra* note 61.

[68] FORTHEM, https://www.forthem.com/membership [https://perma.cc/2GSU-US77].

[69] Marcelo Iury S. Oliveira et al., *Towards a Meta-Model for Data Ecosystems*, PROCEEDINGS OF THE 19TH ANN. INT'L CONF. ON DIGIT. GOV'T RSCH.: GOVERNANCE IN THE DATA AGE 1 (2018).

[70] Aziz Z. Huq, *The Public Trust in Data*, 110 GEO. L.J. 333, 344 (2021).

[71] *Id.* at 344–45.

information that is sometimes shared with others. Platforms like For Them also connect users to online markets for purchases.

Second, there are "Sensing Nets," physical personal devices such as iPhones or Fitbits that collect, classify, and apply digital traces.[72] Platform economies, including gender-tracking apps, are directly tied to sensing devices like physical smartphones that track location information and connect users to the online community.[73]

Third, "data brokers" buy and repackage consumer data across various markets.[74] "If social media and search engines are the storefront of the personal data economy, data brokers are its back office," managing the flow and transactions of information between parties.[75] Data brokers are private, mostly unregulated companies that collect and synthesize large batches of personal data to sell to third parties.[76] This can include many forms of sensitive data, including a user's location, messages, and biometric data.[77] Such data is of high commercial value to advertisers and retailers and provides unparalleled information to buyers, including law enforcement.[78] Law enforcement agencies across the country are major consumers in this sphere of the data economy and have multi-million dollar, multi-year contracts with brokerage companies to directly purchase data packages.[79]

Data brokerage of personal information by law enforcement agencies has serious implications on legal proceedings, worsened by the fact that agencies do not need warrants to make these purchases.[80] Whereas other personal information to which there is a reasonable expectation of privacy typically requires a warrant, law enforcement agencies are legally allowed to buy data packages in large quantities because it is a commodity accessed by a third party.[81] In fact, *anyone* can purchase data from these companies, including "vigilantes."[82] In *U.S. v. Carpenter*, the Supreme Court held that the Fourth Amendment requires law enforcement to have

---

[72] *Id.* at 348.

[73] *Id.*

[74] *Id.* at 346.

[75] *Id.*

[76] *See* FRANKLIN C. SHENKMAN ET AL., LEGAL LOOPHOLES AND DATA FOR DOLLARS: HOW LAW ENFORCEMENT AND INTELLIGENCE AGENCIES ARE BUYING YOUR DATA FROM BROKERS 9 (2021).

[77] *Id.* at 7.

[78] *Id.* at 5.

[79] *Id.* at 7.

[80] *Id.* at 5–6.

[81] *Id.*; Aziz Z Huq & Rebecca Wexler, *Digital Privacy For Reproductive Choice In The Post-Roe Era*, 98 NYU L.R. 555, 582–83 (2023).

[82] Huq & Wexler, *supra* note 81, at 581–82.

a warrant to access historical cell site location information.[83] There is no such requirement for purchasing packages available on the data market. The Electronic Communications Privacy Act of 1986 (ECPA) and the law restricting government access to the public's digital communications, "effectively contains a gap allowing law enforcement to acquire communications data commercially from data brokers . . . ."[84] Because data brokers did not exist in the 1980s when the law was written, the ECPA does not cover them.[85] The law has not been updated since its passage to plug this regulatory loophole, allowing law enforcement to purchase packages from data brokers for unregulated evidence gathering.

Another legal implication of data brokerages is that purchased anonymous data can be de-anonymized by law enforcement.[86] Specifically, law enforcement can combine multiple sources of purchased information to identify the individuals from whom the data came.[87] Law enforcement can triangulate information, using, for example, the help of GPS location data to infer an individual's personal information,[88] or, as this Note later discusses, whether one has or is currently receiving transgender health care.

De-anonymized data can be then used as a starting point for law enforcement to pursue legal charges, including for criminalized trans healthcare. This data could lead law enforcement agencies to seek additional information about a specific person or geographical area. They can do so by obtaining a warrant through a judge, granting access to information stored on applications that the companies would otherwise choose not to share. For example, while TRACE's privacy policy specifically states that it does not sell users' information to others, such as brokers, there is an exception for law enforcement with a warrant.[89] In such a case, TRACE is required to provide information within the scope of the warrant or subpoena.

Specific tools in the digital privacy realm employed by law enforcement to identify potential criminal activity are Geofence and keyword search warrants, which can lead to sharing specific identities of app users.[90] Geofence warrants allow law enforcement to request a given

---

[83] *See* United States v. Carpenter, 585 U.S. 296, 317 (2018).

[84] *See* SHENKMAN ET AL., *supra* note 76, at 7.

[85] *Id.* at 15.

[86] *See id*. at 11–12.

[87] Anya Prince, *Reproductive Health Surveillance*, 64 B.C. L. REV. 1077, 1128-29 (2023).

[88] *Id.* at 1081.

[89] Privacy Policy, TRACE, https://web.archive.org/web/20220702044807/thetrace.app/privacypolicy (July 2, 2022).

[90] *See, e.g.*, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2512, 2529 (2021) ("From January to June 2020, for example, Google received—from domestic

platform like Google to identify all devices or accounts found within specific geographical coordinates during a specific time period.[91] Upon receiving the warrant's output, police can request additional location points from devices associated with the identified coordinates, "to eliminate false positives or otherwise determine whether that device is actually relevant to the investigation."[92] The platform then provides account-identifying information to law enforcement, including the names and the email addresses of its users.[93]

Keyword search warrants operate similarly. Through this process, "police compel the [search engine] to hand over the identities of anyone who may have searched for a specific term, such as a victim's name or a particular address where a crime has occurred."[94] While the Supreme Court has not fully answered whether these kinds of warrants are considered protected searches under the Fourth Amendment, they are broadly considered to be.

There are broad applications of keyword search and geofence warrants, which have been legally used to identify suspects in home arson[95] and murder cases,[96] for example. As such, law enforcement is already deeply embedded in the digital ecosystem, accessing individuals' data in various investigations through specialized warrants. There is no existing documentation of how law enforcement has used these warrants for gender-tracking apps. Nevertheless, given the political context of anti-trans healthcare bills, it is arguably only a matter of time before these tools are employed in the criminalization of trans healthcare.

---

law enforcement alone—15,588 preservation requests, 19,783 search warrants, and 15,537 subpoenas, eighty-three percent of which resulted in disclosure of user information.").

[91] *See* Matthew Guariglia, *Geofence Warrants and Reverse Keyword Warrants Are So Invasive, Even Big Tech Wants to Ban Them*, ELEC. FRONTIER FOUND. (2022), https://www.eff.org/deeplinks/2022/05/geofence-warrants-and-reverse-keyword-warrants-are-so-invasive-even-big-tech-wants [https://perma.cc/7JHG-J3U9].

[92] *See* Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from a "Geofence" General Warrant at 13, United States v. Chatrie, No. 19-cr-00130 (E.D. Va. Dec. 23, 2019).

[93] *Id.* at 14.

[94] *See* Guariglia, *supra* note 91.

[95] *See* Jennifer Lynch & Andrew Crocker, *Colorado Supreme Court Upholds Keyword Search Warrant*, ELEC. FRONTIER FOUND. (2023), https://www.eff.org/deeplinks/2023/10/colorado-supreme-court-upholds-keyword-search-warrant [https://perma.cc/6S58-6UVY].

[96] People v. Meza, 90 Cal. App. 5th 520, 527 (2023) (upholding an overbroad warrant because officers reasonably relied on it and noting "cases that have considered the validity of geofence warrants have also, almost uniformly, determined that such warrants are valid only if they are narrowly tailored to avoid unnecessary infringement on the privacy of uninvolved third parties.").

II. RISKS OF THE DATA SURVEILLANCE ECOSYSTEM TO TRANS PEOPLE

This Part outlines some ways law enforcement may be able to obtain trans individuals' private information. Further, it demonstrates how warrants, including geofence and keyword search warrants, and data broker transactions may be specifically weaponized against gender-tracking app users in this landscape of healthcare criminalization. The three major categories of information accessed by police as a result of these apps are: (1) private personal information, narratives, and communications; (2) location information; and (3) de-anonymized information. This Part will ultimately demonstrate that these apps compile information that may become incriminating and is relatively accessible to police by already prevalent surveillance techniques.

A. Private Personal Narrative Information and Communications

Gender-tracking apps hold large quantities of personal information in each of its features and available platforms. App users are asked for biographical and demographic information such as their name, birthdate, and location to make an account. Subsequently, the apps prompt users to share substantial information in order to personally monitor one's transition, such as photos, inner thoughts, and medical test results. Also, For Them and TRACE offer the ability for users to share some information to other users on the platform as a social media-style post.[97]

If accessed via data brokerage or warrant, law enforcement could gather trans users' plans for medical transition, current treatment results such as blood tests, or photo evidence of a surgery, that could be used in a criminal investigation against them, their family, or medical provider.[98] For example, users receiving gender-affirming healthcare can reveal any amount of potentially incriminating information in a journal entry stored on a gender-tracking app, including the name of a provider.[99] Pictures of shots, pill calendars, or prescription bottles, all commonly shared on the apps, could corroborate whether one is undergoing HRT. A prosecutor

---

[97] *See supra* Subpart I(C).

[98] *See generally* Evans, *supra* note 3 (describing how trans youth and their parents seek information).

[99] In trans internet spaces, it is common for users to share information about their providers, including surgeons. On popular sites, including Transbucket.com, users share pictures of their gender-affirming surgery results from specific surgeons so as to help others make decisions about which surgeon to go to. *See* TRANSBUCKET, Transbucket.com/about [https://perma.cc/M2DC-8ZLD]. This is one way that the trans community leverages the internet to share best care practices. *See also* Harner, *supra* note 36.

could use all of these facts to demonstrate a person is receiving gender-affirming care and identify the prescribing care provider.

Moreover, with a warrant police can access a significant amount of incriminating evidence of an individual's transition through gender-tracking apps that could result in the prosecution of doctors providing trans healthcare. Gender-tracking app users could lead law enforcement to these providers by naming them in their posts, or this data could be used to corroborate other incriminating pieces of information, such as a visit to a gender-affirming care provider. Additionally, social media-style posts that users choose to share with others, like any other form of social media posting on platforms like Facebook or Instagram, do not require a warrant under standard third-party exceptions to the warrant requirement.[100]

Questions raised about how information mining of gender-tracking apps can be used against trans people and their medical providers is similar to concerns that have arisen around period-tracking applications in the wake of the *Dobbs v. Jackson Women's Health Organization* decision, which eliminated constitutional protections for abortions.[101] Approximately one-third of women in the United States currently use or at one point used a period tracking app to record their cycle, including dates, flow levels, and mental and physical symptoms.[102] However, some users have expressed fears about how these apps can create a digital footprint of an illegal abortion, which could jeopardize them and their medical provider.[103] Particularly, Fourth Amendment experts and the wider public have expressed concern that information about ones' period—or lack thereof—could get into the hands of law enforcement and provide evidence for the prosecution of an illegal abortion.[104]

Similar to the gender tracking context, cases have not yet surfaced of law enforcement leveraging period-tracking apps in the prosecution of

---

[100] Brian Mund, *Social Media Searches and the Reasonable Expectation of Privacy*, 19 YALE J. L. & TECH. 238, 244 (2017); United States v. Miller, 425 U.S. 435, 443 ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities").

[101] *See* Dobbs v. Jackson Women's Health Org., 597 U.S. 215 (2022).

[102] Huq & Wexler, *supra* note 81 at 573. Note that "women" is the language used by the author.

[103] Maggie Delano, *Okay, Fine, Let's Talk About Period Tracking: The Detailed Explainer*, MEDIUM (Jun. 28, 2022), https://medium.com/@maggied/okay-fine-lets-talk-about-period-tracking-the-detailed-explainer-2f45112eebb4 [https://perma.cc/6A9T-59TT].

[104] *See* Elizabeth E. Joh, Dobbs *Online: Digital Rights as Abortion Rights*, FEMINIST CYBERLAW 129, 131–33 ("Period tracking apps, which can document a sudden change in your menstrual cycle, are readymade sources of potentially incriminating information.") (citing Hannah Norman & Victoria Knight, *Should You Worry About Data From Your Period-Tracking App Being Used Against You?*, KASIER HEALTH NEWS (May 13, 2022), https://khn.org/news/article/period-tracking-apps-data-privacy [https://perma.cc/2CYC-Z3UF]).

abortion, but law experts have warned that this is impending.[105] Some states' laws are not yet in effect or have been enjoined, and law enforcement is still mobilizing to react.[106] Law enforcement is still learning how to leverage these technologies. Furthermore, there are example cases in which other kinds of digital technology are already being used in the prosecution of abortions, particularly when individuals seeking abortions rely on telehealth or internet services to receive prescriptions for self-medicated abortions both in-state and across state lines, a trend the *Dobbs* decision has accelerated.[107]

For example, consider Celeste, a Nebraska teenager who sought an abortion with the help of her mother.[108] Celeste's abortion was illegal under Nebraska law.[109] Only a couple months prior to the *Dobbs* decision, Celeste and her mother Jessica were charged for using abortion pills to terminate a pregnancy.[110] Law enforcement accessed the girl's Facebook messages to her mother, which revealed her planned purchase and administration of the pills.[111] Detectives had originally subpoenaed Celeste's medical records, which showed she was pregnant.[112] The detectives received a subsequent warrant for her Facebook messages, which included the date and details of the medically induced abortion.[113] Law enforcement charged Jessica, but not Celeste, under the state's anti-abortion law. Jessica was charged with removing and concealing human skeletal remains.[114] This case illustrates the harmful usefulness of digital evidence, legally obtained by warrant, to the prosecution of health crimes such as seeking an abortion.

Gender-affirming apps like TRACE and "The Playground" are ripe for gathering similar kinds of information that could be used against users, families, and medical providers as digital evidence. Imagine Chase, a trans man living in Florida who has been using TRACE since he was three

---

[105] *See, e.g.*, *id.*; Delano, *supra* note 103; Huq & Wexler, supra note 81.

[106] HRC Foundation, *Map: Attacks on Gender Affirming Care by State*, HUM. RTS. CAMPAIGN, https://www.hrc.org/resources/attacks-on-gender-affirming-care-by-state-map [https://perma.cc/8HEC-6TS7].

[107] *E.g.*, Rachel Jones & Amy Friedrich-Karnik, *Medication Abortion Accounted for 63% of All US Abortions in 2023-An Increase from 53% in 2020*, GUTTMACHER (Mar. 19, 2024), https://www.guttmacher.org/2024/03/medication-abortion-accounted-63-all-us-abortions-2023-increase-53-2020 [https://perma.cc/FXC3-9DXJ].

[108] Michael Levenson, *Nebraska Teen Who Used Pills to End Pregnancy Gets 90 Days in Jail*, N.Y. TIMES (July 20, 2023), https://www.nytimes.com/2023/07/20/us/celeste-burgess-abortion-pill-nebraska.html [https://perma.cc/MZV2-S4EQ].

[109] *Id.*

[110] *Id.*

[111] *Id.*

[112] *Id.*

[113] *Id.*

[114] *Id.*

weeks on testosterone. He uploads weekly shirtless pictures into a private photo folder and chats with a friend Elliot, who he met on the app and happens to live ten miles away. They talk about once a week about new developments on testosterone and Chase lets Elliot know that he's looking for a new doctor because his primary care practitioner still deadnames him. Elliot tells Chase over chat that he loves his doctor and can also refer him to a consultation with a local surgeon for top surgery.

Similar to Celeste, police could obtain a warrant for Chase and Elliot's messages on TRACE, using their discussions to identify local providers who are assisting trans patients with gender-affirming care. This, and other information, such as Chase's pictures, intended exclusively for personal use on gender-tracking apps, could be weaponized for prosecution of a local doctor. This hypothetical demonstrates how the sizable amount of information held on gender-tracking apps and the tools already at law enforcement's disposal can be used in tandem for health-based prosecutions.

B. Location Information

Gender-tracking apps collect a large body of location data that could be gathered by law enforcement. For example, gender-affirming apps collect location metadata attached to uploaded photos as a condition for signing up for an account.[115] Location data may also be collected through the services on one's mobile device. Mobile devices located on a network, including computers, phones, and other web-connected devices, compile location information across devices that can be collected by applications.[116]

This location data could be gathered by law enforcement through geofence and keyword-search warrants and be used to identify individuals who have been in the geographical radius of a gender-affirming healthcare provider.[117] For instance, a warrant may ask for device information for all users present within a specified radius of the coordinates of an LGBTQ+ gender clinic during its regular business times. Police would only be able to get such a warrant with probable cause, but should they receive credible information the clinic is providing gender-affirming care, a warrant could

---

[115] *See* Privacy Policy, TRACE, https://web.archive.org/web/20220702044807/thetrace.app/privacypolicy (July 2, 2022).

[116] *See, e.g.*, CTR. FOR DEMOCRACY & TECH, *Re: Comments for November 2015 Workshop on Cross-Device Tracking* (Oct. 16, 2015), https://cdt.org/wp-content/uploads/2015/11/10.16.15-CDT-Cross-Device-Comments.pdf [https://perma.cc/A3YE-CWKU] (describing early forms of cross-device tracking).

[117] *See supra* notes 90–94 and accompanying text.

be issued that uncovers the devices and identities of many of their patients.[118]

Under current laws, criminal charges could not be brought against a patient for receiving healthcare.[119] Nevertheless, this location data could also be gathered with these mechanisms to prosecute gender-affirming healthcare providers and even shut down their gender-care services as a whole. These pressures are already very much present. Missouri passed S.B. 49 in August 2023, which bans the knowing prescription of "cross-sex hormones or puberty-blocking drugs for the purpose of a gender transition for any individual under eighteen years of age."[120] In September 2023, Washington University limited the services of its Transgender Center at St. Louis Children's Hospital in response to the law.[121] Subsequently, the center stated it would cease administering the prescription of these medications, as the new "legal claim [against patients receiving gender-affirming care] creates unsustainable liability for health-care professionals and makes it untenable for us to continue to provide comprehensive transgender care for minor patients without subjecting the university and our providers to an unacceptable level of liability."[122] If hospitals or clinics fear they could be targeted by geofence warrants and anticipate legal charges for each individual who enters their building, they could stop providing care altogether.

C. De-Anonymized Information

Data brokers are particularly dangerous in the gender-tracking app context because of the *massive* amounts and kinds of data they can retrieve, synthesize, and sell for the right price.[123] In purchasing personal information from apps like For Them and TRACE, brokers can catalog a sizable amount of demographic and location information on the thousands of trans users in the form of anonymized data packages.[124] Because For Them's platform is tied into its online binder store and integrated with Webflow and Google Analytics, the app collects information on what trans

---

[118] *See supra* note 90 and accompanying text.

[119] Choi & Mullery, *supra* note 58.

[120] S.B. 49, 102nd Gen. Assemb., Reg. Sess. (Mo. 2023).

[121] Julie Hail Flory, *Statement on Washington University Transgender*, SOURCE (Sept. 11, 2023), https://source.wustl.edu/2023/09/statement-on-washington-university-transgender-center [https://perma.cc/QT7Y-NG4Y].

[122] *Id.*

[123] *See* JUSTIN SHERMAN, DATA BROKERS AND SENSITIVE DATA ON U.S. INDIVIDUALS 9 (Duke University Cyber Policy Program 2021).

[124] *See id*. at 2–6 (describing how various data brokers package and sell information).

people are buying on their site and others.[125] Gender-tracking apps can also access a user's location and know who they are talking to. For Them's chat function, for example, could reveal a network of communications between users and map a national trans community. Each of these interactions and exchanges are purchased as anonymized data points that purchasers, like law enforcement, can later de-anonymize with location and device data to generate catalogs of trans individuals with their exact names and locations. One study found datasets made available by brokers could be de-anonymized and re-identify individuals with 99.98% certainty, given 15 demographic data points.[126]

Concerns of cataloging trans people or creating a trans "registry" have begun to have legal implications. In 2022, the Texas Attorney General's office instructed employees of the state's Department of Public Safety to compile a list of individuals who had changed their gender on their Texas identification documents, including driver licenses.[127] This request came after Texas's ban on trans girls' participation in school athletics and the state's preliminary efforts to remove trans children from their families by claiming gender-affirming care is "child abuse."[128]

In addition to how law enforcement can utilize data brokerage to criminalize doctors and trans people, everyday people who discriminate against trans individuals can also manipulate the data economy. Such actors include "vigilantes" who report doctors to local licensing boards or report parents to child welfare agencies.[129] Coordinated online harassment by individual internet users is a real and present threat to the trans

---

[125] *Privacy Policy*, FOR THEM, https://www.forthem.com/en-CA/pages/privacy-policy [https://perma.cc/RLH9-BZQQ].

[126] Luc Rocher et al., *Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models*, 10 NATURE COMMC'NS 3069, 3073–74 (2019).

[127] Molly Hennessy-Fiske, *Texas Attorney General's Office Sought State Data on Transgender Texans*, TEX. TRIB. (Dec. 14, 2022), https://www.texastribune.org/2022/12/14/ken-paxton-transgender-texas-data [https://perma.cc/VQQ6-LMQP].

[128] *See New Texas Law Bans Transgender Girls From Girl Sports*, WASH. POST (Oct. 26, 2021), https://www.washingtonpost.com/national/new-texas-law-bans-transgender-girls-from-girl-sports/2021/10/26/b972b7e2-33a9-11ec-a1e5-07223c50280a_story.html [https://perma.cc/6VW6-VQGP]; Rina Torchinsky, *In Texas, an Unrelenting Assault on Trans Rights Is Taking a Mental Toll*, NPR (Feb. 25, 2022), https://www.npr.org/2022/02/25/1082975946/anti-trans-bills-texas [https://perma.cc/R6SA-FSFD]; *see also* Letter From Greg Abbott, Governor of Tex., to Jaime Masters, Comm'r, Tex. Dep't of Fam. & Protective Servs. (Feb. 22, 2022), https://gov.texas.gov/uploads/files/press/O-MastersJaime202202221358.pdf [https://perma.cc/EU7X-268L] [hereinafter "Letter From Greg Abbott"].

[129] Letter From Greg Abbott, *supra* note 128; *see also* Mark Joseph Stern, *Texas' Trans Kids Are Targets in a Brutal GOP Culture War*, SLATE (Feb. 23, 2022), https://slate.com/news-and-politics/2022/02/greg-abbott-transgender-children-health-care-ban.html [https://perma.cc/KM6B-5EH7] ("Teachers, nurses, doctors, day care employees, and health care professionals must now inform the state if they believe a child is receiving [gender-affirming] treatment.").

community, including children.[130] Their online hate speech and harassment targets trans individuals, leading to real life consequences, including "bomb threats, death threats, vandalism, Pride flag-burnings, hate crime assaults, [and] hate crime murders."[131] Politicians and far-right media figures have also amplified these doxxing efforts.[132] Therefore, the danger is not only that law enforcement can use this information to directly prosecute physicians, but it also stokes fear amongst the general public that neighbors are turning on neighbors. For example, Arkansas created an enhanced civil liability structure for doctors providing gender-related care.[133] Anyone "acting on behalf of the minor" who has received gender-affirming care may bring a civil action against the healthcare professional who provided the care.[134] As such, private parties who have gathered information on trans healthcare recipients could bring claims against doctors.[135]

Target is a private entity that has been purchasing data broker data for over a decade to advertise to particular consumers who interact with their platforms.[136] In the 2010s, Target developed a new model that applied

---

[130] *See* GLAAD, SOC. MEDIA SAFETY INDEX 2024 4 (2024), https://assets.glaad.org/m/4a1d7323a720f2b9/original/2024-Social-Media-Safety-Index.pdf [https://perma.cc/JY23-RXH2] ("Targeting historically marginalized groups, including LGBTQ people, with fear-mongering, lies, and bigotry is both an intentional strategy of bad actors for attempting to consolidate political power, as well as being a lucrative enterprise (for [] right-wing figures and groups)"); CTR. FOR COUNTERING DIGIT. HATE & HUM. RTS. CAMPAIGN, DIGITAL HATE; SOCIAL MEDIA'S ROLE IN AMPLIFYING DANGEROUS LIES ABOUT LGBTQ+ PEOPLE 6 (2022), https://counterhate.com/wp-content/uploads/2022/08/CCDH-HRC-Digital-Hate-Report-2022-single-pages.pdf [https://perma.cc/35TE-HYKJ] ("dangerous rhetoric is being pushed by a small, extremist group of politicians and their allies who, together, are driving a coordinated and concerted campaign to attack LGBTQ+ kids").

[131] Alejandra Caraballo, *Policies vs. Enforcement: What's Up with Meta's Platforming of Violent Extremist Hate Account "Libs of TikTok"?*, TECH POLICY PRESS (Mar 21, 2024), https://techpolicy.press/policies-vs-enforcement-whats-up-with-metas-platforming-of-violent-extremist-hate-account-libs-of-tiktok [https://perma.cc/F3FP-5LQ6].

[132] Taylor Lorenz, *Meet the Woman Behind Libs of TikTok, Secretly Fueling the Right's Outrage Machine*, Washington Post, (Apr. 12, 2022), https://www.washingtonpost.com/technology/2022/04/19/libs-of-tiktok-right-wing-media [https://perma.cc/BDG2-JD6Z].

[133] S.B. 199, 94th Gen. Assemb., Reg. Sess. (Ark. 2023).

[134] *Id.*

[135] *Id.* ("a representative of a minor injured . . . including *without limitation* a parent or legal guardian . . .) (emphasis added). This structure evokes the infamous Texas "bounty law", which authorized private individuals to sue providers of abortion care. *See* Emma Bowman, *As States Ban Abortion, the Texas Bounty Law Offers a Way to Survive Legal Challenges*, NPR (July 11, 2022), https://www.npr.org/2022/07/11/1107741175/texas-abortion-bounty-law [https://perma.cc/HNJ9-UV7W]; TEX. HEALTH & SAFETY CODE § 171.208. While third parties acting on behalf of minors is an as-yet-untested theory of standing, the threat of such an argument looms.

[136] *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp [https://perma.cc/X46A-N9WU].

data analytics to generate a "pregnancy prediction score" for individual shoppers.[137] The purpose of the score was to send ads and coupons specifically for prenatal vitamins, maternity clothing, and other necessities for expectant parents. The ads were pushed to women in their second trimester, the time when, calculated from mountains of purchasing data, expectant parents most likely purchase items for their new baby.[138] This program gained media attention when the New York Times reported a father found out his teenage daughter was pregnant from a coupon for baby clothes and cribs she received in the mail.[139] Perhaps a private party or law enforcement could similarly use anonymized data sourced from gender-tracking apps, subsequently purchased and resold by data brokers, to create predictive models to identify trans people. Data analytics could account for purchase records for binders, surgery-recovery supplies, and gaffs, or look at search histories for "voice feminization training," "testosterone and acne," and so forth, to create predictive models that find individuals in the process of medical transition.

Gender-tracking apps compile information exclusively on trans people, meaning the data they collect specifically identifies trans individuals and consumers. Most, if not every user on these apps, signed up for the express purpose of tracking their transition. The ability of law enforcement to purchase and de-anonymize gender-tracking app data can therefore help identify individuals breaking states' anti-trans laws that establish penalties for abetting gender-affirming care. While these tactics have not yet been publicly used to de-anonymize and locate trans individuals in this context, it is clear that this technology is readily available in the commercial context and could easily be adopted by law enforcement.

By collecting personal medical and narrative information, location data, and identifiable anonymous information, gender-tracking apps are uniquely susceptible to law enforcement investigations. In these kinds of data, much of the risks are embedded in the regular use of digital platforms and "sensing nets." Gender-tracking apps, like any other app, collect anonymized metadata and location information. The methods of extracting this information are also not unique to this context; technology-driven warrants and data purchasing exist and are used by law enforcement. However, what sets this context apart is the quantity and deeply personal nature of the information shared on the app. Together with the violent political climate in which prosecutions are taking place, transgender people's data is put at serious risk of abuse by these apps. Such great risk

[137] *Id.*
[138] *Id.*
[139] *Id.*

demands action, including maintaining privacy regulations, to protect trans people.

III. EFFORTS TO ADDRESS TRANS DATA PRIVACY

The United States government has left the private personal information of its citizens vulnerable in many ways.[140] Without effective policy in place, some advocate for the public to make smart decisions about how they interact with the digital world. This Part first discusses the limitations of the "digital self-defense" framework and the ways it is not the most effective method to protect trans individuals, particularly trans people of color. Second, this Part analyzes legislation that could put effective security measures in place to protect sensitive health data stored on digital platforms. These policies are both general in their approach to regulating the data economy and specific to providing protections to transgender individuals' health and transition-related information. Lastly, the Part identifies recommendations for future legislation. These recommendations take inspiration from current efforts but tailor general principles to the specific needs of trans users in the digital ecosystem and gender-tracking apps. The issues related to data practices associated with gender-tracking apps illustrate a much wider problem in how American regulators approach individuals' data privacy. As such, the solutions proposed here could be tailored to protect a wide array of populations vulnerable to criminalization and over-policing by the state.

A. Digital Self Defense and Its Limitations

Digital self-defense is a framework used to assess ways that individuals may take steps in their own approach to the internet and digital devices to protect against privacy intrusions.[141]

Some strategies recommended to individuals include deleting apps, erasing browsing and location history, deleting files "properly," and using encrypted channels for communication.[142] Some privacy advocates also recommend using a "'burner' phone (one not connected to an ordinary cell phone account)" or Virtual Private Network (commonly known as a VPN) when accessing the internet.[143] These anti-surveillance strategies theoretically limit the archived information of one's activities.[144]

---

[140] *See generally* Huq, *supra* note 70 (proposing regulatory solutions to data privacy concerns).

[141] *See* JOH, *supra* note 104, at 132.

[142] *Id.*

[143] *Id.*

[144] *Id.*

While taking these steps would generally increase the safety of one's private information on the internet, they are not necessarily accessible in practice, particularly to communities already vulnerable to state violence.[145] Historically, lower-income individuals have "had far less control over the privacy of their homes, bodies, and decisions than their affluent counterparts."[146] For example, receiving public benefits depends on the state's close monitoring of one's family, spending habits, and personal health.[147] These surveillance patterns continue into the digital information age, meaning low-income communities face disproportionate dangers from big data. As a result, "[b]eing poor often means buying a (cheaper) phone with less privacy protective features, having less 'digital literacy' to identify and take appropriate privacy protective steps, and lacking the means to pay for apps or other services that might afford greater privacy."[148]

Consequently, digital self-defense tactics are not realistic for those most deeply impacted by state police violence and the criminalization of reproductive and gender-affirming healthcare. As scholars and advocates have noted, Black and Brown people bear, and will likely more acutely suffer, the brunt of anti-abortion bills.[149] People of color are significantly more likely to receive an abortion and bear the financial burden of traveling far distances for the procedure.[150] Trans women of color experience significant discrimination, physical violence, and over-policing.[151] Therefore, self-defense tactics might be insufficient to address the risks the trans community faces.

---

[145] *Id.*

[146] *See* Mary Madden et al., *Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 WASH. U. L. REV. 53, 58 (2017) (describing the history of poor houses and the development of the modern welfare state as instruments of the surveillance state).

[147] *Id.* at 59.

[148] JOH, *supra* note 104, at 133.

[149] *See, e.g.*, Khiara M. Bridges, *Race in the Roberts Court*, 136 HARV. L. REV. 23 (2022).

[150] *See* Makiya Turntine, *Dobbs v. Jackson Women's Health Organization Will Likely Have a Negative, Disproportionate Impact on Women of Color and Reassert Inferiority Comment*, 46 U. ARK. LITTLE ROCK L. REV. 237, 239 (2023); *see also* Kira Eidson, *Addressing the Black Mortality Crisis in the Wake of Dobbs: A Reproductive Justice Policy Framework Symposium Issue of Gender and the Law One Year Later: The Changed Landscape of Reproductive Rights on the Anniversary of Dobbs: Note*, 24 GEO. J. GENDER & L. 929, 938 (2022) (Arguing the *Dobbs* decision will likely increase the rates of mortality amongst Black mothers).

[151] *See, e.g.*, Janice Joseph, *Multiple Invisibility of Black Victims of Transfemicide: An Intersectional Approach*, 34 PEACE REV. 501, 513 (2022) (demonstrating trans Black women are more likely to be murdered than any other LGBTQ+ subgroup and "face several barriers and persistent discrimination that dehumanize and endanger their lives."); Kris Rosentel et al., *Black Transgender Women and the School-to-Prison Pipeline: Exploring the Relationship Between Anti-Trans Experiences in School and Adverse Criminal-Legal System Outcomes*, 18 SEX RES. SOC. POL'Y 481, 486 (2021) ("Anti-trans school climate and institutional discrimination warrant

B. Ongoing Legislation Efforts

The following Subpart discusses how legislators are attempting to address the privacy risks to the trans community posed by the criminalization of trans identity and the digital surveillance ecosystem. It first analyzes general privacy policies states have implemented or are considering to regulate access to personal information and the data broker industry. In particular, these pieces of legislation aim to regulate police participation in the digital surveillance economy. Next, the Subpart discusses shield-type legislation that protects against law enforcement exceptions to privacy policies. This portion will engage with the *Dobbs* decision particularly and how state legislatures have attempted to respond to protect abortion-seekers from such privacy invasions. Furthermore, this Subpart aims to reflect on the best practices of technology and legislative spaces approaching the issue of sensitive health data in a simultaneously digitizing world and politically reactionary America.

1. General Privacy Legislation

The data broker industry remains very opaque in its operations and nearly untouched by regulation; no federal legislation has addressed the immense power and financial capital these operations hold in our digital ecosystem. Only a few states have attempted to curb data brokers' influence and have only been able to enforce some transparency requirements rather than regulate how transactions take place.

Vermont addressed the issue first when it passed H.764 in 2018.[152] The law "adopt[ed] consumer protection provisions relating to data brokers, including creating a new set of definitions, requiring annual registration, [and] requiring a data security program."[153] The annual registration program requires any entity collecting third-party data for commercial purposes to register with the state.

When the law took effect, regulators saw just how expansive the broker industry really is. The 120-plus companies that registered in 2018 included "long-established credit reporting agencies such as Experian and Acxion to novel online search engines such as Spokeo, and smaller niche actors catering to landlords and insurance companies."[154] The Vermont field alone is massive and includes multi-national credit reporting

consideration as factors that may contribute to the [School to Prison Pipeline] for Black/African American transgender women").

[152] *See* H. 764, 2018 Gen. Assemb. Reg. Sess. (Vt. 2018).

[153] STATE OF VT., SUMMARY OF THE ACTS OF THE 2018 VERMONT GENERAL ASSEMBLY, at 47 (2018), https://legislature.vermont.gov/assets/Legislative-Reports/2018-Act-Summaries-Book.pdf [https://perma.cc/7XY8-9KSA].

[154] Huq, *supra* note 70, at 347.

companies, as well as smaller businesses targeting local housing markets. However, the Vermont law did not require the registry of companies such as Google or Facebook, who collect and store their data.[155] As such, their registry has major holes, thereby limiting the efficacy of the policy's transparency goals.

California followed up with a similar law, the California Delete Act (S.B. 362), approved in October 2023 and enacted in January 2024.[156] The bill not only requires data brokers to register with the California Privacy Protection Agency, but also creates a single "delete mechanism" accessible with the California Privacy Protection Agency website to delete all personal data from a list of registered data brokers.[157] Establishing the "delete mechanism" means that individuals can remove their data currently owned by companies registered with the state and can no longer be sold to other parties, including law enforcement.[158] This is a positive step towards affording individual users and consumers agency over their data.

While these two laws may shed light onto a notoriously non-transparent industry, the problem of commercializing personal data, particularly for law enforcement consumption, remains. Even with greater transparency, police can still freely purchase individuals' data.[159] Federal lawmakers introduced H.R. 4639, the Fourth Amendment Is Not For Sale Act, to specifically prohibit law enforcement from participating in the third-party data economy.[160] If implemented, H.R. 4639 would "amend section 2702 of title 18, United States Code, to prevent law enforcement and intelligence agencies from obtaining subscriber or customer records in exchange for anything of value, to address communications and records in the possession of intermediary internet service providers, and for other purposes."[161] In short, this law would prevent all intelligence agencies and law enforcement from purchasing data without a warrant.

Thus far, H.R. 4639 has wide support from bipartisan representatives in Congress and fifty influential civil liberties organizations across the country.[162] This law would close a concerning gap in the Fourth

---

[155] *Id.*

[156] California Delete Act, S.B. 362, 2023-2024 Leg., Reg. Sess. (Cal. 2023).

[157] *Id.*

[158] *See id.*

[159] *See supra* Subpart I(D).

[160] H.R. 4639, 118th Cong. (2023).

[161] *Id.*

[162] *Coalition Letter Calls for Congressional Hearings on Fourth Amendment Is Not For Sale Act*, BRENNAN CTR. FOR JUST. (Jan. 26, 2022), https://www.brennancenter.org/our-work/research-reports/coalition-letter-calls-congressional-hearings-fourth-amendment-not-sale [https://perma.cc/B75Q-2FBT].

Amendment that law enforcement has leveraged for prosecution. Removing law enforcement as purchasers in the data economy means they could no longer circumvent constitutional protections to receive incriminating or corroborating evidence. Instead, they would need a warrant to access this information, which highlights the importance of imposing stronger restrictions on the police warrant exception.

2. Shield-Type Legislations

While some privacy laws and corporate policies attempt to protect users' data, there are still exceptions that authorize disclosure to and usage by law enforcement.[163] For example, under the Health Information Portability and Accountability Act Privacy Rule, covered providers are prohibited from disclosing protected health information absent a court order, subpoena, or warrant.[164] On the other hand, law enforcement can access this information without Fourth Amendment procedures in some circumstances, including "for purposes of identifying or locating a suspect, fugitive, material witness or missing person," although "the information must be limited to basic demographic and health information about the person," or in the case of child abuse or neglect.[165] This would be particularly dangerous in Texas, where legislators introduced a bill to classify gender-affirming care provided to a minor as child abuse.[166] In such a case, police could justify breaking HIPAA to "protect" a child from receiving gender-affirming care and remove them from their family.

In the gender-tracking sphere, TRACE touts itself as protecting users' data by not selling information to third parties.[167] However, in its policy, TRACE maintains the right to disclose information at the request of law enforcement by the showing of a warrant.[168] Such law enforcement exceptions to privacy policies are not unique and do not curb the

---

[163] Rebecca Wexler, *Privacy Asymmetries: Access to Data in Criminal Defense Investigations*, 68 UCLA L. REV. 212, 229 (2021).

[164] *Id.* at 281.

[165] *Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement*, FED. BUREAU INST. (Oct. 7, 2024), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/emergency/final_hipaa_guide_law_enforcement.pdf [https://perma.cc/UXR4-Z9W4].

[166] Bill Chappell, *Texas Supreme Court OKs State Child Abuse Inquiries into the Families of Trans Kids*, NPR, (May 13, 2022), https://www.npr.org/2022/05/13/1098779201/texas-supreme-court-transgender-gender-affirming-child-abuse [https://perma.cc/MJY4-53LV]; *see also supra* notes 127–28 and accompanying text.

[167] Privacy Policy, TRACE, https://web.archive.org/web/20220702044807/thetrace.app/privacypolicy (July 2, 2022).

[168] *Id.*

prosecution risk trans individuals face in states acting to criminalize their healthcare.[169]

As such, law enforcement has many ways of accessing personal information that people may otherwise consider private. Proponents of these exceptions say that these are important investigatory tools of the criminal legal system and that the personal privacy interest must be balanced with the public safety interests of law enforcement.[170] However, law enforcement leverages these loopholes to specifically target vulnerable populations, including individuals seeking abortions and trans communities.[171]

In response to the loss of federal abortion protections, California—where the right to an abortion is protected under the state's constitution[172]—passed A.B. 1242 to defend out-of-state abortion seekers' personal data from out-of-state warrants. Signed into law in September 2022, A.B. 1242 prohibits court orders for companies based in California to hand over electronic communication records for the prosecution of abortions in any state.[173] The law also imposes civil liability on companies who comply with these orders when they either "kn[o]w, or should have known, that the warrant" would contribute to the prosecution of an abortion.[174] California is a major tech hub, with companies like Google and Facebook. California passing this law is therefore significant in controlling how information is sent out of state to jurisdictions that have criminalized abortion.

C. Recommendations

In response to the concurrent legislative attack on trans youths' access to gender-affirming care, California passed S.B.107 in September 2022. Under the law, a health care provider, service plan, or contractor is prohibited from sharing medical information pertaining to a minor's gender-affirming care with another state's law enforcement agency.[175] Further, S.B.107 prohibits California law enforcement agencies from participating in or assisting an extradition or arrest pertaining to another state's law against gender-affirming care for minors.[176] Here, California is

---

[169] Leah Fowler & Michael R. Ulrich, *Femtechnodystopia*, 75 STAN. L. REV. 1234, 1300 (2023).

[170] *Id.*

[171] *See supra* notes 101–07 and accompanying text.

[172] *See California*, CTR. FOR REPROD. RTS., https://reproductiverights.org/maps/state/california [https://perma.cc/XC98-C76K].

[173] A.B. 1242, 2021-2022 Leg., Reg. Sess. (Cal. 2022).

[174] *Id.*

[175] S.B. 107, 2021-2022 Leg., Reg. Sess. (Cal. 2022).

[176] *Id.*

attempting similar strategies to protect both abortion seekers and trans youth. Both laws protect vulnerable populations against out-of-state warrants targeting their personal data by statutorily prohibiting a police exception in these very narrow instances.

CONCLUSION

The prosecutorial risks gender-tracking apps pose to the trans community are potentially dangerous and highlight the general lack of privacy protections granted to vulnerable populations in the U.S. While reporting has not yet exposed abuse of these apps for the criminal prosecution of trans healthcare providers or patients, geofence warrants and the data broker economy are still very much present tools in the arsenal of policing. However, these vulnerabilities are neither created by, nor unique to, gender-tracking apps. They are integral pieces of the digital surveillance ecosystem and criminal police state. Nevertheless, apps like For Them and TRACE compile uniquely incriminating information in startlingly high quantities. As such, greater regulation and legislation is required to curb the prospective dangers to transgender people in the escalating political climate attacking the community's safety, health, and well-being.

Potential solutions, given the right political moment, could include the following four recommendations: (1) **Push back against police warrant exceptions.** While California attempts to address the issue of out-of-state warrants, law enforcement warrant exceptions remain a major gap through which police can access personal records and sensitive data. (2) **Pass a federal bill similar to A.B. 1242**, which would restrict warrants to companies that would result in the sharing of one's gender-affirming healthcare information and data. (3) **Ensure passage of the Fourth Amendment is Not For Sale Act** federally or by individual states to close the data broker economy's Fourth Amendment loophole. Greater regulations of the data broker economy are also needed. Policy must go beyond emphasizing transparency by taking actions such as **updating the Electronic Communications Privacy Act to include brokers.**

Whether through these initiatives or others, trans communities must be protected as they engage with the Internet. The second Trump administration will only bring greater criminalization and a further emboldened police state. As surveillance of trans individuals increases and access to necessary medical care tightens, community and the decentralized places where trans individuals seek information, such as virtual peer-to-peer networks, will be more necessary than ever. Therefore, we must protect safe spaces where trans people can celebrate the hard-fought milestones of transition and the beauty of growing up.