



Community Safety & Online Data Privacy

Impacts and Policy Recommendations

Deanna Warren, Director of Public Policy - ACLU of New Mexico
Tatiana Prieto, Policy Advocate - ACLU of New Mexico

Agenda



1. Issue overview
2. Community safety impacts
3. Policy Recommendations
4. Conclusion and Q&A



Internet safety is a critical issue to address, for our young people – and everyone.

But right now, New Mexicans risk being tracked and surveilled without any notice every time we open an app, go on social media, or do an online search.

These online entities collect and sell our private information, including who we are, what we like, our health conditions, where we've been, and our political views. At the same time, the information and resources we access online are crucial for our communities.



Online entities collect, process, store, and sell huge amounts of often sensitive, detailed information about every one of us.

Such information can then be used to:

- make discriminatory predictions about people's health outcomes
- deny people housing or jobs
- hike insurance rates
- target users with misinformation and manipulation

Laws protecting our safety and privacy online have failed to keep up.



How our private information is used:

- **Data collection:** Many online service providers, including social media platforms, gather a vast amount of personal data from users, including likes, comments, searches, location, demographics, and more, through their interactions on the platform.
- **Targeted advertising:** highly targeted ads to users based on their interests, behaviors, and demographics.
- **Selling data to third parties:** companies may also sell user data directly to third-party data brokers who then use it for their own marketing purposes.
- **Algorithmic manipulation:** algorithms prioritize posts and ads that are most likely to engage the user based on their profile.



Problems caused:

- ➔ **Privacy issues:** The extensive collection and use of personal data raises concerns about user privacy and potential misuse of information.
- ➔ **Targeting:** Personal data and profiles can allow for the targeting of users online, including through predatory advertising and fraudulent schemes.
- ➔ **Lack of user control:** Many users may not fully understand how their data is being used or have limited options to control its collection and usage.
- ➔ **Discrimination:** The use of algorithms and data can perpetuate bias, disadvantaging certain groups.
- ➔ **Lack of Transparency:** Many consumers are unaware of how their data is used.

What's at Stake.



Our online data impacts every aspect of our lives.

- Housing access
- Job applications
- Insurance rates
- Identity theft
- Safety

It's a fundamental issue of justice, access to resources, and fairness.

What's at Stake.



Data trails can become legal traps or be used for harassment, surveillance or violence.

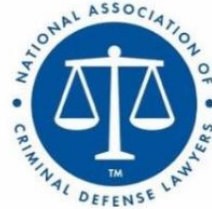
- Cell phone data, app usage, and geolocation sold or subpoenaed.
- Metadata from clinics, protests, and chats used in prosecutions.
- Especially dangerous for communities of color, undocumented people, abortion seekers/providers, Trans youth and caregivers, activists and protesters

Real Threats – Real Stories



NEWS | UNIVERSITY

Sensitive personal data of US military personnel easily bought online, Duke study shows



Trending

SPORTS | FOOTBALL

Inside the ACC's new team payout models, record revenue year and settlement with Clemson and Florida State

By Ranjan Jindal | 06/16/2025

The Data Broker Loophole is Being Exploited to Target Immigrant Communities

Purchased data circumvents sanctuary laws and contributes to the over-surveillance of the movements and behavior of immigrant communities.

Real Threats – Real Stories

Law enforcement is now buying cellphone location data from marketers

This is no longer a matter of creepy ads following you around the internet.

by **Rani Molla**

Feb 7, 2020, 9:40 AM MST



ICE uses data brokers to bypass surveillance restrictions, report finds



Photo by RINGO CHIU/AFP via Getty Images

/ Authors of the American Dragnet study say the agency is increasingly unaccountable to legislators

by **Corin Faife**

May 10, 2022, 8:45 AM MDT



Tech

Data Broker Is Selling Location Data of People Who Visit Abortion Clinics

By Joseph Cox May 3, 2022, 12:46pm



TECHNOLOGY

A company tracked visits to 600 Planned Parenthood locations for anti-abortion ads, senator says

Minnesota Shooting Suspect Allegedly Used Data Broker Sites to Find Targets' Addresses

The shooter allegedly researched several “people search” sites in an attempt to target his victims, highlighting the potential dangers of widely available personal data.

DHS spent millions on cellphone data to track Americans and foreigners inside and outside U.S., ACLU report says

The report published contracts between U.S. Customs and Border Protection, ICE and other parts of DHS to buy location data from Venntel and Babel Street.

Priest outed via Grindr app highlights rampant data tracking

Privacy activists have long agitated for stronger data privacy laws, although in the U.S. they only exist in a few states, and then in varying forms.

INNOVATION > CYBERSECURITY

Black Lives Matter: U.S. Protesters Tracked By Secretive Phone Location Technology

By [Zak Doffman](#), Contributor. © Zak Doffman writes about security, surveillan... ▾

[Follow Author](#)

Published Jun 26, 2020, 11:22am EDT, Updated Jun 26, 2020, 11:51pm EDT



[World](#) ▾ [Business](#) ▾ [Markets](#) ▾ [Sustainability](#) ▾ [Legal](#) ▾ [More](#) ▾

[My](#)

bought in secondary markets. While such data is typically used in online advertising, the FTC has expressed concern that it could facilitate stalking, blackmail, espionage and unlawful government surveillance.

Mobilewalla and Gravy Analytics used data showing the locations of mobile devices at certain points in time to sell products that could profile users based on visits to churches or political events, the agency said.

How it Happens.



Online companies vacuum up massive amounts of our most personal information. These 1000+ data points include –

- **Basic information:** this can include your name, address, phone number, email
- **Financial and employment data:** Credit scores, payment history, current/past credit cards, loans, etc. work history and salary/pay.
- **Purchasing records:** What you buy online, where you buy it, how often you buy certain products including items you may not share with anyone else.
- **Health data:** This can include medications, medical conditions, and interactions with health-related apps or websites.

How it Happens.



Online companies vacuum up massive amounts of our most personal information. These 1000+ data points include –

- **Behavioral data:** Insights into your likes, dislikes, and the types of ads you're likely to click on.
- **Real-time location data:** GPS data from apps that track your commute, where you shop, and how often you visit certain places, which can include sensitive locations.

How it Happens.



Online companies vacuum up massive amounts of our most personal information. These 1000+ data points include –

- **Inferred characteristics:** Based on the websites you visit, articles you read, videos you watch, data brokers draw insights about your lifestyle, income, preferences, religious or political beliefs, hobbies, etc.
- **Relationships with family, friends, and online connections:** by analyzing your network of friends, followers, and connections on social media and messaging apps, data brokers can map out your relationships and even track how frequently you interact with certain individuals to determine the depth of your bonds.

How it Happens.



Then –

- They categorize us (‘rural and barely making it’ ‘LGBTQ+’ ‘Anti-Vaccine’)
- They sell the information
- They’re hacked, which happens often
- Our most sensitive personal info ends up in the hands of anyone who will pay, spammers, shady companies, law enforcement, etc.

Key Takeaways



1. A massive amount of our personal information is collected and sold, even from something as simple as going to a concert.
2. Local laws matter, and companies know how to comply.
3. New Mexico can protect its residents from overreach and exploitation.

Policy Recommendations



Enact robust online data privacy protections. This means:

1. Data minimization
 - a. Only collect what you need to. Beyond that, just ask.
2. No sneaky loopholes
 - a. Exempt regulated data, not full entities
3. Support for small businesses
 - a. Ensure mom & pop businesses aren't overly burdened, but rather have an even playing field
4. Strict protections for especially sensitive information like health data

Policy Goal



From our children to our grandparents, these approaches will provide meaningful protections for all New Mexicans using the internet, and help prevent bad actors from being able to prey on others.

Our families and communities deserve safety and privacy.





Support:

- Provide common-sense protections for everyone online
- Reduce abuses from targeted advertising
- Prevent others from tracking our online activity and precise location without our knowledge
- Prevent the unnecessary collection and sale of our personal information without our affirmative opt-in – helping to keep it out of the hands of those who would use it to manipulate, harass, intimidate, criminalize or discriminate against us.



Policy Goals

- Help prevent profiling and discrimination based on our age, political and religious views, health status, and more
- Give users more control over notifications, messages from strangers, and profile-driven content feeds, with minor-specific protections



Key Provisions

- Data minimization: Collect what you need. Ask permission for more.
- Strict restrictions on sensitive data collection and use: Sets heightened protections for collection and use of sensitive data (i.e., biometrics, geolocation, health data)
- Civil rights: Extends civil rights to online spaces by prohibiting entities from processing data in a way that discriminates or otherwise makes unavailable the equal enjoyment of goods and services.



Key Provisions

- Opt-in consent: the consent the bill requires must be clear and affirmative to use data for advertising or data brokerage.
- Manipulative design restrictions: Prohibits obtaining consent in ways that are misleading or manipulative (e.g., dark patterns).
- Individual rights: Gives consumers the rights to access, correct, and delete personal information about them.
- Strong enforcement



What would this look like in practice?

The mechanisms already exist



Internet safety also means protecting access to the information our families and communities need to be healthy and thrive.

Many other states are also moving to increase privacy and safety protections. Some of these approaches aren't effective, and others would end up cutting off access to essential information and spaces online, especially on topics related to health care and overall well being.

We need to address privacy and safety in a way that protects both privacy AND access, as a holistic approach to safety.

How Do We Compare?

Unlike many other states, NM currently has little to no protections for our:

Biometric data

Location data

Non-HIPAA regulated health data

And more.

But – we also don't want false protections.





The time is now.

- Unprecedented levels of surveillance and data gathering
- Everyone is impacted - with some groups especially targeted and vulnerable: immigrants, LGBTQ+ communities, medical providers, patients, religious groups, elected officials, protestors
- New Mexico communities are already being impacted - our safety and our neighbors' safety is at stake.



**Protect our
Privacy,
Protect our
Communities.**





NM CHISPA Coalition

Includes:

- ACLU National
- ACLU of New Mexico
- Bold Futures New Mexico
- Center for Civic Policy
- Coalition to Stop Violence Against Native Women
- Commission on the Status of Women
- Conservation Voters New Mexico
- Equality New Mexico
- Faith Roots Reproductive Action
- Families & Youth Innovation Plus
- Indigenous Women Rising
- New Mexico Coalition of Sexual Assault Programs
- New Mexico Dream Team
- Planned Parenthood of the Rocky Mountains
- Progress Now New Mexico
- Tewa Women United
- Transgender Resource Center of New Mexico