The Harms of Data Abuse:

Why Washington needs meaningful, enforceable protections.

Because the U.S. does not have a comprehensive data privacy law requiring transparency and accountability for data uses, people have little insight into and even less control over how their information is collected, used, and shared. This lack of regulation – and the secrecy of the companies that exploit our data – makes it difficult for people to understand the full scope of the harms caused by data abuse. When people are denied a vacation rental, charged with a rent increase, or placed on hold an extra 10 minutes, they may never know which companies or organizations sold or shared their information, and how that information affected how they were treated. It seems like we learn about new data abuses every single day. This list of examples describes just a few of the many individuals and communities who are being harmed and the types of data that companies are exploiting.

Muslims: A 2020 Vice Motherboard investigation revealed that the U.S. military is buying the location data of users of Muslim prayer and dating apps like MuslimPro. This surveillance may have a chilling effect on the freedom of religion, as Muslims may be afraid to use Mecca-orienting apps for prayer, or to visit mosques, out of fear they will be targeted by the U.S. government.

Dating app users: People who use dating apps are encouraged to be extremely forthcoming with intimate details about their lives to be matched with the most compatible romantic prospect. Apps then take advantage of this trove of sensitive information by sharing it with other companies. A January 2021 Norwegian Consumer Council report found that OKCupid was sharing users' location and information about their sexual desires, alcohol use, political views, and ethnicity with third parties, while Tinder was sharing users' location, age, gender, and partner preference.

Cell phone users: According to a 2019 Vice Motherboard investigation, AT&T, T-Mobile, and Sprint have all sold customers' locations and personally identifying information to third-party companies, with the information eventually falling into the hands of bail bonds firms and bounty hunters. Providers of cell phone service, which is an essential utility in modern-day society, should not be allowed to share their customers' identities and real-time location with shady third-party companies.

Abortion patients: According to a 2016 Rewire article, geolocation data was used to target visitors to 140 abortion clinics with ads for anti-abortion pregnancy counseling services. Those who obtain abortions should not be subjected to targeted ads about their highly private decision before and after the procedure.

Emergency room patients: Patients waiting for emergency room medical care in Philadelphia were targeted with ads for personal injury lawyers, according to a 2018 NPR article. Given that those seeking emergency medical care are often frightened and in pain, they should not be pushed into making weighty decisions while awaiting care for their injuries.

Black, Indigenous, and People of Color: The U.S. criminal justice system is already profoundly racist, with the NAACP reporting that Black Americans are disproportionately incarcerated at more than 5 times the rate of whites. As the Washington Post reported, a 2019 federal study found that facial recognition tools misidentify Black and Asian men 100 times more often than white men, with even worse results for Native Americans. As the New York Times reported in 2020, New Jersey has banned police use of this technology due to the number of false arrests of misidentified Black men.

Eric González Alfaro, *Legislative Director* | egonzalez@aclu-wa.org | www.aclu-wa.org

ACLU Washington

LGBTQIA+ dating app users: In 2018, Buzzfeed discovered that the Grindr LGBTQIA+ dating app was sharing its users' HIV status and personally identifying information with third parties. Though users have a true interest in knowing the HIV status of their potential partners, one user noted that he stopped sharing his HIV status on the app, explaining that indiscriminate sharing of that information "can put people in danger, and it feels like an invasion of privacy."

Transgender and nonbinary individuals: Facial recognition software only misidentifies the gender of cisgender people about 3% of the time, but misidentifies the gender of trans men up to 38% of the time, according to a 2019 University of Colorado study. Additionally, the study found that nonbinary individuals were mischaracterized 100% of the time, since the systems did not recognize any gender categories other than male or female. In addition to the social exclusion and harms caused by mischaracterization, this technology also has the potential to make it difficult for trans and nonbinary people to travel freely as these recognition systems become more commonplace in airports.

Migrant children and their families: ICE targets unaccompanied migrant children and documents their interactions with them in a private company's data profiling system, according to a 2019 article in the Washington Post. The profiling system then helps ICE agents identify the children's family members for potential arrest and deportation. Our government should respect the vulnerability of unaccompanied migrant children and not use their interactions with them against their family members.

Political protesters: Though the freedom to assemble is a right enshrined in the First Amendment, police have started using facial recognition technology to identify political protesters in crowds, according to a 2020 article in the Washington Post. This has already begun to have a chilling effect on peaceful protest, as many demonstrators now must follow lengthy checklists to try to conceal their identities in a crowd.

Children and teenagers: Though the company claims that no such advertising was ever conducted, Facebook executives in Australia pitched to advertisers that Facebook could identify when teenagers were feeling "insecure" or "worthless," according to a 2017 Guardian report. Children are always more vulnerable to psychological manipulation than adults, and when they are feeling especially insecure, they should be protected, not exploited.

Menstrual cycle tracking app users: Even though users' location is not needed to use the app, individuals who use the MyDays cycle tracking app are continually having their location tracked, according to a January 2021 Norwegian Consumer Council report. Their location and personal information is then shared with a company that markets users' personal life details like "User has arrived at a clinic" or "User might be unfit to drive due to sleep deprivation" to insurance companies and others. People trying to achieve or avoid pregnancy should not fear that insurance companies may use their information to discriminate against them.

Eric González Alfaro, *Legislative Director* | egonzalez@aclu-wa.org | www.aclu-wa.org

ACLU Washington