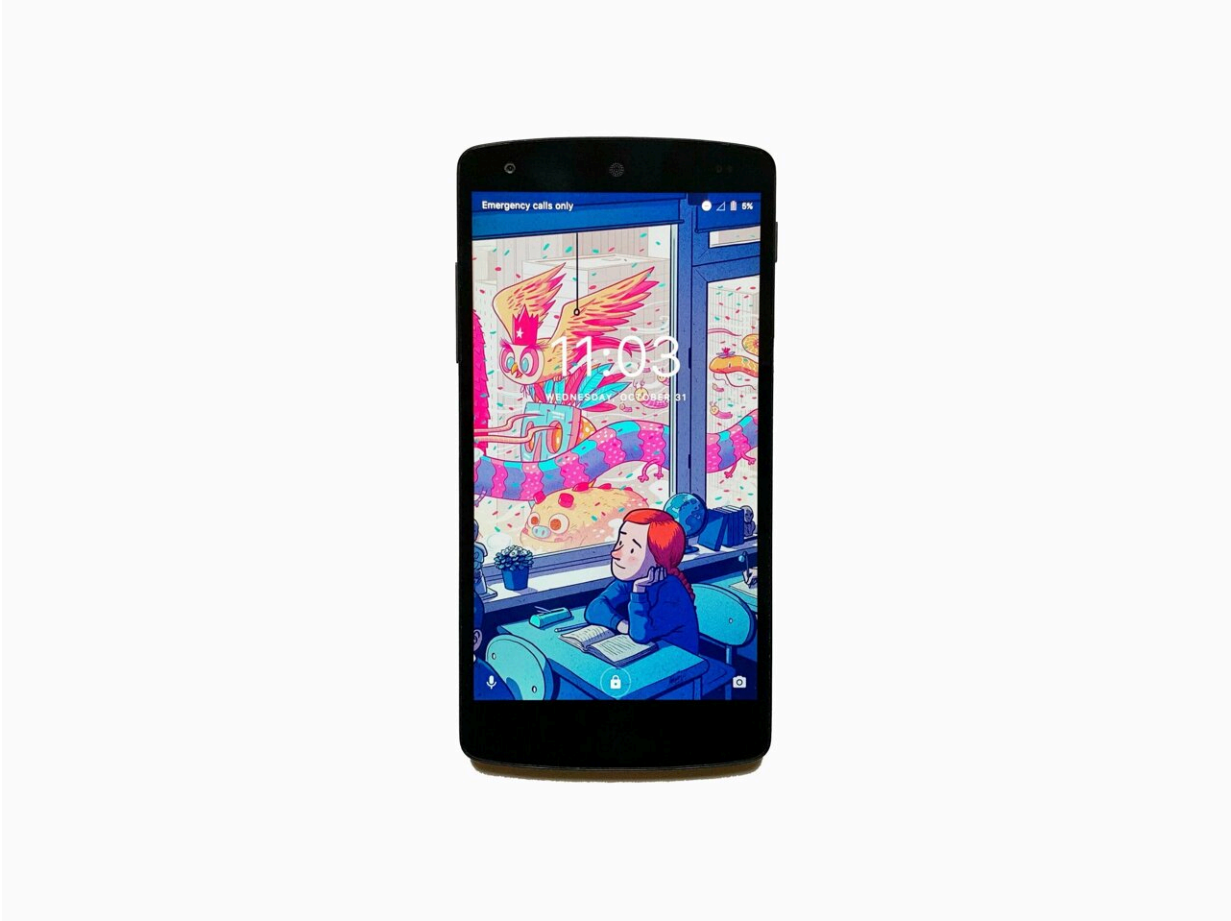
After Roe v Wade, here's how women could adopt 'spycraft' to avoid tracking and prosecution

June 30 2022, by Dennis B Desmond



Credit: Unsplash/CC0 Public Domain

The art of concealing or misrepresenting one's identity in the physical world has long been practiced by spies engaged in espionage. In response, intelligence agencies designed techniques and technologies to identify people attempting to hide behind aliases.

Now, following the U.S. Supreme Court ruling overturning Roe v Wade, women in the United States seeking assistance with unwanted pregnancies have joined the ranks of spies.

The ruling has resulted in several trigger laws coming into effect in conservative states to outlaw abortions in those states. These laws, coupled with groups targeting women's reproductive rights protests, have raised fear among women of all ages about their data being used against them.

Thousands have engaged with online posts calling on women to delete their period tracking apps, on the premise that data fed to these apps could be used to prosecute them in states where abortion is illegal. At the same time, abortion clinics in New Mexico (where abortion remains legal) are reportedly bracing for an influx of women from U.S. states.

As someone who has served as a special agent for the United States Army and Federal Bureau of Investigation, and as a Senior Intelligence Officer with the U.S. Defense Intelligence Agency, I can tell you deleting period tracking apps may not be enough for vulnerable women now.

But there are some tools women can use to conceal their identities, should this be necessary—the same tools once reserved for professional spies.

> Menstrual tracking app Stardust is one of Apple's top three most-downloaded free apps right now. It's also one of few apps that

> has said it will voluntarily—without being legally required to—comply with law enforcement if it's asked to share user data. https://t.co/sJ17VAiLvp
>
> — Motherboard (@motherboard) June 27, 2022

The privacy myth

Apart from espionage, the emergence of the internet created a new impetus for widespread data collection by data aggregators and marketers. The modern surveillance economy grew out of a desire to target products and services to us as effectively as possible.

Today, massive swathes of personal information are extracted from users, 24/7—making it increasingly difficult to remain unmasked.

Data aggregation is used to assess our purchasing habits, track our movements, find our favorite locations and obtain detailed demographic information about us, our families, our co-workers and friends.

Recent events have demonstrated how tenuous our privacy is. Protests in Hong Kong have seen Chinese authorities use cameras to identify and arrest protesters, while police in the U.S. deployed various technologies to identify Black Lives Matter protesters.

Articles appeared in Australian media outlets with advice on how to avoid being surveilled. And people were directed to websites, such as the Electronic Frontier Foundation, dedicated to informing readers about how to avoid surveillance and personal data collection.

What we've learned from both spy history and more recent events is that data collection is not always overt and obvious; it's often unseen and opaque. Surveillance may come in the form of cameras, drones,

automated number plate readers (ANPR/ALPR), toll payment devices, acoustic collectors and of course any internet-connected device.

In some cases when your fellow protesters upload images or videos, crowd-sourced intelligence becomes your enemy.

Data deleted, not destroyed

Recently, a lot of the focus has been on phones and apps. But deleting mobile apps will not prevent the identification of an individual, nor will turning off location services.

Law enforcement and even commercial companies have the ability to access or track certain metrics including:

- international mobile subscriber identity (IMSI), which is related to a user's mobile number and connected to their SIM card
- international mobile equipment identity (IMEI), which is directly related to their device itself.

Ad servers may also exploit device locations. Private companies can create advertisements targeting devices that are specific to a location, such as a women's health clinic. And such "geofenced" ad servers can identify a user's location regardless of whether their location settings are disabled.

Further, anonymised phone track data (like call signals pinging off nearby towers) can be purchased from telecommunications providers and de-anonymised.

Law enforcement can use this data to trace paths from, say, a fertility clinic to a person's home or "bed down" location (the spy term for someone's residence).

The bottom line is your phone is a marker for you. A temporary cell phone with an overseas SIM card has been the choice for some people wishing to avoid such tracking.

Adding to that, we recently saw headlines about facial recognition technology being used in Australian retail stores—and America is no different. For anyone trying to evade detection, it's better to swap bank cards for cash, stored-value cards or gift cards when making purchases.

And using public transport paid with cash or a ride-share service provides better anonymity than using a personal vehicle, or even a rental.

In the spy world, paying attention to one's dress is critical. Spies change up their appearance, using what they call "polish," with the help of reversible clothing, hats, different styles of glasses, scarves and even masks (which are ideally not conspicuous these days). In extreme cases, they may even use "appliances" to alter their facial characteristics.

Then again, while these measures help in the physical world, they do little to stop online detection.

Digital stealth

Online, the use of a virtual private network (VPN) and/or the onion browser, Tor, will help improve anonymity, including from internet service providers.

Online you can create and use multiple personas, each with a different email address and "personal data" linked to it. Aliases can be further coupled with software that removes cookies and browser history, which will help conceal one's online identity.

One example is CCleaner. This program removes privacy-violating cookies and internet history from your device, while improving your device's privacy.

There are also plenty of online applications that allow the use of temporary email addresses and phone numbers, and even temporary accommodation addresses for package deliveries.

To some, these may seem like extreme privacy measures. However, given the widespread collection of identity data by commercial companies and governments—and the resultant collaboration between the two—there's reason to be concerned for anyone wanting to fly under the radar.

And for women seeking abortions in the U.S., these measures may be necessary to avoid prosecution.

Provided by The Conversation