4-21-2023

Cybersecurity and Abortion Access: The Right to Choice Now Means the Right to Protect Data and Privacy for Women and Providers

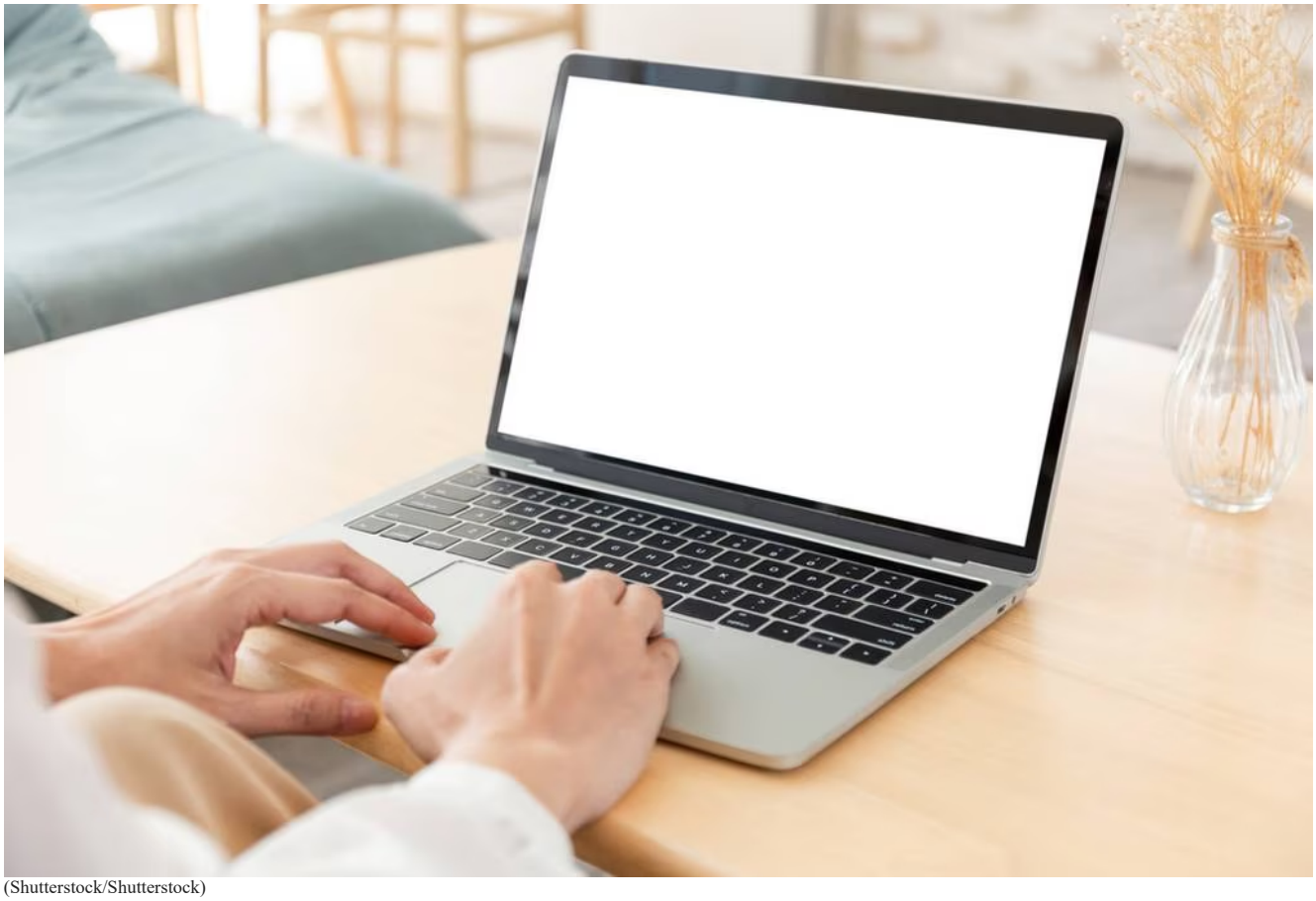
Michael Pastor

Cybersecurity and abortion access: The right to choice now means the right to protect data and privacy for women and providers

By Michael Pastor
New York Daily News • Apr 21, 2023 at 5:00 am

Women seeking abortion care, and the doctors providing it to them, have been subject to physical violence, threats, and intimidation for decades by those who strongly oppose the procedure. Today, opponents are using technology and cyberspace to express their opposition and to carry out disruptive and harmful attacks. In order to protect women and doctors from digital threats that have vastly heightened in recent months, the federal government and state government leaders in jurisdictions where abortion is legal must step up and engage with the tech companies they employ to deliver an immediate response.

In the months following the Supreme Court's reversal of Roe v. Wade last June in their Dobbs decision, many governors signed laws banning or heavily restricting abortion access. Another hurdle is playing out in the nation's highest court this very day after a Texas federal judge nullified the Food and Drug Administration's decades-long approval of mifepristone, a drug widely used for abortions. Its use would be banned unless the decision is overruled on appeal.



(Shutterstock/Shutterstock)

As a result of these strictures, many women have been left with no choice but to travel to states where abortion care providers can still legally operate. For reasons related to physical safety, and the difficulty travel can pose to those who are pregnant, these trips can be precarious. But they are made even more so because of the cyber risks these women face while making them.

Indeed, technology plays a crucial role in connecting patients to abortion care providers: when they schedule appointments; when they provide personal identifying information that is collected and stored; when they receive care; and during post-procedure appointments or communications. Knowing the importance of technology in the provision of such medical care, opponents may seek to attack a provider's systems to shut down or impair the provision of care, or to disclose publicly the names and addresses of those who are seeking, or have sought, abortion access.

The consequences of a hack and theft of sensitive data about abortion patients could be calamitous. Patients could face targeted harassment or violence if cyber criminals reveal abortion care data. Women crossing state lines to flee abusive partners and obtain abortions could find themselves tracked, stalked, harassed, or worse. Beyond that, the medical data could be used by overzealous law enforcement officers in anti-abortion states who might seek to bring criminal charges.

The Daily News Flash
Weekdays

Catch up on the day's top five stories every weekday afternoon.

By submitting your email to receive this newsletter, you agree to our **Subscriber Terms & Conditions** and **Privacy Policy**.

ENTER YOUR EMAIL ADDRESS >

Elected officials and technology companies need to address these threats head-on and take steps to protect women seeking and receiving abortion care in multiple ways.

The Biden administration is now working to strengthen protections for these groups by starting the process of updating HIPAA regulations. It's a significant step, but there's more that can simultaneously be done.

First, California Gov. Gavin Newsom recently announced grants in California for abortion care providers for both physical plant security and cybersecurity efforts. States where abortion is legal should adopt this approach with any eye towards ensuring the grant programs are not administratively onerous. States should provide the grants with accompanying offers to connect abortion providers with law enforcement and lead cyber officials who can give technical guidance and share threat intelligence. To the extent local governments are providing abortion services directly through publicly-funded hospitals, state budgets should appropriate funds to those local entities for cybersecurity enhancements and proper IT staffing.

Second, as the White House and federal cyber officials roll out the National Cybersecurity Strategy announced in March, they should treat abortion providers just like any other vital medical care providers, such as acute surgery facilities. At the same time, law enforcement and cyber intelligence agencies should dedicate resources to scanning for credible threats specific to reproductive health providers and alerting providers when necessary.

Finally, technology companies regularly provide elevated hardware, software, and cybersecurity services to customers, like hospitals, whose functions are deemed "critical." These companies should offer the same technology and services to abortion providers, whose care is as "critical" to their patients. When offering heightened goods and services, the technology companies should be sensitive to the limitations that many community-based abortion care providers may face, including stretched financial resources and a likely minimal in-house technology team.

With these sensible cybersecurity steps, those in government and the technology sector can protect women and their medical providers from being the victims of malicious and deliberate cyber crimes. The threats posed are clear and present, and the time to act is now.

Pastor is the director of the James Tricarico Jr. Institute for the Business of Law and in-house counsel, senior fellow, and adjunct professor at New York Law School. He is also the former general counsel of the New York City Cyber Command.