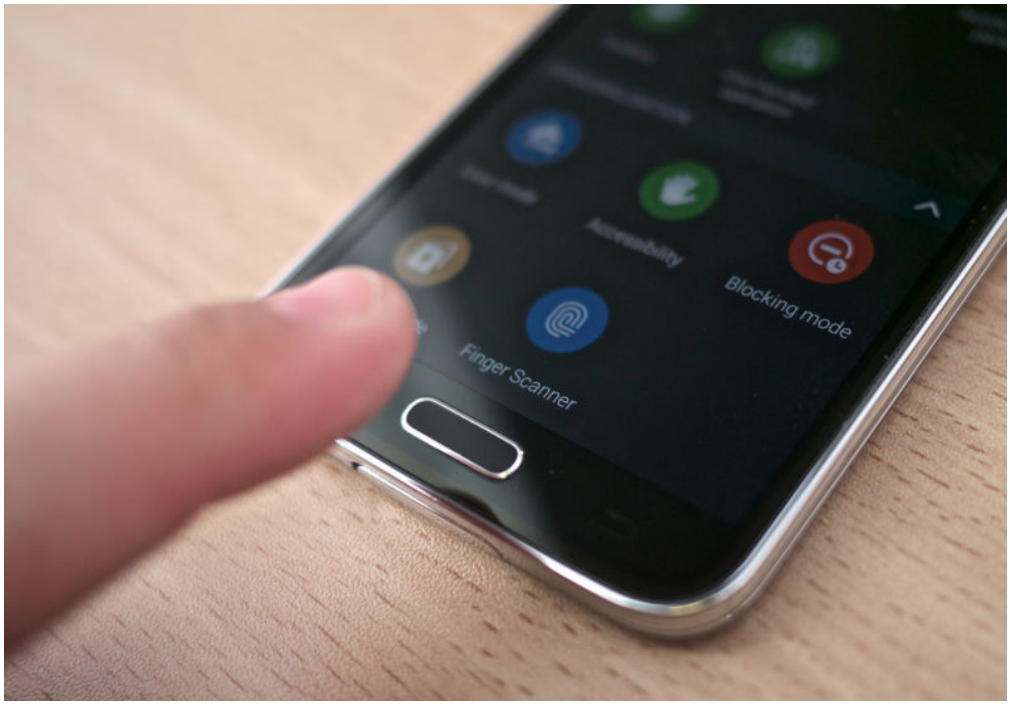
NEW MEANING TO THE WORD "DIGITAL" —

Court rules against man who was forced to fingerprint-unlock his phone

Unlocking a phone like this "is no more testimonial than furnishing a blood sample."

CYRUS FARIVAR - 1/18/2017, 11:06 AM



Kārlis Dambrāns

Enlarge

155

A Minnesota appellate court ruled Tuesday against a convicted burglar who was forced by a lower state court to depress his fingerprint on his seized phone, which unlocked it.

FURTHER READING

Here's what a "digital Miranda warning" might look like

This case, *State of Minnesota v. Matthew Vaughn Diamond*, marks the latest episode in a string of unrelated cases nationwide that test the limits of digital privacy, modern smartphone-based fingerprint scanners, and constitutional law.

In 2015, Diamond went to trial and was convicted of the burglary and two other lesser charges. He was sentenced to 51 months in prison. Diamond appealed largely on the grounds that being ordered to unlock his phone constituted a violation of his Fifth Amendment rights against self-incrimination.

Being enticed or even compelled to hand over passcodes or fingerprint-enabled passcodes gets to the heart of what law enforcement calls the "going dark" problem. Authorities say that modern "unbreakable" encryption frustrates lawful investigations aimed at tech-savvy criminals who refuse to unlock their data.

As Ars has reported before, under the Fifth Amendment, defendants cannot generally be compelled to provide self-incriminating testimony ("what you know"). But giving a

fingerprint ("what you are") for the purposes of identification or matching to an unknown fingerprint found at a crime scene has been allowed. It wasn't until relatively recently, after all, that fingerprints could be used to unlock a smartphone. The crux of the legal theory here is that a compelled fingerprint isn't testimonial, it's simply a compelled production—like being forced to hand over a key to a safe.

Had the defendant been forced to disclose his passcode (instead of depressing his fingerprint) to his phone, the constitutional analysis likely would have been different.

"Instead, the task that Diamond was compelled to perform—to provide his fingerprint—is no more testimonial than furnishing a blood sample, providing handwriting or voice exemplars, standing in a lineup, or wearing particular clothing," the appellate court found.

Give 'em the finger

FURTHER READING

To beat crypto, feds have tried to force fingerprint unlocking in 2 cases

Within weeks of the October 2014 burglary, Diamond was arrested, and the Chaska Police Department got a warrant to search his seized phone. However, investigators were initially stymied by Diamond's passcode on his phone. They then went back to the court and obtained a motion to compel Diamond to press his finger on the phone's fingerprint reader to open the device. He refused and was found in contempt of court—and then finally complied. Diamond provided his fingerprint, and the phone was "immediately searched," months after it was initially seized.

After unlocking the phone, a detective obtained "incriminating evidence" of the burglary. The specific make and model of the phone is not specified in the court's opinion, but it is likely to have been an Android phone. Since the introduction of the fingerprint scanner on iPhones, a passcode is required after 48 hours or after a reboot of the device.

According to the appellate court's opinion, however, there was a slight twist in what the court actually ordered. During an April 2015 contempt of court hearing, there was confusion about which of his fingerprints would actually unlock the phone. Addressing the prosecutors, the district court ordered, "Take whatever samples you need."

The appellate court's opinion continued:

> Diamond then asked the detectives which finger they wanted, and they answered, "The one that unlocks it." It is clear that the district court permitted the state to take samples of all of Diamond's fingerprints and thumbprints. The district court did not ask Diamond whether his prints would unlock the cellphone or which print would unlock it, nor did the district court compel Diamond to disclose that information. There is no indication that Diamond would have been asked to do more had none of his fingerprints unlocked the cellphone. Diamond himself asked which finger the detectives wanted when he was ready to comply with the order, and the detectives answered his question. Diamond did not object then, nor did he bring an additional motion to suppress the evidence based on the exchange that he Initiated.
>
> In sum, because the order compelling Diamond to produce his fingerprint to unlock the cellphone did not require a testimonial communication, we hold that the order did not violate Diamond's Fifth Amendment privilege against compelled self-incrimination.

Diamond's attorney, Cathryn Middlebrook, did not immediately respond to Ars' request for comment as to whether she would appeal further up to the Minnesota Supreme Court.

CYRUS FARIVAR

Cyrus is the Senior Business Editor at Ars Technica, and is also a radio producer and author. His first book, *The Internet of Elsewhere*, was published in April 2011.

EMAIL cyrus.farivar@arstechnica.com // **TWITTER** @cfarivar

READER COMMENTS 155 SHARE THIS STORY

← PREVIOUS STORY NEXT STORY →

Related Stories

Today on Ars

RSS FEEDS
VIEW MOBILE SITE
VISIT ARS TECHNICA UK
ABOUT US
CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS