
WorkED
PROTECTING
OUR NATION

WorkED

PRIVACY vs. SECURITY

WHICH WOULD YOU RATHER HAVE?

SNOWDEN

WorkED

TYPES OF SURVEILLANCE

INTERNET MONITORING

PURCHASING HISTORY

VOICE RECOGNITION

FACIAL RECOGNITION

VIDEO, VOICE, AND TEXT-BASED TRANSMISSIONS

WorkED

Recent Government Hacks

FBI hacks vulnerable US computers to fix malicious malware

US justice department says bureau hacked devices to remove malware from insecure software

▲ The FBI's campaign did not actively fix the underlying vulnerability. Photograph: Sean Gallup/Getty Images

The FBI has been hacking into the computers of US companies running insecure versions of Microsoft software in order to fix them, the US Department of Justice has announced.

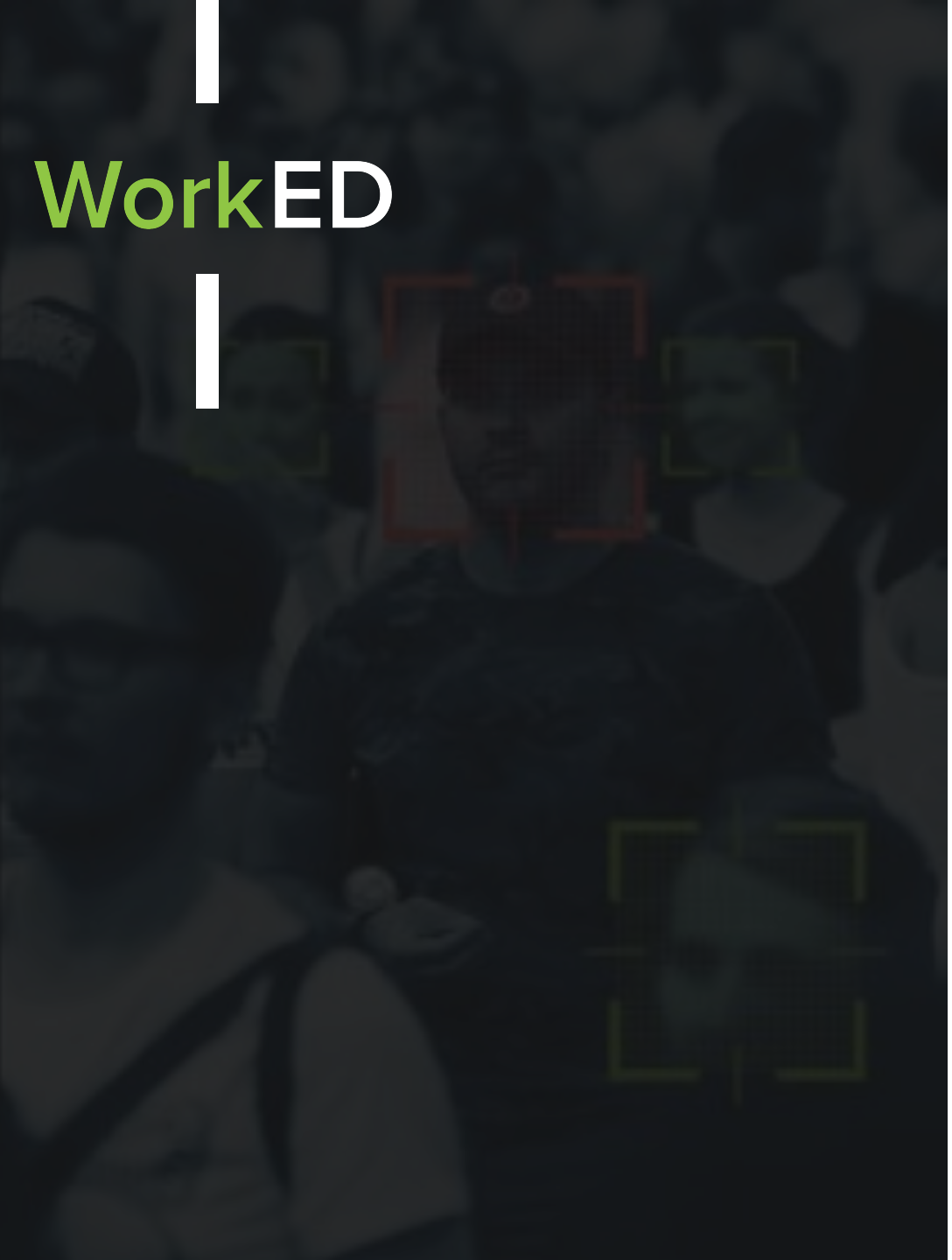
The operation, approved by a federal court, involved the FBI hacking into "hundreds" of vulnerable computers to remove malware placed there by an earlier malicious hacking campaign, which Microsoft blamed on a Chinese hacking group known as Hafnium.

Texas power companies automatically raised the temperature of customers' smart thermostats in the middle of a heat wave

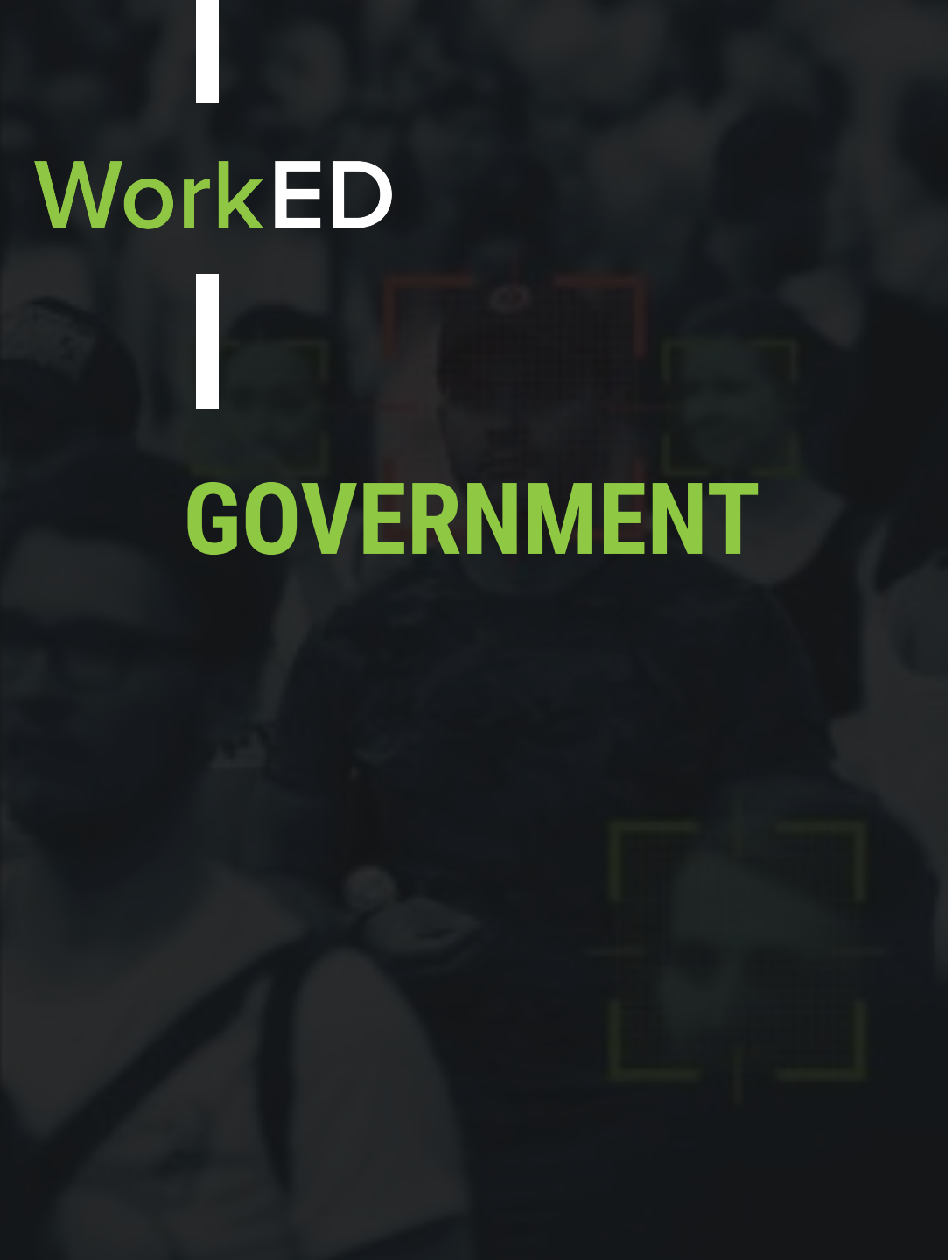
Texas power companies heated up some customers' homes last week by remotely controlling their smart thermostats, KHOU 11 reported Thursday.

One resident in the state, which is facing a heat wave that is straining its power grid, told KHOU 11 his family had awoken from a nap sweating and shocked their home had gotten as hot as 78 degrees Fahrenheit.

It turns out they had enrolled their thermostats in an energy-conservation promotion called Smart Savers Texas, run by a company called EnergyHub, in partnership with power companies. The program gives EnergyHub permission to adjust participants' smart thermostats remotely during times of peak energy demand, in exchange for entry into a sweepstakes.



- The NSA reviewed over **534 million phone calls and text messages** in 2017 alone.
- Facebook, Google, Apple, and other leading online services **give customer data to the NSA** including emails, messages, and documents.
- **Facebook** is currently being **sued by millions of people** for releasing unauthorized video of people on their webcams
- The NSA's Tailored Access Operations unit develops hacking exploits that enable the **NSA to break into any consumer electronic device or IT systems**.



WorkED

GOVERNMENT

- Should they **be involved** or should they not?
- **Business** vs **Personal**
- Businesses want **more involvement** more help/support and more guidance on policies and guidelines.
- People want left alone and for **more privacy** with little to no involvement
- Does our nation **even need more help**?

WorkED

- The NSA often coercively **persuades device manufacturers** to build vulnerabilities into products that they can exploit.
- They've also intercepted product shipments to **install their own backdoors**.
- **Your cellular device tracks your location** using GPS and phone tower triangulation which **can be shared** with the NSA and law enforcement agencies.

WorkED

- **Conversations** you have in the presence of your **cellular phone**, **even when it is powered off** can be eavesdropped on.
- The **NSA accesses** credit card networks, payment gateways, and wire transfer facilities around the world allowing them **to follow every cent** of where money comes from, and what it's spent on.
- **Millions of images a day are collected** for facial-recognition from social media and other means.


WorkED
IS SURVEILLANCE BAD,
AND WHAT IS THE ALTERNATIVE?

WorkED

CYBER RELATED THREATS TO NATIONAL SECURITY

Espionage

Sabotage of service

Election hacking

Data leaks

Insider threat

Deepfake

Terrorism and Cyberterrorism

Propaganda, Misinformation, Disinformation

WorkED

November 8, 2016

- Millions of voters in the presidential election **were influenced** by thousands of fake social media accounts that **spread fabricated news articles and disinformation** from Russian-controlled media.
- Hackers associated with the Russian Military Intelligence Service **infiltrated** systems of the Democratic National Committee, Democratic Congressional Campaign Committee (DCCC), and Clinton campaign officials, publicly **releasing stolen files and emails** during the election campaign.


T | Opinion
WorkED


WorkED
PROTECTING OUR NATION
QUESTIONS?
THANK YOU