Home / Tech / Security

# How to secure Windows 10: The paranoid's guide

**Worried sick over Windows 10's privacy settings? There's a lot you can do to lock them down, but you will lose some functionality along the way.**

Written by **Steven Vaughan-Nichols,** Senior Contributing Editor

Aug. 5, 2015 at 9:50 a.m. PT

Just because you're paranoid doesn't mean that they're not out to get you.

With some work you can lock Windows 10 privacy settings down but at the cost of some functionality. PinboxThat said, I think some people's fears about Microsoft looking over your shoulder are over-the-top. And, I speak as someone who looks at Microsoft with a great deal of suspicion.

What you need to realize is that Microsoft has made Windows 10 both a desktop and a cloud operating system. Adding cloud functionality means that when you run Windows 10 you'll be sharing far more information with Microsoft and its partner customers than ever before.

For example, while Windows 10 doesn't have a keylogger it *does* collect your keystrokes and voice to improve spell-checking and voice recognition. Before having a fit about this, keep in mind that *every* cloud-based software-as-a-service (SaaS) program does this to one degree or another. Google Docs, Apple's Siri, Office 365, whatever -- they all collect not just your final words but every keystroke and spoken syllable that went into making those words.

It's another case with Wi-Fi Sense. You don't need to be afraid that Wi-FI Sense will let any of your Skype, Outlook, or Hotmail contacts use your Wi-Fi network without your permission. Yes, Wi-Fi Sense is on by default, but take a closer look. It doesn't permit anyone to use any of your Wi-FI networks without your specific permission.

**Locking down Windows 10**

Still don't trust these new "features?" I can't blame you. This is not the Windows you've known and used for years. This is a Windows that exists both on your PC and in Microsoft's cloud. Here's how to lock down Windows 10 and make it more of a PC-centric operating system.

First, head to Settings/Privacy. There you will find no fewer than 13--count 'em, 13--different privacy settings screens. The major settings are under the 'General' screen. The other screens are concerned with which apps can and can't access your calendar, camera, messages, microphone and so on.

On the General screen, you'll see your Advertising ID. This is your unique ID number. Think of it as being like a web cookie and you won't be far wrong. It's used to identify you to Windows apps advertisers. So, for instance, if you're a big Dallas Cowboy fan, you can count on seeing ads for Cowboys gear. Microsoft claims it doesn't link this ID with your name, email address, or other personal information.

Of course, they don't need to. Any company that does modern web advertising is going to have you pinned down with our without this ID. Welcome to the 21st century. Personally, I've already turned it off.

If you're still concerned about keylogging, head to Privacy/Speech, inking & typing. Think long and hard about whether to use Microsoft's "Getting to know me" improvements. Steve Hoffenberg, VDC Research's Director of IoT & Embedded Technology worries, for instance, that these Windows 10's "features" violate Health Insurance Portability and Accountability Act (HIPAA) privacy requirements. If his fears are valid, this means medical offices and health insurance companies should turn off this Windows 10 setting.

I doubt he's right, but I'm no lawyer. Even so, were I working with transactions that fall under Sarbanes- Oxley (SOX), Gramm-Leach-Bliley (GLB), or HIPAA, I'd turn off this feature, and its related setting, "Windows 10 Input Personalization." Better safe than sorry.

Be aware, however, that if you turn off the "Getting to know me," this will also disable both dictation and Windows 10's voice-activated assistant Cortana,

---

**/ ready?**

**I like Windows 10 but I'm going back to Windows 8.1**

**Read now** →

Next, you'll want to use "Manage my Microsoft advertising and other personalization info" to decide on whether you want advertisers to show you ads based on your browsing history and interests. Better still, skip that page and head directly to Microsoft personalized ad preferences and opt out of everything. Advertisers already know far too much about me as it is.

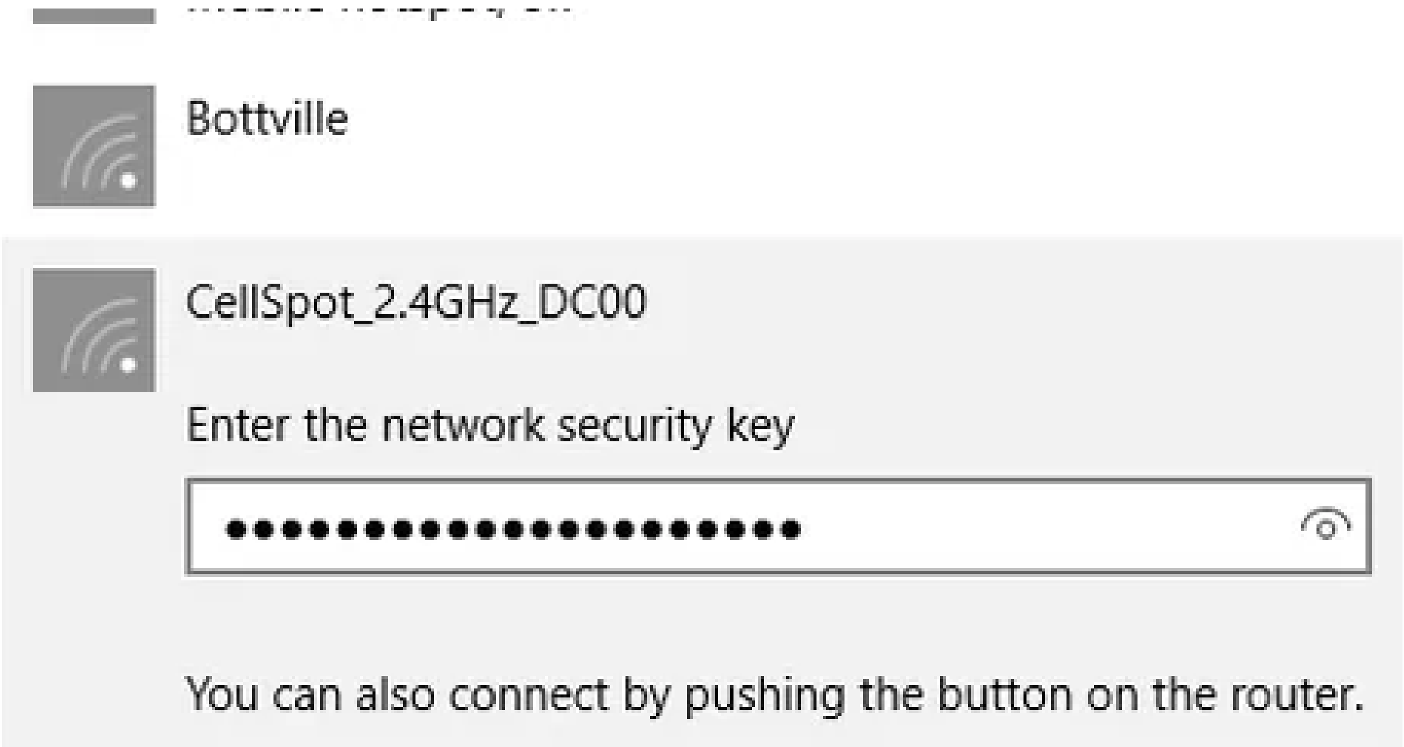
You'll also want to look at each individual setting page to make sure that Microsoft and Windows have just as much access as you feel comfortable with. So, of course you want Windows' Calendar app to access your calendar data (obv) -- but share it with advertisers via App connector? I don't think so!

Be sure to go through each setting even if you don't think they'll matter. By default, each and every privacy setting is set to give Microsoft and friends the maximum possible access. This is *not* a good thing.

Moving on: Head to the Location settings and turn them off. While your PC probably doesn't have a GPS like your smartphone, you'd be amazed at how accurately your location can be pinned down using Wi-Fi access points and IP address. I've never been comfortable with letting anyone track me and I turn location off on every device I own except when I need GPS directions.

If you turn off location services, though, you won't be able to fully use Cortana. That's annoying because Cortana is one of Windows 10's best features. It's helpful to just ask your computer a question and get useful, personalized answers. But like its older relatives, Siri and Google Now, for Cortana to show to its best advantage it needs access to an enormous amount of personal data. For instance, Cortana must have locations services on. Cortana also watches pretty much everything you write, say and do on your PC. For example, it keeps track of your flights by detecting "tracking info, such as flights, in messages on my device."

**/ ed bott**



Bottville

CellSpot_2.4GHz_DC00

Enter the network security key

●●●●●●●●●●●●●●●●●●●●●

You can also connect by pushing the button on the router.

**How to protect your wireless network from Wi-Fi Sense**

**Read now →**

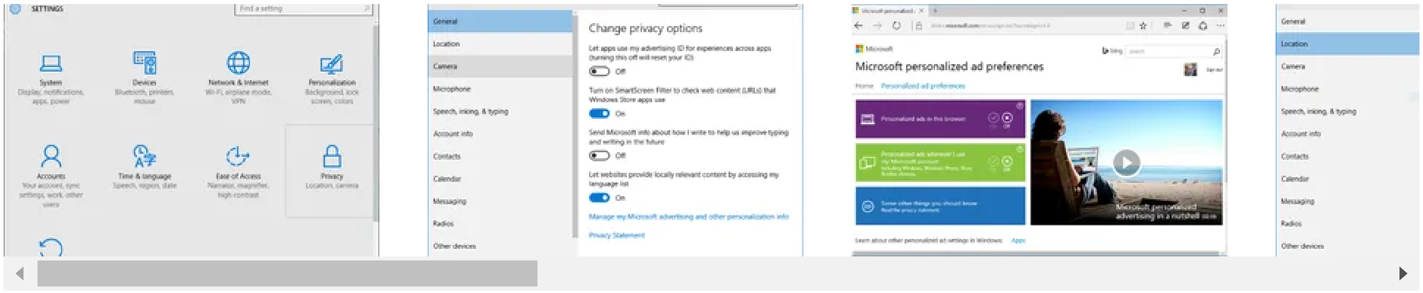
That's both incredibly handy and incredibly creepy. If you find it more disturbing than useful, head to Cortana's settings, under Cortana and Search, and turn off everything there that doesn't pass the smell test. Cortana will be less useful, but you'll get more privacy.

Another approach to locking down Windows 10 is the open-source "Disable Windows 10 Tracking." This brand-new program claims that it disables telemetry collection, certain Windows services, and other tracking. At this point, this is a bare-bones program and only Windows experts should use it.

Still not private enough for you? Then don't use Windows 10, Chrome OS, iOS, Android, or any other system that's tied closely into the cloud. Instead, use Linux as your desktop operating system. By default, Linux is the only mainstream operating system that still relies primarily on true desktop apps.

Not ready for such a radical move? Well, actually, it's not that radical. If you can use Windows, trust me, you can use Linux distributions such as Ubuntu 15.04 or Mint 17.2.

## Windows 10 Privacy: Step by step


SETTINGS
Find a setting
System
Display, notifications, apps, power
Devices
Bluetooth, printers, mouse
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Accounts
Your account, sync settings, work, other users
Time & language
Speech, region, date
Ease of Access
Narrator, magnifier, high contrast
Privacy
Location, camera
General
Location
Camera
Microphone
Speech, inking, & typing
Account info
Contacts
Calendar
Messaging
Radios
Other devices
Microsoft personalized ad preferences
Home
Personalized ad preferences
Personalized ads in this browser
Personalized ads wherever I use my Microsoft account
Some other things you should know
Microsoft personalized advertising in a nutshell
Learn about other personalized ad settings in Windows.
Apps

Change privacy options

Let apps use my advertising ID for experiences across apps (turning this off will reset your ID)
Off

Turn on SmartScreen Filter to check web content (URLs) that Windows Store apps use
On

Send Microsoft info about how I write to help us improve typing and writing in the future
Off

Let websites provide locally relevant content by accessing my language list
On

Manage my Microsoft advertising and other personalization info

Privacy Statement

Otherwise, get busy locking down Windows 10. Good luck.

## Related Stories

- Want Windows 10 to stop tracking you? Now there's an app for that
- How to protect your wireless network from Wi-Fi Sense
- Windows 10's Wi-Fi Sense is not a security risk. Here's why
- Does Windows 10 really include a keylogger? (Spoiler: No)

Editorial standards

show comments ↓

Home / Business / Enterprise Software

# When Windows 10 support runs out, you have 5 options but only 2 are worth considering

**Microsoft will officially end support for its most popular operating system in October 2025. Here's what you should do with your Windows 10 PCs before that day arrives.**

Written by **Ed Bott,** Senior Contributing Editor

April 22, 2024 at 12:29 a.m. PT

BrianAJackson/Getty Images

In less than two years, Microsoft will draw the final curtain on Windows 10 after a successful 10-year run.

That news shouldn't come as a surprise to anyone. The end date is right there on the Microsoft Support document that lists "products retiring or reaching the end of support in 2025." The schedule is defined by Microsoft's Modern Lifecycle Policy, which is documented on the Microsoft Lifecycle page: "Windows 10 will reach end of support on October 14, 2025. The current version, 22H2, will be the final version of Windows 10, and all editions will remain in support with monthly security update releases through that date."

**Also: Windows 11 FAQ: ZDNET's upgrade guide and everything else you need to know**

When a Windows version reaches its end-of-support date, the software keeps working, but the update channel grinds to a halt:

> **[There] will be no new security updates, non-security updates, or assisted support. Customers are encouraged to migrate to the latest version of the product or service. Paid programs may be available for applicable products.**

That part in the middle sounds encouraging, doesn't it? "Customers are encouraged to migrate to the latest version of the product or service." Unfortunately, that's not a supported option for customers running Windows 10 on hardware that doesn't meet the stringent hardware compatibility requirements of Windows 11. If you try to upgrade one of those PCs to Windows 11, you'll encounter an error message, and Microsoft is adamant that it will not extend the support deadline for Windows 10.

**Also: Windows 11: Do these six things right away after you finish setup**

If you're responsible for one or more Windows 10 PCs that fail Microsoft's Windows 11 compatibility tests, what should you do? You have five options.

## Option 1: Ignore the end-of-support deadline completely

You could do nothing at all -- just continue running your unsupported operating system and hope for the best. That's a bad idea that exposes you to the very real possibility that you'll fall prey to a security exploit. I don't recommend this strategy. If you're intent on doing so, consider installing the free 0patch agent to deal with any security issues that aren't addressed by Microsoft. That option is free for personal use, but for business or enterprise use, you'll need to pay for 0patch support at a rate that equates to a few dollars a month.

## Option 2: Buy a new PC

Microsoft and its partners would like you to replace that unsupported hardware with a new PC. You might even be tempted by one of the shiny new AI PCs, with their custom neural processing units, or maybe a powerful gaming PC, but throwing away a perfectly good computer seems wasteful, and it's not an option if you're hanging on to Windows 10 because you have mission-critical software that won't run on the new OS.

## Option 3: Ditch Windows completely

You could keep your old hardware and replace Windows 10 with the flavor of Linux you prefer. If you've got the technical know-how and experience to manage the transition, that option is worth considering. For the overwhelming majority of consumers and businesses that have existing investments in Windows software, however, it's not a realistic alternative.

**Also: Thinking about switching to Linux? 9 things you need to know**

The final two options are more attractive.

## Option 4: Pay Microsoft for security updates

Do you remember the official support document that I quoted earlier? The one that says there will be "no new security updates" after Windows 10 reaches its end-of-support date? It turns out that's not exactly true. Microsoft will indeed continue developing security updates for Windows 10, but they won't be free. Microsoft announced in December 2023 that it will offer Extended Security Options (ESUs) for Windows 10; these subscription-based updates will be available for up to three years.

How much are these paid-for updates going to cost? Microsoft finally revealed the price list in April 2024. If you're an administrator at an educational institution with a deployment of Windows 10 Education edition, you're in luck. Those extended updates will cost literally a dollar per machine for the first year, $2 for the second year, and $4 for the third and final year, taking you all the way to 2028.

The rest of us aren't so lucky:

> **Business customers will need to pay dearly to stick with Windows 10. A license for the Extended Security Updates (ESU) program is sold as a subscription. For the first year, the cost is $61. For year two, the price doubles, and it doubles again for year three. The blog post doesn't do the math on those, probably because the total is uncomfortably high. A three-year ESU subscription will cost $61 + $122 + $244, for a total of $427.**

In the original announcement of Extended Security Updates last year, a Microsoft spokesperson said that there will be a version of this program for consumers, but the company has yet to provide any additional details.

## Option 5: Upgrade your old hardware to Windows 11

That pesky compatibility checker might prevent you from upgrading your Windows 10 PC the easy way, but there are indeed officially supported ways to install Windows 11. You just have to jump through a few technical hoops.

**Also: The best Windows laptop you can buy: Dell, Samsung, Lenovo, and more**

You can find all the details in a Microsoft Support bulletin titled "Installing Windows 11 on devices that don't meet minimum system requirements." That document packs a lot of FUD into just a few paragraphs:

> **Installing Windows 11 on a device that does not meet Windows 11 minimum system requirements is not recommended. If you choose to install Windows 11 on ineligible hardware, you should be comfortable assuming the risk of running into compatibility issues.**
>
> **Your device might malfunction due to these compatibility or other issues. Devices that do not meet these system requirements will no longer be guaranteed to receive updates, including but not limited to security updates.**
>
> **The following disclaimer applies if you install Windows 11 on a device that doesn't meet the minimum system requirements:**
>
> **This PC doesn't meet the minimum system requirements for running Windows 11 - these requirements help ensure a more reliable and higher quality experience. Installing Windows 11 on this PC is not recommended and may result in compatibility issues. If you proceed with installing Windows 11, your PC will no longer be supported and won't be entitled to receive updates. Damages to your PC due to lack of compatibility aren't covered under the manufacturer warranty.**
>
> ***[emphasis in original]***

Don't be fooled by the language in the bulletin. As I've noted before, the document really doesn't say that Microsoft is going to cut off your access to updates; it simply says your PC is no longer supported, and you're no longer "entitled" to those updates. That word is a tell on Microsoft's part, disclaiming legal responsibility without actually saying what it will do.

**Also: Here's why Windows PCs are only going to get more annoying**

The installation instructions that allow you to bypass the compatibility check are in a separate support article: "Ways to install Windows 11." To perform an upgrade, you need to create the following registry key values:

- Registry Key: HKEY_LOCAL_MACHINE\SYSTEM\Setup\MoSetup
- Name: AllowUpgradesWithUnsupportedTPMOrCPU
- Type: REG_DWORD
- Value: 1

You still need a Trusted Platform Module (TPM), but even an old TPM 1.2 chip will do. If your PC doesn't have that hardware, it's probably more than 12 years old, and maybe you should replace it after all.

If you don't want to mess with the registry, and you're willing to do a clean install, just create a bootable Windows 11 installation drive and use that option, which bypasses the compatibility checker completely. You'll need to restore your data files from a backup or from the cloud, and you'll also need to install your software from scratch, but that's no more difficult than setting up a new PC.

## / featured

**Switzerland now requires all government software to be open source**

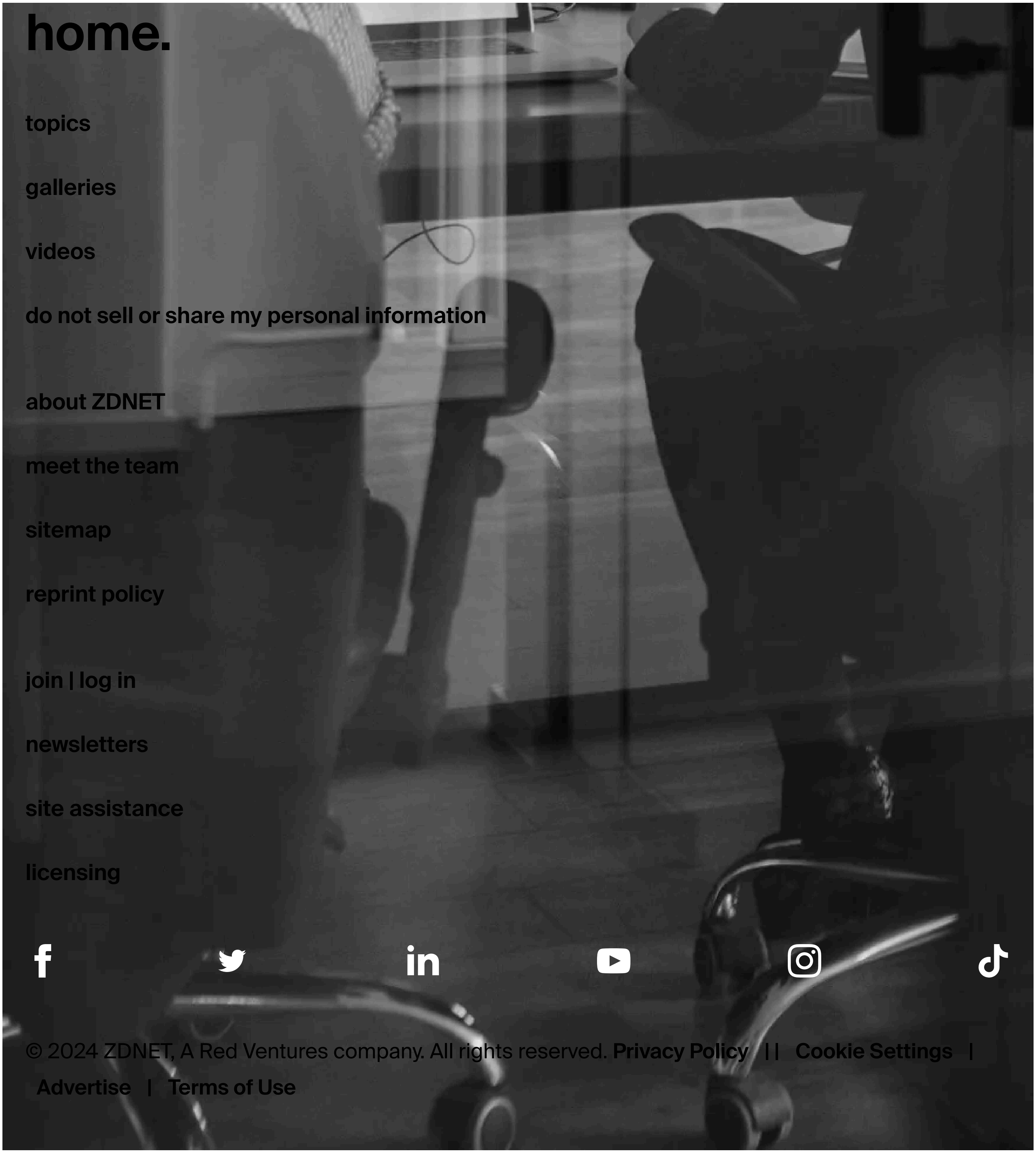
**I replaced my Samsung Galaxy S24 Ultra with the Z Fold 6 for a week - and can't go back**

**Can't he dramati audio -**

**Editorial standards**

show comments ↓

ZDNET
we equip you to harness the power of disruptive innovation, at work and at



home.

topics

galleries

videos

do not sell or share my personal information

about ZDNET

meet the team

sitemap

reprint policy

join | log in

newsletters

site assistance

licensing