Protected Computing

Protected Computing transforms how, when, and where data is processed to technically ensure the privacy and safety of your data.

Computing is no longer happening just on a computer, or on a phone - but across your home, in your car, on your wrist and in the cloud. Unlocking personalised, helpful experiences while protecting user privacy in an increasingly complex environment presents new technical challenges.

That's why we've engineered Protected Computing, a new technical solution to keep personal data private, safe and secure.

Today, Protected Computing:

- Enables Android to suggest the next phrase in your text, while keeping your conversation completely private
- Helps Pixel know when to keep your screen awake, while continuously deleting ambient signals as they're processed
- Allows Chrome to alert you to compromised passwords, without knowing a single one

Principles of Protected Computing

Minimise the data footprint

We shrink the amount of personally identifiable data altogether – collecting less and deleting more, using techniques like edge processing and ephemerality. If the data doesn't exist, it can't be hacked.

De-identify data

From blurring and randomising identifiable signals to adding statistical noise, we use a range of anonymisation techniques to strip your identity from your data, so it is no longer linked to you.

Restrict access to data

We restrict access through technologies like end-to-end encryption and secure enclaves. This is about making it technically impossible for anyone, including Google, to access your sensitive data.

Safer with Google

Learn more about how Google keeps more people safe online than anyone else at safety.google