NordVPN®

Personal Devices Research

Table of contents

Background

What makes a device personal? Is it a matter of ownership? Is it control over what happens to it? Or is it the fact that it is what connects us as individuals to our friends, family, colleagues, and the rest of the world? It's a bit of all these things. And, just like with our personal data, when our device comes under attack, it is very personal.

How often do you hand your phone to a friend or family member to show them a picture, look something up, or message or call someone? It's a natural thing to do, especially since so much of our lives is now run on devices of some kind or another. And who do you share your devices with on a more regular basis? Your partner? Your children? Other family members, friends, flatmates, colleagues? The list goes on. Sharing is a part of our digital lives, so it's also a part of privacy. After all, what is privacy but the ability to control when, how, and with whom our data is shared?

Researcher Helen Nissenbaum calls this aspect of privacy contextual integrity, or the appropriate flow of information. This means that we might want to share information in certain contexts, like sharing photos of our children with faraway grandparents on social media or in a messaging app, but that doesn't mean we want to share that information with everyone, like companies or governments. It also means we want our data to only be used for the purposes we intended. For example, we might not want images of our face to be scraped off social media by AI companies and used to train potentially discriminatory technologies like facial recognition. Or we might be looking for a surprise birthday present for a family member and not want adverts for it to follow us across websites and spoil the surprise if the person happened to see them. There are so many different contexts and reasons we use devices and the internet, and we need to maintain the integrity of these different contexts.

We can think about data and privacy both as something we do and something we have. It is our behaviors, every act of sharing or not sharing — all of that adds up to define the expectations and norms of how data should be shared. And we expect certain audiences but not others, like family but not governments. Every single thing we click on can be tracked by our internet service provider (ISP), search engines, advertisers, governments, and others. This requires technical and legal protections, but there are also social aspects involved: privacy is something we do together — it is part of how we act in a digital society. This includes how we protect ourselves and our relationships in and with technology. It includes issues of our identities and the different roles we play between work and home, parent, partner and child, different groups of friends or hobbies, etc. Privacy is a collective action to empower all users with the skills and tools they need.

The Me and My Big Data project outlined three types of data skills. Data Doing is what we might expect, our ability to use technology to share information, as well as to change our privacy settings. Data Thinking is our ability to think critically about how our data is being shared. It includes issues of business models, regulation, and power. Particularly important, but often overlooked, is Data Participation — our ability to help others improve their skills and our communities of improving privacy. This is even more important when we start to think about sharing devices, particularly if that is between work and home or involves teaching our children to be safe online.

Methods

As a security and privacy company specializing in VPNs, Nord Security has a no-logs policy, meaning it does not collect data about its users. This is an important part of our mission, but it means that data for our research must be collected elsewhere, primarily through specific surveys of the public or through technical data of server loads — something completely detached from user data.

This report draws on data taken from several surveys of users across the globe and in specific national settings. The first source is a pair of surveys on Encryption Habits in the US and UK. These surveys were conducted on 7 April 2020 through a Pollfish panel. In each survey, we surveyed 700 people aged 18+. The people surveyed are representative of the overall population across characteristics like age and gender.

The second main source is a survey on Monitoring Family Members, conducted on 21 January 2021 through CINT, of residents aged 18+ from eight countries (US, Canada, Australia, UK, Germany, France, the Netherlands, and Poland). Again, the people surveyed are representative of the overall population, and we surveyed 1,000 people in each country, for a total of 8,000 people.

The third source is Cyber Security Potential, a survey of 1,000 NordVPN users taken in July 2020. We also draw on data by Nord Teams into business VPN usage in relation to working from home during the pandemic. This research compared the busiest times of day for business VPNs pre-pandemic, during March-April 2020, and again in January 2021. No user data was collected, but the VPN server usage indicates the levels of activity of business users and, by extension, those connected to their business network from home.

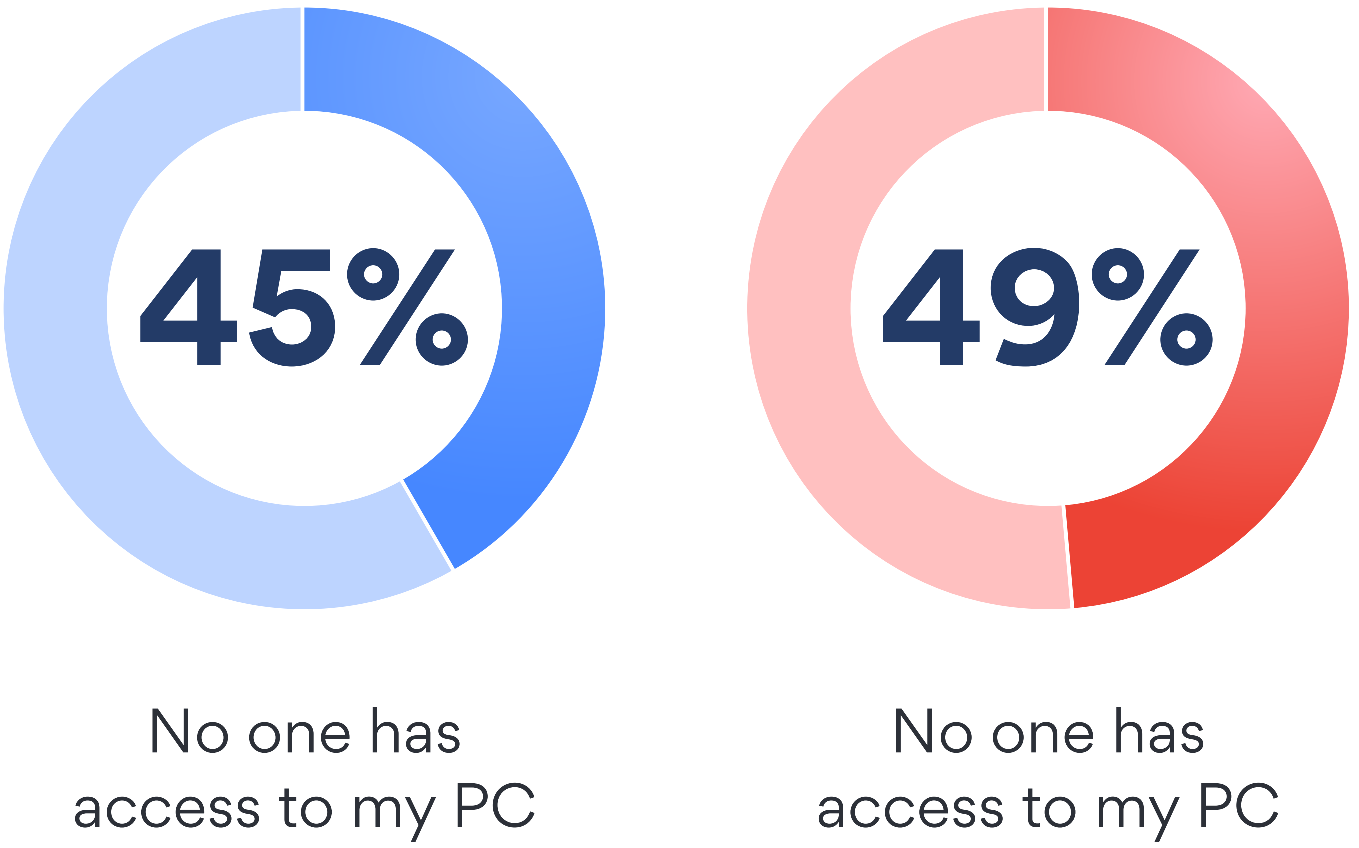
Personal devices

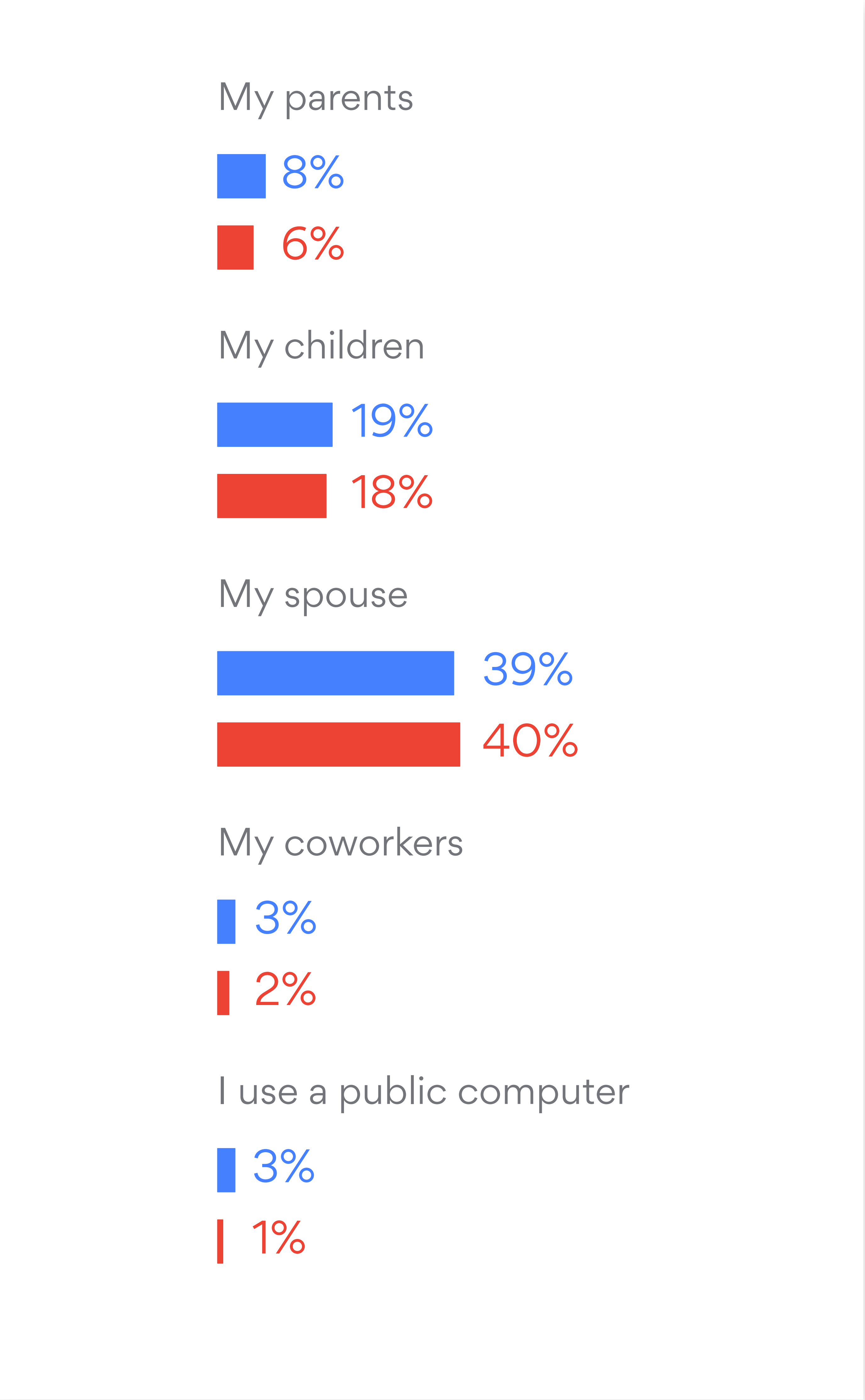
Around half of people surveyed in the US and UK would be extremely concerned about losing their computer or device. Our devices, as well as what is stored on them, are often incredibly important to us. In a networked world, and particularly in the context of the global pandemic and the need for online connections to friends, family, and work, this is not surprising. But we are often not the only ones using our personal devices. Around half of people surveyed both in the US and UK share their devices with other people. This may include sharing with parents, children, a spouse or partner, colleagues, or using a public computer.

Our personal devices are not as personal as the name suggests. For example, it makes sense that two-thirds of people in the UK who share devices with their children also share devices with their spouse (the number is slightly lower in the US). But the data also suggests that intergenerational sharing is commonplace. More than 1 in 5 people who share devices with their parents also share them with their children. This also matches the finding that people in the age range 25-34 are least likely to keep their devices completely private — they are possibly more likely to have younger children and close contact with their own parents, so they also share more evenly across different groups. Older people (age 54+) are most likely to share with their spouse and only sometimes with their children, which suggests that sharing tends to work upwards within the family.

Who, besides you, has access to your personal computer?

● USA ● UK

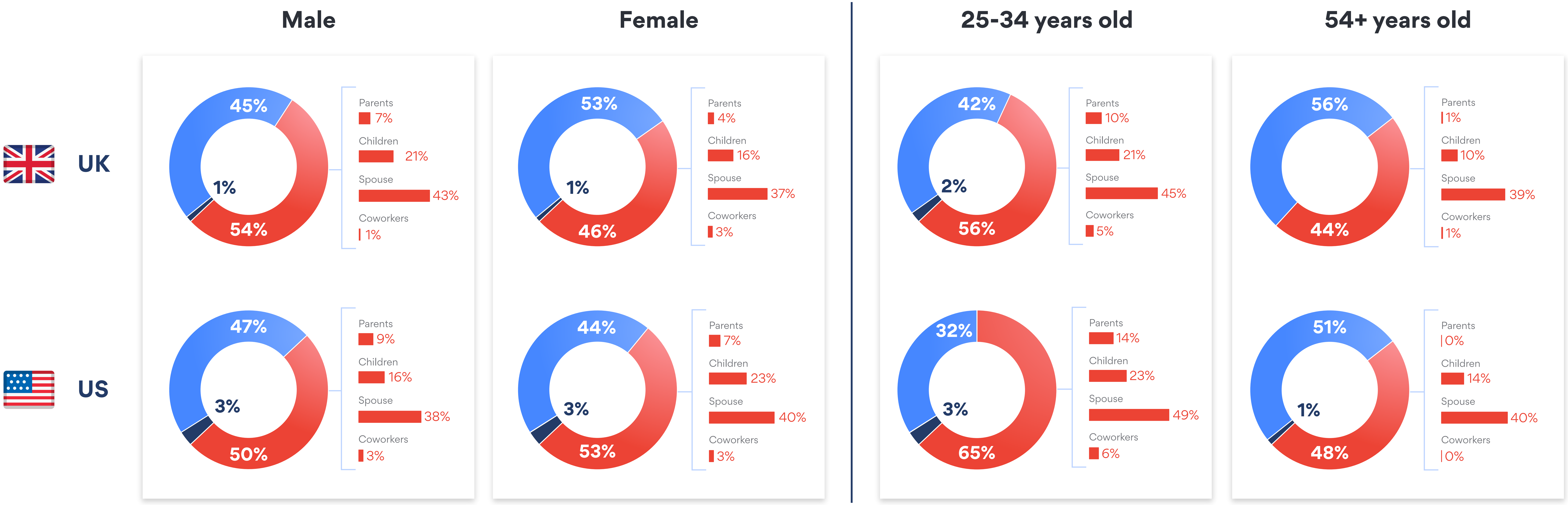




Who are people sharing their devices with?

(by age and sex)

● No one else has access to personal computer ● Use public computer ● Other people have access to personal computer



Sharing habits

Gender-based sharing habits seem to differ by location. In the US, women are more likely to share their device (56.39% do, compared with 52.94% of men), whereas women in the UK are significantly less likely do so (only 46.66% do, compared with 55% of men). This flipping of sharing is echoed in who shares most with their children, and, to a lesser extent, with spouses, but across both the UK and US men are more likely to share devices with their parents. Having more children tends to mean greater likelihood of sharing devices with them, but it also means people are more likely to share devices with their spouse as well.

So, larger families tend to be more sharing. In the UK, people identifying as Black or Asian were more likely to share devices with parents and children. Similar results can be seen among those identifying as Black, Asian, or Hispanic in the US, but they share not only with children and parents but also co-workers. This might be contextualized by the comparatively lower income of those groups among the people surveyed (with the exception of those identifying as Asian in the US). While income by itself was not a consistent indicator of device sharing, when combined with race, it highlights the need to think intersectionally about what motivates or influences different groups' behaviors when it comes to devices.

But there is something more worrying than sharing devices with close family or colleagues, who we generally trust. And that's using public computers. Again, income by itself is not a defining factor for relying on public devices, although factors like higher education may hide other forms of privilege as students make greater use of, for example, devices in libraries. So, we need to think carefully about which groups within a certain context are more likely to need secure and private access to shared devices. The terms and context of sharing devices are important, demonstrating the different ways sharing can occur and the need to build better collective protections into our skills, behaviors, and the technological systems on which we rely.

Personal relationships

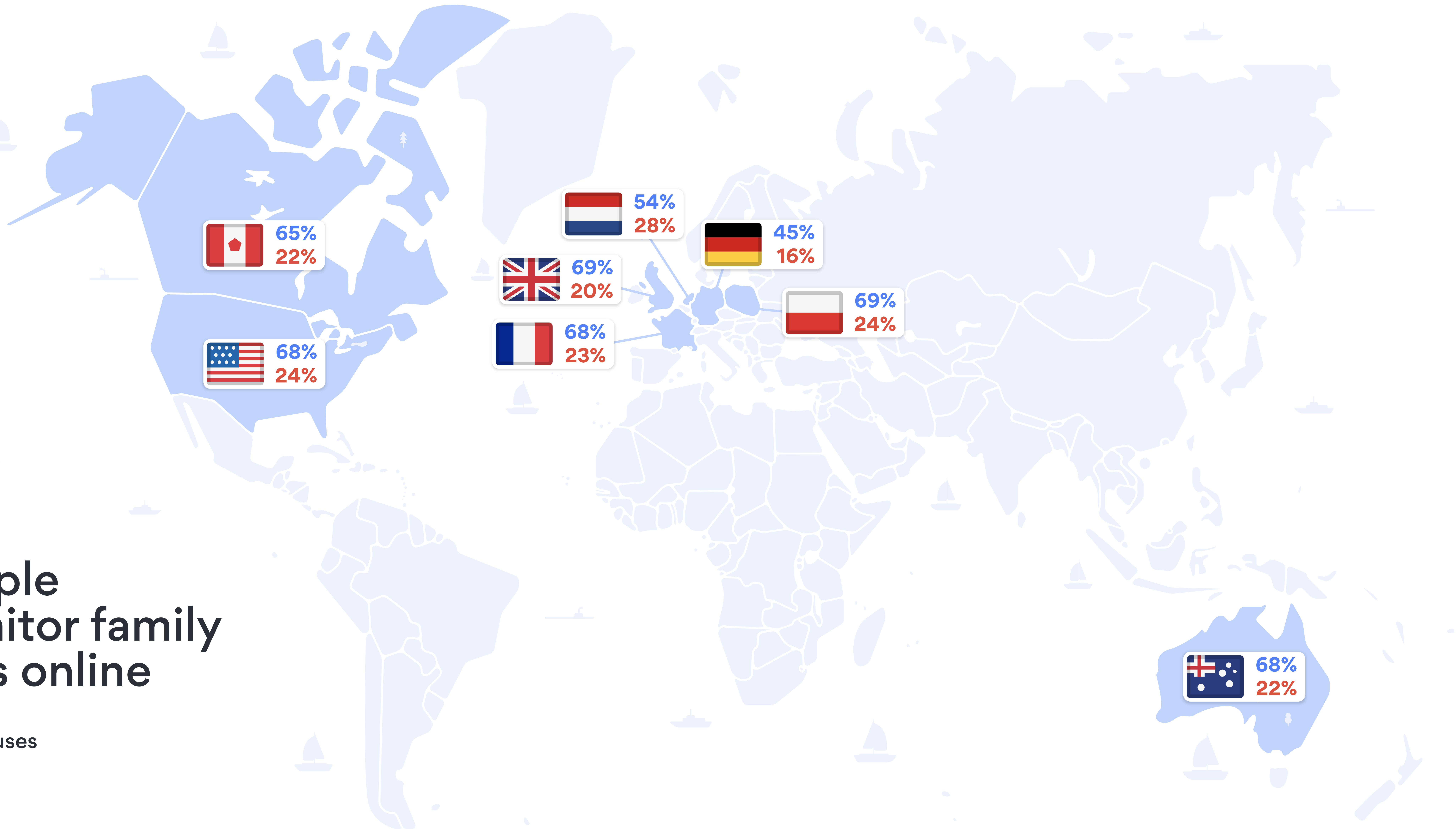
Sharing devices doesn't mean we care less about them or about the data on them. In fact, it's often the reverse. People who share their devices with their children are more likely to rate personal photos kept on their devices as extremely valuable. They are also generally more likely to consider different types of files kept on their devices (including medical and tax records or work documents) as extremely valuable. The increased value of information on devices shared with children echoes the increased responsibility parents have in supporting their children to access digital resources safely. The relationships around shared devices are important, as are the ways in which we share and the trust or support we show one another.

How does this sense of responsibility for our family's privacy manifest itself? We asked people in eight countries to what extent they monitor what their children and partners do online. We have seen that our spouse is the person most likely to have access to our personal devices, but what knowledge do we have about what they do online (whether on our device or their own)? Even in the notoriously privacy-conscious Germany, almost 1 in 6 at least sometimes monitor what their spouse does online, while more than 1 in 5 do so in the US, Canada, Australia, the UK, France, and Poland, and more than a quarter in the Netherlands. This could suggest something about the levels of trust or about wanting to know what is happening on our devices and networks. And, if online activity includes a lot of social media, it may also be that what our partners do online is also about us. Privacy and personal data are often not just about an individual. They tend to show our relationships, whether that's through what we post online, who we search for presents for, or even the metadata of who we message most often.

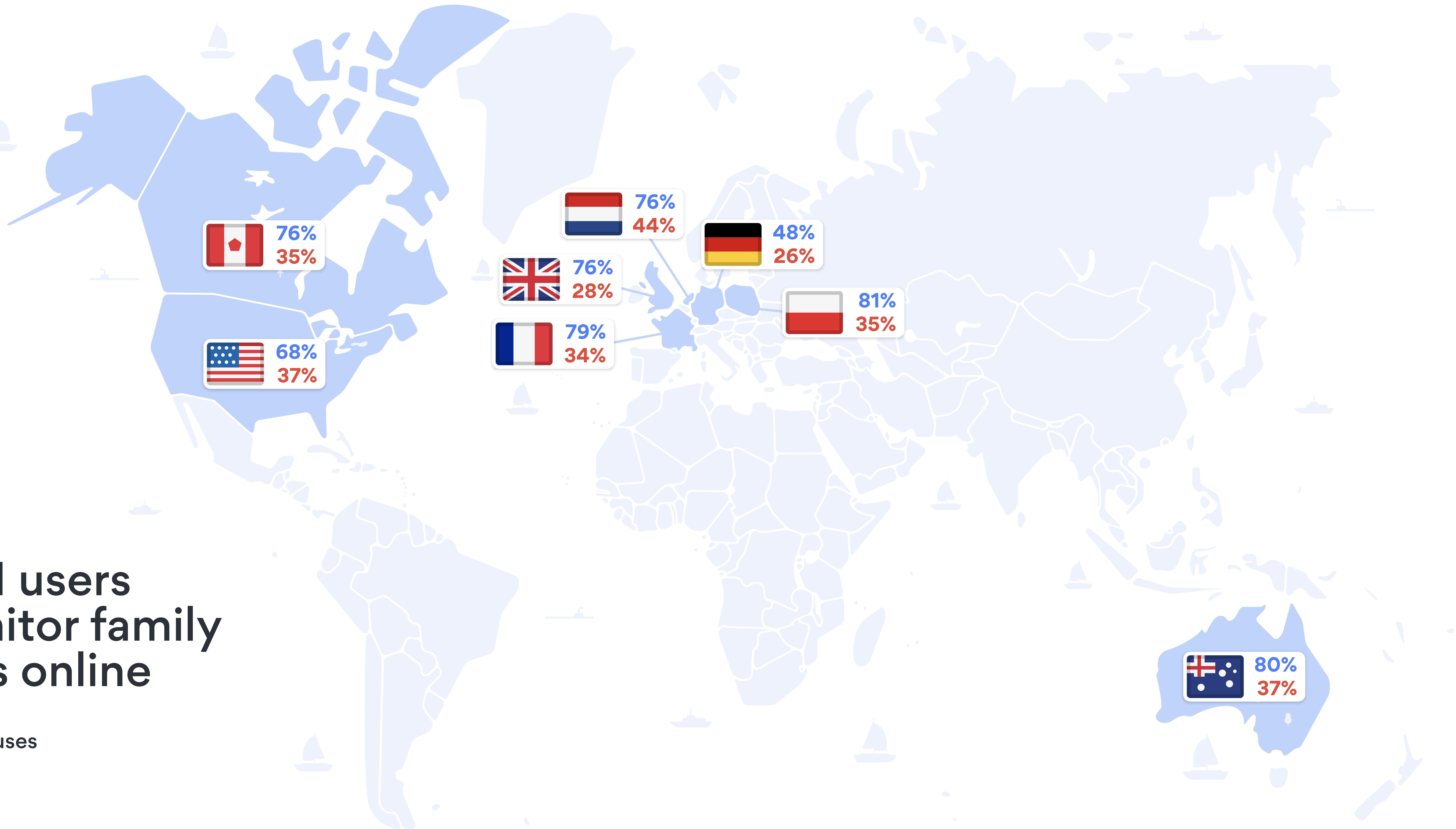
We bear a particular level of responsibility for our children, and this is no different online. Around two-thirds of people in the US, Canada, Australia, UK, France, and Poland monitor their kids online at least some of the time, while more than half do in the Netherlands. Perhaps, unsurprisingly, under half of parents in Germany monitor their kids online as well. With children, the issue of monitoring gets more complicated, as people might feel different levels of responsibility depending on their children's age and the types of content they are allowed to access. There is also a potential split between taking responsibility for what your children are doing and for teaching them how to be safe online. Again, this might be different for different ages. For example, you might check what YouTube videos are being recommended to your toddler to avoid Peppa Pig turning into animal slaughter. With your teenagers, you probably want to talk to them about issues like privacy, safety, and consent so they can manage their online life themselves. And, of course, this is an ongoing process as children get older, and each parent-child relationship will develop its own balance and boundaries of monitoring and teaching.

% of people who monitor family members online

● Kids ● Spouses



% of VPN users who monitor family members online



● Kids ● Spouses

Across all countries, people with children are more likely to be VPN users, and VPN users with children are more likely to monitor what they do online (except the US, where it evens out). To a lesser extent (but not so with the Netherlands or Poland), those with partners are more likely to be VPN users. We can infer that having other people to think about makes you more likely to consider extra methods of protecting your devices and data.

Children are learning how to be online, and in the process are learning about interactions with other people in different contexts. So, it's important to promote healthy and safe norms and expectations. Watch too closely, and you risk showing them that surveillance is normal. Avoid difficult conversations, and you potentially leave them under-equipped in digital life. We want to protect our children while enabling them to grow. Children are already more privacy-aware when it comes to hiding things from their parents. Counter to the assumption we tend to hear that kids don't care about privacy online, they often just have more immediate priorities like parents and teachers. Selecting a balance of privacy tools, showing respect for your children's privacy, and a supportive environment can be helpful in empowering them to grow as individuals.

Privacy and data literacy are collective practices, things we do together, and it is important to support one another in productive ways. Tools such as VPNs, privacy-preserving search engines, and other cybersecurity technologies can be a useful support for building families and communities of better privacy.

Work and personal devices

It's not just our families we share devices with. Sometimes our colleagues have access to our devices too. In the US, people working in more senior positions — from supervisor up to director — are more likely to share their devices with colleagues. In the UK, this is true of supervisors and middle managers but less so for higher-up positions. The increased sharing by management could be due to the need to share information quickly with their teams or even because they often rely on assistants and other supporting staff to sort out practical issues. So, it might make sense to temporarily hand someone your device to show them something or ask them to do a quick task.

On the other hand, it could also be due to management having greater access to devices, or access to better devices. It's not really surprising that the most sharing positions in our surveys appear to be HR Managers in the US and Chief Technical Officers in the UK, which makes sense given these roles' specific focus on working with people or technology respectively. Or it could be due to the growing trend of BYOD (Bring Your Own Device) — not just in businesses but also in education, where, for those who can, it makes sense to bring their own device to allow more resources for providing them to those who can't. But this raises particular concerns of access, privacy, and security for children.

There are also freelance or gig-workers to think about, who may have to provide their own tech and for whom work and personal time can already be very blurred. There are many reasons why personal devices might be used at work or shared with colleagues. But this can lead to a blurring of contexts that might compromise the privacy and/or security of our devices and data.

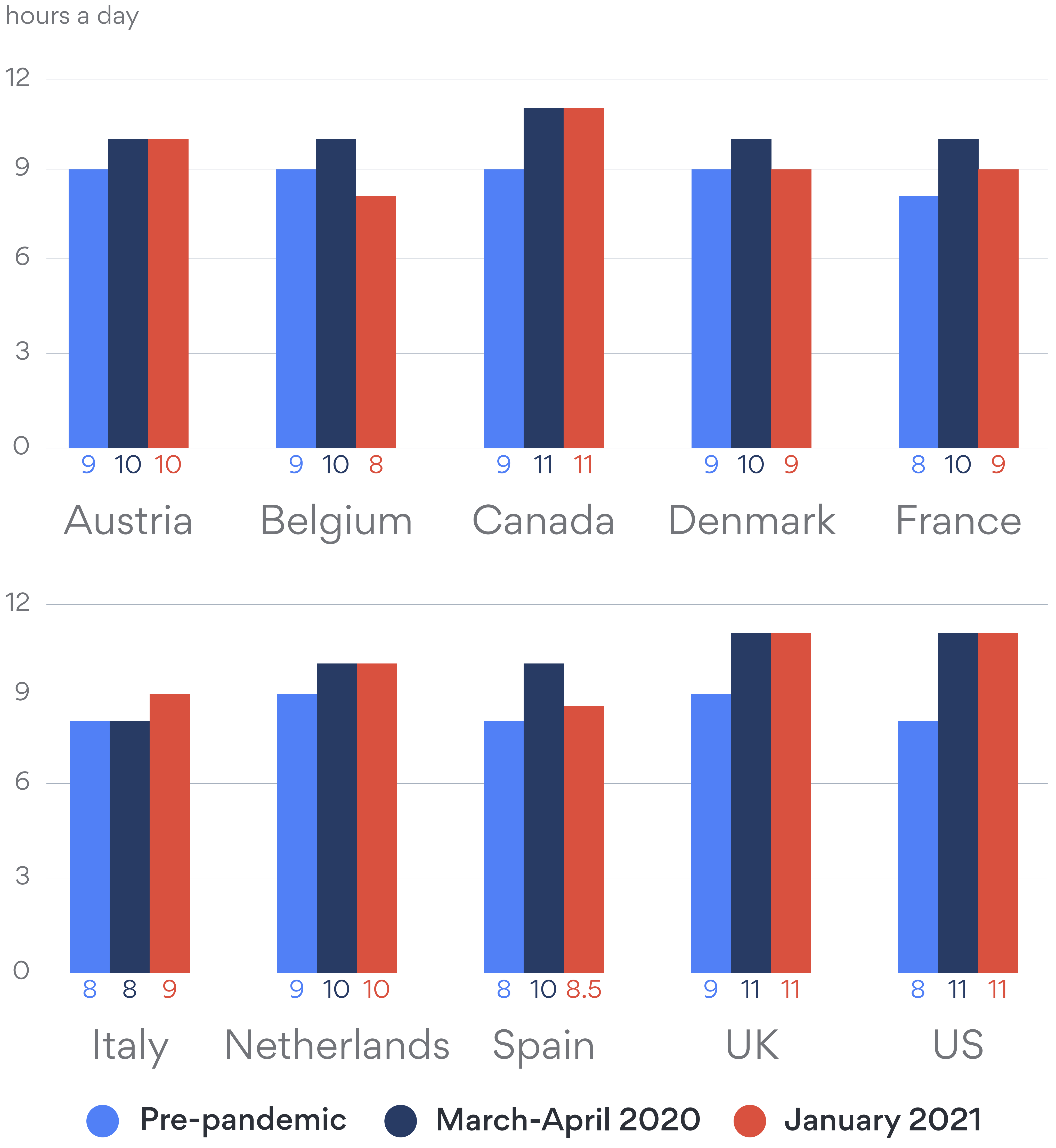
It's not just at work that there is a crossover of devices. The pandemic has radically shifted what work and private mean for our time and space. This has knock-on effects for our devices and digital habits. Organizations rushed to get their employees set up not just with devices but also access to work networks, and all these things needed securing in ways that an on-site network or immobile devices like desktops don't necessarily need. Our research showed that business VPN connections didn't just increase in the number of users during the pandemic, but the hours people spent connected to work also increased. We can use this data to show the extension of the work day by an average of 2.5 hours, and there's little to no disconnection at lunch. But with children and partners at home, the personal will also overlap with work time (perhaps, this is why people felt the need to work longer, including on holidays). With the increased pressures many people have had, such as caring for family or home-schooling children while still trying to get a full work day in, divisions will inevitably be broken down between work and personal time.

Working from home means working more for most people

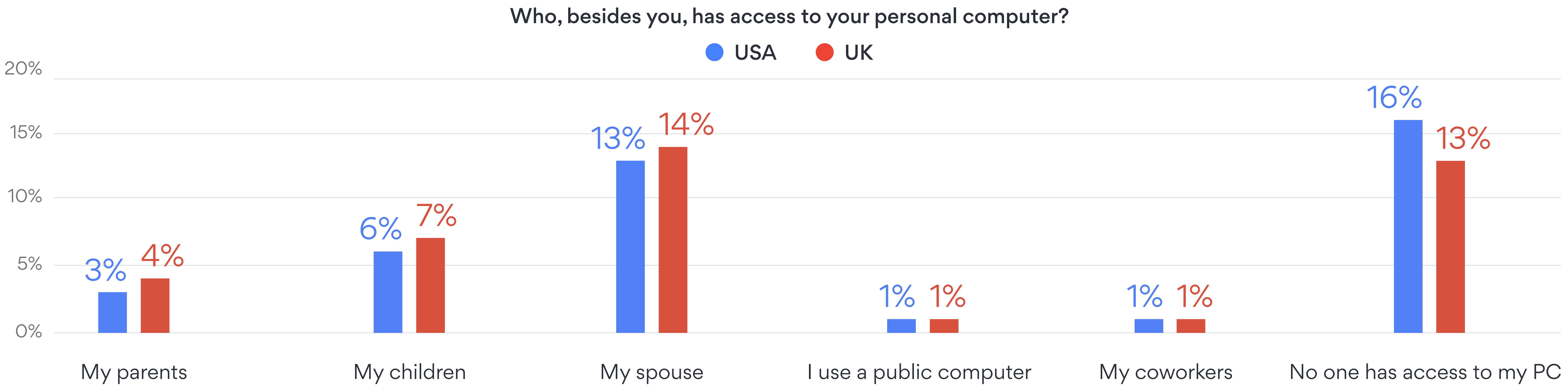
Working from home has impacted not only our work patterns or home offices. The extension of work into home life has implications for working conditions and the mental strain of the pandemic. But the extension of work tech into home offices and home networks also has implications for the blurring of personal and work devices and data.

Lockdown aside, how often do we check work emails on our personal phones? Or quickly work on files on our own laptop to meet a tight deadline? Over 30% of people keep work-related files on their own computers. And only half of these have sole access to their device. Spouses are the biggest group with access to devices holding work files, but it also includes children and parents, as well as a small number of co-workers.

Working from home means working more for most people



% of people who store work-related files on their computer



We can use work files on personal devices as another indicator for the increasing level of crossover between work and personal tech needs. Businesses may need to think not only about setting up work VPNs on work devices, but it is likely to be in their interest to provide employees with personal VPNs and other privacy-enhancing technologies. For example, almost 1 in 6 people who store work-related files on their computer don't use any form of file protection. If these personal devices were exposed to attacks, it could be work data on the line. This is particularly worrying given that, for example, over half of those surveyed working in government and public administration positions in the UK don't use any form of file protection.

Generally, those in the most senior positions are better at protecting files on their personal devices, with full disk encryption being a popular option providing protection if the whole device is lost or stolen. But, in the US, a quarter of the CEOs surveyed didn't use any form of file protection. And there are also administrative and clerical positions to think about, who may have access to sensitive documents as a matter of routine but may have less access to tools that protect them and their data (40% of those surveyed in the UK who were administrative staff didn't use any form of file protection).

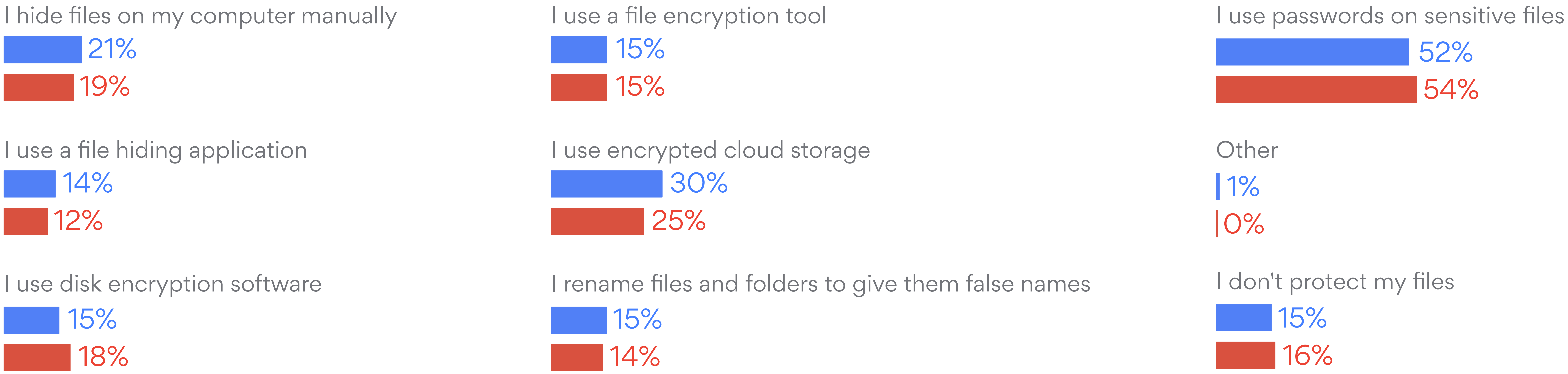
Everyone should be afforded the same protections, as many different people have access to sensitive or important documents at some point. Again, it may be in businesses' best interest to support employees' personal data habits rather than trying to maintain a disappearing separation between work and personal tech.

How do you protect your files?

● USA ● UK

There are clear risks for businesses here, but the implications of the blurring go both ways. People's home networks and devices might be under increased likelihood of attack with the new levels of working from home, as attackers hunt for potentially weaker protections. This could put their personal data at risk as well. Privacy and security are, now more than ever, a matter of collective responsibility and making sure everyone has the right tools and skills at their disposal to make sure everyone's data is protected.

% of people who store work-related files on their computer



How do people secure their devices and data?

Protecting not just ourselves but the people we share our devices and data with is something for us to think about. But it hardly ever features in privacy/security narratives or considerations around digital skills and technologies, which tend to focus on individual protections or separate out business and individual interests. Sharing devices puts a twist on how we secure our devices and data. But how do we protect ourselves at the moment? To answer this, we also need to ask: Who are we protecting ourselves from? Different contexts of sharing and privacy create different priorities and different needs and might require different types of response.

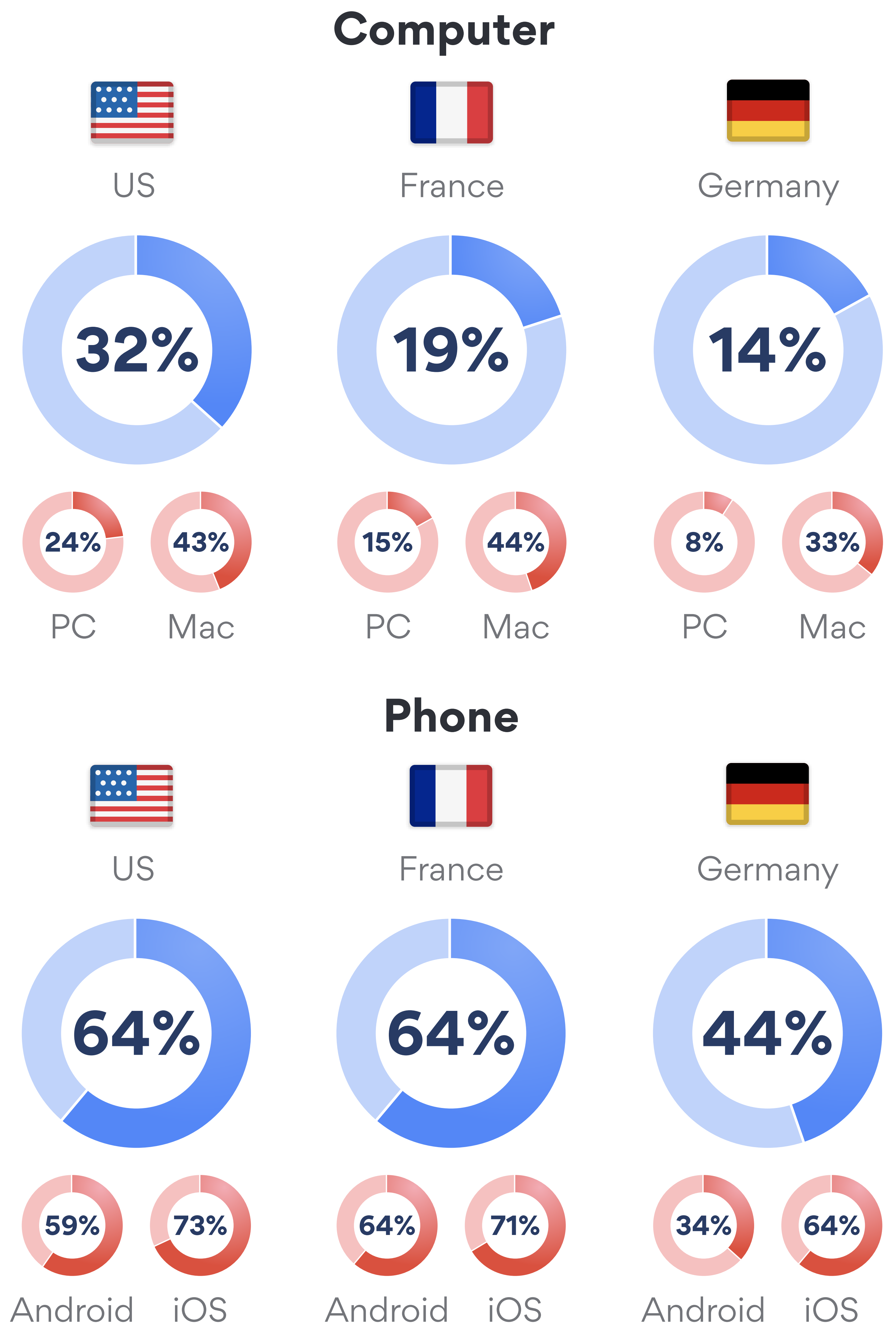
For example, we might expect antivirus to be standard these days. But, of the people surveyed in the US, 32% still do not have antivirus on their computer, although France and Germany were significantly better (19% and 14% respectively).

This is also quite different between PC and Mac users. Only 24% in the US didn't have antivirus on a PC (compared with 15% in France and only 8% in Germany), whereas 44% of Mac users in the US and France and 34% in Germany had no protections. Our narratives can take a long time to change, and the perception that Macs are less prone to being attacked can lead to lack of protections when significant numbers of Mac OS vulnerabilities have been discovered over the years. It also shows the need for different tools, which is why NordVPN is integrating an additional security functionality.

The numbers without protection are even higher when we compare personal computers to mobile devices. 64% of people surveyed in the US and France and 44% in Germany did not have antivirus protection on their phone. This breaks down to 59% of Android users in the US, 64% in France, but only 34% in Germany, versus iOS users at 73% in the US, 71% in France, and 64% in Germany. Again, Apple users are perhaps operating under a false sense of security, but the assumption that any smartphone is automatically secure can be dangerous.

And it's not just operating systems. There are major disparities between devices and ranges, with cheaper Android devices often coming pre-filled with privacy-infringing bloatware. And our phones are in many ways more personal than computers — we have them on us most of the time and increasingly use them for a wider range of activities, particularly at the crossover of family, work, and social contexts. So, we should be taking extra precautions.

# people without antivirus on PC compared to phone

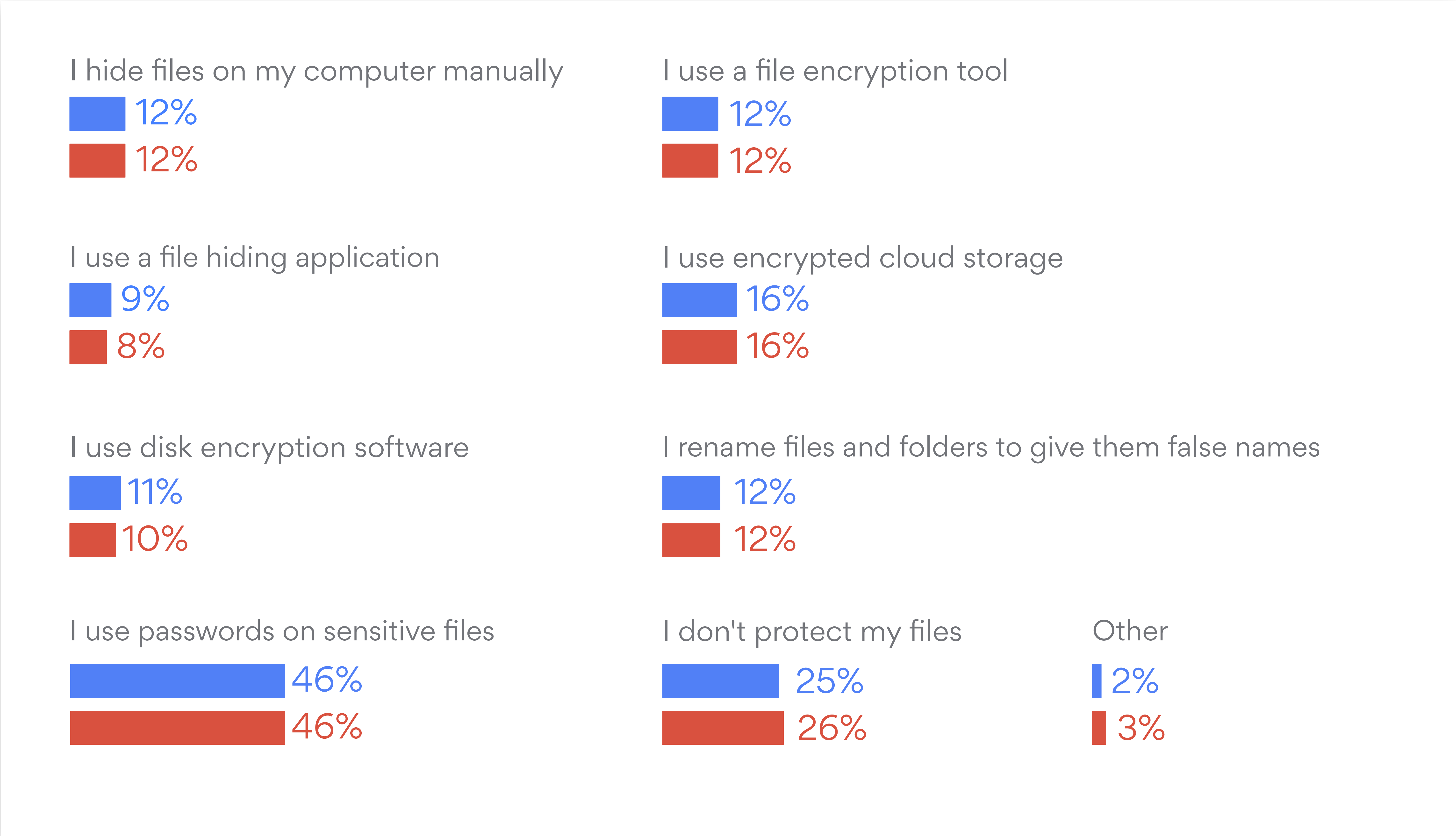


What about files? Well, this might depend more on who we are trying to keep data safe from. Different techniques suit different purposes. In our survey of encryption habits in the US and UK, around a quarter of people didn't use any file protection. But use of methods varied. If you're hiding things from other people using the device, then manually hiding or renaming files might be sufficient, and these techniques were each used in about 12% of cases. The most popular method of file protection (a little over 45%) was using passwords on sensitive files, relying on the protections afforded by, for example, Microsoft Excel for built-in encryption. This spans other users on the device as well as some limited protections from external attackers. Bearing external factors in mind, full disk encryption use was around 10%, which can help protect all your data if the device is stolen wholesale. How many of us keep data remotely in the cloud? But only around 16% use encrypted cloud storage. We are relying on trusting the privacy and security of cloud providers, as well as how secure our connection to them is when uploading or downloading. Which protections suit you will depend on who is using your devices, what kind of files you keep on them, and what methods you might have readily available. Improving our knowledge and the tools we can benefit ourselves and our families.

How do you protect your files?

● USA ● UK

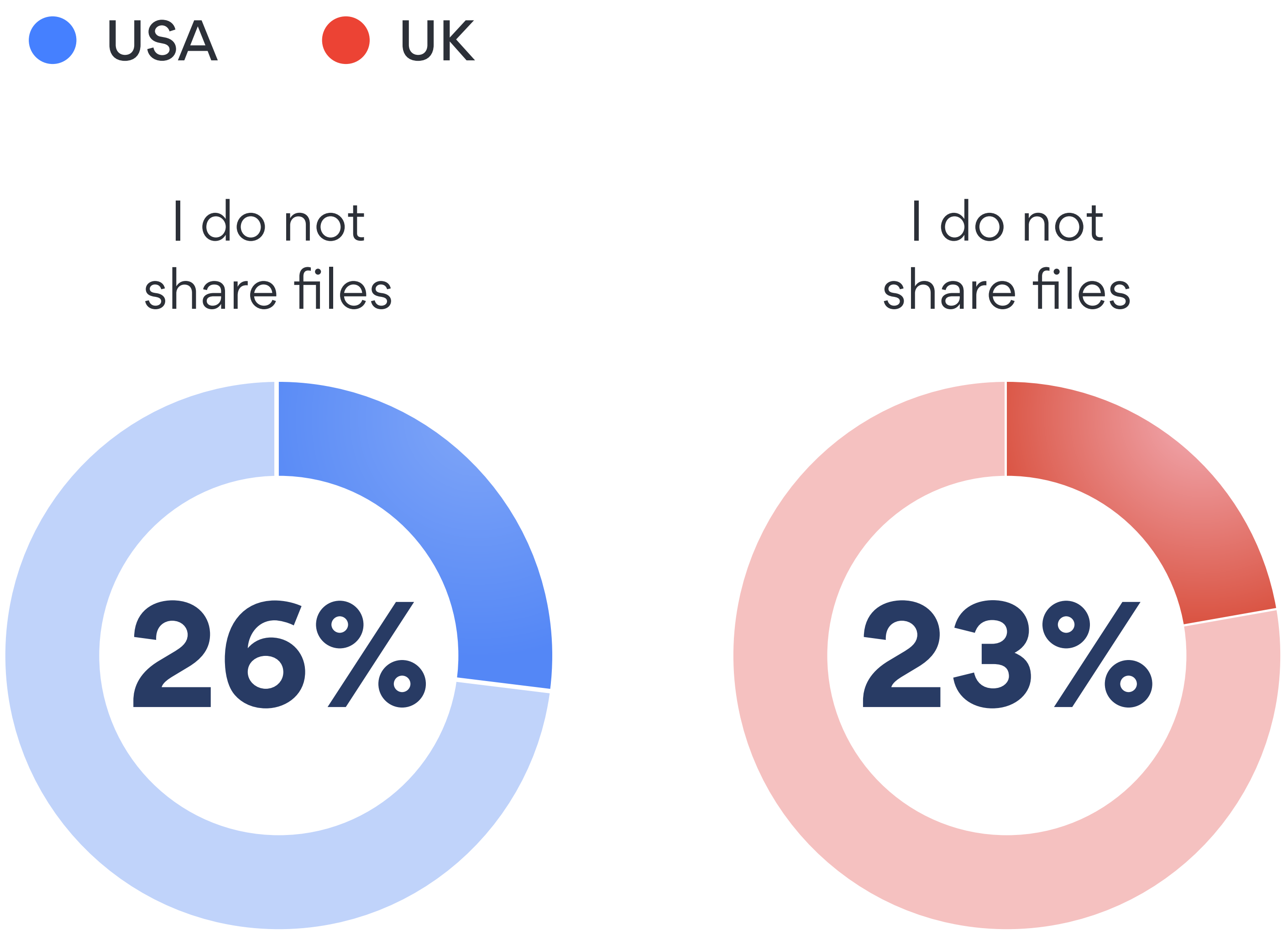
File encryption habits in US/UK

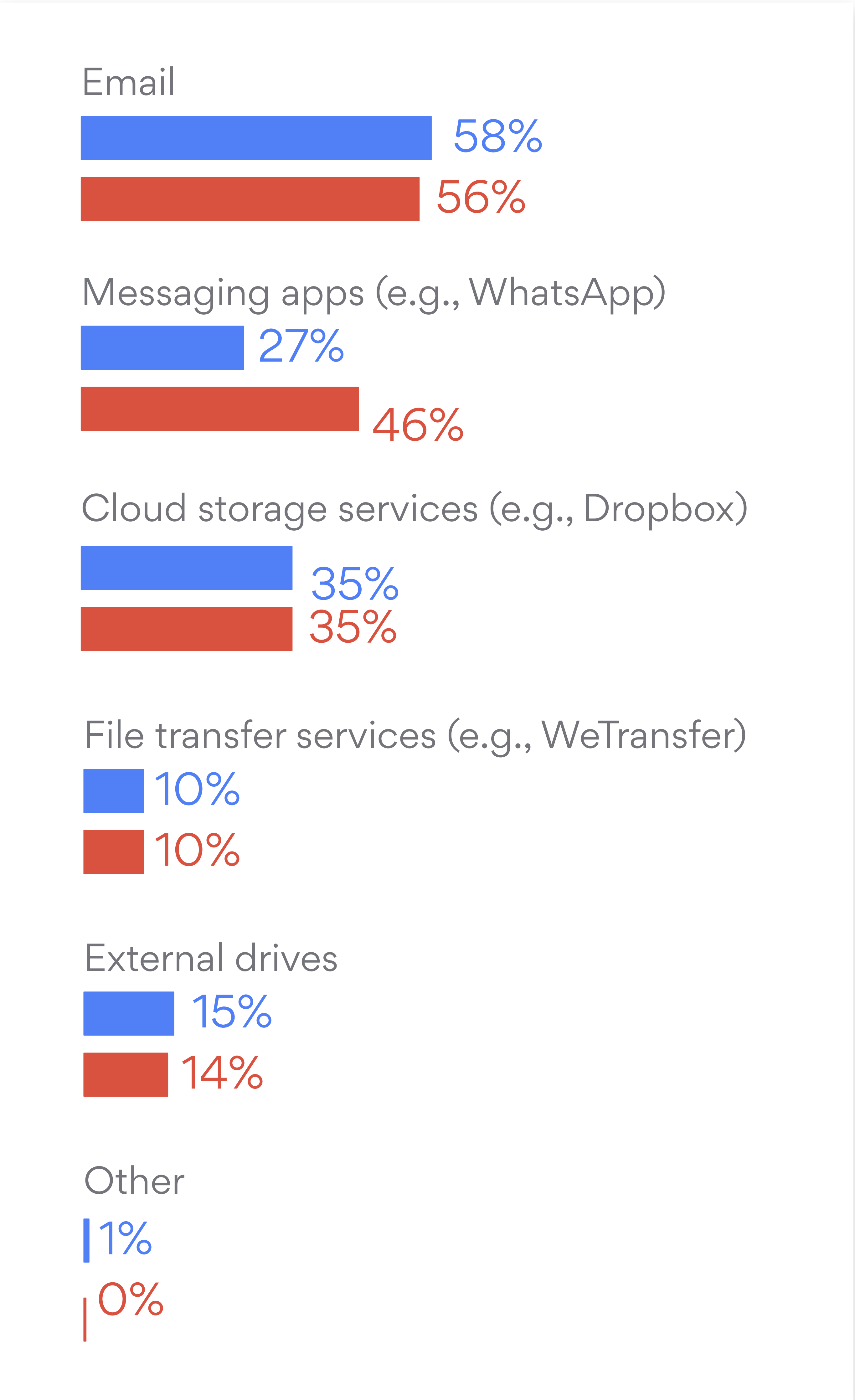


These are issues of responsibility and managing risk for the contexts we care about. But what about sharing outside a device? What methods do we use for sharing files? Email is unsurprisingly the most popular at over 50%, but this is often unsecure, relying solely on https for a secure connection and trusting our email provider. Similar concerns apply to cloud storage, used by just over a third of people surveyed. Messaging apps like WhatsApp, which offer better protection with end-to-end encryption, were more widely used in the UK (46%) than the US (only 27%). Even these methods rely on the privacy policies of your message service provider, with some being recently called into question.

External drives bring their own risk of loss, whether the drive itself being misplaced or stolen, or the data being corrupted. Again, different techniques serve different contexts, but most need better protections. And the metadata of whom and when we are sharing with can lead to further leaks, showing the need to establish secure connections like VPNs, particularly for business uses. It's never just about the data itself. Who we are sharing with and what medium we use for sharing can reveal information about our habits and potential points of attack. Adding extra protections like a VPN can help keep our traffic private and secure, as long as it is with a company that can be trusted, which is why NordVPN, for example, maintains a strict no-logs policy that is regularly audited. Methods like this cut across different contexts, like storing family photos in the cloud, kids watching videos online, or sharing work files with colleagues, and so can provide incredibly useful tools for protecting devices that have shared users and shared uses.

What do you use for file sharing?





Keeping your devices and your family safe

How good are your privacy and security knowledge and habits? The Nord Security National Privacy Test tests your cybersecurity know-how. It's useful to have a regular check of our habits to make sure we are doing what we can. But what measures can we take to keep ourselves, our work, and our families safe? As our blog post on 20 bad internet behaviors to avoid outlines, there are some simple tricks we can do:

- Use different secure passwords for your accounts. A password manager can help you with that;
- Keep devices and apps up to date;
- Make sure sites you visit use https (check for the padlock symbol in the address bar), especially if you're giving over important information like credit card details;
- Make sure your networks are secure. For example, by changing the default Wi-Fi password to something more unique;
- Use a VPN, especially if you're on public Wi-Fi, where you should be extra careful;
- Be cautious when clicking links, especially in emails.

Perhaps, most importantly, share advice with your family, especially if you share devices. Whether it's tips for keeping your data private or awareness of the latest scams, privacy and security are something we should be doing together. Check out our Education Hub for more information, tips, and advice.

Businesses can take extra precautions and are often in a position to support employees with better infrastructure. Business VPNs are important, particularly for the new needs of secure home working, and NordVPN Teams has a handy checklist to help. Make sure your employees have the knowledge and tools they need. And think about how you can support your employees on their personal devices and personal online activities as well. Remember — it's in everyone's interest for better security and privacy.

Conclusion

Sharing is normal. It is an essential part of life online and is the reason technologies like the internet were created in the first place. But we all have certain expectations about what information we are sharing, who we are sharing it with, and what they use that information for. And it's not just data that we share — it is devices and networks too. We regularly share devices with family members like partners or children, and even if we all have our own devices, it is normal for other people to have access to them at least some of the time. There are also devices that are inherently shared, like the smart devices tied more to the home or office than to any individual.

Sharing devices creates some additional concerns for privacy. Our devices aren't necessarily as personal as we think they are, and there are issues around what other people are doing on or with our devices that might put everyone at risk. But it can also be an opportunity. By sharing responsibility for privacy, we can better protect everyone in our family or workplace. Setting devices up with appropriate tools (like VPN, password managers, encrypted cloud storage), improving everyone's awareness and skills, and taking collective action to support each other has massive benefits for everyone. We need to take extra care when sharing devices, but, if we are aware of the steps we should all be taking anyway, then we can establish better privacy norms together.