BIZCOMMUNITY

What will happen to digital privacy in the upcoming decade?

By Marco Preuss

1 Apr 2020

Your data is now everywhere. Your phone. Your smartwatches. Your smart home. And if something goes just a little bit wrong - it will disappear in just one click.

Marco Preuss is Director, Global Research & Analysis Team, Europe at Kaspersky

With digitalisation continuing to grow around the world, many services are becoming more and more data-driven. The collection of users' personal information improves consumer experiences and delivered services, yet also poses additional online threats and risks.

The past decade has demonstrated several cases proving that sometimes it is not only a risk but a certain danger. With that in mind, we reflect on what could happen with a privacy hazard in the 2020s.

#1 Regulations arise, allowing advanced security and control

As we see it now, governments will continue to excerpt stricter control over user data and tighten security. This may be blamed on intensifying terrorism and instability in the world and worryingly wide access to users' personal information from businesses.

#2 We expect to see risks

While the rationale behind the above is clear, enhanced access to user data naturally implies many risks, such as unauthorised access and consequently compromising privacy or even leaking information.

The biggest challenge posed to regulating parties will always be constantly adapting regulations at the same speed new technologies are developed. We currently don't see a huge trend in companies changing their behaviour in dealing with user data.

The only improvement is that users are being asked to give their consent over how the data is used, and it is now mandatory in many countries. We don't see any strong trend in adding real-life security for protecting sensitive user data. Moreover, there's already a growing gap between regulation and real-life practice.

With the latter being much faster – we have toothless regulations as a result.

The advice here is simple – try to limit your data-sharing patterns online. Avoid exposing your data and sensitive information unless it is necessary.

#3 Counter-tools will emerge, fueling the cyber-battle for privacy

The trends outlined above will clearly drive privacy protection technologies. Tech-savvy users will know their way around such solutions, with more technologies arising to circumvent them – inevitably extending the arms race in this area.

At the same time, users will become more proactive when it comes to their privacy, and this will influence higher demand for password managers, VPN services, tokens for two-factor authentication (2FA) and special privacy solutions.

However, protection mechanisms like 2FA tokens and password managers are just at the endpoint, while attacks and misuse are often happening at the backend. These tools are good and needed to protect the local environment but do not protect against attacks and abuse of the utilised systems (e.g. the cloud).

VPNs are useful to protect against data collection in certain scenarios (like real IP-addresses, geolocation) but still do not protect against voluntarily shared data by users with services (e.g. Google, Facebook etc.).

The advice here is to keep an eye on new ways to protect your privacy and use only trusted solutions. Invest your time in exploring the issue because the security of your privacy is not just a new luxury – it is as essential as brushing your teeth every day.

#4 Viral entertainment apps aren't going anywhere

Amusing online tests and other applications that gamify the processing of user data harvesting and collection will still be around as they bring engagement to owners and entertainment to users. However, while compromising their data – and this is why their enduring popularity should not stay unnoticed, nor underestimated.

The advice here is to, if possible, not to take part in unnecessary applications of the kind and do not share your private information. Nothing comes for free, and if something does – it is mostly paid for with your discreetly collected data.

#5 New practices and methods of protection against disinformation and attacks on democratic processes will emerge

Actually, these attacks have happened for many years already – and there is no reason for them to stop. The upcoming decade will not only open yet another round in the political pendulum of global society due to a new US presidential election – new technology for fake visual and audio IDs already exist.

These two factors will bring undesired attention and abuse from all sorts of parties. The good thing is that where there is action, there is also reaction – and we definitely can count on new methods to withstand the risks of public manipulation.

What does it have to do with privacy? If you’re not vigilant, your data could be exploited in these manipulated visual and audio IDs. To protect yourself from this, do not expose yourself if you are not sure you are dealing with a proven and truly secure platform.

#6 IoT vendors will start investing in security on a new scale

The last few years have been very turbulent for the cybersecurity industry. Hacks and specific malware, data breaches, geopolitical tensions and disinformation campaigns across the globe – you name it - have all caused challenges.

We think that this sort of activity will push vendors to a new level of collaboration for the sake of security. Amazon, Apple, Google, and the Zigbee Alliance have announced the creation of a new working group to develop and promote the adoption of a new, royalty-free connectivity standard to increase compatibility among IoT products, with security as a fundamental design tenet. Hopefully, others will follow their lead.

In that sense, the 2020s will be an interesting decade filled with both challenges and opportunities.

ABOUT THE AUTHOR

Marco Preuss is Director, Global Research & Analysis Team, Europe at Kaspersky