Privacy and security aspects of 5G technology

The fifth-generation mobile network (5G) does not just boost current mobile communications network performance, but also enables the convergence of communication networks with another foundation of the digital era – computing. The entanglement of these two aspects defines a complex ecosystem, composed of heterogeneous stakeholders, technologies, methodologies and best practices. While this ecosystem offers new opportunities for digitalisation (a key reason 5G technology is seen as a cornerstone of European resilience and is one of the seven flagship areas of the European Recovery and Resilience Facility), the ecosystem's complexity nevertheless poses unexplored and unexpected concerns, risks and challenges. This is particularly the case for security and privacy aspects, which threaten the feasibility of future 5G development. As well as the need for awareness of these risks, these factors might lead to the need to address vulnerabilities that may leave personal data or sensitive information at risk.

An increasingly large share of the ballooning global population accesses services via the web. Indeed, accelerated by the Covid-19 pandemic and driven by the billions of connected internet of things (IoT) devices, worldwide traffic peaked at over 700 terabits per second in 2020. More than 73% of this access took place 'while on the move' (i.e. through mobile phone networks or wireless connections). The sheer size of this traffic overburdens and strains existing networks, making a case for their upgrade. The 5G network is expected to respond to these growing needs in Europe and beyond. The intended outcome is for 5G to connect everyone and everything, anywhere. A reduction in the digital divide and the provision of unrivalled network performances should deliver positive ripple effects throughout society, ranging from efficient and sustainable manufacturing and logistics processes, to reliable and resilient facilities for healthcare and safety services.

To ensure this outcome, 5G provides for a two-pronged strategy: first, a 5G connectivity platform across different sectors of society can enable use cases that could disrupt traditional processes and improve humans' quality of life by making living environments smarter and safer. This improvement would be unattainable without the active and responsive IoT devices of today. Second, the network can be re-envisioned through 5G, as a dynamic infrastructure that adapts to the changing requirements of applications (and not vice versa).

The unrivalled capability and flexibility of 5G technology has been made possible by a decades-long process of convergence between computing and telecommunications, as well as by the 'softwareisation'
of communication networks, their components and their functionalities. Whereas previously, each discipline focused on a complex system with specific stakeholders, rules, processes, technologies and experiences, a new ecosystem has been formed by merging them. Here, telecommunications and computing collaborate to enable new scenarios, and stakeholders in the two systems can extend their business offering and compete with each other. Throughout this epochal shift, a wide debate on privacy and security issues has unfolded. The complexity of the 5G ecosystem requires deep insight into its main components, and especially into how the components affecting privacy and security interact with each other. A recent STOA study, on which this briefing is based, makes an impact assessment focused on the identification and analysis of the new potential risks, challenges and opportunities that 5G technology entails with respect to privacy and security, drawing on a research conceptual map divided into four categories (privacy, security, technologies, ethics/politics).

The methodology for this impact assessment is built on three pillars: (i) a document-based analysis of specifications, regulations and scientific literature to identify the risks, challenges and opportunities related to innovations of 5G technology with respect to privacy and security; (ii) stakeholder involvement, built on a quantitative analysis of information from a wide array of stakeholders, and on a qualitative analysis based on feedback from a group of experts; and (iii) case studies that illustrate the risks, challenges and opportunities identified.

The analysis identified six privacy concerns, six security concerns and two ethics concerns, permitting a gap analysis of the current technical specifications (which are still under definition at the time of writing) and regulations. On this basis, the study puts forward 27 policy options for potential enhancement of the next releases of technical specifications and regulations. These policy options are organised into three dimensions (privacy, security and ethics), as set out below.

1. Policy options for privacy risks and challenges

1.2 Transboundary data flow and 5G

- **1 ’5G ecosystem parties establish controller/processor in the European Economic Area’** – Any organisation involved in the EU 5G ecosystem should establish a controller or a processor in the EEA and should encourage its own legal departments to perform a transfer impact assessment (TIA).
- **2 ‘Adopt hybrid data location storage’** – A potential alternative path could adopt a hybrid approach where personal or sensitive data is stored locally, close to and within an individual’s national boundaries (edge cloud), with less-sensitive data stored in the cloud.
- **3 ‘Adopt a personal data wallet’** – A personal data wallet – a digital area where individuals can access data, provide consent and receive notifications – could be considered a fundamental tool for exercising the rights to privacy and data protection.

1.3 High-speed data rate

- **4 ’Revise data breach notification deadline’** – New legislation could consider a downward revision, based on higher speeds and data rate, of the time limit to notify a data breach.
- **5 ‘Establish continuous consent’** – 5G technology providers need to establish advanced dynamic and continuous consent processes and notifications, to ensure individuals’ rights to rectification, erasure and notification.
- **6 ’Adopt state-of-the-art protection mechanisms’** – 5G technology providers need to adopt the most advanced encryption systems, and anonymisation or pseudonymisation techniques, and to design high-speed alert systems in case of data breaches.

1.4 High traffic density and location accuracy

- **7 ’Consider 5G impacts in the final version of the proposed e-privacy regulation’** – EU policy-makers could consider the impact of 5G technology when approving the final version of the proposed e-privacy regulation.
Privacy and security aspects of the 5G technology

1.5 Large number of connected devices (IoT)
- 8 'Consider a standard validation framework' – New European legislation should consider the impact of a human-unmanageable number of connected devices, and how data matching, correlation and information extraction is to be performed to profile and track users through their devices.
- 9 'Consider the impact of more attractive devices and services' – The European legislator should consider the impact of the more attractive devices and services available from the media and entertainment sector, and that most of the users are minors.

1.6 Internet protocol (IP)
- 10 'Observe evolution of non-IP networking' – New European legislation should observe the evolution and outcomes from the European Telecommunications Standards Institute (ETSI) Working Group on non-IP networking, which addresses new 5G services.

1.7 Privacy as an open issue
- 11 'Monitor privacy aspects' – New European legislation should monitor the evolution of the privacy issue in the next specification and deployment of 5G technology.
- 12 'Ensure data sovereignty' – The 5G ecosystem requires the cooperation of several stakeholders located worldwide. Implications for data sovereignty should be considered in EU Member States’ regulations and strategic plans (93 % of experts agreed).

2. Policy options for security risks and challenges
2.1 Network 'softwareisation' and flexibility
- 13 'Consider standards for network components' – Standard rules and procedures should be considered to reduce ambiguities between network components.
- 14 'Consider compulsory security controls' – Security controls cannot be considered optional in an architecture specification that claims to adhere to security-by-design principles.

2.2 Multiconnectivity and device density
- 15 'Monitor the evolution of multiconnectivity' – Service providers should monitor and frequently report on the evolution of multiconnectivity and related protection mechanisms, to evaluate trends in attacks and the efficacy of protection.

2.3 Protocols and interoperability
- 16 'Facilitate collaboration to contribute to new protocols' – Stakeholders should make a common effort to contribute to new protocols, to introduce a game-changer in cybersecurity.
- 17 'Foster the resolution of interoperability issues in new protocols and regulations' – Regulators and standardisation organisations should consider interoperability between different applications within ongoing specifications, standards and regulations.

2.4 Identifiers and encryption
- 18 'Adopt full anonymisation of end-to-end subscriber identity' – Stakeholders should make a joint effort to fully anonymise subscribers' identity end-to-end (i.e. from mobile equipment to core network).
- 19 'Converge to new and standard cipher algorithms' – Stakeholders should make a joint effort to converge new standardised cipher algorithms for wider adoption of 'everything connected'.

2.5 New stakeholders and frameworks
- 20 'Define clear stakeholder roles' – Stakeholders should make a joint effort to clearly define roles, and set up a constant collaboration to agree on the implementation of common security measure standards.

3
2.6 Cybersecurity standards

- **21 'Accelerate cybersecurity standards'** – While existing cybersecurity guidelines are implemented by service and component providers in line with their internal procedures, 5G should adopt common standards for cybersecurity (87 % of experts agree).

3. Policy options for ethics risks and challenges

3.2 Lack of citizen awareness of the impacts of 5G on ethical aspects

- **22 'Provide democratic access to information about 5G'** – Democratic access should be provided to an adequate amount of information on 5G ethics impacts.
- **23 'Promote critical thinking about data practices in the 5G ecosystem'** – People’s awareness and critical thinking should be nurtured in the context of digital and data literacy within lifelong education projects, as well as in schools.
- **24 'Produce an ethics regulatory framework for 5G'** – A tailored regulatory framework for applied 5G ethics (in the same way as there are other kinds of applied ethics, such as AI ethics, robo-ethics, etc.) should be produced at the EU level.

3.3 Technology and use of personal data

- **25 'Adopt indicators to measure the multidimensional societal impacts of 5G'** – Improvements promised by 5G and related technologies should be evaluated against key societal indicators, such as energy efficiency, wellbeing and life expectancy, environmental footprint, and reduced harmfulness to human beings (87 % of experts agree).
- **26 'Promote accountability, trustworthiness and reliability of actors in the 5G ecosystem'** – The accountability, trustworthiness and reliability of 5G and related technologies (e.g. AI, IoT, robotics, etc.) should be considered in the regulatory framework for the implementation of 5G verticals (e.g. e-health, smart cities, energy, etc. – 87 % of experts agree).

We can conclude that with 5G we are facing another epochal shift in the history of technological innovation, where human values and technical knowledge seem to be progressively intertwined, opening up questions of opportunity and risk not only for humans, but also for the entire ecosystem.

This document is based on the STOA study ‘Privacy and security aspects of 5G technology’. The study was written by Carmela Occhipinti, Luigi Briguglio, Antonio Carnevale, Riccardo Santilli, Emanuela Tangari and Andrea Iannone of CyberEthics Lab. Srls, at the request of the Panel for the Future of Science and Technology (STOA), and managed by the Scientific Foresight Unit, within the Directorate General for Parliamentary Research Services (EPRS), European Parliament. STOA administrator responsible: Zsolt G. Pataki.

**DISCLAIMER AND COPYRIGHT**

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.


[stoa@ep.europa.eu](mailto:stoa@ep.europa.eu) (contact)


[http://epthinktank.eu](http://epthinktank.eu) (blog)