**FORUM:** GA3

**QUESTION OF:** Protecting individual rights to privacy in the digital age

**SUBMITTED BY:** France

THE GENERAL ASSEMBLY,

*Recalling* that the Internet, created in 1991, has never been under the jurisdiction of the law and can, therefore, be used as any individual sees fit,

*Having examined* that the use of the Internet results in the trade of people’s privacy for the services provided, while also noting that companies and hackers have the possibility of, for example, storing personal data, using the cameras on any given device at any given time and pinpointing the exact location of a certain device,

*Alarmed by* the unawareness of people towards their lack of privacy upon using the Internet and the digital footprint they leave,

*Stressing the fact that* people’s data are stored abroad from where the individuals live, which results in this information falling under said countries' legislations, and that therefore individuals can no longer control or have any say in what happens to their personal information,

*Noting further* that these digital devices and online services are necessary to a majority of individuals on a daily basis, and that there should be clear regulations protecting the privacy of every person wishing to use them,

1. Advocates for the development of adequate and sustainable solutions to deal with the specific challenges of our time by:
   1. requiring the appointment of Data Protection Officers for companies and organizations with more than fifty employees
   2. creating new legal obligations for data controllers to notify data protection authorities (“National Commission for Informatics and Liberties”) in the event of a data security breach, and expanding the role of data protection authorities to include a network of regional offices
   3. conducting Annual Activity Reports to increase data protection and privacy rights of a nation’s constitution;
2. Urges an international version worldwide version of the European Union General Data Protection Regulation (EUGDPR) to be formed which forces all existing organisations to respect their users' privacy, with the aim of:
   1. harmonizing data privacy laws across Europe everywhere
   2. protecting and empowering all EU citizens' data privacy data privacy worldwide (Ecuador)
   3. reshaping the way organizations across the region approach data privacy;
3. Emphasizes the need to further educate people on Internet safety, focusing specifically on unknown topics to the general public, such as but not limited to the digital footprint left by individuals and the dangers of personal data being owned by large corporations and hackers, as well as how individuals can protect their digital privacy, through:
   1. the national media
   2. the education curriculum for children
   3. seminars held for any interested adults;
4. Requests that all functional apps on the market provide users with different variants that they can choose from when downloading them, which should also clearly show that they:
   1. offer users a standard, simplified version which provides users with the basic functions of the app and only uses personal data that is specifically required for these functions
   2. provides a normal version too, which does require users to make a choice between paying a minor fee to download the app and have their privacy guaranteed or getting the app for “free” and allow their data to be used in exchange by the respective corporations, as is currently the case;
5. Encourages that all functional apps on the market be bound to a law which requires them to provide their clients with information about the use of their personal data when using their app, by:
   1. clearly showing in a format that is easy to understand before downloading the app what specific personal data users agree to give to the app and how this information will be used by the app, as part of their privacy policy
   2. having the option that users can, at all times, within the app have the option of seeing where their data are being transferred;
6. Adopts the Digital Republic Act to:
   1. enhance the rights for individuals through the Data Protection Act, which will improve the general rights of citizens on the decision and controlling of their personal data and which forces controllers to give individuals the right to exercise their rights electronically with upheld data (South Korea)
   2. utilize additional information from data users which will:
      1. require data controllers to inform users on the length of time that personal data will be stored or the measures used in determining that period
      2. inform users on the rights of sharing and obtaining personal data through online communication services that will be processed after death, including the right to provide final instructions regarding the methods of grasping personal data
      3. process medical data research and give parent(s) or legal guardian(s) of a minor under 18 the rights to process data under the Data Protection Act, where in the case of certain types of medical research mentioned in the Public Health Code, minors above the age of 15 may object to their parent(s)' or legal guardian(s)' request in accessing their personal data and therefore may exercise the right to access and rectify processed data
   3. enable post mortem rights to privacy for:
      1. citizens, so they can choose how personal data will be processed after death, where civilians will provide instructions for storing or publishing personal data before passing and where general steps are to be taken, enabling qualified third parties or bodies modeled after the Commission nationale de l'informatique et des libertes (CNIL) to take initiative, as well as specific steps are to be taken concerning individuals' instructing controllers on the utilization of data of those deceased
      2. civilians, so they can have the authority to erase data from profiles on social networks or alternative web platforms and where relatives and/or heirs are to protect the rights and data of those who have passed if the decision has not been made by the individual at the time of his/her passing;
7. Conducts the transference of data to non-EU Member States for users who give full consent under the Multinational Data Transfer Network (MDTN) in cases of:
   1. ensuring that individuals have the opportunity to prosecute any infringement on their right to privacy
   2. the protection of the data subject’s life
   3. the protection of the public interest
   4. the need to meet obligations ensuring the establishment, exercise, or defense of legal rights
   5. the consultation of a public register intended for public information and open for public consultation
   6. the conclusion or performance of a contract between the data controller and the data subject
   7. the conclusion of a contract, or the performance of a contract that has either been concluded or is to be concluded, in the interest of the data subject between the data controller and a third party;
8. Utilizes criminal sanctions, issued under penal codes, in cases of violating personal rights to data processing if any of the following are obtained:
   1. data indicating a person’s registration number in the National Register of National Persons, unless specifically authorized to
   2. data without taking necessary precautions in preserving the protection of data
   3. information of an individual under fraudulent, unfair, or unlawful practices
   4. data for direct marketing motives, regardless of objection
   5. medical data, without a data subject’s knowledge of the right of access, correction, or objection
   6. data that directly or indirectly reveals trade union memberships or moral principles of a data subject without consent
   7. automated data from its intended use
   8. personal data for a State that does not belong to the European Union;
9. Asks all nations to enforce the A/C.3/71/L.39/Rev.1 in order to address questions of human rights and create new techniques in improving the effectiveness for the freedom of humans;
10. Further encourages all States to promote an open, accessible and secure communication technology environment so that the wishes for privacy in the digital age can be realised;
11. Calls upon states to impose new legislation that serves as a disincentive to engage in unlawful practices and hinders hacking personal data, including but not limited to:
    1. increasing the penalty for criminal activity of hacking that concerns digital privacy rights, specifically from a 6-month prison sentence with 1,000 USD bail to a 2-year prison sentence with 5,000 USD bail, with the punishable kinds of actions including:
       1. the unauthorized congregation of personal data
       2. the usage of personal data for a unfair or unlawful benefit of any sort
       3. the selling of personal data;
12. Strongly calls upon companies and groups in possession of sensitive private personal data to increase data encryption and higher-technology security firewalls;
13. Instructs states to discontinue the utilization of secret mass surveillance and communications' interception, such as collecting, storing and analysing the data of all users relating to a broad range of means of communication (i.e. emails, telephone calls, video calls, text messages and browsing history), which will be completed through means of:
    1. educating states that this is a violation of personal data rights and that it is not necessary to protect national security, as well as the fact that this causes a threat to democracy as a system of secret surveillance set up to protect national security undermines democracy
    2. banning secret mass surveillance through the punishment of international law, including but not limited to international sanctions; (Poland)
14. Further requests a legal prohibition on selling biometric data to or from parties wishing to gain a financial benefit from it, with the following specifications:
    1. biometric data includes DNA, facial geometry, voice, retina or iris patterns and fingerprints
    2. the data may be kept in the possession of parties utilizing the information for national security and criminal investigation purposes, such as law enforcement agencies, border control or investigation bureaus
    3. the aim of this prohibition is to diminish cases of identity theft, thus avoiding unlawful tracking, theft and monitoring of individuals, thus further combating violations of digital privacy rights.