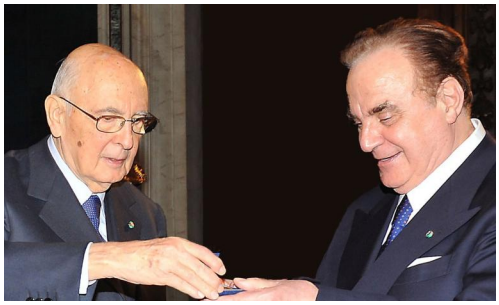
AGENZIA STAMPA QUOTIDIANA NAZIONALE
Prima Pagina News



Primo Piano - *The so-called privacy on the Internet*

Roma - 20 nov 2021 (Prima Pagina News) **At the beginning of last June, 8.4 billion stolen passwords were made public around the world. This large collection - made available to everyone – is named “RockYou2021” and is stored in a text file measuring 100 GB.**

On October 4, WhatsApp, Facebook and Instagram were blocked and hence all sensitive data was logically copied upon the initiative of skilled hackers, of whom our planet can boast anonymous categories of them with superior and exceptional abilities that care little about prime numbers. At the same time, when we connect with thousands of multilingual copy-and-paste websites, they come up come up with a pathetic piece of software that begins with the phrase "We care about your privacy". And in Italy where “amore” (love) has always rhymed with “cuore” (heart), some people think that users - while reading this - take out their handkerchiefs to wipe away the tears of emotion because there is someone who lovingly thinks of them, not realising that, instead, it is tears of laughter. Others say that there are laws to protect the few naive and gullible users, but they forget a proverb and a key to political thinking. The proverb is: “every law has its loophole” and the key is: “laws are a superstructure”. Hence many people are curious to know whether the advertising of the Internet giants respects confidentiality - commonly known with the barbarism privacy - and whether the establishment protects them from the many bad hackers. It is in the interest of the advertising by Internet giants (the establishment) to use each user’s privacy, such as monitoring the chat history (primarily WhatsApp) or the content of calls, because the methods and means to do so exist. Just watch excellent US series, starting with the gripping Mr. Robot and other series, to understand that fresh and young minds are enough to do so. Imagine what scruples the Internet giants may have in the face of ethical values such as confidentiality and secrecy. The risk-benefit ratio of the Internet approach is high, as what is at stake is not Kantian ethics (the superstructure) - which is worth very little - but profits in any currency, whether real or in bitcoins (the structure). There are many ways in which the Internet giants, and private hackers, can control users’ privacy, which are really beyond many web users’ cognition. It is natural that most of our privacy is exposed by ourselves to third parties. We all know that there is a word on the Internet called “search”. Basically, for most people who are particularly active on the Internet it is very easy - for one who is interested in the matter - to discover the forms in which privacy oxymoronically manifests itself all out in the open. Most of the time people do not know how much privacy they expose in a search or in simple surfing. We think it is impossible for ordinary third parties to know who are those who investigate web surfers. I am referring to both decent people and criminals. Before being discovered, however, even a criminal has a right to privacy. The Internet giants and independent hackers have data and systems that we mere humans cannot even imagine. The Internet

giants help the police to catch intruders, saboteurs or other criminals, and can often provide very comprehensive information on suspects, including last address, area of activity and so on. As usual, the problem is a moral - therefore negligible - one: intruders, saboteurs or other criminals previously used to be ordinary citizens. Therefore, as they are monitored, so are we. This is logic not inference. As noted above, the data of the Internet giants and private hackers is more abundant and vast than many ordinary people may think. When the Internet giants carry out data analysis and optimise advertising, the connection by third parties has huge commercial value (the structure). Hence the motivation and skills of the Internet giants and hackers in data connection are astonishing. The vast majority of the Internet users, in fact, have not a deep understanding of all this and may think that an Internet giant does not know about a user or another when they connect to a web page or when they send top secret documents to their counterparts. At the same time, the scarcely skilful people - albeit aware that they are being taken for a ride by stories about privacy protection - reappraise the old systems: personal meetings in unthinkable places; delivery by systems reminiscent of old 1950s-1980s movies. In practice, the cunning incompetent people reverse one of the first absurd statements of the digital age: 'With the Internet, books will disappear'. It did not take long to realise that a book in pdf format is unreadable and its use is only for finding strings in it, i.e. sentences or words. The above mentioned Internet giants often use the same set of advertising and management platforms for different products, whether they are deployed on the households' Internet or in the dangerous and ruinous deep web, which is the part of the iceberg below sea level. If the leader of an Internet giant wants to maximise the data value, he/she asks to check all the "clicked" components of the product, so as to obtain the accuracy of tags - i.e. the sequence of characters with which the elements of a file are marked for further processing – in view of getting the maximum advertising revenue (the structure). At the same time, the mobile Internet (i.e. the one that can be accessed by smartphones, which used to be ridiculously called mobile phones) provides more possibilities to locate people, obviously more accurately than the fixed one at home. Hence those who do not want people to know that they are at home, and go elsewhere with their smartphones, communicate their wandering location, believing they are invisible. In fact, if we think about it, home desktop computers often provide inaccurate data to those who spy on us to find out our tastes and preferences. For example, it happened that some background data showed that 3,000 users, with an average age of 30-40, seemed to be suddenly getting younger. Hence the Internet giant was initially surprised, but shortly afterwards realised that many children were using their parents' computers. To remedy this, the Internet giants - in close liaison with the telephone industry - have gone beyond the primitive and very common scenario of family desktop computers and Internet café shared workstations for young adults, and made parents and grandparents equip their underage children with smartphones. In this way, an Internet giant has a perfect framework for monitoring, controlling and diversifying tastes for narrower age groups, thus obtaining higher profits (the structure) to the detriment of privacy (the superstructure). The telephone industry is grateful for this, as its profits simultaneously rise, thanks to buyers who barely know how to use 5% of the functionalities of the aforementioned device. Many people have not even clear understanding in their minds as to the data connection. For example, if the product/desire/curiosity

A and the product/desire/curiosity B are used at the same time, and A and B belong to the same Internet giant, it is actually very easy for it to establish a data connection mechanism to share any of the user's desires through specific characteristic information. Such a system is used to recommend a product/desire/curiosity or use the same advertisement that the user personalises without realising it. Many people think they are being clever by having separate accounts for different purposes. Apparently it looks that way, but in reality it is easy for the Internet giants to know the relationship existing between these accounts and put one and one together. The smartphone is an even better container for the Internet giant and the hacker to collect unique identifying information from that “device”, such as that user's number, phone book and other data. In fact, while the user is not sufficiently security-conscious, many software installations (i.e. apps) already collect various pieces of information by default. In turn, the identifying information from that device (the smartphone) is used by various software located in remote servers. If the product/taste/desire belongs to the same Internet giant or if the same third-party data company provides technical support, it is actually very easy to obtain the users' data through them. Moreover, when the apps are installed, the phone numbers of the naive unfortunate users have been collected on the remote server without their knowledge. This is because when most people install apps, the privacy authorization step by default is simply ignored. It is annoying for users to read all those long pages and therefore, in the future, the Internet giant will say that it is their and not its fault if it spies on their privacy, because they authorised it to do so! Provided that it is true that if they refuse, it “morally” does as they have chosen. Probably the naive people still think so.

di Giancarlo Elia Valori Sabato 20 Novembre 2021

Verbalia Comunicazione S.r.l. Società Editrice di PRIMA PAGINA NEWS
Registrazione Tribunale di Roma 06/2006 - P.I. 09476541009
Iscrizione Registro degli Operatori di Comunicazione n. 21446

Sede legale : Via Costantino Morin, 45 00195 Roma
Redazione Tel. 06-45200399 r.a. - Fax 06-23310577
E-mail: redazione@primapaginanews.it