ieee.es
Instituto Español de Estudios Estratégicos

Opinion
Paper

30/2013 22 marzo de 2013

*Luis de Salvador Carrasco**

CONTROL AND SAFETY MEASURES FOR CITIZENS: RISKS

This document has been translated by a Translation and Interpreting Degree student doing work experience, LUCÍA RODRÍGUEZ PAJARÓN, under the auspices of the Collaboration Agreement between the Universidad Pontificia Comillas, Madrid, and the Spanish Institute of Strategic Studies.

CONTROL AND SAFETY MEASURES FOR CITIZENS: RISKS

Abstract:

The access from third countries authorities to PNR and SWIFT records is a measure needed to implement the law enforcement against international crime and terrorism. This collaboration has several troubles: the chance to violate civil rights, and on the other hand, the chance to process such data in intelligence activities beyond law enforcement. The above mentioned cases had an impact in the media from the point of view of violation of civil rights, but the second view was subdued. Concerning this topic, it is important to take into account that there are other sources of data about citizens, not only with regard to data communication between states, but other sources managed by private and public institutions, that are more or less open to third parties.

Keywords: PNR, SWIFT, SIS, Europol, Open Sources.

INTRODUCTION

The fight against terrorism and international crime involves the collection of information from individuals, as it can not be otherwise, and the exchange of information between the security agencies of various nations. This way of acting is basic, fundamental and necessary to counter threats that have increasingly global nature and know no boundaries.

Collecting, filtering and analyzing massive data on citizens has a cumulative effect. Obviously, that data has an impact on the reduction of the individual freedoms, regardless of whether it is considered that each control measure can be effective and seen as a "necessary" and "proportional violation" of the rights that our society considers essential.

Spanish Security Strategy (ESS from now on) provides that the immediate availability of information and intelligence has been one of the measures that has significantly improved the fight against terrorism. Therefore, within its strategic lines of action we find that of improving these information systems, including improving coordination between national and international organizations, both through communications with police and intelligence services of other countries.

Now, one might wonder to what extent the security collaboration becomes a vulnerability itself, by allowing third parties to carry out intelligence work on the data given for a definite purpose, diverting its aim. This was brought to light due to the communication of data about passengers on flights to the United States, or the access to capital movements by the authorities of that country.

The ESS is aware of the threat of espionage "by states, groups or individuals, in order to achieve information for economic or political gain," emphasizing that "economic espionage is also of particular importance". The ESS notes that this activity "has adapted itself to the new security, taking advantage of the possibilities offered by new information and communication technologies" and that is necessary "to face the activities of foreign intelligence services."

In this respect, the encroachments in and through cyberspace in order to obtain information have been identified as the main information filtering threat to unwanted third parts. But it is not necessary to resort to information systems violations to access the data sought. In some cases, this information is directly accessible by the governments of other countries when agreements, or factual situations, allow access to data bases. In other cases, access to those databases by other governments, or third parts of a different nature, is readily available for free or on payment.

In the search for more effective cooperation and in order to facilitate procedures for citizens and institutions, public authorities and private entities have automated their files providing access to them through the Internet. The query through the net is a very important qualitative change, as it allows a much more agile and quicker access to a massive volume of data without needing an infrastructure of contacts or link staff. Now that infrastructure is virtual and provides access to information on government employees and government operations, to data on citizens through access to public records, to information on capital movements or passengers and reservations. Each of these records provides a partial view of a part of society, but overlapping ones with another so a fairly complete picture of it can be created.

PASSENGER AND RESERVATION DATA

In relation to the communication of information on commercial flights travelers, it was recently brought to light that data on passengers who fly over US airspace, even if North America is not their final destination, is communicated to the US authorities, which materialized the possibility to veto the boarding of some of them. As a consequence of that, the access of third countries to information on the movement of people is now a current issue.

There are agreements to provide API data, i.e. in advance information about the passenger boarding an airline, to the customs authorities of the destination country of an international flight. This information is not sent in all cases, but only when the country you are traveling to has implemented this requirement to airlines, like the UK. This allows the authorities to know our arrival before getting to the immigration control, in some cases up to 72 hours before the flight. Therefore, API data is not part of the case described in the preceding paragraph, in which data on passengers whose final destination was not the United States was processed by the U.S. authorities.

In both cases, the goal of the information submitted in the framework of the Secure Flight program, is to feed the ATS, the DHS (Department of Homeland Security, equivalent to a Ministry of Internal Affairs) automatic selection system, that for every person that crosses the borders of the United States examines the data collected from it to classify that person in a group of interest, for example, as a terrorist. The flexibility of such systems is large and has a lot of different possibilities of usage, in particular when accessing the PNR records or Passenger Name Record.

PNR records are not equivalent to API data. PNR is the generic name given to passenger file cards generated by airlines and travel agencies in their reservation systems for the purpose

of commercial management services. It archives all the information related to a specific trip itinerary, including data on the passengers as type of food, wheelchair needs, means of payment (if it is by credit card that would be included in their number), passport data, if they are minors, etc. The analysis of all the PNR of a passenger provides information about their behavior, their profile, their religion, the changes reflected in their preferences and about matches in flight seats or other passenger's flights.

The globalization of the reservation system has left four main companies in the sector: AMADEUS, Sabre, Galileo and Worldspan. AMADEUS is the most widespread system in Europe and is used as much to flight booking as to hotel stays, theater tickets, etc. The business group is distributed across multiple countries, the company headquarters are in Spain, and the management of databases in Germany.

In such systems, data from customer profiles is stored without time limit. It is the system user who created the profile, e.g. the travel agency, the only one that can disable or cancel it. When the profile is turned off, the system saves it for 30 days in which the user can reactivate it again, but if after those 30 days it has not been revived, the system proceeds to its final disposal. In general, each airline can access the data that the travel agency has been included in the PNR file, provided that it is involved in the information contained in the PNR (since it is part of the itinerary) and in the service management, as in the case of generating the API data.

Access used by the customs authorities can be made, technically, in PUSH or PULL mode. In the latter one, airlines set a number of parameters (e.g. flights with a particular destination) and the system automatically sends to the destination authority the PNRs that meet the selected conditions. By contrast, the PULL mode enables free access to PNRs by the customs authorities of third countries as if it were the airline itself, without restriction when, for example, the accessed PNR corresponds to a flight with destination to that country.

The PUSH system is currently active for the Canadian authorities, the British ones, the Australian ones and the North American ones under certain agreements with the European Union. The PULL system, that allowed much broader access, has been enabled for the North American, Australian and New Zealander authorities, in the last years. As noted above, this system allowed access to passenger's data without restrictions, regardless of of their destination, and even to records of domestic intra- European flights. This situation occurred because of the pressure that the U.S. government exerted directly on airlines, it broke the plane of equality with the European Union since it allowed realizing and analysis of passengers information far beyond the fact of terrorism prevention, and was brought to light as a result of the pressure from the Estonian authorities when they realized that there was access to data from some prominent people of the same nationality.

FINANTIAL INFORMATION

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a privately held company based in Belgium that provides a network to financial institutions around the world in order to send and receive information on financial transactions in a secure, standard and reliable environment. Among other things, it defines bank identification codes known as SWIFT codes. SWIFT does not facilitate the transfer of funds, but sends payment orders that shall be settled by financial institutions. Its services are used by, approximately, 80% of international transactions, and two thirds of the total volume of such transactions are originated in European countries. The messages are processed and stored in Belgium, and they include information on the origin and destination of the transaction, on the amounts, names, addresses and the values used in the same. The storage is not permanent, but lasts for 124 days.

Access to such data is very interesting when determining the operation of illegal financial networks since it allows building a tree of relationships between persons (natural or legal) that make international transfers. To access these data, the TFTP agreement (Terrorist Finance Tracking Programme), that is a bilateral agreement between the EU and the U.S.A. that allows access to financial messaging data stored by SWIFT to the U.S. Treasury Department upon request to States. The execution of the agreement is currently under the control of Europol, which has the role of checking the implementation of the agreement from the operational point of view. In particular, it controls whether the requests from the U.S. authorities to obtain financial messaging data meet certain specific requirements.

This agreement corrects an imbalance that originated when SWIFT backup servers were located in USA and, therefore, under the powers of the PATRIOT Act, which allowed unrestricted access by U.S. authorities, without the control of the European authorities. This was a situation very similar to the PNR case that arose, in this case, given the regulatory framework changes that stripped a file of protection, instead of implementing a login system. It follows the importance of the study of other countries' legislation, the ones in effect as the proposals, to take preventive measures before a situation as the one indicated happens again.

But not only the data hosted on SWIFT systems have been accessed or are accessible. All U.S. financial institutions must allow access to their records under threat of the Treasury Department freezing their assets. On the other hand, and outside the scope of international transactions, SWIFT data are not the only financial data files accessible by third parts. There are other accessible data, but with entirely different information nature, such as solvency

files, which contain information of the financial status of the people included in them. There are negative files, managed by private entities (ASNEF - EQUIFAX, EXPERIAN, CCI, etc.) or public as in the case of CIRBE . The positive files, as PERSUS, contain those citizens who voluntarily subscribe in order to prevent the fraudulent use of their personal data by third parts to the detriment of their identity , solvency and economic assets, for that aim, data like the ID, phone , checking accounts, etc, is provided. The access to them is regulated, since it is limited to lenders, financial institutions, credit cards, etc, with interests in the stored data and, technically, that data is protected by a number of security measures. The reality is that these files are threatened by third parts access, abuses, leaks and security breaches that leave the information stored in them exposed.

In relation to equity information, there are entities that provide a wide variety of data on legal persons (indirectly natural such as freelancers, administrators and others) to estimate their solvency and that allow looking up through the Internet using the subscription process. Even if the majority of companies comply with the law, there have been some cases of black market data for evaluating solvency and locating natural persons. Those ones also operate with subscription mechanisms and offer merging data from various sources, such as electoral rolls of different years, municipal registers, repertoire of subscribers to telephone services, systematic collection of data from individuals in official gazettes, etc. This allows tracking changes of addresses and other contact information over time, finding matches with other people and establishing relationships between them.

EXCHANGE OF INFORMATION FOR SECURITY ISSUES

The exchange of information of purely police nature is the most interesting and realistic tool for making the coordination of the fight against various forms of international crime effective. It is also one of the aspects that may raise public alarm, although they really are the most protected, both technically and legally, and where the flow of information is more restrictive. That exchange is traditionally performed occasionally through the networks established in the framework of Interpol, Europol and specific forums.

The Hague Programme, adopted by the Council of Europe in 2004, collected the Union priorities for strengthening the area of freedom, security and justice. One of their findings to improve cooperation in the fight against terrorism and organized crime was to launch the so-called "principle of availability", whose aim is to facilitate cooperation between police and judicial authorities of the EU Member States, allowing an exchange of information with the least possible effort, which implies greater ease of access to national databases.

Technological infrastructure for online access to information shared between different European authorities, such as the Schengen Information System or SIS, was already available. The purpose of this system is to have a common dump and an exchange of information mechanism of signing databases of each country in relation to persons wanted for arrest, foreigners for the purpose of refusing entry, disappeared persons, witnesses, people and vehicles under surveillance and stolen goods or documents. The access and dumping of this information is strictly controlled in accordance with the legislative development of the Schengen Agreement, the information available online is very limited, and it is not accessible by countries outside the agreement, providing information through the contact points of the SIRENE offices.

In turn, within the framework of Europol, a number of systems for the exchange of online information were developed. On one side, the Safe Implementation of the SIENA Information Exchange Network, used to manage the exchange of operational information between Europol Member States and third countries with a cooperation agreement, the latter by indirect access. On the other side, the Europol Information System EIS, housed at The Hague, is a database with information about suspects and convicted persons, vehicles, IDs, criminal methods and organizations, for combating all forms of serious international crime and terrorism. This database is accessible by Europol national units, duly authorized civil servants when in specific situations, third parts that may have indirect access through Europol. Future versions of the system will include biometric information, such as DNA profiles, fingerprints and photographs. Finally, we have developed Analysis Files or AWF (Analytical Work Files), which are databases on a particular criminal record, which contains information of criminals, suspects, contacts, collaborators, victims, witnesses and informants. It is powered and accessed by the various national authorities and members of Europol.

The Principle of Availability is further developed in the "Prüm Decision" of 2008, on the cross-border cooperation deepening. Specifically, it aims to improve the exchange of information between the authorities responsible for preventing and investigating crimes by making available the information contained in national files to counterparts of the signatory countries, with restricted use depending on the purpose that justified the transmission. The decision establishes dispositions regarding access to computerized files of DNA analysis, and regarding their creation if they do not exist. It will allow searches through national contact points thanks to a matching system. Also, automated fingerprint identification systems will be established, which will be an evolution of EURODAC and data access to registration records of national vehicles by plate and VIN.

When celebrating large social events, an exchange of data from people who are considered a threat to public order and safety, or who may commit a crime, will be planned, and an improvement in the exchange of information on people within the framework of fight against terrorism will be established.

The technological infrastructure that was available so far was not far enough to meet the requirements of the new decision, so that the 1st December 2012 the European Large Scale ICT systems Agency was launched effectively, it was in charge of the operational management of large information systems in the field of home affairs and its headquarters were in Tallinn, with development and support centers in Strasbourg and St. Johann in Pongau (Austria). It carries out operational management tasks of the Visa Information System (VIS), EURODAC and, from the spring of 2013, the second generation Schengen Information System or SIS II.

The VIS contains information, including biometric identification data, on visa applications lodged by nationals of third countries that require a visa to enter the Schengen area and, therefore, must be accessible by the consular offices or by companies subcontracted for these visa services. The SIS II will provide new capabilities, including the addition of biometric data such as photographs and fingerprints, and new categories. The following steps will be integrating the Registered Traveler Program and the Entry / Exit System, which are part of the Smart Borders strategy. In the same framework, a common European police files index is been developed as well as a way of increasing the efficiency in finding and sharing police records between Member States.

In the judicial area, several Member States including Spain, have already exchanged information electronically on criminal records under the pilot project Network of Judicial Registers. This project has resulted in the European Criminal Records Information System (ECRIS) for the exchange and updating of criminal records and thus making it impossible to escape from your criminal past by moving from one country to another. In practice, the ECRIS is a distributed system of interconnected databases of criminal records of all the Member States. Every country has to keep criminal records accessible, and in the case of sentence to a non-national, the obligation to forward this information to his or her country of origin. The ECRIS contains information on EU citizens, not on nationals of third countries, and that is why the idea of creating a European index of non-EU nationals that have been condemned is being considered.

ONLINE INFORMATION

Both PNR and SWIFT records are maintained by private companies and are subject to international regulations. There are other records that are maintained by the public authorities and third parts and they are accessible through the Internet in a more or less directly way, in some cases due to the momentum of the Law 11/2007 on electronic access of citizens to public services.

Censuses and electoral rolls, both discussed above, are records with limited access to the political parties, to the Administration and to the provision of public services. The reality is that illegal behavior makes this information available to third parts. In the same way, the massive collection of data from individuals through searches in official gazettes (names, addresses, ID's and other appointments, fines and other notifications) is regulated and limited by the parameters of the servers, which does not prevent from irregularly using it in a practical way.

Public records are not new and its existence provides legal guarantees for economic activity. However, their computerization and, above all, the ability to access the Internet in a more or less anonymous and massive way, represent a qualitative change in the way of providing access to such information. Of course, the application of the law 11/2007 speeds up processes to citizens and management companies but on the other hand, provides a huge source of information for anyone anywhere in the world.

Not all public records are freely available through the Internet, some of them are restricted to the existence of a legitimate interest and others are accessible dodging the law or through collaboration with third parts such as agencies on the Internet. Those third parts are, for example, the General State Administration, the Register of Companies, the General Data Protection Register, the Register of Community trade marks, the Register of Foundations, the Official Registry of Accounting Auditors, the Registry of Property and Economic Rights of Senior Officers, the Property Rights Register, the Real Estate Cadastre, the Civil Register and the Register of Vehicles of the DGT (Directorate General of Traffic in Spain). Although most of the before mentioned offer information concerning legal persons, laterally, they provide enough information about activities of individuals, their links to businesses or ownership rights.

In other cases, the requirements for access to records are more complex, require electronic signatures or they are not directly accessible via the Internet, such as, for example, the Register of Wills Advance, the General Register of acts of last will, the Register of Contracts of Death Coverage Insurance or the Register of Intellectual Property.

This is not an exhaustive list of all the registers in the hands of the government or individuals who have a more or less restricted broadcasting. For example, in the marketing field we find the Common File of Advertising Treatments Exclusion, a Robinson list, which contains contact information of citizens, linking postal addresses, email, phone numbers, etc. The participation in it is voluntary and is accessed by accredited companies in the sector.

Many professional associations show their collegiate lists online for free. In the field of supply, we find the CUPS file or Universal Code Supply Point which contains information on energy services subscribers, including billing information or addresses. Without going into the data set that will be available once the Law of Transparency and Access comes into effect, the Senior Officer files are already available for online access in the web portals of the various national and regional chambers. We will not enumerate either the data related to Internet services, telecommunications, social networking, people search services, etc., which deserve a separate chapter. We have to keep in mind that the data on each Spaniard is approximately included in some 300 different databases.

CONCLUSIONS

The exchange of information between authorities of different States, between those in charge of the security and the fight against crime and terrorism, is of paramount importance in a globalized world. Without it, it is not possible the prevention of threats nor the effectively persecution of the organized crime.

This exchange of information has to respect several principles. The first one is the principle of reciprocity in terms of the quality of information exchanged; the second one is the principle of proportionality in terms of the quantity and quality of the information requested. Although those principles are fulfilled, during the exchange of information with other countries there are two factors we also have to take into account: the extent to which the rights of citizens are affected, and the fact that, once the information is out of our control, such States may perform other intelligence tasks beyond those declared, or even send them to third parts.

While this latter circumstance may occur, and therefore it is necessary to take it into account when implementing information exchange agreements, this can not make us lose perspective of what data is already being provided in a more or less openly way and where are the real vulnerabilities through which information is leaked.

PNR and SWIFT cases should serve as an example of how important the constant surveillance of new products, services or regulatory initiatives in the world of information technology must be. Also the needs first to measure the extent of the exchanges that are

being made, then to conduct a critical review of the data that is directly or indirectly accessible to third parts and finally to incorporate technical mechanisms to detect massive and systematic consultations to data bases available in open access. All this taking into account not only the perspective of the rights of citizens, but also its impact on the increase of global security and, thirdly, of national interests.

Luis de Salvador Carrasco[*i]
PhD in Computer Science

*** NOTE:** The ideas contained in the ***Opinion Papers*** are the responsibility of their authors and do not necessarily reflect the opinion of the IEEE or the Ministry of Defense.