Digital Hyper-Transparency: Leading e-Government Against Privacy

*†Ana Rodríguez-Hoyos, *†José Estrada-Jiménez, *Luis Urquiza-Aguiar, ‡Javier Parra-Arnau and †Jordi Forné
*Departamento de Electrónica, Telecomunicaciones y Redes de Información
Escuela Politécnica Nacional (EPN)
Quito, Ecuador.
†Department of Telematics Engineering
Universitat Politècnica de Catalunya (UPC),
Barcelona, Spain.
‡Department of Computer Engineering and Mathematics
Universitat Rovira i Virgili,
Tarragona, Catalonia.
{ana.rodriguez, jose.estrada, luis.urquiza@epn.edu.ec}@epn.edu.ec, javier.parra@urv.cat, jforne@entel.upc.edu

***Abstract*—For a long time, the Internet and web technologies have supported a more fluid interaction between public institutions and citizens through e-government. With this spirit, several public services are being offered online. One of such services, though not a standard one, is transparency. Strongly encouraged by open-data initiatives, transparency is being marketed as a powerful mechanism to fight corruption. Leveraging communication technologies, societies are broadly adopting online transparency practices to give the general public more control over the scrutiny of state institutions. However, a neglected implementation of transparency may cause almost unlimited access to large amounts of information, a side effect we call hyper-transparency. Inevitably, serious privacy risks arise for the individuals in this context. In this work, we analyze the emergence of hyper-transparent practices in Ecuador, a country recently involved in a fierce attempt to offer free access to public information as a fundamental right enabled through e-government. Moreover, we systematically dissect the large amount of microdata released online by Ecuadorian public institutions. Accordingly, we also unveil here a scenario where sensitive information of public employees is openly released under transparency laws. After exposing potential privacy violations, we elaborate on some mechanisms aimed at protecting citizens from such violations.**

***Index Terms*—privacy, transparency, e-government, personal information, disclosure**

I. Introduction

During the last years, there has been a growing concern about the indiscriminate collection of personal information performed by governments and other entities that are natural hubs of such data. Their opaque operation, commonly without permission, creates said concern. However, in the name of transparency, an even more evident threat to the privacy of citizens is posed by public entities enabling e-government.

It is well known that public institutions concentrate a lot of personal information generated from their interactions with most of the citizens. Such information may go from tax payment records to basic service consumption patterns. Moreover, the state holds additional data (e.g., salaries) of a particular group of individuals: public employees, which are a significant part of the population of a country. E-government initiatives encourage a digitized management of all this information, not only to get more out of it, but also to facilitate the inclusion of citizens in the public sphere. Though much of this information can be catalogued as sensitive, being hold by the state, it is a consensus to consider it safe by default. Nevertheless, e-government brings about paradigms such as transparency (yesteryear harder to be massively implemented) that spawn new privacy risks.

E-government entails processing information in online platforms, and transparency builds on the explicit disclosure of data (to give citizens open access to the public affairs). Then, the inherent requirement of these mechanisms to release data (though often partially) generates privacy risks that must be addressed. Such risks arise from the fact that this (potentially personal) information, when publicly released, could be aggregated and processed to freely identify, classify or even track individuals online.

To illustrate the severity of these privacy issues, we analyze them in Ecuador, a small country where the efforts of the state to implement e-government and transparency started just a few years ago. In an attempt to build a more accountable, participative and less corrupt democracy [7], they probably got too transparent public information systems. Sadly, whereas rankings are published to catalogue transparent societies [1], the lack of standard metrics [8] implies that the perception of transparency could be arbitrarily manipulated [9]. Moreover, transparency is tightly related to multiple factors, so finding a tradeoff with privacy is very complex [10], especially when the benefits of transparency enabled by e-government may be overrated [11].

The efforts towards e-government and transparency in Ecuador, and surely in other countries, have been so abrupt that have brought to light many privacy breaches that, although evident, have been extensively neglected by the society. On the contrary, several information management practices, enabled

978-1-5386-2521-7/18/$31.00 © 2018 IEEE

TABLE I
Illustration of information released by public institutions under the Ecuadorian transparency law; in this case, a payroll.

National identity number	Full name	Budget item number	Position	Salary	Additional income	Annual income
1712345678	Juan Manuel Flores Jaramillo	565	Assitant	1000	100	14,200
0200405436	Mara Luisa Castro Carrillo	243	Account advisor	2000	150	25,800
3467135623	Carlos Luis Torres Mera	100	Minister	5000	500	66,000

by law, have been quickly accepted as normal and useful by citizens. We try to shed some light on the implications for individual privacy of these paradigms and we depict various protection strategies.

II. Towards Digital Hyper-Transparency in Ecuador

In general, transparency is related to accountability [7]. To that end, i.e., to be transparent, an entity has to provide information. The more information is provided, the easier is for others to "see" what actions are performed or how decisions are made. Accordingly, being transparent requires disclosing a great wealth of information. In fact, laws enforcing transparency build on a constitutional right of access to public information [6].

It is not different in Ecuador. A law enacted in 2004 seeks for transparency and free access to public information as fundamental rights of Ecuadorians [19]. The jurisdiction of this law covers all the institutions funded by public resources, or "public institutions", and that are required to periodically advertise in the Web what is known as "public information". As expected, the cited law describes public information broadly as "all the information that emerges or that is held by public institutions." Also, for publication purposes, the law specifies the minimum items that must be released online. Some exceptions include confidential information, i.e., information derived from personal and fundamental rights of people.

The Ecuadorian transparency law specifies that at least 15 items of information be released by every public institution through their websites, including, e.g.: the organic structure and legal base, the directory, the salaries of employees, the services offered, and the contractual processes. As a result of this provision, all public institutions periodically release hundreds of files containing information not only about their operation itself, but also about their employees.

We believe that it is not necessary to release so much information, but the law is by no means specific with regard to the granularity of the data to be published. Particularly, we refer to very granular information about unitary entities, such as employees, that certainly hold their own interests and rights. With regard to employees of public institutions, we are struck by the extremely detailed data revealed when enforcing the literal c of article 7 of the Ecuadorian transparency law. As illustrated in Table I, public institutions disclose a dataset containing national identification numbers, full names, budget item numbers, positions, salaries, additional icomes, and the total annual incomes of their employees. We have at least a slight doubt that releasing so much information is useful or even practical for the purposes of transparency.

As suggested in Sec. I, another source of transparency has emerged in the public sector over the last years: e-government. Motivated by a culture of digitalisation of paperwork, some public institutions in Ecuador have begun to offer part of their services online. Putting aside the tax declaration and payment services offered by the SRI (Internal Revenue Service), we talk about simple services that offer electronic certificates, appointment scheduling, online payment, but especially, information.

Let us illustrate by example some of the benefits brought by e-government in the Ecuadorian context. These e-government services turn to be very useful for Juan, an Ecuadorian living in Quito. To meet the annual mechanical review of his car, he gets an appointment through the website of the transit agency (ANT). Even his birth registry can be issued electronically for a cost lower than taking a taxi to the Civil Registry. Moreover, to pay his home phone service bill, Juan monthly checks the invoice on the website of the telephone company and then uses the electronic channels of his bank to transfer the corresponding value. In addition, having commited a traffic violation, Juan finds out the value of his fine and, again, pays it through Internet. Seeking to apply for a job, he finds it very practical to obtain a record of his academic degrees, a certificate of having a job in the public sector (also the institution), and a certificate endorsing his entirely clean criminal record; all of this making a few clicks. As a model citizen, Juan can declare and pay his taxes using his private web account on the SRI website. To top it off, through a module of this interface for payment of taxes, Juan can check, as a hobby, whether or not some of the politicians he supports are also paying their taxes. We depict this hyper-transparent platform in Fig. 1, including some of the public services offered along with the personal attributes that are available to Juan.

The ideal scenario set out in the previous paragraph has a dark flipside. From all the items of information retrieved by Juan in our example, only a few, such as electronic invoices, are offered through a private interface; the rest is *publicly* available on the Web. Namely, privacy attackers can also retrieve his information, as seen in Fig. 1. Also supporting hyper-transparency, a very striking effect is observed from the availability of the information described: for each service, not only the intended information is released about Juan, but also additional attributes. The same occurs for the rest of citizens. Then, not only the amount to be paid for Juan's traffic fines is published on the Web; other details are also released such as the date and place of the offense, a precise description of the infraction, and even a photograph of his car and its plate at the exact moment of the infraction. Juan's transparent

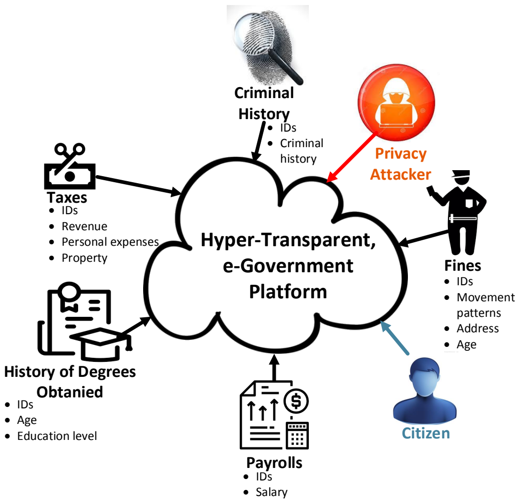

Fig. 1. Hyper-transparent platform publicly disclosing multiple personal attributes in Ecuador.

condition is also evidenced because his phone service bill can be obtained publicly from the telephone company if one knows Juan's phone number or his last names. As with his traffic fines, some other attributes are leaked: Juan's full name, address, debts, telephone consumption time, additional services (Internet, TV), and benefits for elders. As if that were not transparent enough, the telephone company has an open phone book system which, using Juan's last name as search criteria, might reveal all the phone lines he has contracted, their numbers, and the corresponding addresses. Juan realizes that other systems complement his transparent profile with public information about his education (where he studied and when), job, and criminal record. For Juan, this gets closer to the dystopia described in [17] when he grasps that the online system of a ministry, called Social Registry, openly allows anyone to obtain some of the demographic data of a census made in 2014, including: his full name, age, gender, marital status, data of his sentimental partner, and the existence or not of a disability condition. In addition to his salary, Juan's income and housing taxes are also published online. Besides, these systems disclose the address, property valuation, and construction area (for housing taxes).

Table II includes at least 17 unique personal attributes that can be learned about Juan from the ecosystem we have described above. Among the institutions releasing this data are: universities, ministries, or specific public institutions. Most of these attributes are disclosed through specific services offered by public institutions to ease the interaction with citizens. Certainly, a very detailed profile can be constructed about Juan and many other individuals in the name of transparency and e-governance. Thus, the consequence is an hyper-transparent ecosystem that still many people may not appreciate, but maybe it should, because Ecuadorians do care about their privacy [5].

III. Jeopardizing Privacy in the Name of Transparency: The Case of Ecuador

In this section, we analyze the impact of an hyper-transparent ecosystem on the privacy of individuals. We portray the personal attributes openly revealed due to transparency policies and by e-government implementations. Then, we unveil the derived privacy risks in the context of Ecuador.

A. Personal Data: The Raw Material for Compromising Privacy

Personal data means information that relates to an individual. They are structured by attributes, each of which represents a feature or characteristic of a person. A dataset where subjects are individually described using a set of attributes is refered to as *microdata*. Although the values of some attributes (e.g., marital status, sex, address) can be shared among various individuals, the attributes called *identifiers* are pieces of information that relates to a unique individual, thus identifying her. An identifier may be a social security number, a national identification number, a driver's license number, and also a full name. Evidently, any other attribute published along with an identifier (e.g., the salary with the national identity number) can be inequivocally associated to the individual to whom the data belongs. Thus, to protect the privacy of data subjects, identifiers are generally removed from the data before it is released or shared. All other attributes hardly say something specific about an individual when seen individually. However, the combination of very few of them could be so unique that may inequivocally identify an individual within the population of a country [2]. For this reason, these attributes are usually called *quasi-identifiers* and mostly refer to demographic attributes such as age, sex, address, birth date or marital status. Among quasi-identifiers, we can also find other attributes called *confidential attributes* that carry sensitive information of an individual, e.g., salary, religion or health condition. Naturally, if confidential attributes become matched to an identified individual, it may cause her significant damage to her reputation, thus representing a serious risk for her privacy.

Many other attributes can significantly enrich a user's profile as seen by a privacy attacker, particularly those derived from non-conventional data currently generated through the Web. We refer, e.g., to the fingerprint left by a web browser when the user surfs the Web (which could be very unique) [4], the interests and behavior of users, and their movement patterns [12]; all of these attributes can be learned from online user interactions.

As motivated in Section II, plenty of these attributes are deliberately disclosed by public institutions in Ecuador in the name of both transparency and e-government initiatives. Ironically, most of this information is a by-product of the information originally intended to be revealed, i.e., most of this personal data would be unnecessarily disclosed. This information is plagued with identifying attributes. Furthermore, a variety of less specific demographic attributes (quasi-identifiers) are also disclosed, including: age, sex, address, education level,

TABLE II
POTENCIAL PRIVACY ATTACKS AND PROTECTION STRATEGIES ACCORDING TO THE PERSONAL ATTRIBUTES DISCLOSED BY PUBLIC ONLINE SERVICES

Public online services	Objective	Intended information offered (examples)	Personal information released	Potential privacy attack	Protection approach
Tax Payment	To serve as a transparency tool that can reveal the subjects that may be evading paying taxes	Income tax Housing tax Foreign exchange tax	National identity number	Identification	Suppression
			Revenue	Classification	Generalization
			Personal expenses	Classification	Generalization
			Property characteristics	Classification	Suppression
Transparency	To give citizens access to information of public institutions (law)	Employee payrolls Contracting processes	National identity number	Identification	Suppression
			Full name	Identification	Suppression
			Salary	Classification	Generalization
Debt consultation	To give citizens easy access to information about their debts at different public instances	Payment of basic services Payment of traffic fines	National identity number	Identification	Suppression
			Address	Surveillance	Suppression
			Amount of properties	Classification	Suppression
			Age	Classification	Suppression
			Movement patterns	Surveillance	Suppression
Verification	To enable verification of data about people and companies (useful in certain procedures, e.g., hiring or rental of housing)	Criminal record check Education degrees obtained	National identity number	Identification	Suppression
			Criminal history	Classification	Access control
			Education level	Classification	Access control
			Shares in companies	Classification	Accesscontrol
			Work place	Surveillance	Access control
			Marital status	Classification	Access control
			Disability condition	Classification	Access control
			Age	Classification	Suppression

marital status, and even data related to the sentimental partner of individuals. Attributes concerning sensitive information are also carelessly and openly disclosed; we found here economic and judicial data. Some of these attributes are: salary, revenue, shares in companies, properties in general, criminal history, legal proceedings, and even the existence or not of a disability condition.

The Ecuadorian entities holding all this information are multiple. Firstly, all universities have large repositories of degree written works containing full names of the students who graduated there (a large set of individuals). Also, entities offering highly demanded services, e.g., the SRI, commonly allow a match among full names and national identity numbers when querying their online systems. This match enables getting the national identity number of a any citizen whose full name is known, and viceversa. This is as well possible through the payrolls published under the mandate of the transparency law, but the population covered reaches “only” public employees. Furthermore, this individual’s identity number is generally the argument required to query the rest of public online services.

Our analysis just shows that this hyper-transparent ecosystem in Ecuador is full of personal data openly available to an undefined but huge amount of potential privacy attackers. In addition, access to this ecosystem is so open that third party services [13] are freely aggregating the personal information obtained from public online systems, by concentrating all the queries done to such services through a mashup central interface. These third-party services are already making money by offering a consolidated summary of public personal information about individuals.

B. Privacy Risks Derived from Transparency in Ecuador

Given the magnitude of the distortions, it is straightforward to expose the privacy risks brought about by the personal data available on public online services due to the application of the transparency law or an incorrect implementation of the e-government paradigm in Ecuador. In this Section, we characterize some of these risks by explaining the privacy attacks that may derive from the disclosure of the attributes described in Section III-A.

Identification attacks enable an attacker to inequivocally single out an individual among others within a given population, e.g., through an identifier that enables an attacker to distinguish a subject (the victim) from others. Once an identifier of the victim is known, it is relatively easy for an attacker to couple more attributes (e.g., sensitive ones) to the identity of the victim. In fact, personal information is always indexed or associated with identifiers and that way it is usually disclosed. Thus, the identification of an individual increases her privacy risk in the same way that identifying a criminal facilitates tracking him down.

In Ecuador, the risk of identification is high because online documents and interfaces providing public information are also revealing powerful identifiers. In this context, several ways exist to obtain the identifiers of a victim. For instance, with the name of the victim in question, one just has to look at the payroll of the institution where she works to find out her national identity number matched to her name. If the victim is not a public employee, the same matching (national identity number - full name) is still possible through most of the online services offered by public institutions for verification because these services, such as residential telephone bills, are publicly available. These services allow per-individual basis queries that, after receiving an individual’s full name (or part of it) as argument, they return the expected information, e.g., her income tax paid, but also additional information, such as her national identification number.

This *information leaking practice* not only implies divulguing identifiers, but also addresses, movement patterns, economic data, etc. As mentioned, the transparency policies derive in the publication of identifiers, full names, and salaries of citizens. Furthermore, tax payment verification services [14], [15], intended to serve as a transparency tool to expose tax evasion, also disclose individuals’ identifers, revenue, personal expenses, and even property characteristics of people who

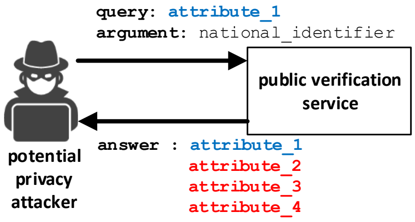
query: attribute_1
argument: national_identifier
public verification service
potential privacy attacker
answer : attribute_1
attribute_2
attribute_3
attribute_4

Fig. 2. Illustration of personal information leaking practice in Ecuadorian e-government platforms.

are not tax evaders. Finallly, services are offered that enable verification of people's data revealing plenty of personal information, such as criminal history, education level, shares in companies, work place, marital status, disability condition and even age. To sum up, these online public services are providing too much information, in fact, more than requested, significantly increasing the privacy risk of these data subjects. This practice is illustrated in Fig. 2.

With so much personal data at his disposal, a privacy attacker has several options to vulnerate the intimacy of a victim after identifying her. Another of such options is *classification attacks*, which seek to group individuals according to a given parameter, e.g., their purchasing power. For instance, with the economic data publicly provided by the SRI, it is perfectly possible for an entitity (such as a credit provider) to catalogue people in terms of the amount of taxes they pay. Then, this entity could refuse credit to people paying low taxes, because they would have a low income. On a more critical scenario, criminals could use this information to turn classification tasks into an outlier detection strategy that reveals prime targets [16] subject of robbery or even murder.

Ambiguous transparency policies and unrestricted access to online systems holding personal information configure a potential *surveillance platform*. Surveillance refers to an ongoing observation of our "movements" which is perfectly possible in an hyper-transparent ecosystem where personal information (including movement patterns, address and work place) are accessible to an undefined amount of privacy attackers. This surveillance could easily become massive because the information disclosed belongs to all Ecuadorian citizens and particularly to public employees of institutions such as the police, the army, the navy, public schools, and even the public health system. Namely, there are millions of citizens and thousands of public employees whose privacy may be compromised.

In Table II we try to systematize the analysis done in Sections II and III by matching the online services offered by Ecuadorian public institutions with the personal information they disclose, the potential privacy attacks built on this information, and the protection approaches we describe in the next Section. From this table, it is clear that most of these services make it possible the match between name and national identity number, which essentially derives in leaking identifers. Also, we see that much of the personal information released makes individuals prone to classification attacks, which might lead to discrimination, retaliation, and blackmail [16].

Ironically, besides risking privacy when implemented poorly, transparency does not seem to be a panacea. Informationt tends to flow only from citizens (lying there the massive risk of privacy) and, when it comes to the great powers, its application is even seriously punished. Thus, transparency does not always lead to more accountability [18] or less corruption. As it happens with Mexico, one of the most transparent countries could still be considered among the most corrupt [18], [21].

IV. Privacy Protection Strategies

The vagueness of transparency-related laws and the careless implementation of e-government platforms are prompting serious privacy risks for a large part of the Ecuadorian population. These are operational flaws in the handling of personal information, so they can be tackled by regulating the flow of this information to the Web. Thus, we next address some strategies aimed at protecting privacy by reducing the amount of personal information publicly released. The technical approaches in this direction build on disclosure control techniques to regulate the amount of information released online, i.e., mainly, generalization and suppression of data. Notwithstanding, a legal framework is also required to standardize privacy protection practices when personal information is handled. The strategies we propose below are aligned with these practical and legal focuses.

Evidently, we first propose tackling hyper-transparency by minimizing the information published online. Data *suppression* is the first way to do it, thus, a mandatory first step should be removing identifiers such as national identity numbers and full names at least from payrolls of public institutions released under the transparency law. This might be applicable immediately because the law edicts publishing the salary *per position* and not per employee (a form of data generalization), as in Uruguayan law [20]. The same strategy could be applied with other documents containing personal identifiers. In this regard, we also suggest modifying the operation of e-government platforms so that useless services are disabled, as well the match between full names and national identity numbers.

Removing identifiers is not always enough to protect privacy, since a few quasi-identifiers combined can have a powerful identifying capability. Thus, if an attacker knows that his victim's data is contained in a dataset (e.g., a payroll), he could take advantage of this property of quasi-identifiers and individuate his victim, even if her identifiers have been previously suppressed. To overcome this risk, *generalization* can be applied to quasi-identifiers to obfuscate identifying combinations of attributes. Generalization implies replacing attribute values with a more general value, e.g., using a range of years (1980-1990) instead of a specific year (1985) when referring to the date of birth of an individual; or publishing a category of salary (high, medium, or low) instead of revealing its exact value.

While the availability of some sensitive information online may be useful (e.g., invoices or pending debts), such utility has sense only for the data owner. Thus, privacy could be preserved by restricting the *access* to this private information only to data owners, by means of an authentication module. On the other hand, there is potentially sensitive data that must stay publicly accessible for verification purposes (e.g., criminal history or education records) and its access should not be restricted. Then, in order to discourage malicious requests of information and to balance the transparency model among requesters and data subjects, the online platform could also ask for information to those making requests in the first place. Namely, e.g., a platform could ask the requester for his identifier, full name, and motivations, before releasing the criminal history of an individual. The data subject could even receive a notice alerting him that he is being investigated and by whom. In Table II, we include some of the strategies that could be applied to protect privacy when each of the mentioned personal attributes are disclosed. Since much of this data is unnecessarily disclosed, in most cases suppression is the more reasonable approach. For sensitive information that needs to be released for transparency purposes (such as salary), we propose generalization. Finally, for information released for verification purposes (e.g., criminal history or education record), we propose access control built on the provision of information by the requester.

Depending on the privacy needs of particular individuals, some services should allow them to opt out from being part of a public data set. Actually, this should be a right of data subjects. This is already possible for the phone book service offered by CNT, but very few people know about it.

Although these strategies are guided by common sense and some margin is given for its application, by the transparency law, none of them are applied by default. Thus, a legal framework to protect privacy could help accelerate their adoption, particularly in a context where hyper-transparency is becoming the norm. Such a legal framework would guarantee and make visible the basic right of individuals to privacy over the still legitimate right to access public information.

V. Conclusions

Transparency and e-government are means to facilitate the interaction among citizens and public institutions that require the disclosure of much information. However, a careless management of personal information may lead to hyper-transparency. It involves an unreasonable disclosure of personal data, which may result in dangerous distortions as shown in the Ecuadorian society. In this ecosystem, at least 17 personal attributes can be learned online about an individual, leading to serious privacy risks. Using this information, both identification and classification attacks can be performed against user privacy, e.g., to match identifers with sensitive attributes. Consequently, several of the online services offered by Ecuadorian public institutions are disclosing personal information in multiple contexts. This yields potential privacy risks that we have presented in this work along with the suggested protection approaches. The main strategies to prevent these privacy risks, before transparency policies are applied, entail well-known approaches such as data suppression and generalization.

Acknowledgment

This work was partially supported by the Spanish Ministry of Economy and Competitiveness (MINECO) through the projects “INRISCO”, ref. TEC2014-54335-C4-1-R, and SecMCloud”, ref. TIN2016-80250-R; as well as by the European Commission through the H2020 project “CLARUS’.

References

[1] “Global Right to Information Rating — What do you want to Know?”, Rti-rating.org, 2017. [Online]. Available: http://www.rti-rating.org/. [Accessed: 25- Oct- 2017].

[2] L. Sweeney, “Achieving k-anonymity privacy protection using generalization and suppression”, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 05, pp. 571-588, 2002.

[3] D. Berliner, “The political origins of transparency”, The Journal of Politics, vol. 76, no. 02, pp. 479-491, 2014.

[4] K. Boda, . Fldes, G. Gulys and S. Imre, “User Tracking on the Web via Cross-Browser Fingerprinting”, Information Security Technology for Applications, pp. 31-46, 2012.

[5] J. Estrada, J. C. Estrada, A. Rodriguez and C. Tipantuna, “Ecuador y la Privacidad en Internet: Una Aproximacin Inicial”, Revista Politcnica, pp. 36-44, 2015.

[6] D. Berliner, “The political origins of transparency”, The Journal of Politics, pp. 479-491, 2014.

[7] C. Bertot, P. Jaeger, J. Grimes, “Promoting transparency and accountability through ICTs, social media, and collaborative e-government”, Transforming Government: People, Process and Policy, pp. 78-91, 2012.

[8] C. Bertot, P. Jaeger, J. Grimes, “Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies”, Government information quarterly, pp. 264-271, 2010.

[9] A. Acquisti, L. Brandimarte, “Gone in 15 seconds: The limits of privacy transparency and control”, IEEE Security and Privacy, pp. 72-74, 2013.

[10] A. Acquisti, J. van den Hoven, “Big and Open Linked Data (BOLD) in government: A challenge to transparency and privacy?”, Government Information Quarterly, pp. 363-368, 2015.

[11] F. Bannister, R. Connolly, “The trouble with transparency: a critical review of openness in egovernment?”, Policy and Internet, pp. 363-368, 2011.

[12] S.Li, A. Ashok, Y. Zhang, C. Xu, J. Lindqvist and M. Gruteser, “Whose move is it anyway? Authenticating smart wearable devices using unique head movement patterns”, 2016 IEEE International Conference on Pervasive Computing and Communications (PerCom), 2016.

[13] Ecuador Legal Online, “Consultas archivos - EcuadorLegalOnline”, EcuadorLegalOnline, 2017. [Online]. Available: http://www.ecuadorlegalonline.com/category/consultas/. [Accessed: 25- Sep- 2017].

[14] Servicio de Rentas Internas, “Consulta de impuesto a la renta y salida de divisas”, 2017. [Online]. Available: https://declaraciones.sri.gob.ec/consultas-renta-internet/consultaNaturales.jsf. [Accessed: 26- Sep- 2017].

[15] Municipio de Quito, “Consulta de Obligaciones”, Municipio de Quito, 2017. [Online]. Available: http://consultas.quito.gob.ec/. [Accessed: 3- Sep- 2017].

[16] T. Press, “Divided by Citizen Wealth Tables”, Nytimes.com, 2017. [Online]. Available: https://goo.gl/3WJMnJ. [Accessed: 2- Oct- 2017].

[17] G. Vattimo and D. Webb., “The transparent society”, Cambridge: Polity Press, 1992.

[18] M. Easton, “UK government 'most transparent' in the world”, BBC News, 2015. [Online]. Available: http://www.bbc.com/news/uk-30883472. [Accessed: 5- Oct- 2017].