sciendo

The new economic good: Your own personal data. An integrative analysis of the Dark Web

Vanesa – Madalina VARGAS
Bucharest University of Economic Studies, Bucharest, Romania
Vargas.vanesa13@yahoo.com

Abstract. *Do you remember the times when the copyright or a patent had no economic value? Neither do I, because this happened more than 300 years ago when the printing activity took place completely free. It was the eighteenth century, when France, England, Germany and the United Kingdom realized that the author was pretty important for the state and the first regulations appeared. Exactly like the intellectual property, in the new era of technology, dynamic change and growing e-commerce, the data with personal character is the newest economic good. More and more studies and journals show that in the near future the personal information will also have an economic value since databases are so important for businesses, but also for other institutions like the police or even intelligence agencies. The current article is the first in a row of a complex research regarding the importance of the personal data in the current economy and its actual value in an organization. Further studies will be needed in order to conclude and create a model for measuring the value of personal data. This first step is a research and a detailed analysis of the current status-quo. The changes that appeared after the entry of the European directives regarding General Data Protection Regulation will be analyzed. Another significant section of the article is a close review of the personal data black market. In order to submit this aspect as clear and objective as possible, further research on the dark internet (Onion) was conducted and prices for clones of credit cards, Amazon or PayPal accounts and cloned personal documents were examined and charted.*

Keywords: Personal data, Privacy, Data pricing, Information sharing, Self-disclosure, Personal data monetization.

Introduction

Personal Data

Personal data is the information related to a person. It does not matter if it relates to his or her private, professional or public life (name, photograph, email, bank information, social media posts, medical information, IP address computer, etc.).

The EU rules on the protection of personal data apply when this information allows a person to be directly or indirectly identified. The EU Charter of Fundamental Rights specifies that everyone has the right to the protection of personal data in all aspects of life: at home, at work, at shopping, when receiving medical treatment, at a police station or on the Internet. 74% of Europeans believe that disclosure of personal data is an increasingly important part of modern life, but at the same time, 72% of Internet users are worried that they have to communicate too much personal data.

Some of the most important aspects regulated through the General Data Protection Regulation are: the right to be informed and to be forgotten, the right to access personal data, the right to design and give clear consent for processing own personal data. Where personal data are obtained directly from the data subject, the operator shall provide at least the following information to the data subject, unless that person already possesses the following information: the identity of the operator and his representative, if any; the purpose of data

processing; additional information such as: recipients or categories of data recipients; if the provision of all required data is mandatory and the consequences of the refusal to provide them; the existence of the rights provided by the present law for the data subject, in particular the right of access, data interference and opposition, as well as the conditions in which they can be exercised.

Any person concerned has the right to obtain from the operator, on request and free of charge with a request per year, the confirmation that the data concerning him / her are processed or not by him / her. For example, the commercialization of property rights between universities and companies (Dima, et al., 2017). An operator is obliged, when processing personal data concerning the applicant, to communicate to him, together with the confirmation, at least the following: information on the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed; communicating in an intelligible form the data subject to processing, as well as any available information on the origin of the data; information on the operating principles of the mechanism by which any automatic processing of data relating to that person is carried out; information on the existence of the right to interfere with data and the right to object and the conditions under which they may be exercised.

Dark Internet

Before starting our study in services and products available in the Dark Internet, some concepts and important definitions must be presented. The criminal underground (another expression for this concept; or Dark Web/Net) is known as a place (websites, forums or chat rooms) where criminal activities are encouraged and industrialized. When we talk about selling or buying personal data, we are aware of the fact that this is a criminal activity. This underground system is a part of the cyberspace.

More specific, Dark net is the dark part of the internet that is not found by search engines like Google or Bing. The hidden part of the network is used by users who value or really need privacy. Since websites in Dark net can not be found by search engines, users need to know exactly where they want to go. However, there are landmarks: for example, so-called hidden wiki. Payment is made in the dark Internet almost exclusively with the digital currency Bitcoin. This way, it is also very difficult to find out who is the author of a payment. The phenomenon made headlines for the first time in 2013 when the US operator of the virtual transshipment point "Silk Road" was arrested. The Leipzig district court sentenced a 20-year-old in 2015 to seven years in prison for selling 914 kilograms of drugs on the Internet. He used darknet forums.

For accessing the Dark net, it is necessary to install suitable software. The most used one is the Tor network. "Tor" stands for "The Onion Router" and is offered as free open software, with which one can search an intricate way through thousands of computers of volunteers.

The data is encased and freed from one encryption after the other, hence the name comparison with the onion. This software directs each data packet - perhaps the request to reach a particular web page - over numerous individual servers. Where exactly this request comes from, can be no longer traced. So an anonymous surfing is possible.

All data is transmitted encrypted. Each server on the way of the data package takes care of a part of the decryption until the user finally gets to see the unencrypted result (through a web page).

This encryption is responsible for the fact that even hidden websites can exist, which can not reach an ordinary browser. Those websites usually "hide" behind a long string of characters and numbers, followed by the suffix ".onion" - this part is popularly referred to as darknet.

A recent report on black hat market from Dell SecureWorks titled Underground Hacker Markets, reveals "a number of noteworthy trends, the most interesting of which is the growing interest in personal data." The major difference between now and 2013 is that the market is booming with personal data information. From driver's license and passports until utility bills and social security numbers, everything is for sale, because it is "a second form of authentication by service providers." The people who want to buy a new identity, the underground market offer all types of services, everything that is needed to commit identity theft.

Literature review

The existence of the personal data on the black market is a reality, and it should not be proven. An integrative analysis of the data sold on the underground market was never conducted before.

However, studies about security breaches were made and the results are quite interesting. Even the behavioral impact of these breaches was closely studied. Huberman et al. (2005) had an experiment where people assigned a value to their own personal data.

Acquisti and Grossklags (2007) investigated the diffusion of private data, where Beresford et al. (2012) conducted an experiment on the willingness of people to pay a value for their privacy. This is how the personal data became an actual economic good, like one's safety. The monetization of this type of data is actual and real. The European Commission itself underlined the idea that more and more business models are based on monetizing data and that the market for consumers' data is growing fast. (Commission Staff Working Document, 2015)

Despite the pure play online business models, when the boundaries between Old Economy and New Economy are fading, traditional Brick and Mortar retailers are starting to engage in various activities on Internet combining the electronic commerce with traditional operation. Moreover, the inter-connected and dynamic external environment of our age organizations are faced with more challenges to achieve success (Fonseca, L.M. and Domingues, J.P., 2017). This attracted the attention of researchers on a new business model that begins to integrate these channels: physical and electronic. (Onete, Vasile, Vargas, 2018)

Many consumers give their personal data in exchange to access different digital services, which are more or less real, but surely not the value of their personal data. This happens for more than 50% of film, e-books, TV-content or game, 77% of streamed events and 30% of cloud systems or antivirus software. (Commission Staff Working Document, 2015)

Another important aspect to be mentioned is the fact that with a growing data economy, the prices for personal data are going down. For example, a zip code is nowadays 0.05 cents worth, while in 2006 its value was 50 cents (M2M, 2013). The reason is not only

the fact that the data collection is now easier and cheaper, but also that a lot of organizations are collecting data and it is widely used for marketing and profiling purpose (OECD, 2014).

Methodology

One complex aspect of the current analysis was the information retrieval and data preparation. The correct extraction and preparation of the data from the dark web will have a major impact on the success of the study. The information retrieval process should be able to gather the latest news items regarding sensitive data available over the internet and all the major price changes during the last period of time.

The birth of e-commerce caused dramatic changes in how the new companies handled their business processes and marketed their products and services, so there was a need for a new referent to capture the newly developed modes of operation (Vasiliu et al., 2016). This research is focused on the existence of sensitive, personal data available for sale and in particular in the underground market and aims to provide knowledge and understanding by exploring the Tor websites.

In terms of methodology, this study is based on a literature review approach in an attempt to assembly definitions and typologies of criminal crews that commercialize this type of data. An average price was calculated for each type of good/service sold on the dark side of the internet: counterfeited credit cards, PayPal accounts, social media accounts, passports and other personal documents.

The purpose of the study is to find the real value of the personal information and to create a model through further articles and studies in order to build a model for measuring each type of sensitive data.

Results and discussions

Integrative analysis of the sensitive data as an economic good on the Dark Internet

In order to monetize stolen sensitive data, there are two steps included. The first one is the actual data theft, the access to someone's credentials. There are different ways to steal personal data: from complex methods like phishing campaigns, malware attacks or hacking databases, up to very simple approaches like promising a "free" product or service in exchange of some personal data. Unfortunately, the second one is progressively present and the consumer is easier than ever to be fooled. Unknowing the real value of your personal data is the biggest mistake made by most of the people.

The second step in monetizing data theft is "the cashout", turning the stolen data into money by sale. The criminal crews exchange the sensitive data in the Dark Internet through the Tor Network hidden service.

One of the most sold "service" that can be found in the Dark Web is the credit card data (IntSight Cyber, 2018). In the last few years, the data bank is more and more available on the dark web. The way in this data enters the underground market is by hacking financial institutions and stealing blocks of account login credentials and credit card information. The recent report from IntSights Cyber Intelligence shows that in 2018 the amount of stolen bank data increased with more than 138% in comparison with the previous year. Furthermore, the credit card data available on the Dark web grew at 149% (IntSight Cyber, 2018).

In the underground market there are two types of goods in the credit card section: the CVV and the "dumps". The first option is an electronic credit card record (it stands for card

verification value) and it gives access to name of the credit card holder, the credit card number, the verification value and expiration date. All the data is necessary for online payments and this type can be used strictly in electronic commerce. The "dumps" are real clones of the credit cards. The magnetic stripe of the credit card is copied when introduced in a hacked ATM (automated teller machine) and collected in a computer. This stolen data is afterwards written onto a new, fake credit card. This second type is used is the physical stores. The prices for each type of credit card are variable, depending on the seller, the country of the credit card holder, expiration date and the most important factor, the balance. Nevertheless, the dumps are usually more expensive, because the methods by which they are produced are more complex. In addition, the online transactions made with a CVV can not be so high, because online purchases can be faster tracked.

An important source for finding out the current value of the personal credit card is the Secure Works Network, where the market prices for this type of services are updated. As in the image below, different prices for credit cards can be checked in United Kingdom / Australia/ Canada, United States or in Europe/ Asia.

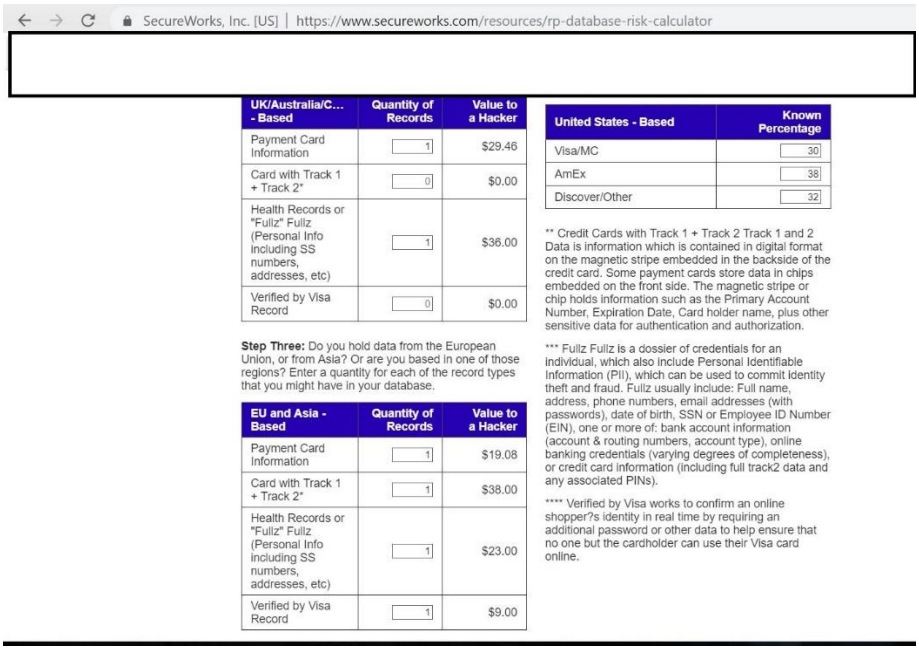

Figure 1. Credit card value to a hacker

Source: https://www.secureworks.com/resources/rp-database-risk-calculator

One of the biggest traders in the underground market is Rescator. This player provides any type of good regarding credit cards through a very friendly interface. It offers consumers the option to have an advanced search after country of the credit card holder, the dump type and mark, but also the debit or credit category. The image taken from the website presents exactly what other options for advanced search are available and the range of prices.

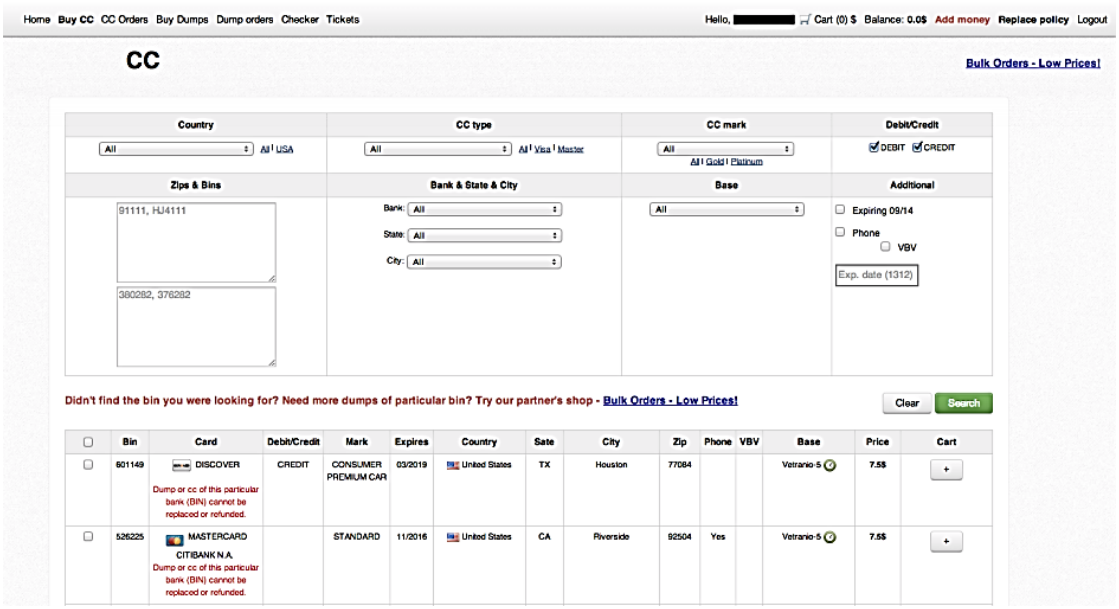

Figure 2. Rescator – database of stolen cards

Source: https://qz.com/260716/these-are-the-websites-where-hackers-flip-stolen-credit-card-data-after-an-attack/

A detailed and more rigorous analysis has been carried out for this article regarding price range for the credit card goods. The following table shows the results of the average price on each type of credit card and most common geographical areas.

Table 1. Prices for fresh credit cards (all prices are in $)

Country/ Type	Visa/ Master	American Express	Fullz info*
US	6	7	25
UK	14	25	35
CA	15	20	35
AU	18	20	30
EU	25	35	45

Source: Authors' own research based on chat with operators in Tor forum (http://crimenc5wxi63f4r.onion/)

The "fullz info" credit card contains more information about the credit card holder, like full name, date of birth, phone number, emails, address, employee ID, online banking credentials, bank account and PINs.

The real value of the personal data can be found into another item very popular in the dark web: PayPal accounts. These accounts are sold even if they do not have a credit card linked to them. The prices are, of course, higher for the accounts with credit cards. They are very useful because are they used for selling further other goods or services under a fake name and identity. The prices also vary depending on the country of the account holder or age. For example, a Business account can be sold for $10 if there is no credit card linked to them and have zero balance.

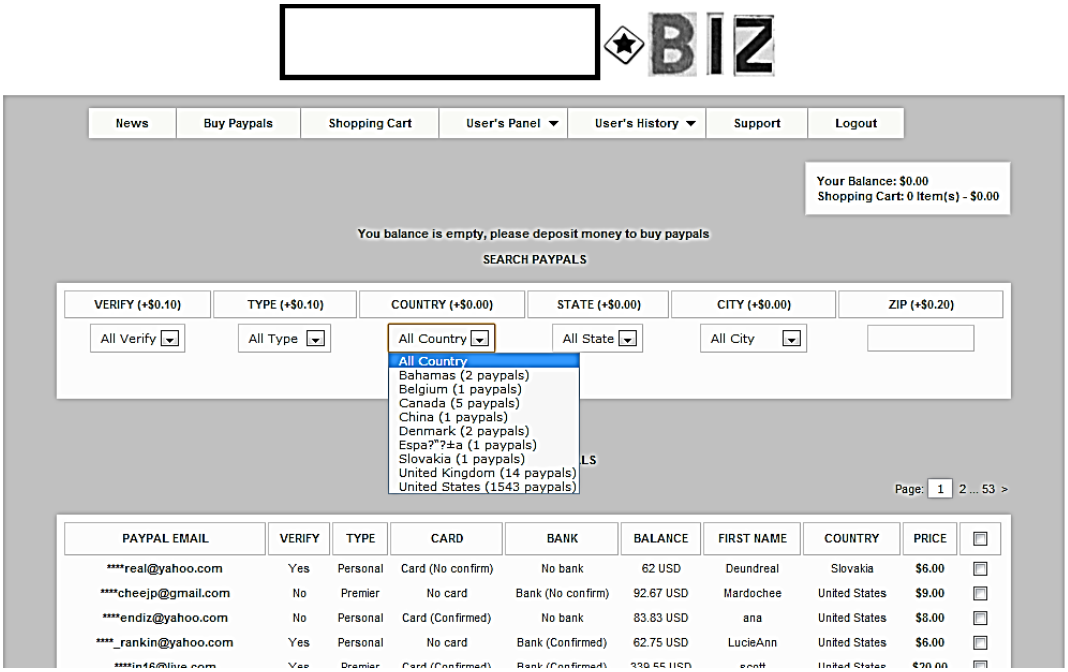

Figure 3. PayPal hacked accounts

Source: Authors own research based on: https://www.webroot.com/blog/2013/02/20/new-underground-e-shop-offers-access-to-hundreds-of-hacked-paypal-accounts/

A commodity found in the underground market is the online account credentials. There are specific markets for this type, but are also sold through forums. The most wanted credentials are the ones from Amazon, Facebook, Email, eBay and Instagram. For auction frauds are very popular the eBay accounts. Meantime, for phishing campaigns the social media accounts are preferred. In order to transfer money or to buy expensive good the Apple, PayPal and Amazon accounts are the most common Platforms used.

Figure 4. Hacked Facebook account

Source: https://resources.infosecinstitute.com/hacking-communities-in-the-deep-web/#gref

In the picture above is offer for one Facebook account on the Dark web. Prices are variable, but the offers are plenty. Since the new General Data Protection Regulation, Facebook offers its customers the option to download all the data Facebook collected about yourself. This option is very important for the criminals if an account is hacked. The downloaded data can be further sold with higher prices than the Facebook account itself. The

data can build an entire profile of someone's preferences and can be sold to marketing agencies or even interested corporations. Moreover, the downloaded data can be used for the creation of another type of good often purchased on the black market, the fabricated personal documents.

The fraudulent documents commonly found on the dark web are: passports, driver license, social security cards, professional certificates, visas, adoption certificates, diplomas and college degrees, birth and marriage certificates, resident permits, emancipation documents, working permits and many more.

One of the most popular personal data in the United States is the acquisition of working security card with a name and valid address at prices starting $250. This is happening because there are many illegal workers in the United States. The counterfeited card can "guarantee" a safe working place. Sometimes, the underground market dealers offer for a few more dollars also a utility bill with same name and address to the security card in order to make the deal more trustworthy. The utility bill can be used for a valid and safe identity verification process.

By far the most wanted fraudulent document outside the United States is the passport. The US passports are almost impossible to find on the black market because the United States law enforcement is believed to be infiltrated in the hacking communities and therefore it is risky to commercialize them. For the non-US passports the prices begin from $200 until $1000.

Figure 5. Counterfeited documents: Passports and Ids with Bitcoin price
Source: https://www.fakeid.co.uk/how-to-buy-fake-id-with-bitcoin

An integrated analysis of the prices for the dark web counterfeited passports was conducted and the following table shows the average value for the documents on each country.

Table 2. Prices counterfeited documents (all prices are in $)

Country/ Document	Passport	Real, physical passport	License ID Card
United Kingdom	1.792	17.116	120
United Stated	-	-	900
Canada	3.500	-	250
Poland	2.677	12.237	120
Belgium	1.981		250
Germany	1.832	8.216	250
Austria	2.677	14.684	250
Spain	1.560	-	49
Portugal	1.027	14.684	-
Denmark	2.667	-	-
Peru	2.800	-	-
Italy	1.560	14.684	199
Russia	3013	-	99
Japan	3.000	-	-

Source: Authors' own research based on chat with operators in Tor forum and onion marketplace(http://crimenc5wxi63f4r.onion/)

All sellers provide the insurance that the documents are officially registered in the governmental databases, but there is no real certainty. The buyer must assume his/her own risk that the document is valid. For a few more dollars, some of them send also a selfie with the passport holder if they have any.

There are several types of passports sold on the dark web. There is the most popular one, which is a counterfeit of the real one. It is the most common sold and it has a medium price. Another type is the digital print of a passport, which does not include any physical form of it. In the most of the time, this type of passport digital print is accompanied by other forms of verification like a utility bill, a driver license of a selfie of the real owner holding their passport. Anyway, the extra evidence increases the price of the package. The reason someone would buy such a digital print with evidence is to regain access to a fake account and to prove the identity. The table below will highlight some prices for digital print passport from various countries.

Table 3. Prices for hacked digital prints passports (all prices are in $)

Country	Price	Notes
Australia	27.65	No extra
Canada	102.96	Includes selfie
China	10.40	Sold in pack of 10
Finland	8.32	No extra
France	18.99	Includes utility bill
Germany	12.48	No extra
Italy	14.68	Sold in pack of 10
Romania	12.48	No extra
Russia	11	No extra
UK	51.99	Includes driver license
UK	61.19	Includes utility bill + selfie
USA	115	Includes selfie

USA	18.36	No extra

Source: Authors own research based on: https://www.comparitech.com/blog/vpn-privacy/passports-on-the-dark-web-how-much-is-yours-worth/

The most expensive type of passport is the real one, no counterfeit. The certainty that a passport is real and not a copy is very low and the price for such a document starts at minimum $10.000. For this reason, the market for this type of documents is not very popular or at least almost impossible to be found on the dark web. The providers offer also additional services for each interested person like documents duplicating ($500 - $2.000), visa / stamps attachments ($1.000 - $6.000) or erasing criminal records (eye scan or finger print from several databases) ($3.000 - $10.000).

Conclusion

Your own personal data is for sale. This is a truth and we have to admit it. All the analyzed evidence shows us that other people use this data to grow their businesses and others just to sell it forward. Globalization led to a dramatic increase in the level of competitiveness in all business sectors around the world (Dimyati, M. and Subagio, N.A., 2018)

In the analysis conducted through this study, it is highlighted the fact that in the underground market of the deep web is an articulate offer for online service accounts and other personal information. The big organizations from this market are providing an increasing number of services and goods in order to perform illegal activities. Understanding these implications has high practical relevance to personal privacy and keeping sensitive data safe.

Moreover, a constant monitoring of the underground market is crucial for security experts, but also for ordinary people in order to be aware of the online threats.

A further study will be conducted based on the current data in order to create a model for measuring the value of each sensitive information on the internet.

References

Acquisti, A., Grossklags, J., 2007. When 25 cents is enough: willingness to pay and willingness to accept for personal information. In: Workshop on the Economics of Information Security (WEIS).

Beresford, A., Kübler, D., Preibusch, S., 2012. Unwillingness to pay for privacy: a field experiment. Econ. Lett. 117 (1), 25–27.

Bischoff P. (2018), *Passports on the dark web: how much is yours worth?* , Retrieved from: https://www.comparitech.com/blog/vpn-privacy/passports-on-the-dark-web-how-much-is-yours-worth/.

Commission Staff Working Document, Impact Assessment Accompanying the document Proposals for Directives of the European Parliament and of the Council (1) on certain aspects concerning contracts for the supply of digital content, COM/2015/0634 final.

Dima, A., Hadad, S., Luchian, I., (2017), "Review on the dimensions of business-university alliances", Proceedings of the 11th International Conference on Business Excellence, pp. 64-73, DOI: 10.1515/picbe-2017-0007.

Dimyati, M. and Subagio, N.A. (2018), "Customer trust as mediator in the creation of customer relationship intention", Management & Marketing. Challenges for the Knowledge Society, Vol. 13, No. 1, pp. 710-729, DOI: 10.2478/mmcks-2018-0001.

Fligner Z. (2014), *These are the websites where hackers flip stolen credit card data after an attack*, Retrieved from: https://qz.com/260716/these-are-the-websites-where-hackers-flip-stolen-credit-card-data-after-an-attack/.

Fonseca, L.M. and Domingues, J.P., (2017), "How to succeed in the digital age? Monitor the organizational context, identify risks and opportunities, and manage change effectively", Management & Marketing. Challenges for the Knowledge Society, Vol. 12, No. 3, pp. 443-455. DOI: 10.1515/mmcks-2017-0027.

Huberman, B., Adar, E., Fine, L., 2005. *Valuating privacy. Secur. Priv. IEEE 3 (5), 22–25.*

Infosec Institute (2018), *Hacking communities in the Deep Web*, Retrieved from: https://resources.infosecinstitute.com/hacking-communities-in-the-deep-web/#gref.

IntSights Cyber Intelligence, Financial Services Threat Landscape Report, July 2018, retrieved from: https://www.prnewswire.com/news-releases/new-research-from-intsights-cyber-intelligence-finds-135-year-over-year-increase-in-bank-data-for-sale-on-dark-web-black-markets-300678803.html, (accessed on 23 November 2018).

More-with-mobile, 'Prices and Value of Consumer Data' (2013) http://www.more-with-mobile.com/2013/06/prices-and-value-of -consumer-data.html (accessed 12 October 2018).

OECD, Data-driven Innovation for Growth and Well-being, Interim Synthesis Report (2014).

Secureworks (2018)*, The Underground Hacker Markets are Booming with Counterfeit Documents, Premiere Credit Cards, Hacker Tutorials and 100% Satisfaction Guarantees.* Retrieved from: https://www.secureworks.com/resources/wp-underground-hacking-markets-report.

Onete B C, Vasile V, Vargas V, 2018, Online Business Models and Typologies, *New Trends in Sustainable Business and Consumption,* BASIQ 2018.

Secureworks (2018), Underground Hacker Report Database Value Calculator, Retrieved from: https://www.secureworks.com/resources/rp-database-risk-calculator.

Webroot (2013), *New underground E-shop offers access to hundreds of hacked PayPal accounts*, Retrieved from: https://www.webroot.com/blog/2013/02/20/new-underground-e-shop-offers-access-to-hundreds-of-hacked-paypal-accounts/.