Milana PISARIĆ, PhD*
Assistant with PhD
Faculty of Law, University of Novi Sad

Review Scientific Article
Recieved: 5 November 2021
Accepted: 3 February 2022
UDK: 343.983.2:004.056.55
https://doi.org/10.47152/rkkp.60.1.4

COMMUNICATIONS ENCRYPTION AS AN INVESTIGATIVE OBSTACLE

Due to novel technology solutions, primarily peer-to-peer, encryption and service providers located abroad, the ability of the law enforcement agencies to execute legally authorized traditional (even special) investigatory means is becoming increasingly problematic. Communication encryption, particularly end-to-end encryption in smartphone applications hinders law enforcement authorities' practical ability to wiretap communications, although in a legal position. This phenomenon is globally recognized as "Going Dark" problem. All these challenges have necessitated legislative action. So far two different approaches have been recognized in addressing this problem: mandatory exceptional access and legalized hacking of target. In this paper we explore the viability and implications of both of them, in order to identity the most viable solution for overcoming investigative barrier, i.e. enabling the authorities to conduct surveillance of electronic communications.

Keywords: electronic communication, surveillance, encryption, lawful hacking.

* E-mail:mpisaric@pf.uns.ac.rs

1. Introduction

One of the most commonly used type of smartphone application are instant messaging applications (e.g. WhatsApp, Viber, Signal). Communication through such a messaging service is very popular nowadays, since it is cheap, fast and simple. Unlike short message system (SMS) which are sent within the mobile telephony network, the exchange of instant messages (IM) within these applications is based on the connection of the devices, in which they are installed, with computer network. In this process, communications transmitted across a network are sent in packets: a message is first broken up into smaller segments, which contain the destination address, the source address, and other information, such as the number of packets and reassembly order of packets, and after packets arrive at the destination device, they are reconstructed again. If not hidden on the path over the network, the content of packets is not resistant to surveillance - a number of security threats exists, like packet sniffing and man-in-middle attack. That is the reason why the computer security community has been advocating widespread adoption of secure communication tools, the so-called privacy-enhancing technologies (PETs). [1] In order to protect the communication of their users, IM application developers have been implementing different PETs, including disappearing messages and end-to-end encryption.

Although this kind of protection is legitimate, it goes also in favor of criminals, since it supposedly makes communications bullet-proof for wiretapping, hence authorities, although in legal, are not in technical position to surveil them. Thereby, the encryption of communication, particularly end-to-end encryption, is nowadays a major cause of problem in the investigative process. In order to overcome this problem, some states have implemented, or are contemplating about implementing legislation that would require communication service providers and IM application developers to make their products and services "wiretap-friendly, by inserting wiretapping capabilities into communications infrastructure and applications. There is yet another possibility – not to create new vulnerabilities, but to exploit existing weaknesses.

In the first part of this paper the author examines the problem for law enforcement agencies posed by encryption of communication, in the second part possibilities for overcoming this problem are analyzed, while the third part is devoted to the malware enabled surveillance, i.e. lawful hacking.

1 There are different ways to protect communications – e.g. by using anonymizing services, like the Tor, i2p or GNUnet networks and secure services for logging in remotely (i.e., virtual private networks).

2. The problem

For several years the law enforcement agencies (the LEA) throughout the world have been warning that changes in telephony and some of newer communication technologies have hindered their practical and technical ability to conduct electronic surveillance and access the criminals' communications. Since the core of the problem is technology itself, mainly the encryption, the problem might be solved by addressing that very technology. This may seem as a reasonable request, nevertheless, before accepting it as such, one must first be acquainted with the nature of encryption in order to consider whether such a weakening of communication infrastructure is even possible without endangering encryption at whole.

2.1. Communications Encryption

Mobile phones were primarily designed to serve as a means of communication, and although a modern smartphone has been additionally equipped with numerous features, the communication is still its main function. Since more and more people use them, while expecting a reasonable amount of privacy, the importance of securing communications has become imperative for hardware and software producers, as well as different service providers. The primary protective technology is cryptography (as it has been for centuries), as a way to transmit messages that are only decipherable to the intended receiver, hence indecipherable to an interceptor. Encryption, as a cryptographic method, by which individuals can securely store or communicate data, is a mathematical process in which an algorithm uses a specific key to encrypt data, i.e. to translate it from plain text into unreadable, incomprehensible form. Once encrypted, the data can be securely stored on a device or transmitted across computer network.[2] That means that only a party with a proper key[3] may decrypt and read the encrypted data, and even in a case the data is accessed, intercepted or otherwise compromised, unauthorized third party only sees the data in its unintelligible form. Encryption of electronic communication is a type of data-in-transit, asymmetric encryption.

Modern encryption technology is an essential cybersecurity tool, which aims to keep electronic communications safe, by enabling users to communicate

2 Encryption may be used for data-at-rest (data stored on hardware of a device or on a remote cloud server) or for data-in-transit (data transmitted in computer network from one device to another) (Pisarić, 2020: 1085).

3 Regarding the key used, there are two main types of encryption: symmetric (typically used to protect data-at-rest) and asymmetric (commonly used in secure web-browsing, emailing, and messaging) (Pisarić, 2020: 1082).

without fear that third party without a key could understand their communications. In past few years, especially following Snowden's surveillance revelations, the public became significantly more aware of privacy and information security and the need to protect them. In order to meet these expectations, technology industry has increasingly introduced built-in and easy-to-use encryption to meet customer requirements and address evolving cybersecurity risks. Nevertheless, certain forms of encryption, particularly end-to-end encryption of data in transit, exclusively used in instant messaging applications, create problems for the LEA.

2.1.1. End-to-end encryption

End-to-end encryption (E2EE) refers to a form of encryption of data in transit, which facilitate that only the sender and intended recipient (end users) can read/see the message in plaintext, since only they (i.e. the applications on their devices) hold the keys to decrypt the message. E2EE takes place on either end of a communication - data is encrypted (made incomprehensible) on a sender's device before being sent, then transmitted over the network via the server of a service provider, still in an unreadable form, and finally is decrypted (made comprehensible) at a recipient's device. To be more precise, only the communicating users, i.e. endpoint devices, hold the cryptographic keys, while the server of the (communication) service provider acts only as messenger, passing along communication, that it can't decipher itself. In other words, E2EE makes it impossible even for the service provider to access or grant access to the plaintext of encrypted communication.

Except E2EE, encryption of communication may occur in different stages of communication process (Koops, Kosta, 2018:891): a) connection encryption, by service provider, or (b) transport encryption by service provider,[4] (c) E2EE is performed by provider of communication software (e.g., WhatsApp) on top of the channel managed by traditional telecommunication companies, or (d) E2EE performed by end users.[5] Since in first two cases the providers hold the cryptographic

4 In both of these types communications are encrypted on the sender's end, delivered to the server of provider, decrypted there, re-encrypted, and then delivered to the recipient, and decrypted on their end – meaning that the communication is actually in plain text on a provider's server. In a case of gaining the access to the server, one would be able to read, modify, delete, add, or delay any message between the server and all connected clients' devices.

5 If the communications are E2EE encrypted by the user, the LEA are allowed to use whatever technologies they have at their disposal to unlock lawfully intercepted and transmitted encrypted communications. However, there is a question of *nemo tenetur* principle with regard to compelling the user to turn over an encryption key (Pisarić, 2021: 402).

key, the encryption might be removed upon a court order or the providers might have to make the initial key available to LEA. However, in case of E2EE, this is not possible, because neither service providers nor providers of communication software have a capacity to decrypt communication since they do not possess keys.

2.2. Investigative barrier

The LEA have been traditionally authorized to lawfully access, intercept and record communication. These powers make sense only if the LEA are able to sensually perceive intercepted content data by listening or reading. With E2EE this is not the case.

Although the first free, widely used E2EE encrypted messaging software, Pretty Good Privacy (PGP), was released in 1991, until recently most communication applications did not provide any E2EE protection. However, ever since 2013 the share of unrecoverable encryption as a share of total communications traffic has been growing, as IM becomes increasingly dominant mode of communication and many popular IM applications have implemented E2EE by default (meaning there is no need for any type of user opt-in, activation, manual installation, nor any kind of in-depth technical knowledge of encryption techniques[6]).[7]

The use of such applications prevents unauthorized parties – including, telecom providers, Internet providers, and even that provider of the communication service (WhatsApp, for example) – from being able to access the cryptographic keys needed to decrypt the conversation and read messages in plaintext (they only see encrypted data). That led the LEA to claim that they are, although legally in power to intercept, practically powerless - since the interception of content data encrypted in transit is worthless without the corresponding possibility of decryption.

But how serious is this Going dark" problem? There are only few publicly available data which could demonstrate the LEA's inability to access content data. For example, in USA the number of state wiretaps reported in which encryption

6 Other E2EE tools that may be deployed by user are: OTR ('Off the Record', for secure instant messaging), Internet telephony applications, like SilentPhone, Signal, or DIME (aka Dark Mail) and specific plug-ins for Chrome, Firefox and other browsers. *FlyByNight* is a system that hides sensitive information posted on Facebook through a client-side JavaScript based encryption. OpenPGP and S/MIME encryption schemes, as well as MIME and HTML email are used for E2E cryptographic protection of e-mail (Müller et al, 2019, 24).

7 Signal, launched in 2013 have allowed encrypted communications via text messages. WhatsApp adopted Signal technology to provide encryption by default for its users starting in 2014 on Apple devices, and extended to all users by 2016.

was encountered decreased from 343 in 2019 to 184 in 2020, of which 183 the LEA were unable to decipher the plain text of the messages; as for federal wiretaps a total of 214 federal wiretaps were reported as being encrypted in 2020, of which 200 could not be decrypted (Administrative Office of the Courts, 2020)- However, these numbers are not representative nor sufficient, especially since they are used for describing the "Going dark" problem and for justifying some questionable approaches to E2EE as a way to "brighten the situation".

Although the use of E2EE present a barrier, it has some limitations, since there are many ways to implement it incorrectly, and other weaknesses that are exploitable exist, so the LEA can find ways around encryption, by employing existing techniques to collect evidence that is inaccessible otherwise - for example, access to communications metadata,[8] access to non-encrypted data stored in cloud services. These workarounds are prosperous in most cases (Pisarić, 2021:396).

One cannot dispute that encryption, particularly E2EE, hinders the investigation process, and in a near future, if present conditions persist, this adverse impact is expected to grow. Thus, there is a serious question of what is to be done.

3. Possibilities to overcome the problem

There are two different normative approaches to handle the problem of E2EE hindering the surveillance of communications: 1) Mandating technology companies and communication service providers to build in security flaws that could enable the LEA to enter encryption system (Back door option), and 2) Authorizing the LEA to hack into a target device through existing vulnerabilities in end-user software and platforms (Front door option).

3.1. Back door option – mandatory exceptional access

Legislators have forced traditional communications services providers to provide the LEA lawful interception, mandating them to embed a security weakness into their product or service, which could be used in the event of a criminal investigation, pursuant to a court order. With encryption, in order to remain decryption capability, this would mean mandating producers of encryption hardware/

8 The fact that a message is sent to a certain person (or received) on a certain day and at a certain time will be apparent – and these metadata are useful for investigative process as well. Newer E2EE tools do not only encrypt data, but also encrypt metadata (e.g. DIME and ProtonMail) and information shared.

software and communication service providers to deliberately integrate a wiretap interface and control system, in order to be able to act upon a surveil and monitoring request of a state's authority (Mandatory Exceptional Access). This idea may be implemented through key escrow or recovery agents - key escrow refers to the case in which a trustee holds a key for each user, while recovery agent hold a master key that could decipher data of all users of a specific encryption algorithm (Schuster at al, 2017:81). The US government unsuccessfully attempted to introduce a key escrow system via Clipper-chip in the 1990s, meaning that the government would have the access to decoding keys beforehand (Pisarić, 2020: 1092). This idea was debated within so-called "First Crypto war". As for recovery agents, law might create the mechanism of accessing the keys afterwards, meaning that all communication service providers are required to remain the capability to enable communication interception in plain text (decrypted). This idea is being debated within so-called "Second Crypto war", since several countries (mainly the Five Eyes counties) have recently opted for back door option.

There are at least two reasons in favor of this approach: a) it provides direct access to plaintext, by removing the additional decryption steps, and b) it is less expensive compared to identifying and exploiting existing vulnerabilities in encryption software, or even creating the new ones. While this type of mandate may sound easy, there are some important issues that must be taken into consideration. Not only it is problematic to statutory define the telecommunications carrier in a way to comprehensively include all providers of electronic communication (for example, to oblige communication applications providers - like WhatsApp), they are over-the-top services, rather than communications channel providers, hence often beyond the scope of traditional wiretapping obligations. There is also the serious issue of mandating the intermediary beyond the national jurisdiction. Still, the greatest challenge is of technical and security nature.

A large number of researchers, technical and industry experts are opposing mandatory building vulnerabilities into technology and stressing out serious security concerns. Namely that insertion of these mechanisms will necessarily weaken the system as a whole, endanger its structural integrity and compromise the security of all users—including those not under investigation (Pisarić, 2021: 404). Also, this would be an expensive burden for IT companies, since a wiretap interface would have to be integrated over a wide range of services. For all these reasons, cryptography and information security experts believe that it is exceedingly difficult and impractical, if not impossible, to devise and implement a system that gives the LEA exceptional access to encrypted data without compromising security at the same time. There is another way for providing LEA the access to encrypted communications.

3.2. Front door option - targeted surveillance at end points

Although the content of communication is protected E2EE from surveillance, there are still two vulnerable points left in communication process: the ends (terminal devices). If the end would be compromised, that would enable access to keys, or communication in plain text (before encryption, or after decryption) in real time, ex nunc. This could be achieved by gaining access to a user device, which leads us to other solution, where the LEA act as hacker – i.e. use vulnerabilities in hardware and software of device to bypass security measures and access data.

Errors and flaws may be found in each and every software and hardware, which can be exploited. A number of vulnerabilities may be found in modern encryption software as well: mathematical errors in the encryption algorithm, flaws in the random-number generator that provides inputs to the algorithm, or gaps in the algorithm's integration into the broader software or operating system. A type of vulnerability that is of special importance is the one that is discovered and exploited prior to public awareness, or disclosure to the vendor (so-called zero-day vulnerability).

The vulnerabilities may be also used in order to overcome seemingly undefeatable encryption and access communication protected by it. The idea is to authorize the LEA to target a specific end device and gain access to it, i.e. hack into it, by employing malicious software based on some vulnerability that is exploited. In case of need for surveillance of electronic communication conducted via applications that provide E2EE, the LEA might use a mechanics of employing a vulnerability for accessing a target system, since even the most perfect encryption mechanism may have some flows, so a more viable solution to bypass and undermine encryption, compared to creating new vulnerabilities, is to use the existing ones.

4. A lawful hacking – a malware enabled wiretapping

Even in more and more complex technological environment the LEA needs to have an ability to execute authorized surveillance of electronic communication. Since most of IM services nowadays use E2EE and since interception through the service provider is therefore not possible, interception at the source before encryption, or at the destination after decryption, may be the only way to capture the contents of communications. So, instead of introducing new vulnerabilities to communications networks and applications, the legislator could enable them to use existing vulnerabilities in software and hardware and regulate this as a special investigation measure.

Although a malware enabled interception may resemble by the name to "ordinary" telecommunications surveillance, it is technically not to be compared - rather it should be regarded as a secret digital break-in into device. A term "hacking" is to be used because it reflects the core of this investigation measure, that is, non-consensual access to a device. Also, unlike the traditional interception which takes place somewhere along the line, interception and monitoring concerns unencrypted content data in conducted in a time point before communication even begin, i.e. before the data is sent and transmitted, or after communication is finished, i.e. after the data is received.

The main tool for lawful hacking is malware - malicious software installed surreptitiously by third parties on a computer system without the users' knowledge or consent. The use of malware by LEA is generally referred to policeware, govware, Trojan horses (Trojans), etc. The malware enables the LEA to remotely access a target device and may serve various purposes – to compromise a device's functions, circumvent its access controls, monitor the user's activity or appropriate, corrupt, delete and change computer data. The further discussion is limited to its use for the purpose of intercepting communications, and not for the purpose of remote search of a device (Pisarić, 2021:407). In case of communication surveillance enabled by malware, it will function as a wiretapping device, such as a packet sniffer or a keystroke logger (for messages).

The LEA's use of vulnerabilities to enable wiretapping involves more uncertainty than traditional approaches, hence raises a number of unique technical and legal issues that must be carefully taken into legal consideration.

4.1. Technical issues

There are five distinct steps in surveillance enabled by malware: 1) prephase, 2) gaining access to the target's device, i.e. hacking, 3) installation of monitoring software 4) malware execution, i.e. interception of communication, 5) reporting.

Since an operating system recognize malware as threatening, it cannot operate undetected unless it exploits a vulnerability in the target device. So, the pre-phase of information-gathering starts with identification of the proper target device and its scanning for common vulnerabilities. A malware sends information from the target's device to the LEA: e.g., target device's IP address, MAC address, operating system type and version, browser type and version, last URL visited, etc.[9]

9 Like a malware known as a Computer Internet Protocol Address Verifier ("CIPAV").

Since the exploits must be exquisitely tailored to particular versions, in order to execute a hack into a device, LEA must previously (in the pre-phase) find the proper vulnerability that is going to be used. There are several ways through which malware may be installed on or delivered to a target device: a) on a device (in situ), in case police have physical access to a device, most commonly via removable hardware (floppy, CD, USB etc.), b) remotely (drive-by), or c) covertly accessing a device using the user's username and password (Škorvánek et al, 2020: 1008). The most practical way of delivery is to perform the installation of malware over a remote connection.[10]

Once a malware successfully exploits a vulnerability and enters the device, after circumventing security protections and by undertaking a number of measures in order to remain undetectable, it begins to run with the user's file access rights and execute the task on a suspect's device, i.e. to collect information from the target's device or network, extract and transmit them to an external controlling entity, i.e. to a LEA server. For the purpose of communication surveillance, the police monitoring system may monitor the user's activity in real time, i.e. listen to their conversations and receive messages in plaintext before they are encrypted, or after they are decrypted on an end-point device. The malware resides on the hard drive until it is disabled, and it reports to a remote controller regularly or continuously, constantly updating a police dossier of what it has learned, or it might report at one point in the future, uploading a bundle of information acquired over time (Ohm, 2017, 323). Also, the integrity of the malware and the limitation of its functions to the purpose of enabling surveillance are a prerequisite and guarantee that the collected evidence could be used in the course of criminal procedure.

Having been introduced with possibility of LEA power to hack back, we must stress out the importance of legal implementation of technical requirements for the use of malware in criminal investigations.

4.2. Legal issues

Although lawful hacking is definitely a more desirable alternative to the restriction of encryption, the debate on how lawful hacking should be regulated, is still in its early stages (Liguori, 2020: 344). In recent years lawmakers in several

10 Remotely installation of malware may occur via web browser or via voluntary download, since there are different points for Trojans to target a device, including infected attachments in email, malware on *a particular* web pages, poor implementations of network protocols, or users downloading and voluntarily executing booby-trapped programs or opening a file containing a specific, vulnerable application, or even to intervene when a program is updated by transferring manipulated software.

countries have introduced into their law lawful hacking powers, as a way to overcome encryption. Explicit lawful hacking provisions on the use of such a hacking technique is given to of the LEA in several European countries, e.g. France, Germany, Italy, the Netherlands.

As the intrusion into a device, without the consent of the owner, could result in a significant infringement of the right to privacy of targeted individuals and/or third-parties, as well as the security of the data and information system, even if conducted by the authorities, lawful hacking legislation should respect at least the minimum safeguards and requirements (UN General Assembly, 2016). To be more precise, legitimacy and necessity of creating proper normative framework must be met (Pool, Custers, 2017:130). The first condition for legitimacy is the existence of a clear legal basis for the investigative power to hack back. The second condition - legitimate aim – is also met, since the use of hacking technic serves the fight against crime. The third condition - necessity in a democratic society- is assessed by the effectiveness, proportionality and subsidiarity of such measures. As for effectiveness there is a question would this investigative power help the authorities to overcome the problem– however, there are still not enough fact-based figures available on the cases in which use of malware would be a suitable, necessary or even indispensable. As for proportionality, the use of hacking techniques should be limited to crimes of a substantial gravity, i.e. only to the most serious offences. In this sense, it must be pointed out that exploiting zero-day vulnerabilities may not be regarded as proportional. As for subsidiarity, it remains to be seen if such an investigative power would be, and to which extent more efficient than their alternatives, since the LEA has more data and possible investigative approaches than ever before.

Therefore, although it is indisputable that the LEA have the interest to engage in such a hacking tactics, the use of it should be limited to situations where they are strictly and demonstrably necessary to achieve a legitimate the aim, which importance should be proportionate to the technique's impact on competing rights and freedoms. Also, other less intrusive means should first be exhausted where practicable.

Following legislative recommendations should be taken into consideration when the legal basis for this investigatory power is considered: complete transparency in the use and scope of surveillance techniques; independent supervision and oversight mechanisms; safeguards relating to the nature, scope and duration of possible measures, as well as the grounds for ordering them and the remedy; and notification of individuals that have been subjected to communications surveillance (UN Human Rights Council, 2013). Hacking practices have to be appropriately targeted, and the integrity of data must be preserved - for that reason an

appropriate tool have to be selected, and a process of certification of the relevant malware has to be established with appropriate verification systems ensuring impartiality and confidentiality.

5. Conclusion

In recent years, the rapid evolution of technology, especially the spread of easy-to-use, strong encryption of communication, and its criminal misuse has made criminal investigations more difficult and less efficient, by bringing the emergence of anti-forensic measures apt to hide, alter, destroy or render impossible to obtain evidence. Although E2EE protects legitimate interests, it also protects online criminal activities, as it hinders the ability of state authorities to intercept data transmitted via these applications, frustrating the LEA's investigations and prosecutions. This led the LEA to claim that they lost practical power to legally intercept and gain access to communications ("Going dark problem"). There has been a debate for some years between public officials requiring the mandate for companies to facilitate access to encrypted data for the LEA, and security and technology experts responding by pointing out that doing so is impossible without introducing irredeemable security flaws.

In proposing controls on the use of encryption, it is advocated that backdoors should be embedded in encryption systems for the purpose of law enforcement. Several countries have approached encryption through the lens of mandatory access. Under this approach, companies must build backdoors into their encryption software so that they can provide the LEA with access to plaintext when the information is lawfully requested. So, in a case a judge orders a warrant to them to hand over certain information in a decrypted format to the government, the messaging app or the government agency could use this "backdoor" to give decrypted information to the government.

However, as strong encryption's essential role in modern communication systems, the idea of diminishing and endangering it via backdoor solution should be considered dangerous.

The subject of debate should therefore be the question what legal and technical measures governments should implement to facilitate the LEA's access to encrypted communication and which safeguards are necessary to ensure that such access measures do not infringe civil liberties or weaken critical security architecture. One of the most suggested alternatives is to lawful hacking. The essence of this proposal is to envisage a new investigation power, which would enabling criminal investigations without compromising encryption. When traditional investigative

techniques do not work and if conditions envisaged by the law, there is no reason why LEA should not be able to hack back, i.e. to use a malware as an investigative tool. The idea is to enable the LEA to deploy hacking tools by exploiting security vulnerabilities that already exists in operating systems and applications to obtain access to communications of the targets of wiretap orders. In other words, authorities might hack into a target device and monitor electronic communication even it is protected by E2EE when transmitted, by using a malware that exploits some vulnerability, in order to obtain encryption keys or communications before they're encrypted or after they're decrypted on the target's device.

Lawful hacking seems to be a viable alternative to the restriction of encryption or the mandatory exceptional access: Instead of requesting technology companies to sabotage their own security systems and knowingly compromise the security and privacy of their users, this alternative focus on observing and exploiting preexisting (and often unintended) security holes.

Currently, the need for malware-aided investigation is nowadays connected to a target's use of encryption, especially with regard to E2EE in IM applications. When viewed in socio-technical context one cannot dispute that the need to use malware will increase with future technology developments which concern the use of encryption (5G, quantum computing etc.) since encryption, when applied properly, can render the LEA possibilities impossible, especially on the darknet. However, this investigative power to hack back must be regarded as a special investigative measure. This means the proper legal normative framework of lawful hacking comes with a complex set of issues that have to be addressed particularly by taking into account the legitimacy (i.e., accordance with the law and legitimate aims) and necessity (i.e., the effectiveness, proportionality and subsidiarity).

References

- Administrative Office of the Courts (2020) Wiretap Report 2020, available at: https://www.uscourts.gov/statistics-reports/wiretap-report-2020.
- Koops, B.J, Eleni Kosta, E. (2018) Looking for Some Light Through the Lens of "Cryptowar" History: Policy Options for Law Enforcement Authorities Against "Going Dark". *Computer Law & Security Review*, 34, pp. 890–900, DOI: 10.1016/j.clsr.2018.06.003
- Liguori, C. (2020) Exploring Lawful Hacking as a Possible Answer to the "Going Dark" Debate. *Michigan Technology Law Review*, 26 (*2*), pp. 317-345.

- Müller, J., Brinkmann1, M., Poddebniak, D., Schinzel, S., Schwenk, J. (2019) Re: What's Up Johnny? Covert Content Attacks on Email End-to-End Encryption. *17th International Conference in Applied Cryptography and Network Security* (pp.24-42), Bogota: Springer.
- Ohm, P. (2017) The Investigative Dynamics of the Use of Malware by Law Enforcement. *William & Mary Bill of Rights Journal*, 26 (*2*), pp. 303-335.
- Pisarić, M. (2020) Enkripcija kao prepreka otkrivanju i dokazivanju krivičnih dela. *Zbornik radova Pravnog fakulteta u Novom Sadu*, 54 (3), pp.1079–1100, DOI: 10.5937/zrpfns54-26929
- Pisarić, M. (2021) Enkripcija mobilnog telefona kao prepreka otkrivanju i dokazivanju krivičnih dela – osvrt na uporedna rešenja. *Anali Pravnog fakulteta u Beogradu*, 69(*2*), pp. 391-416, DOI: 10.51204/Anali_PFBU_21205A
- Pool, R.L.D., Custers, B.H.M. (2017) The Police Hack: Back Legitimacy, Necessity and Privacy Implications of The Next Step in Fighting Cybercrime. *European Journal of Crime, Criminal Law and Criminal Justice, 25* (*2*), pp.123-144, DOI:10.1163/15718174-25022109
- Schuster, S. , Berg, M.v.d, Larrucea, X., Slewe, T., Ide-Kostic, P. (2017). Mass surveillance and technological policy options: Improving security of private communications. *Computer Standards & Interfaces*, 50, pp.76-82, https://doi.org/10.1016/j.csi.2016.09.011
- Škorvánek, I., Koops, B.J., Newell, B.C., Roberts, A. (2020) "My Computer Is My Castle": New Privacy Frameworks to Regulate Police Hacking. *BYU Law Review*, 2019 (*4*), pp. 997-1082.
- UN General Assembly (2016). The right to privacy in the digital age, available at: https://digitallibrary.un.org/record/858023?ln=en.
- UN Human Rights Council (2013). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40, available at: https://undocs.org/A/HRC/23/40.