Federico Costantini

“Pretty Good Privacy” – Smuggling in the Information Age

If a sense of limitation is inherent in the human condition, a smuggler can be seen as the embodiment of a demiurgic figure, who claims to challenge both nature and institutions.[1] In ancient times, a frontier was seen as a zone potentially populated with divinities – the *pomerium* (sacred no-man's-land) in Rome (Coarelli, 2000)[2] – while in the modern era it represented the absolute independence of the sovereign in relation to other states and religious authorities (Hobbes, 1651). One can then easily understand why *contraband* has always been severely punished: in ancient times, it was a form of impiety against the 'natural' order imposed by the political authority, in modern age, it was a sort of disenchantment for the legal system and the bureaucracy. One recalls a wide range of examples, from the myth of Prometheus, the Titan who smuggled fire from the gods and delivered it to humans,[3] to Al Capone, the Italian mobster who trafficked spirits during Prohibition[4] in the United States.

The frontier is where smuggling is put to the test: it is the battleground between the smuggler and the customs officer. The former has to create and take advantage of an 'information asymmetry' against the latter, typically by means of deception, since the trafficked goods are carried through hidden passages or concealed under the guise of worthless objects. As a demiurge connects two spheres – the mundane world and the realm of ideas – in the delicate act of creation, a smuggler finds or creates paths crossing the frontier, linking domestic territory to the outside world.

Today, it is known that information technologies flatten physical barriers, and the sharing of data – with undeniable practical benefits – inevitably involves control of information, which is held by a new kind of power that, as such, has no limits other than technological. In this context, we can see in encryption[5] the same contrast between reality and appearance that we find in the act of smuggling: important infor-

[1] The demiurge is a semi-divine figure that we can find in the dialogues of Plato, especially in the *Timaeus*, and in Gnostic mythology (Jonas, 1954). In the Platonic myth, it gives to matter the shape of ideas, and therefore connects experience and transcendence, while in the Gnostic view it expresses the conflict between these two dimensions. In the latter perspective, in which existence is a condition of suffering for humankind, this figure can be conceived as a guardian of the laws of nature and therefore as a kind of jailer. Salvation to humans, therefore, can only be a sort of emancipation by appropriating of supernatural, hence demiurgical, powers. Salvation identifies itself with freedom and implies the violation of the natural order.

[2] The *pomerium* was a strip of territory surrounding a settlement. It was considered sacred and therefore impassable, so the transit could only be allowed through the town's gates.

[3] http://en.wikipedia.org/wiki/Prometheus.

[4] http://en.wikipedia.org/wiki/Al_Capone.

[5] 'Encryption' is the process of converting ordinary information (called 'plaintext') into unintelligible text (called 'ciphertext'), while 'decription' identifies the reverse process. The cypher is the key that enables the program to perform the processes of encoding and decoding (Norman, 1973). On the epistemological aspects of espionage short after '9/11' (Horn and Ogger, 2003).

mation can be hidden inside insignificant files. Indeed, coding *plaintext* and decoding *ciphertext* respectively extend or tighten the domain of available resources.[6] Incredible amounts of data can appear or vanish in a moment: this kind of control is a power so immense that hackers are often compared with magicians[7] (Stefik, 1996; Haker, Borgmann and van Erp 2005; Fioriglio 2010).

In this essay, I will address the problem of smuggling on the new battlefield named Information Society, where the information asymmetry between smuggler and customs officer occurs in a different way than it did with respect to the border of ancient political communities and the frontier of modern states, because the sole purpose of the contrast between the two figures is the control of information. After providing some legal premises for the concept of smuggling and a few technical details about cryptography, I will focus on a legal case that occurred nearly twenty years ago concerning the 'smuggling' of the encryption system called "Pretty Good Privacy" (henceforth "PGP") across US borders. I shall comment briefly on its most significant legal issues, and finally I will draw some theoretical conclusions.

Preliminary legal clarifications

From a strictly legal point of view, one can make a distinction between two kinds of activity concerning contraband: illegal trade occurring when a state's legal system is in danger, referred to as "contraband of war", and the activity in peacetime commonly called "smuggling". It is useful to provide explanations for both concepts.

The term "contraband of war" refers to a set of transactions in international trade that is intended to prevent the procurement of enemies. There are several ways in which this phenomenon occurs: the delivery may be made directly to the hostile state, or through neutral countries; prohibitions may also cover items specifically designed for war, such as weapons and munitions, or common goods that acquire specific relevance by their destination, such as food supplies for an army. Following international customary law (de Groot, 1625), in order to facilitate diplomatic relations and international business, states issue specific lists of goods that, being considered or alleged contraband of war, are forbidden or submitted to very strict regulations (Jessup and Deák, 1932, 1933 a, b).

"Smuggling" refers to a diverse set of phenomena involving the crossing of boundaries, which can be qualified as illegal for several reasons: because the trade of certain goods is strictly regulated as such (i.e. pharmaceuticals), due to infringement of customs taxation, or because it is part of a composite crime (i.e., trafficking in persons).

Taken as a whole phenomenon, we can identify two profiles for smuggling, which involve: (1) the foundation for prohibitions, and (2) the effectiveness of prescriptions.[8]

(1) According to the conceptual model of modern sovereignty, laws rely not on the justice of conducts prescribed – or the injustice of actions forbidden – but on the effective power to punish infringements. This means that, for example, trafficking in human beings shall be prohibited just because the law requires it, not because it is an abomination in and of itself. In accordance with this view, a law that would make it legitimate – or actively promote it, for absurdity's sake – should be cherished and enforced (Kelsen 1960).

[6] The message contained in 'cypertext' can not be understood without the key that enables the encoding process. In this sense owning the access code means to widen the horizons of the available information.
[7] The figure of the 'computer wizard' symbolically expresses the supernatural powers of the demiurge. Technology is a tool of salvation, knowledge of which is the guarantee of freedom and is reserved for a select few.
[8] Hereinafter I will use the word 'smuggling' in a general sense.

(2) In international commerce, goods traded are increasingly accompanied by documents that represent them (for example, the Air Way Bill for goods carried by planes). Thus, the customs control is performed indirectly: not by monitoring the displacement of physical goods, but by checking their shipping documents. Consequently, we can also say that smuggling has changed in the 'physical world': it has become less focused on the hidden movement of things across the border, and more focused on the avoidance of customs procedures (for example, with forgery of invoices). Therefore, deception remains a key feature of smuggling.

Technical explanations

Encryption has always been important, but in the Information Age it became crucial. Just as decency is part of human nature, and society requires that certain matters be kept confidential, governments have often made use of encryption tools in the transmission of messages of strategic importance (i.e., the greek *scytale*, the Roman Caesar's *cipher*). Recently, as a result of the importance of information in wartime (for example the breaking of the Enigma Code in World War II which was pivotal for the Allied victory),[9] the development of automation technologies has enabled the improvement of more complex methods – cryptographic systems – requiring the use of increasingly sophisticated devices (mechanical, electrical, electronic, quantum theory based) to encode and decode communications.

Of the two kinds of existing cryptography – 'symmetric' and 'asymmetric'[10] – the latter (and most often used) was invented in 1976 at Stanford University by Whitfield Diffie and Martin Hellman (Diffie and Hellman 1976a, b). According to the theoretical model they proposed, soon after three researchers at MIT – Ronald Rivers, Adi Shamir and Leonard Aldeman – developed a technology – named RSA – that has been the basis of security in electronic communications since then.[11]

During the Cold War the U.S. divided technologies into two categories: the tools that had an exclusive military application, called "munitions", were entrusted of the State Department, and civil technologies also suitable for exploitation in war, called "dual use technologies", were delegated to the Department of Commerce. In 1976 the U.S. government issued the AECA (Arms Export Control Act),[12] which provides a very strict regime for arms exports contained in the ITAR (International Traffic in Arms Regulations).[13] Within ITAR the USML (United States Munitions List)[14] provided a very detailed list of goods whose export required permission from the Department of State The AECA included cryptographic systems in the USML,[15] thereby establishing that the export of cryptographic systems would be severely punished as 'con-

[9] It is known that the communications of the Nazi army were based on a rather advanced encryption that was decoded by a group of British researchers. In this discovery, a decisive contribution was provided by Alan Mathison Turing, a famous mathematical genius whose studies are moreover crucial to the birth of artificial intelligence.

[10] In 'symmetric' cryptography, the key used for encryption is the same as that used for decoding; it is older, and is the only one to be used until the 1970s. In the 1960s, IBM introduced a particular algorithm, DES (Data Encryption Standard), which was adopted and strengthened by the NSA (National Security Agency). Here the keys are different: one is called 'private', the other 'public', hence the 'asymmetry' in this kind of cryptography.

[11] Rivest, R.L., A. Shamir, and L.M. Adleman, 'Cryptographic communications system and method', U.S. patent # 4405829, 1983.

[12] Title II of Pub. L. 94-329, 90 Stat. 729, enacted June 30, 1976, now in Title 22 USC § 2778 and § 2794 (7).

[13] In Title 22 CFR, Title 22, Chapter I, Subchapter M, Parts 120-130.

[14] In Title 22 CFR, Title 22, Chapter I, Subchapter M, Part 121.1.

[15] Title 22 C.F.R. 121.1 (XIII)(b)(1) (1994): "cryptographic... software with the capability of maintaining secrecy or confidentiality of information or information systems".

traband of war'.[16] Although cryptography was included in the USML, financial organizations were pressing for permission to use cryptographic systems worldwide in order to protect electronic transactions. The federal government granted the use of cryptography only to large companies able to manage very high security standards. Later, in 1992, several companies, gathered in the Software Publishers Association, made an agreement with the U.S. government for permission to export software with 'weak' encryption.[17]

The "Pretty Good Privacy" case

In order to explain the famous legal case concerning the 'smuggling' of the cryptographic technology called PGP, I will consider the following topics: (1) the circumstances in which the case took place, (2) the judicial proceedings and (3) the outcome and subsequent events.

(1) In 1991, the U.S. Senate was debating a bill that would have granted the government access to messages through devices placed by the producers in communication equipment.[18] Shortly before the proposal was shelved in response to public protests, a computer scientist and civil activist named Philip R. Zimmermann wrote a public-key encryption software package for the protection of electronic mail with the aim of defending citizens' freedom of speech.[19] The 1.0 DOS version of program was released freely to his friends and – it seems, not by the author – was uploaded on the Internet, which then had 30 million users. Various reactions were immediately unchained: i.e., activists all over the country, fearing that government could inhibit the spread of the program, uploaded it on different BBS[20] by connecting their computers to public telephones (Kerben 1997, 129), while some providers – such as CompuServe Inc. – removed the software from their servers to avoid being sued.[21]

(2) In 1993, federal prosecutors began investigations against Zimmermann for the infringement of AECA (Arms Export Control Act) and ITAR (International Traffic in

[16] "Any person that knowingly violates the Export Administration Act (EAA) or the regulations of, is subject to a fine of up to five times the value of the exports involved or $ 50,000 whichever is greater, or imprisonment of up to five years or both" 50 U.S.C. 2410(a) (1994); and: "Any person that willfully violates the EAA or the regulations of, is subject to five times the value of the exports up to $ 1,000,000 ($ 250,000 for an individual), or up to ten years of imprisonment, or both" 50 U.S.C. 2410(b)(1)(A)(B); and finally: "The violation of the Arms Export Control Act (AECA) or the International Traffic in Arms Regulation (ITAR) is punishable by a fine up to $ 1,000,000, or imprisonment of up to ten years, or both." 22 U.S.C. 2778 (c) (1994. See also: 22 C.F.R. 127.3 (1996).

[17] The encryption was considered 'weak' if the 'symmetric' key was lower than 40-bit or the 'asymmetric' key was below 512-bit. For example, the Netscape browser was first released in two versions, depending on the security protocol SSL, international (40-bit) and domestic (128-bit, which was later reduced to the same length of the international version). The 40-bits encryption was not at all sure, as could be violated in two days. Users protested because the government imposed limits on the safety of their financial transactions in the name of national security.

[18] Senate Bill 266 "Comprehensive Counter-Terrorism Act", Introduced on January 24, 1991.

[19] https://www.philzimmermann.com/EN/background/index.html. Zimmermann wrote the program in just six months. During this time, he was out of work and used all the savings of his family, so that he was likely to be evicted with his wife and two children. The software name "Pretty Good Privacy" comes from "Ralph's Pretty Good Grocery" in humorist Garrison Keillor's "Prairie Home Companion" radio show.

[20] The BBS (Bulletin Board Systems) were a tool for sharing information very popular before the advent of the World Wide Web.

[21] The first commercial disputes also arose: RSA Data Security Inc., which held the license for the distribution of the RSA technology on US territory, undertook a legal action against Zimmermann, claiming that the diffusion of PGP had infringed their rights. In order to resist their claims, Zimmermann signed a distribution sub-license with Viacrypt (Phoenix), which was also a dealer of the RSA: at that time, PGP was sold for $100 (DOS version) and $125 (Windows version). Another company, the Austin Code Work (Austin, Texas), began distributing software similar to PGP called Moby Crypto, containing encryption.

Arms Regulations), because PGP enabled users to encrypt their files with extremely "strong" keys (512-bit, 1024-bit, 1280-bit, 2048-bit) that far exceed those permitted by law.[22] In February, US Customs agents showed up at Zimmermann's home to seize documents concerning PGP.[23] On November 4, 1994 Zimmermann was arrested at customs in the International Airport of Dulles (Colorado), returning from travel in Europe (Stay 1997, 581). On that journey Zimmermann was writing the book published in 1995 under the title *PGP Source Code and Internals* (Zimmermann 1995). In it, he transcribed the whole source code of his program, so that anyone in the world – beyond the US border – could re-write the software.

It needs to be emphasized that to 'smuggle' the program, Zimmermann did not pass any frontier, he did not even transmit anything through the Internet; he created instead an intellectual work: just a book, but one symbolic of freedom of expression. Some very delicate issues arose. We can express them in three questions:

(1) How could the US government prosecute a citizen for exercising freedom, which is the pillar of the American Dream?

(2) How could the US government indict one single person, while everyone in the world already was using PGP?

(3) How could the US government condemn the inventor of a system that had become a *de facto* technological standard (Atkins, Stallings, and Zimmermann 1996, Callas et al. 2007)?

As written by John Perry Barlow, the visionary prophet of cyber culture (and former lyricist for "The Grateful Dead")

> "The genie of guerrilla cryptography is out of the bottle. No one, not even its maker, can stuff it back in or keep it within what America laughably calls its borders. The genie is all over the Net. It's in your hands as you hold this book. Summon it with a conscience. But be prepared to summon it if you must." (Barlow, 1995)

On January 11, 1996, the federal investigation against Zimmermann ended with the archiving of charges.[24] The press statement of an assistant attorney general was very laconic: "No change in the law, no change in policy. If you're planning on making encryption available over the Internet, or other means, better check with the State Department first." (Kerben 1997: 131).

Soon after, Zimmermann yielded the rights on his algorithm to a company named Network Associates Inc., which in 2002 was acquired by PGP Inc., which was merged with Symantec Corporation in 2010.

(3) From the statement of the public prosecutor, we can understand that the government did not admit defeat, yet we can guess that something was going to happen. Indeed, it happened very soon. In July 1996, the US government, along with thirty-three other countries, signed an international agreement, the *"Wassenaar Arrangement on Export Controls for Conventio-*

[22] Just to give an idea of the effectiveness of PGP, I can report that it was said that a decent computer would have taken about 280,000 years to force open the encryption (Kerben, 1997) p., 129.

[23] In September 1994, a Federal Grand Jury in San Jose (California) issues subpoenas to Viacrypt – namely on September 9, 1994 – and to Austin Work Code (Austin, Texas) – precisely on September 17, 1994 – requiring evidence concerning the distribution of PGP.

[24] We can read from the text of the provision that the action performed by Zimmermann fits perfectly in the provision of Title 22 CFR § 121.1, Category XIII(b) (1995), which forbids export of: "Information Security Systems and equipment, cryptographic devices, software, and components specifically designed or modified therefore, including: (1) Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems, except cryptographic equipment and software as follows: (i) Restricted to decryption functions specifically designed to allow the execution of copy protected software, provided the decryption functions are not user-accessible.".

nal Arms and Dual-Use Goods and Technologies",[25] which prescribed that the export of cryptographic systems were subject to government authorization if they exceeded 56bit keys (symmetric encryption) or 512 bit (asymmetric cryptography). On October 1, 1996, Vice President Al Gore announced the administration's intention to remove cryptographic systems from USML and place them under control of the Department of Commerce, so that the authorization would not have to be requested from the Department of State.[26] On November 16, 1996, the US Government proposed a new initiative called the "Clipper Chip III", pursuant that the export of 'strong' encryption would be allowed if equipped with a key recovery system.[27] More recently, after an initial partial disclosure in 1999, in 2009 the federal government submitted the export of cryptography to the Export Administration Regulations (EAR),[28] putting it under the supervision of the Department of Commerce's Bureau of Industry and Security. The regime, as provided in the Commerce Control List,[29] draws a rather complex system of restrictions divided by product type and destination (the states are divided into groups A, B, C, E).

Legal issues in the PGP case

From a legal perspective, the issues raised by the PGP case are still very much present, even after twenty years. Considering the reasons why smuggling encryption was considered legitimate despite the violation of severe prohibitions, I can identify three main profiles that correspond to the abovementioned questions. They involve: (1) the protection of freedom of expression, (2) the safeguard of privacy and (3) the right to legal defence. It is useful to scrutinize each profile.

(1) It is known that the First Amendment of the U.S. Constitution protects freedom of expression.[30] This is the principle, as we have seen, invoked by Zimmermann in support of his action. The protection of freedom of speech is also contained in the discipline of the ITAR, and particularly in the provision that excludes the application of the prohibitions in the case of "public domain".[31] The courts interpreted these regulations holding that the definition of the list of prohibited goods were exempt from judicial review – as an expression of sovereignty – and thus the inclusion of encryption could not have been discussed.[32]

[25] The participating states – the number of which nowadays has reached forty-one – regularly meet in Vienna. See www.wassenaar.org. The European Union has established a legal framework pursuing this international agreement, see: Council Regulation (EC) No 428/2009 of May 5, 2009 "setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items", in OJ L 134, 29.5.2009, p. 1-269, recently amended with Regulation (EU) No 599/2014 of the European Parliament and of the Council of April 16, 2014 "amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items", in OJ L 173, 12.6.2014, p. 79-83. Encryption is contained in Annex I, 'List of dual-use items', Category 5 – Part 2 'Information security'. The term 'Export' is extensively defined as follows: "transmission of software or technology by electronic media, including by fax, telephone, electronic mail or any other electronic means to a destination outside the European Community; it includes making available in an electronic form such software and technology to legal and natural persons and partnerships outside the Community. Export also applies to oral transmission of technology when the technology is described over the telephone" art. 2 c. 2 (iii), Reg. (EC) 428/2009.

[26] Executive Order No. 13,026, 61 Fed. Reg. 58,767 (1996), signed by the President on November 15, 1996.

[27] See recently http://www.foia.cia.gov/sites/default/files/DOC_0006231614.pdf (Schwartzbeck, 1997).

[28] Title 15 C.F.R. Chapter VII, Subchapter C.

[29] Supplement No. 1 to Part 774 Category 5 Part 2 – Information Security.

[30] "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances", The First Amendment, U.S. Constitution.

[31] "(a) Public domain means information which is published and which is generally accessible or available to the public: (1) Through sales at newsstands and bookstores; […]" 22 CFR Chapter I, Subchapter M, Part 120, § 120.11.

[32] See: United States v. Martinez 904 F2d 601 (11th Cir 1990), (Stay 1997, 600).

However they stated that depending on the circumstances, encryption, as such, could also be considered “public domain” and then be included in the exception that permitted free circulation within national territory. The federal government expressed its position on the matter in other legal cases, with quite questionable arguments: in the “Karn case”, granting the export of a book containing lines of code, but not of an identical executable file;[33] in the “Bernstein case”, on the pretence that the prohibition on the use of foreign languages in communications under rules that came into force during World War II[34] was enforceable in peacetime; in the “Junger case”, pretending that the exclusion applied to teaching cryptography at a university to noncitizens students.[35]

(2) The Fourth Amendment[36] has been traditionally considered the conceptual pillar of the doctrine of privacy, (Warren and Brandeis 1890), but does not play a special role in the protection of encryption, as if it was overshadowed by the debate on freedom of expression. Moreover, confidentiality of communication is a value whose defence in courts has always been very challenging, as shown by the cases Olmstead[37] and Katz.[38]

(3) The principle established by the Fifth Amendment[39] draws out a further aspect of cryptography, that here for lack of space I can only mention. The privilege against self-incrimination becomes relevant as it inhibits the state to force a person – i.e. a suspect – to reveal the credentials necessary to access information that he had previously encrypted. Yet, very recently a court of Virginia Beach Circuit Court (2nd Judicial Circuit of Virginia) decided that this rule does not apply to biometrics (such as fingerprints), because they don’t involve an act of will, but rather they are similar to DNA samples: just a measurable quality of the physical body (Hulette 2014). This solution seems contradictory, because the same information can receive different legal protection depending on the system of protection previously chosen by the owner.

[33] On February 12, 1994 Phil Karn asked the Department of State whether approval was required to export a book containing lines of code and documentation of a cryptographic program (Schneier, 1993). The answer was that this did not require permission. On March 9, 1994, he asked if it could be exported in the digital version and received a negative response by the same officer, William B. Robinson. In the judgment on the appeal of the denial, the government refused to include the export of software as freedom of expression and the judge agreed this position. See: Karn v. United States Department of State, No. 95-CV-01812 (D.D.C. filed Sept. 21, 1995).

[34] See: 32 CFR § 1801.48 (1945). It was forbidden not only to speak in languages other than English, French, Portuguese and Spanish, but also to use “any word, term, phraseology or language having a double meaning”. See: Bernstein v. United States Department of State, No. C95-0582-MHP (N.D. Cal. filed February 21, 1995). In this case, the Court decided in favour of the export of encryption. See: (Reiman, 1996).

[35] Junger v. Daley, 209 F.3d 481 (6th Cir. 2000).

[36] “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized”, The Fourth Amendment, U.S. Constitution.

[37] Olmstead v. United States, 277 U.S. 438 (1928). With this decision, which contains the famous dissenting opinion of Justice Brandeis, was recognized as legitimate wiretapping of a bootlegger without judicial authorization.

[38] Katz v. United States, 389 U.S. 347 (1967). This judgment overruled the Olmstead sentence, recognizing the right to privacy of a bookie who used a pay phone to collect bets.

[39] “No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.”, The Fifth Amendment, U.S. Constitution.

Conclusions on PGP and "smuggling technologies"

In the information age, we can assume that our territory is defined by the domain of available resources, information is the good carried, and a boundary consists only of reaching the limit of data processing capacity. Secrets are the most valuable kind of information, and the most precious technologies are those that allow maintaining or eradicating them. Two observations can be made from this perspective:

(1) The availability of resources is independent of geographic location. Information is not a physical entity to move, neither a document to be checked, but an immaterial and volatile object, so that in order to prevent contraband the sovereign should isolate completely its territory from the rest of the world, however this is impossible.

(2) The control of information is a measure of power in the physical world. For states, potentially any information that is not at hand is a threat, thus secrecy as such has to be removed, and transparency has to be promoted in the name of national security.

The world community of Internet users considers Zimmermann a hero.[40] Today cryptography is widely used in order to ensure confidentiality, data integrity, authentication, and non-repudiation (i.e., electronic commerce, e-mail messages, electronic signatures, Digital Rights Management), but it's difficult to say that the case was a complete victory for supporters of smuggling. Indeed, the PGP case teaches that the relationship between smuggling and encryption is two-sided, because encryption could be a tool of traditional contraband, and smuggling could be seen as a sort of encryption. Hereinafter I deepen both observations.

(1) Zimmermann claimed to have invented PGP in the name of freedom of expression, and exported it to support dissidents fighting totalitarian regimes. In this sense, encryption can be seen as a practical tool for spreading democracy. Zimmermann was a brilliant smuggler, certainly: he took advantage of an exception in the law, hiding the source code in plain sight, where everyone could see it. He was very lucky too, if we think about what happened recently to Edward Snowden or Edward Bradley/Chelsea Elizabeth Manning. Today, however, this view reveals all its naïveté not only because it does not takes into account the 'neutrality' of technology, as scholars pointed out,[41] but also because it was, after all, ideological (Fukuyama, 1992). We have seen in recent years that, in addition to the most peaceful dissidents, even ruthless terrorists can benefit from encryption, and on this issue we do not find a satisfactory response within the ideological conflict between libertarianism and authoritarianism.

(2) To define smuggling as a semantic process means to focus on 'asymmetric information', which constitutes its epistemological structure, as introduced in the foreword of this article. The best perspective on the issue is given by the acknowledgment that the one who encodes a message has first-hand control of the information, and

[40] http://www.internethalloffame.org/inductees/philip-zimmermann.

[41] Zimmermann insisted on this point during a hearing held on June 26, 1996 in front of the "Subcommittee on Science Technology and Space of the US Senate Committee on Commerce, Science and Transportation." Encryption is cherished as a tool for the protection of freedom of thought, available to opponents of totalitarian regimes, and ultimately as an instrument of transparency and democracy. In this regard, Zimmermann added "The information revolution... contributed to the fall of the Soviet Empire", https://www.philzimmermann.com/EN/testimony/index.html. This is quite an optimistic perspective, since technology is a neutral tool, which can be used for good and evil. See: (Metzl 1996, Ball, Girouard, and Chapman 1997). Ball et al., criticizing Metzl, point out three problems and three solutions in the use of information technology by organizations involved in protecting Human Rights: (1) message authenticity and integrity, solved by digital signatures; (2) content surveillance, solved by encryption; (3) traffic analysis, solved by anonymous remailers.

ultimately that there is no substantial difference between a smuggler and a customs officer.[42] For states, as for companies and common people, it becomes crucial to own technologies that preserve secrets and to penetrate those of others. The purpose for which it is done does not matter, nor the entity that holds it. Control of information is a power to which everyone has to bow down, just as in a new religion.

The advent of the information age has not only weakened physical boundaries, but it has also raised higher barriers, defined as 'cyber borders'. The Internet itself has been weaponized and increasingly put under military control (Schmitt, 2013). As a result, any electronic signal theoretically could fall into cyberwarfare, and thus be filtered, scanned, or intercepted. Therefore it doesn't makes sense anymore to distinguish between "contraband of war" and "smuggling" since, for example, it is no longer necessary to carry weapons across a border: one could find files on the Internet[43] containing layouts for 3D-printing them where ever needed (Feinberg, 2014).

Facing this scenario, nevertheless, I hope there is still an option for some sort of contraband to exist. Maybe we should learn to smuggle ourselves, as human beings, by circumventing the control of information. We should certainly defend our moral freedom in the face of the system, that is to say, we should grow our intelligence in order to recognize the distinction between good and evil as something real, something that no one can manipulate or encrypt. Let us say it is an 'art' that we need to learn, and as such, it cannot be controlled by a computer.

[42] The two positions are perfectly symmetrical: someone (the smuggler) encrypts the message preventing others (the customs officer) to access the content that, being hidden, flows through customs control, unless someone (the customs officer) would find the credentials, and then access the ciphertext, overcoming the barriers (the cypher) posed by the sender (the smuggler).

[43] For example, paying them in Bitcoin, which is an encrypted currency, and downloading them from the Deep Web.

When the Price is Right?" *Medical Law International* (online) 1 (17) ((1993): 17-32. Viewed November 11, 2011. http://mli.sagepub.com/content/1/1/17.full.pdf+html.

http://en.wikipedia.org/wiki/Ciclosporin. Viewed October 18, 2014

http://www.ungift.org/knowledgehub/en/about/trafficking-for-organ-trade.html Viewed July 5, 2014.

http://www.nlm.nih.gov/medlineplus/druginfo/meds/a601207.html (October 18, 2014)

Wilkinson, Stephen and Eve Garrard. "Bodily integrity and the sale of human organs." *Journal of Medical Ethics* (online) 22 (6) (1996): 334-339. Viewed: November 11, 2011. http://ccj.sagepub.com/content/24/3/212.full.pdf+html).

Ralf Čeplak Mencin: *Smuggling opium from Afganistan*

Arbabzadah, Nushin. *Afghan rumour bazaar: Secret sub-Cultures, hidden worlds and the everyday life of the absurd.* London: Hurst & Company, 2013.

Barfield, Thomas. *Afghanistan: A cultural and political history.* Princeton: Princeton University Press, 2010.

Booth, Martin. *Opium: a history.* London: Simon & Schuster Ltd, 1996.

Chouvy, Pierre-Arnaud. "Opiate smuggling routes from Afghanistan to Europe and Asia." *Jane's Intelligence Review* 15, No. 3 (2003): 28-31.

Chouvy, Pierre-Arnaud. *Opium: Uncovering the politics of the poppy.* London: I.B. Tauris, 2009.

Clammer, Paul. *Afghanistan*. Footscray: Lonely Planet Publications, 2007.

Encyclopaedia Britannica online

Griffiths, John C. *Afghanistan: land of conflict and beauty.* London: André Deutsch, 2011.

Macdonald David. *Drugs in Afghanistan: Opium, Outlaws and Scorpion Tales.* London: Pluto press, 2007.

McCoy, A.W. *The politics of heroin. Cia Complicity in the global drug trade.* New York: Lawrence Hill Books, 1991.

Mills, Nick B. *Karzai, The failing American intervention and the struggle for Afghanistan.* New Jersey: John Wiley & sons, 2007.

Nawa, Fariba. *Opium Nation: Child Brides, Drug lords, and One Woman's Journey Through Afghanistan.* New York: Harper Perrenial, 2011.

Oeppen, Ceri, and Angela Schlenkhoff. *Beyond the "Wild tribes": Understanding modern Afghanistan and it's diaspora.* London: Hurst & Company, 2010.

Rasanayagam, Angelo. *Afghanistan, a modern history.* London: I.B.Tauris, 2010.

Rashid, Ahmed. *Descent into Chaos.* London: Penguin books, 2009.

UNODCCP (United Nations Office for drug control and crime prevention). 2001. *Global illicit drug trends.* New York: United Nations.

UNODCCP (United Nations Office for drug control and crime prevention). *Afghanistan Opium Survey.* New York: United Nations.

UNODC (United Nations Office for drugs and crime). 2003. *The opium economy in Afghanistan.* New York: United Nations, 2002.

UNODC (United Nations Office for drugs and crime). *Afghanistan opium survey.* 2014. New York: United Nations.

Federico Costantini: *"Pretty Good Privacy" – Smuggling in the Information Age*

Atkins, D., W. Stallings and Philip R. Zimmermann. RFC 1991. PGP Message Exchange Formats. Network Working Group, 1996.

Ball, Patrick, Mark Girouard and Audrey Chapman. "Information Technology, Information Management, and Human Rights: A Response to Metzl." *Human Rights Quarterly* 19 (4)(1997): 836-859.

Barlow, John Perry. *Introduction to The Official PGP User's Guide* by Philip R. Zimmermann, Cambridge, Mass., MIT Press, 1995.

Callas, J., L. Donnerhacke, H. Finney, D. D. Shaw and R. Thayer. RFC 4880. OpenPGP Message Format. Network Working Group, 2007.

Coarelli, Filippo. "Mundus, pomerium, ager: la concezione dello spazio a Roma." *Paesaggi di potere: problemi e prospettive: atti del seminario Udine 16-17 maggio 1996*, ed. Giorgio Camassa, Armando De Guio and Francesca Veronese, 285-292. Roma: Edizioni Quasar, 2000.

de Groot, Huig. *De iure belli ac pacis libri tres, in quibus ius naturae et gentium, item iuris publici praecipua explicantur.* Parisiis: apud, Nicolaum Buon, 1625.

Diffie, Whitfield and Martin E. Hellman. 1976a. "Multiuser Cryptographic Techniques." Proceedings of the June 7-10, 1976, National Computer Conference and Exposition.

Diffie, Whitfield and Martin E. Hellman. 1976b. "New Directions in Cryptography." *IEEE Transactions on Information Theory* 22 (6): 644-654.

Feinberg, Ashley. “The World Just Got a New, Entirely 3D-Printed Metal Gun.” *Gizmodo*, 2014. Viewed October 27, 2014. http://gizmodo.com/the-world-just-got-its-second-all-3d-printed-metal-gun-1651348942.

Fioriglio, Gianluigi. *Hackers, Passato e presente.* Roma: Nuova cultura, 2010.

Fukuyama, Francis. *The End of History and the Last Man.* New York; Toronto; New York: Free Press; Maxwell Macmillan Canada; Maxwell Macmillan International, 1992.

Haker, Hille, Erik Borgmann and Stephan van Erp. “Introduction: Cyberspace – Cyberethics – Cybertheology.” *Concilium* 40 (1) (2005): 7-11.

Hobbes, Thomas. *Leviathan or The Matter, Forme and Power of a Common Wealth Ecclesiasticall and Civil.* London: Printed for Andrew Crooke, 1651.

Horn, Eva and Sara Ogger. “Knowing the Enemy: The Epistemology of Secret Intelligence.” *Grey Room* 11 (2003): 58-85.

Hulette, Elisabeth. “Police Can Require Cellphone Fingerprint, not Pass Code.” *The Virginian-Pilot*, 2014. Viewed October 30, 2014. http://hamptonroads.com/2014/10/police-can-require-cellphone-fingerprint-not-pass-code.

Jessup, Philip C. and Francis Deák. 1932. “The Early Development of the Law of Contraband of War I.” *Political Science Quarterly* 47 (4): 526-546. doi: 10.2307/2142952.

Jessup, Philip C. and Francis Deák. 1933a. “The Early Development of the Law of Contraband of War II.” *Political Science Quarterly* 48 (1): 62-93. doi: 10.2307/2143040.

Jessup, Philip C. and Francis Deák. 1933b. “The Early Development of the Law of Contraband of War III.” *Political Science Quarterly* 48 (3): 333-358. doi: 10.2307/2143151.

Jonas, Hans. *Gnosis und spätantiter Geist.* 2 vols. Vol. 2. von der Mythologie zur mystischen Philosophie, Forschungen zur Religion und Literatur des Alten und Neuen Testaments. Göttingen: Vandenhoeck & Ruprecht, 1954.

Kelsen, Hans. *Reine Rechtslehre. Mit einem Anhang: Das Problem der Gerechtigkeit.* 2 ed. Wien: Franz Deuticke, 1960.

Kerben, Jason. “The Dilemma for Future Communication Technologies: How to Constitutionally Dress the Crypto-Game.” *CommLaw Conspectus* 5 (1997): 125-152.

Metzl, Jamie F. “Information Technology and Human Rights.” *Human Rights Quarterly* 18 (4)(1996): 705-746.

Norman, Bruce. *Secret Warfare.* New York: Dorset Press, 1973.

Reiman, Phillip E. “Cryptography and the First Amendment: The Right to be Unheard.” *The John Marshall Journal of Information Technology & Privacy Law* 14 (2) (1996): 325-345.

Rivest, R.L., A. Shamir and L.M. Adleman. Cryptographic communications system and method, patent US 4405829 A. 1983.

Schmitt, Michael *N. Tallinn Manual on International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence.* Cambridge-New York Cambridge University Press, 2013.

Schneier, Bruce. *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* New York: Wiley, 1993.

Schwartzbeck, Michael. 1997. *Encryption Technologies,* formerly Top Secret, approved for release by NSA with redactions September 10, 2014. National Security Agency.

Stay, Ronald J. “Cryptic Controversy: U.S. Government Restrictions on Cryptography Exports and the Plight of Philip Zimmermann.” *Georgia State University Law Review* 13 (2) (1997): 581-604.

Stefik, Mark. *Internet Dreams. Archetypes, Myths, and Metaphors.* Cambridge Mass.: MIT Press, 1996.

Warren, Samuel D. and Louis D. Brandeis “The Right to Privacy.” *Harvard Law Review* 4 (5)(1890): 193-220.

Zimmermann, Philip R. *Pgp: Source Code and Internals.* Cambridge, Mass.: Mit Press, 1995.

SMUGGLING ANTHOLOGIES READER

PREVIEW

SMUGGLING

Smuggling Anthologies Reader

Publisher Museum of Modern
and Contemporary Art,
Dolac 1/II, Rijeka, Croatia
www.mmsu.hr

For the publisher Slaven Tolj
Editor in chief Ana Peraica
Editorial board Giuliana Carbi,
Sabina Salamon, Marija Terpin Mlinar

Authors Ana Peraica, Sabina Salamon, Giuliana Carbi, Marija Terpin Mlinar, Marija Mitrović, Tomislav Brajnović, Stephan Steiner, Gia Edzgveradze, Darinka Kolar Osvald, Aleksandar Garbin, Dragica Čeč, Petra Jurjavčič, Federico Sancimino, Michele Di Bartolomeo, Društvo bez granica, Róbert Tasnádi, Anja Medved, Bojan Mitrović, Jan Lemitz, Victor López González, Božo Repe, Melita Richter, Azra Akšamija, Balázs Beöthy, Mira Hodnik, Tanja Žigon, Krešo Kovačiček & Associates, Milan Trobič, Monika Fajfar, Anonymous, Tanja Vujasinović, Can Sungu, Zanny Begg, Oliver Ressler, Vana Gović, Alexandra Lazar, Cristiano Berti, Soho Fond, Marco Cechet, Lorenzo Cianchi, Michele Tajariol, Ana Smoković, Hassan Abdelghani, Ralf Čeplak Mencin, Dušan Radovanović, Ivo Deković, Igor Kirin, Nikola Ukić, Federico Costantini

Translations Petra Julia Ujawe and Nilesh Ujawe (Slovenian to English), Lidija Toman and Slobodan Drenovac (Croatian to English), Rajka Marinković (Marija Mitrović's essay), Virginia Dordei and Maja Lazarević Branišelj (Italian to English)
English copyediting Kate Foley

Photo documentation Robert Sošić (set up in Rijeka), Aleksandra S. Mutić (set up in Idrija), Fabrizio Giraldi

Design Mileusnić+Serdarević
Printed by Kerschoffset
Zagreb, January 2015
Catalogue no. 333
ISBN 978-953-6501-93-9

CIP zapis dostupan u računalnom
katalogu Sveučilišne knjižnice
Rijeka pod brojem 130606039

Culture

EU culture — This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

mmsu

SMUGGLING
ANTHOLOGIES
READER

SMUGGLING

CONTENTS

3 To smuggle vs. to be smuggled

References

[1] Vladimir Petek: *Ponte Rosso*, film still, 1971.

List of contributors
(in alphabetical order)

Aleksandar GARBIN, artist, Rovinj
Aleksandra LAZAR, freelance curator, Belgrade/London
dr. Ana PERAICA, independent scholar, Split
Ana SMOKROVIĆ, teaching assistant, Faculty of Philosophy and Social Sciences, Rijeka
Anja MEDVED, artist, Nova Gorica
dr. Azra AKŠAMIJA, Professor at Faculty of Architecture, MIT
Balázs BEÖTHY, artist, Budapest
dr. Bojan MITROVIĆ, independent scholar, Trieste
dr. Božo REPE, Professor at University of Ljubljana, Ljubljana
Can SUNGU, artist, Istanbul/Berlin
Cristiano BERTI, artist, Ancona
Darinka KOLAR OSVALD, curator at Museum of Slovenian Police, Ljubljana
dr. Dragica ČEČ, Assistant Professor at University of Primorska, Koper
Društvo bez granica, art association, Rijeka
Dušan RADOVANOVIĆ, artist, Belgrade
dr. Federico COSTANTINI, Assistant Professor at University of Udine
Federico SANCIMINO and Michele DI BARTOLOMEO, financial police, Gorizia
Gia EDZGVERADZE, artist, Düsseldorf
dr. Giuliana CARBI, President of Trieste Contemporanea, Trieste
Hassan ABDELGHANI, artist, Pula
Igor KIRIN, artist, Düsseldorf
Irena GUBANC, designer and illustrator, Ljubljana
Ivo DEKOVIĆ, Professor at Hochschule for Media and Design, Aachen
Jan LEMITZ, artist, Düsseldorf
Krešo KOVAČIČEK, artist, Rijeka
Lorenzo CIANCHI, artist, Milano
Marco CECHET, artist, Bologna/Berlin
dr. Marija MITROVIĆ, Professor at Faculty of Humanities, University of Trieste
Marija TERPIN MLINAR, curator at Municipal Museum of Idrija
dr. Melita RICHTER, Professor at Faculty of Humanities, University of Trieste
Michele TAJARIOL artist, Pordenone
dr. Milan TROBIČ, journalist at RTV Slovenia, Ljubljana
dr. Mira HODNIK, archive adviser in the Historical Archives Ljubljana, Idrija
Monika FAJFAR, art historian, Ljubljana
Nikola UKIĆ, artist, Düsseldorf
Oliver RESSLER, artist, Vienna
Petra JURJAVČIČ, cultural anthropologist, Idrija
Ralf ČEPLAK MENCIN, curator for Asia and Oceania at Slovenian Ethnographic Museum, Ljubljana
Róbert TASNÁDI, communication researcher, assistant at University of West Hungary, Szombathely
Sabina SALAMON, curator at Museum of Modern and Contemporary Art, Rijeka
Soho FOND, artist, Tallinn
dr. Stephen STEINER, Professor at University of Vienna
Tanja VUJASINOVIĆ, artist, Zagreb
dr. Tanja ŽIGON, Assistant Professor, Faculty of Arts in Ljubljana
Tomislav BRAJNOVIĆ, Assistant Professor at Academy for Applied Arts, Rijeka
Vana GOVIĆ, freelance curator, Rijeka
Victor LÓPEZ GONZÁLEZ, artist, Valencia/Leipzig
Zanny BEGG, artist and writer, Sidney

Thank you for participating

Alessio BOZZER and Giampaolo PENCO, Videoest srl
Lyz GLYNN, artist, Boston/Los Angeles
Dora MEDVED, Davorka MEDVED, Damir MEDVED,
Vesna LUKANOVIĆ and Robert ZENERAL,
members of Društvo bez granica, Rijeka
Denise ZANI, independent journalist

Museum of Modern and Contemporary Art, Rijeka

Group exhibition *Smuggling Anthologies*, MMSU & Mali Salon, October 22 – December 4, 2013
Artists: Društvo bez granica, Hassan Abdelghani, Azra Akšamija, Zanny Begg, Balász Beöthy, Cristiano Berti, Tomislav Brajnović, Marco Cechet, Lorenzo Cianchi, Ivo Deković, Soho Fond, Aleksandar Garbin, Janez Janša, Janez Janša, Janez Janša, Igor Kirin, Krešo Kovačiček & Associates, Victor López González, Anja Medved, Dušan Radovanović, Oliver Ressler, Can Sungu, Michele Tajariol, Robert Tasnádi, Nikola Ukić, Tanja Vujasinović
Archival material: Police Museum, Zagreb

Solo exhibition *Work* by Janez Janša, Janez Janša, Janez Janša, Mali Salon, November 14 – April 12, 2013

Performance *Tobacco Standard*, Krešo Kovačiček & Associates, ferry terminal and railway bridge, October 24, 2013 at 7 pm

Screening , Mini Art Kino Croatia
November 18 – 20, 2013:
My Border by Nadja Velušček and Anja Medved, November 18
Crossroads of the Iron Curtain by Róbert Tasnádi, November 19
Ariel by Ivo Deković, Igor Kirin, Nikola Ukić
Green Border by Nikica Klobučar and Tomislav Šoban, November 20

Symposium, Astronomical Centre, Rijeka October 23 – 24, 2013
Lecturers: Cristiano Berti, Dragica Čeč, Sándor Goják, Mira Hodnik, Aleksandra Lazar, Dora Medved, Melita Richter, Ana Smokrović, Ksenija Šabec, Róbert Tasnádi, Franc Trček

Idrija Municipal Museum

Workshops “The Methodology of Record Keeping and Documenting Residues of the Former Rapallo Border” and “Examples of Good Practice in Exploitation of Former Borders Forts Potential in Favour of Sustainable Development and Tourism”, Idrija Municipal Museum, April 10 – 11, 2014

Group exhibition *Smuggling Anthologies/ (Pre)tihotapljene antologije*, Idrija Municipal Museum, September 10 – November 2, 2014
Artists: Društvo bez granica, Cristiano Berti, Marco Cechet, Lorenzo Cianchi, Ivo Deković, Irena Gubanc, Igor Kirin, Jan Lemitz, Victor López González, Anja Medved, Dušan Radovanović, Soho Fond, Michele Tajariol, Nikola Ukić, Tanja Vujasinović,
Items, photos, documentary and archival material: Slovenian Police Museum, Ljubljana; National Gallery of Slovenia, Ljubljana; Historical Archives Ljubljana, Idrija Unit, Idrija; Austrian State Archive, Vienna; Robert Fonda, Marija Krajnik, Ivica Kavčič, Federico Sancimino, Michele Di Bartolomeo, Urban Šlabnik
Live music performance of the song *Kontrabant*: Adijo kultura

Thematic exhibition *Cheat Sheet from A to Z*, October 2 – November 2, 2014

Screening *Smugglers On Canvas*, An Evening of Documentary Films on Smuggling, November 4, 2014
Save the Film! by Antonio Perajica
My Border by Nadja Velušček and Anja Medved

Museum story time for children *Shhh, Smugg-lers!*, October 11, 2014
Film *Melhiorca and Her Smuggling Bag*, January, 2015

Trieste Contemporanea, Trieste

Group exhibition *Smuggling Anthologies*, Studio Tommaseo, Trieste, November 7 – December 17, 2014
Artists: Društvo bez granica, Azra Akšamija, Zanny Begg, Cristiano Berti, Alessio Bozzer, Tomislav Brajnović, Marco Cechet, Lorenzo Cianchi, Ivo Deković, Soho Fond, Igor Kirin, Krešo Kovačiček & Associates, Victor López González, Anja Medved, Dušan Radovanović, Oliver Ressler, Can Sungu, Michele Tajariol, Nikola Ukić, Nadja Velušček, Tanja Vujasinović

Artist talk and video screening, Jan Lemitz, Studio Tommaseo, Trieste, November 4, 2014

Artist talk and video screening, Anja Medved, Studio Tommaseo, Trieste, November 11, 2014

Symposium, Museo Revoltella Auditorium, Trieste, November 7, 2014
Lecturers: Cristiano Berti, Tomislav Brajnović, Marco Cechet, Federico Costantini, Gia Edzgveradze, Liz Glynn, Bojan Mitrović, Marija Mitrović, Božo Repe, Ana Peraica, Melita Richter, Michele Tajariol, Denise Zani, Tanja Žigon

Screening at the symposium
Save the Film! by Antonio Perajica
Blue and Black Jeans by Alessio Bozzer, a co-production of Videoest srl and Trieste Contemporanea
A Tribute to the Soviet Underground Business Scene in Tallinn by Soho Fond

Symposium, Idrija Municipal Museum,
September 11 – 12, 2014
Lecturers: Cristiano Berti, Ralf Čeplak Mencin, Dragica Čeč, Mira Hodnik, Petra Jurjavčič, Darinka Kolar Osvald, Melita Richter, Robert Zeneral, Tanja Žigon, Stephan Steiner, Róbert Tasnádi, Milan Trobič

Curator: Sabina Salamon
Co-curator: Ksenija Orelj for *Work* by Janez Janša, Janez Janša, Janez Janša
Project manager: Nataša Šuković
Project assistent: Nadežda Elezović
Public relations: Ivo Matulić
Museum educator: Milica Đilas
Documentation: Diana Zrilić
Secretary: Tatjana Roglić Jelovica
Accountancy: Stošija Baljak Gržančić
Exhibition set-up: Sabina Salamon
Technical set-up: Vanja Pužar, Anton Samaržija
Collaborators: Kristina Barišić, Martinela Dragičević, Ivana Lučić, Dunja Tišma
Blog editors: Nadežda Elezović, Dunja Tišma
Visual identity: KKA – vizualne komunikacije
Photography, set-up: Robert Sošić
Photography, symposium: Kristina Barišić
Radio jingles: Zoran Medved, Vedrana Vrhovnik
Trailer: Kristina Barišić, Ivana Lučić
Thanks to: Željko Jamičić, Senior Curator, Police Museum, Zagreb

Curator: Marija Terpin Mlinar
Project assistant: Lili Strmšek
Public relations: Marija Terpin Mlinar, Lili Strmšek
Blog editor: Lili Strmšek
Workshop mentors: Aleksander Jankovič Potočnik, Anton Marn, Ad Pirum; Marija Terpin Mlinar
Exhibition set-up: Dado Andder, Marija Terpin Mlinar
Technical set-up: Dado Andder, Jože Bogataj, Edi Božič
Collaborators: Anja Brelih, Mirjam Gnezda Bogataj, Davorin Lenko, Sandro Oblak, Grega Žorž
Visual identity: Dado Andder, Studio Koder d.o.o. Idrija
Trailer: Dado Andder, Studio Koder d.o.o. Idrija
Film: Matjaž Mrak, Friendly production; Nika Leskovšek, Petra Stare, Andrej Štular, Rok Šinkovec, Boris Romih
Translation: Ujawe Translations, Petra Julia Ujawe s.p.
Photography, set-up and symposium: Aleksandra S. Mutić

Curator: Giuliana Carbi
Project assistants: Costanza Grassi, Bojan Mitrović
Public relations: Giuliana Carbi, Costanza Grassi
Exhibition set-up: Manuela Schirra
Technical set-up: Antonio Giacomin, Arlon Stok
Collaborators: Aldo Cherubini, Virginia Dordei, Serena Maffei, Emanuela Marassi, Massimiliano Marianni, Alessandra Nicolini, Giampaolo Penco, Marco Rotondo
Web editor: Arlon Stok
Visual identity: Manuela Schirra
Translations: Virginia Dordei, Liana Rotter
Photography, set-up and symposium: Fabrizio Giraldi, Aleksandra S. Mutić

**The project was made possible
thanks to the financial support of:**

Ministarstvo
kulture
Republika
Hrvatska
*Ministry
of Culture
Republic
of Croatia*

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA KULTURO

REGIONE AUTONOMA
FRIULI VENEZIA GIULIA

comune di trieste

Sponsors

ZIDGRAD
G.P. IDRIJA d.d.

Zavarovalnica
Maribor
Naprej z vami

KOMUNALA d.o.o.
IDRIJA Carl Jakoba 4

triglav

kliping

www.rps.si

dp
tiskarna

KASKADER
ZAHTEVNA TERENSKA DELA

Media partners

Kulturpunkt.hr

MojaRijeka.hr

NOVI LIST

primorske novice

Primorski val

HRT RADIO RIJEKA

RI TV

SMUGGLING
ANTHOLOGIES

Smuggling Anthologies

This reader is published in conjunction with the exhibitions/symposia/research within the project *Smuggling Anthologies*

m m s u

MESTNI MUZEJ IDRIJA
MUZEJ ZA IDRIJSKO IN CERKLJANSKO

tsc
ont

creative commons