TILT (TILBURG INSTITUTE FOR LAW, TECHNOLOGY, AND SOCIETY)
LAW & TECHNOLOGY
WORKING PAPER SERIES

"My Computer Is My Castle": New Privacy Frameworks to Regulate Police Hacking

Ivan Škorvánek[1], Bert-Jaap Koops[1], Bryce Clayton Newell[2], and Andrew Roberts[3]

[1]Tilburg University, TILT
I.Skorvanek@uvt.nl, e.j.koops@uvt.nl

[2]University of Kentucky, School of Information Science
brycenewell@uky.edu

[3]University of Melbourne, Melbourne Law School
arob@unimelb.edu.au

TILT Law & Technology Working Paper No 003/2019
01 April 2019, Version: 1.0

This paper can be downloaded without charge from the
Social Science Research Network Electronic Paper Collection
http://ssrn.com/abstract=3348711

An overview of the TILT Law & Technology Working Paper Series can be found at:
http://www.tilburguniversity.nl/faculties/law/research/tilt/publications/workingpapers/

Pre-Press Draft, February 2019; Forthcoming in BYU Law Review

citation: Ivan Škorvánek, Bert-Jaap Koops, Bryce Clayton Newell, and Andrew Roberts**,** "My Computer Is My Castle": New Privacy Frameworks to Regulate Police Hacking, Pre-Press Draft, February 2019, forthcoming in *BYU Law Review*.

Abstract

Several countries have recently introduced laws allowing the police to hack into suspects' computers. Legislators recognize that police hacking is highly intrusive, e.g., to personal privacy, but consider it justified by the increased use of encryption and mobile computing—both of which challenge traditional investigative methods. Police hacking also exemplifies a major challenge to the way legal systems deal with, and conceptualize, privacy. Existing conceptualizations of privacy and privacy rights do not always adequately address the types and degrees of intrusion into individuals' private lives that police hacking powers enable. Traditional privacy pillars such as the home and secrecy of communications do not always apply to computer-based police investigations in an era of mobile technologies and ubiquitous data. In this Article, we conduct a comparative legal analysis of criminal procedure rules in the United States, Germany, Italy, the Netherlands, and the United Kingdom to see which privacy frameworks law-makers and courts apply when regulating policy hacking. We show that while classic privacy frames of inviolability of the home and secrecy of communications remain adequate for some forms of police hacking (observation and interception), they fail to capture novel and fundamentally different ways in which the most intrusive forms of police hacking (covert online searches and remote surveillance) impact privacy in twenty-first-century society. Our analysis shows the emergence of two new frameworks that have the potential to begin filling this void: 1) a container-based approach, focusing on the computer as protection-worthy in itself—or the "informatic home," and 2) a content-based approach, focusing on the protection of data—or "informatic privacy." Since both approaches have valuable benefits and potential drawbacks, we propose that a complementary application of the two might work best to capitalize on their advantages over traditional privacy frameworks to regulate police hacking.

This is a pre-press draft; forthcoming in *BYU Law Review*

"My Computer Is My Castle": New Privacy Frameworks to Regulate Police Hacking*

Ivan Škorvánek,[1] Bert-Jaap Koops,[2] Bryce Clayton Newell,[3] and Andrew Roberts[4]

ABSTRACT

Several countries have recently introduced laws allowing the police to hack into suspects' computers. Legislators recognize that police hacking is highly intrusive, e.g., to personal privacy, but consider it justified by the increased use of encryption and mobile computing—both of which challenge traditional investigative methods. Police hacking also exemplifies a major challenge to the way legal systems deal with, and conceptualize, privacy. Existing conceptualizations of privacy and privacy rights do not always adequately address the types and degrees of intrusion into individuals' private lives that police hacking powers enable. Traditional privacy pillars such as the home and secrecy of communications do not always apply to computer-based police investigations in an era of mobile technologies and ubiquitous data.

In this Article, we conduct a comparative legal analysis of criminal procedure rules in the United States, Germany, Italy, the Netherlands, and the United Kingdom to see which privacy frameworks law-makers and courts apply when regulating policy hacking. We show that while classic privacy frames of inviolability of the home and secrecy of communications remain adequate for some forms of police hacking (observation and interception), they fail to capture novel and fundamentally different ways in which the most intrusive forms of police hacking (covert online searches and remote surveillance) impact privacy in twenty-first-century society. Our analysis shows the emergence of two new frameworks that have the potential to begin filling this void: 1) a container-based approach, focusing on the computer as protection-worthy in itself—or the "informatic home," and 2) a content-

---

* The research for this Article was made possible by a grant from the Netherlands Organisation for Scientific Research (NWO), project number 453-14-004. We thank Leo Nobile and Aldo Sghirinzetti for research assistance. All translations in this Article are by the authors, except where otherwise indicated.

[1] PhD Researcher, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University.

[2] Professor of Regulation and Technology, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, the Netherlands.

[3] J.D., Ph.D., Assistant Professor, School of Information Science, University of Kentucky; Research Associate, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University.

[4] Associate Professor, Melbourne Law School, University of Melbourne.

based approach, focusing on the protection of data—or "informatic privacy." Since both approaches have valuable benefits and potential drawbacks, we propose that a complementary application of the two might work best to capitalize on their advantages over traditional privacy frameworks to regulate police hacking.

INTRODUCTION

In recent years, law-makers in several countries have introduced police hacking powers into their domestic law. Relatedly, scholars have noted that police use of malware is also becoming more common. These developments have been driven, at least in part, by the increasing use of "encryption and anonymization tools" by individuals and device manufacturers[5] and the proliferation of mobile computing technologies.

First, the fact that many communications services use end-to-end encryption, often by default, combined with the fact that these providers often do not fall within the scope of traditional wiretapping obligations (because they are over-the-top services rather than communications channel providers), implies that traditional interception—which takes place somewhere along the line—has become useless when it comes to capturing the contents of communications.[6] Relatedly, the increasing prevalence of hard-disk encryption also contributes to these developments.[7] Frequently,

---

[5] *See* Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570, 577, 579 n.28 (2018); Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 GEO. L.J. 989 (2018); Stephanie K. Pell, *You Can't Always Get What You Want: How Will Law Enforcement Get What It Needs in a Post-CALEA, Cybersecurity-Centric Encryption Era?*, 17 N.C. J.L. & TECH. 599 (2016); Susan Hennessey, *The Elephant in the Room: Addressing Child Exploitation and Going Dark*, HOOVER INST. (2017), http://www.hoover.org/sites/default/files/research/docs/hennessey_webreadypdf.pdf; *see also* Paul Ohm, *The Investigative Dynamics of the Use of Malware by Law Enforcement*, 26 WM. & MARY BILL RTS. J. 303, 303 (2017) (ascribing this position to the FBI as a primary justification for using malware).

[6] *See, e.g.*, MIRJA GUTHEIL ET AL., LEGAL FRAMEWORKS FOR HACKING BY LAW ENFORCEMENT: IDENTIFICATION, EVALUATION AND COMPARISON OF PRACTICES 8 (Policy Department for Citizens' Rights and Constitutional Affairs ed., 2017); Bundestag, *Pro und Contra Staats•trojaner bei der Anhörung zur Strafrechts•reform*, DEUTSCHER BUNDESTAG (June 1, 2017) https://www.bundestag.de/dokumente/textarchiv/2017/kw22-pa-recht-strafrecht/508168 (Ger.); *Ustawa o Policji uzasadnienie* [Explanatory Memorandum to the Police Act], KOMENDA GŁÓWNA POLICJI at 15-16, http://bip.kgp.policja.gov.pl/download/18/17000/UstawaoPolicji-uzasadnienie.doc (last visited Jan. 27, 2019) (Pol.); *Kamerstukken II* 2015/16, 34 372, no. 3 at 7-10 (Neth.).

[7] Felix Freiling, Christoph Safferling & Christian Rückert, *Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung: Rechtliche und technische*

investigators have still been able to identify IP addresses and other identifying information through, for example, regular use of peer-to-peer software clients[8] or software capable of scanning torrent networks.[9] However, when users move their illicit activities to the so-called "dark web," utilizing privacy-protecting measures to avoid identification, successful investigation becomes much more difficult without the use of police hacking techniques.

Second, the increase in mobile computing—notably, smartphones, laptops, and tablets—and cloud computing implies that traditional search-and-seizure powers are becoming less effective and less practical. Moreover, the rise of wireless networking, enabling broad access to the internet from many different access points, diminishes the usefulness of a wiretap on a specific access point. Often, the police will be aware of some logical address of a computer (e.g., an IP address) but not its physical location. The difficulty in locating a computer to be searched is compounded by anonymization techniques, such as onion routing, which obfuscate the source of communications or cyber-attacks. Police hacking is a useful way of countering this trend, since it enables the police to search computers remotely without having to know where they are physically located.[10]

Together, these developments are frequently captured by statements that law enforcement is "going dark" or that they are being confronted with an otherwise unsurmountable "encryption problem."[11] As framed by former FBI Director James Comey, "Going Dark" means that,

> [t]hose charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so.[12]

Herausforderungen, JURISTISCHE RUNDSCH., 19 (2018) (referring to full-disk encryption).

[8] *See, e.g.*, United States v. Blouin, CR16-307 TSZ (W.D. Wash. filed Aug. 15, 2017) (finding that peer-to-peer scanning software "is not analogous to . . . [a] NIT [because] [i]t does not place any program on the target computer or give the Government access to anything other than the items in the 'shared' folder, which are available to anyone using a similar peer-to-peer file-sharing program."); United States v. Gray, 641 Fed.Appx. 462, 464 (6th Cir. 2016); United States v. Ganoe, 538 F.3d 1117 (9th Cir. 2008).

[9] *See, e.g.*, United States v. Hoeffener, No. 4:16CR00374 JAR/PLC, *1 (E.D. Mo. Aug. 25, 2017).

[10] *See, e.g.*, *Id.* at 19 (discussing challenges of anonymization); *Kamerstukken II* 2015/16, 34 372, no. 3 at 10-13 (Neth.).

[11] LEX GILL, TAMIR ISRAEL & CHRISTOPHER PARSONS, SHINING A LIGHT ON THE ENCRYPTION DEBATE: A CANADIAN FIELD GUIDE 39, 51 (May 2018).

[12] James B. Comey, Director, Federal Bureau of Investigation, *Going Dark: Are*

Comey tied the challenges faced by the FBI directly to the rise of encryption, both to intercepting "data in motion" (encrypted transmission) and accessing "data at rest" (encrypted storage).[13] As a consequence, the argument goes, allowing the police to covertly access computers remotely may well be the best way to enable law enforcement to retain the capacity to collect evidence, without resorting to cruder and (even) more contestable measures such as compulsory backdoors in communications services.[14]

Against this backdrop, a surprising number of countries have introduced varying police hacking powers into their domestic law. Legislators in these countries generally recognize the (potential) intrusiveness of police hacking into individual lives and privacy but have determined that the risks inherent in "going dark" necessitated legislative action. Notably, police hacking powers vary considerably by jurisdiction, and because of the varying functionalities and scopes of hacking powers, there is considerable confusion about the ways and degrees in which these new powers (might) infringe fundamental rights. Police hacking is one of several developments that challenge the way legal systems deal with privacy: legal frameworks based on traditional notions of home and communications content as key pillars of privacy protection do not apply well to computer investigations in an era of mobile technologies and ubiquitous data.[15] Instead, new frameworks seem to arise that may be better suited to contemporary digital investigations, based on the notion that computers, rather than or besides homes, should be people's bastion of privacy protection: "my computer is my castle."[16]

Technology, Privacy, and Public Safety on a Collision Course?, FBI (Oct. 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

[13] *Id.*

[14] *See* Bert-Jaap Koops & Eleni Kosta, *Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark*," 34 COMPUTER L. & SECURITY REV. 890 (2018) (arguing that "legal hacking powers . . . could be the only realistic policy option to preserve some light in an era of dark communication channels").

[15] *See infra*, Part IV(A); Bert-Jaap Koops, *On legal boundaries, technologies, and collapsing dimensions of privacy*, 3 POLITICA E SOCIETÀ 247 (2014) (discussing how current privacy frameworks are inadequate to regulate digital investigations); *see also* Bert-Jaap Koops, Bryce Clayton Newell, Tjerk Timan, Ivan Škorvánek, Tomislav Chokrevski & Maša Galič, *A Typology of Privacy*, 38 U. PA. J. INT'L L. 483 (2017) (for an overview of the current pillars of privacy protection).

[16] *Cf.* Michael D. Ricciuti & Kathleen D. Parker, *My Phone Is My Castle: Supreme Court Decides that Cell Phones Seized Incident to Arrest Cannot Be Subject to Routine Warrantless Searches*, 58 BOS. B.J. 7 (2014) (discussing cell phones as new object of privacy protection in the context of searches incident to arrest); Bert-Jaap Koops, Bryce Clayton Newell & Ivan Škorvánek, *Location Tracking By Police: The Regulation of "Tireless and Absolute Surveillance,"* 9 U.C.I. L. REV. (2019) (forthcoming) (discussing new privacy paradigms

In this Article, we identify and compare how five countries conceptualize the infringement of privacy in the context of police hacking. We examine what these varying approaches can tell us about the status and nature of privacy protections in the twenty-first century. We conduct a comparative analysis of privacy protection within the procedural criminal law of five countries in which police hacking has been regulated and/or in which there has been interesting discussion about the issue: Germany, Italy, the Netherlands, the United Kingdom, and the United States. These jurisdictions were chosen based on their centrality to a larger, ongoing research project on protecting privacy in the twenty-first century and include a mix of common-law and civil-law jurisdictions. The broader methodological considerations driving this country selection have been outlined elsewhere.[17] We analyze statutory and case law at the federal level in our countries to highlight the primary safeguards in the law; lower-level regulations and guidelines are beyond the scope of this paper. As we are interested in the rationale for imposing certain safeguards, we also analyze legislative histories and policy debates to determine which privacy frameworks have guided law-makers to impose (or not impose) certain safeguards. Our paper is limited to hacking by law enforcement authorities; we leave aside hacking by intelligence agencies.

The paper is structured as follows. In Part I, we explain what police hacking entails, in terms of the terminology involved, the ways in which police can hack into computers, and the goals or functionalities of such hacking. Part II gives a bird's-eye overview of police hacking regulations in our five jurisdictions. We then analyze the regulation of police hacking in more detail in Part III, discussing which safeguards apply to the different functionalities of police hacking. Part IV focuses on the privacy paradigms that underlie these safeguards; we highlight to what extent law-makers resort to classic privacy frames (such as protection of homes and communications

---

emerging in the context of police location tracking). *See also infra* Part IV(B).

[17] *See* Koops et al., *supra* note 15, at 504-506. In this Article, we exclude the jurisdictions addressed in the larger project that lack regulation or substantial doctrinal literature on police hacking (Canada, Czech Republic, and Poland). In Canada, police hacking powers (often referred to as "lawful access" provisions) have "languished on the Canadian agenda" due to a series of unfavorable "federal elections and successful civil liberties opposition to the legislation, along with businesses' resistance." Christopher Parsons, *Stuck on the Agenda: Drawing Lessons from the Stagnation of "Lawful Access" Legislation in Canada*, *in* LAW, PRIVACY AND SURVEILLANCE IN CANADA IN THE POST-SNOWDEN ERA 261 (Michael A. Geist ed., University of Ottawa Press 2015). In Poland, police hacking is not regulated in criminal procedure law, although a provision allowing covert access to data has been recently included in Art. 19 of the Police Act. Nevertheless, the issue has not been taken up extensively in the domestic literature. In the Czech Republic, explicit regulation of police hacking does not exist, and we could not unearth any relevant sources showing that it is taking place under more general surveillance provisions, despite hints of it being so.

content) to guide their stipulation of safeguards, and which new privacy frames are emerging in the regulation of police hacking. The Conclusion summarizes the main findings and provides an outlook on the traditional and new privacy frames used to regulate police hacking.

I. BACKGROUND: POLICE HACKING

A. Terminology

Before examining how and where police hacking takes place, we need to explain the terminology used. Law-makers and authors use an amazing variety of terms to refer to activities by law enforcement agencies that enable them to covertly access computers.[18] A simple umbrella term is "police hacking"[19]—or, more generally (although it also includes hacking by security and intelligence agencies), "government hacking."[20] Similarly, some authors talk of "lawful hacking," to distinguish the practice from criminal hacking.[21] To avoid negative associations that the term "hacking" may trigger, however, governments tend to avoid the term altogether and use some suitably vague or technical-sounding term instead. For example, in US courts, the use of the term "malware" to describe authorized government hacking activities has also occasionally proven controversial, with at least one federal district court noting that the term, as defined in Black's Law Dictionary,[22] was not

---

[18] Mayer, *supra* note 5, at 575 n.16 (observing that "[g]overnment documents have referred to hacking with a wide variety of terms, including Network Investigative Technique (NIT), Computer and Internet Protocol Address Verifier (CIPAV), Internet Protocol Address Verifier (IPAV), Remote Access Search and Surveillance (RASS), Remote Computer Search, Remote Search, Web Bug, Sniffer, Computer Tracer, Internet Tracer, and Remote Computer Trace"); MARCO TORRE, IL CAPTATORE INFORMATICO. NUOVE TECNOLOGIE INVESTIGATIVE E RISPETTO DELLE REGOLE PROCESSUALI 12-13 (Milano, Giuffrè Editore 2017) ("high-court case-law uses terms such as 'computer sensor' and 'intruding agent;' doctrine prefers 'online searches,' 'covert remote acquisition,' spyware, atypical captures, Trojan horses and State viruses. . . In this contribution it seems preferable to use the expression 'remote control systems' (RCS).") (internal references omitted).

[19] MIRJA GUTHEIL ET AL., *supra* note 6.

[20] Mayer, *supra* note 5 (using the term "government hacking").

[21] Steven M. Bellovin, Matt Blaze, Sandy Clark & Susan Landau, *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1 (2014).

[22] Black's Law Dictionary considers "malware" slang, and forwards readers to "malicious technology," which is defined as "Any electronic or mechanical means, esp. software, used to monitor or gain access to another's computer system without authorization for the purpose of impairing or disabling the system. Examples of malicious technology are Trojan horses, time-outs, keystroke logging, and data-scrambling devices." *Malicious Technology*, BLACK'S LAW DICTIONARY (10th ed. 2014).

necessarily appropriate "[d]ue to the negative connotations associated with the word."[23] Additionally, UK law speaks of "Computer Network Exploitation" or "Equipment Interference,"[24] while in the US, the term "Network Investigative Techniques" (NITs) is frequently used.[25] The Dutch law-maker has used the overly broad term "investigation in a computer" (*onderzoek in een geautomatiseerd werk*) as a label for police hacking.[26]

Rather than using an umbrella term, however, we can also refer to police hacking based on the particular target or aims behind the activity. Thus, when police hacking aims to copy stored data, it might be called an "online search" (in Germany: *online-Durchsuchung*[27]; in Italy: *perquisizione online*[28]), and when it is targeted at intercepting communications, it might be called "source telecommunications surveillance" (in Germany, *Quellen-TelekommunikationsÜberwachung*[29]) or simply "interception" as in the US.[30] Frequently, police hacking is also referred to in terms of the primary tool used: malware or "policeware,"[31] "State viruses,"[32] "State Trojans" or "federal Trojans,"[33] or "intruder agents."[34] In Italy, the most commonly used term to indicate police hacking is "computer sensor" (*captatore*

---

[23] United States v. Matish, 193 F. Supp. 3d 585, at 601-02 (E.D. Va. 2016). *But see* United States v. Werdene, 883 F.3d 204 (3rd Cir. 2018) ("The FBI's solution was the NIT, a form of government-created malware that allowed the FBI to retrieve identifying information from Playpen users located all around the world."); United States v. Workman, 863 F.3d 1313 (10th Cir. 2017) (judge used the term freely to describe the government's conduct, for example, stating that, "in this case, the FBI seized and assumed control, using malware to identify and find the individuals accessing child pornography").

[24] *See* Investigatory Powers Act 2016, Code of Practice, Equipment Interference (March 2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf.

[25] Orin S. Kerr & Sean D. Murphy, *Government Hacking to Light the Dark Web: What Risks to International Relations and International Law?*, 70 STAN. L. REV. ONLINE 58, 59 (2017).

[26] Art. 126nba Dutch CCP.

[27] Freiling et al., *supra* note 7, at 18.

[28] Federica Iovene, *Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale*, 3-4 DIRITTO PENALE CONTEMPORANEO 329 (2014).

[29] Stephan Beukelmann, *Online-Durchsuchung und Quellen-TKÜ*, NEUE JURISTISCHE WOCHENSCHR. SPEZ. 440, 440 (2017).

[30] *See, e.g.*, 18 U.S. Code §2510(2)-(4) (referring to "interception" and defining "intercept" in the context of accessing electronic and oral communications).

[31] Bart Jacobs, *Policeware*, NEDERLANDS JURISTENBLAD 2761 (2012).

[32] Cass. Sez. VI, 26 maggio 2015, n. 27100, CED Cass. 2015 ('Musumeci') (It.).

[33] Dennis-Kenji Kipker, *Kipker: Vom Staatstrojaner zum staatseigenen Bundestrojaner*, Z. FÜR RECHTSPOLIT. 88, 88 (2016).

[34] Cass. Sez. VI, 26 maggio 2015, n. 27100 ('Musumeci').

informatico).[35]

Where the hacking is limited to specific functionalities, such as the remote and covert search of a hard disk, more specific terms such as "online search" can be used. Such usage requires care, however: a "search" in criminal law typically refers to a one-off activity, focused on accessing existing (stored) data; in contrast, an "online search," for instance in the German context, encompasses not merely a one-off search of existing data but also real-time collection of data generated during the period of execution, making the term "online search" rather misleading.[36] Similarly, using "policeware" or "State Trojans" can be too narrow if, beyond purely remote searches, the investigatory conduct can also take the form of physically installing a keylogger on a computer or logging in to someone's account with a phished or intercepted password.

In this Article, we use the term "police hacking" for purposes of convenience, as an umbrella term that encompasses the broad array of possible police powers and methods that police might use to covertly access computers for purposes of criminal investigation. In contrast to euphemisms that serve as a rhetorical tool to downplay or obfuscate the intrusiveness of the measure, such as "Network Investigative Techniques" or "investigation in a computer," the term "hacking" clearly pinpoints the core of this investigation measure: non-consensual access to a computer. This umbrella term has the benefit of encompassing all forms of access—both physical and remote—and all kinds of tools or modes of access.

B. Modes of hacking

Police hacking can be done in different ways.[37] The main tool for police hacking is malware, which can be installed on (or delivered to) a target computer in three ways. The first and most direct form is to install malware when the police have physical access to a computer, for instance, covertly entering a dwelling to install a keylogger onto a computer[38] or uploading the software at a border check.[39] Social engineering might sometimes work to trick the targeted user into, for example, inserting an infected USB stick into their computer.[40]

---

[35] Art. 266(2) Italian CCP; Torre, *supra* note 18.

[36] Freiling et al., *supra* note 7, at 13.

[37] *See*, *e.g.*, Code of Practice, *supra* note 24, paras. 3.2-3.3(discussing various modes of police hacking).

[38] Torre, *supra* note 18, at 16.

[39] Tanja Niedernhuber, *Die StPO-Reform 2017 – wichtige Änderungen im Überblick*, JURISTISCHE ARBEITSBLÄTTER 169, 171 (2018).

[40] Giuseppe Vaciago & David Silva Ramalho, *Online searches and online surveillance:*

Because physical access is often not possible, the second basic form will be more common: remotely infecting the computer with malware. This happens largely in the same way as cybercriminals deploy malware, namely to send a message to a target computer user and use social engineering to trick the user into opening an attachment or clicking on a link, which will then covertly install the malware.[41]

As with criminal malware, the infection of someone's computer with policeware is an extremely far-reaching measure. It basically enables police to take over remote control without the computer user's knowledge, allowing copying, transmitting, altering, or removing data, turning on the webcam and microphone, etc. Hackers speak of this level of user rights in terms of "I own you," and the idea of law enforcement agencies "owning" someone might well be seen as "deeply disturbing."[42]

A third and less intrusive form of police hacking is covertly accessing a computer using the user's username and password. These credentials might be obtained through phishing and other forms of social engineering or by using software to guess passwords,[43] or they may perhaps have been found during a regular search or through interception. Hacking into a computer or cloud service using lawfully obtained credentials also allows searching all the user's data, but it does not enable remote control to the extent that malware infections do.

C. Functionalities of hacking

Police hacking and policeware can serve many purposes. These techniques have been called a "Swiss army knife"[44] and a "bulimic device,"[45] emphasizing the multi-purpose nature of police hacking. These metaphors

---

the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings, 13 DIGITAL EVIDENCE AND ELECTRONIC SIGNATURE L. REV. 88, 89 (2016).

[41] *See, e.g.*, Torre, *supra* note 18, at 15; Graf, STPO §100B ONLINE-DURCHSUCHUNG BECKOK STPO MIT RISTBV UND MISTRA (Graf ed., 31 ed. 2018).Rn. 27; Mayer, *supra* note 5, at 574-76, 583-84; OFF. OF THE INSPECTOR GEN., *infra* note 114.

[42] Jacobs, *supra* note 31, at 2762.

[43] *Kamerstukken II* 2015/16, 34 372, no. 3 at 34.

[44] BERT-JAAP KOOPS, CHARLOTTE CONINGS & FRANK VERBRUGGEN, ZOEKEN IN COMPUTERS NAAR NEDERLANDS EN BELGISCH RECHT 61 (Wolf Legal Publishers 2016).

[45] Luigi Palmieri, *La nuova disciplina del captatore informatico tra esigenze investigative e salvaguardia dei diritti fondamentali. Dalla sentenza "Scurato" alla riforma sulle intercettazioni*, DIRITTO PENALE CONTEMPORANEO 59, 60 (2018) (quoting Leonardo Filippi, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi ma sbagliano la terapia*, IL PENALISTA (Sept. 6, 2016), http://ilpenalista.it/articoli/news/lispe-perqui-intercettazione-itinerante-le-sezioni-unite-azzeccano-la-diagnosi-ma).

carry the connotations of a likely tendency of the tool to include ever more purposes (with so many nifty gadgets that the original function—cutting—is lost from sight), thriving on an unstillable hunger for ever more data. As parts II and III (*infra*) will show, most jurisdictions allow some functionalities of police hacking but not others, or they apply different conditions to the various functionalities. It is therefore important to distinguish the precise functionalities that laws on police hacking—in general or in specific cases—allow.

We draw from Dutch law to provide an overview of possible functionalities, since it has the most extensive list, as our starting point.[46] Drawing from Dutch law, we see that police hacking can, in principle, be used for the following purposes:

A. **Capturing specific types of data**. This is the least intrusive form, focusing only on acquiring certain data needed for the investigation. Dutch law gives as examples of this functionality the capture of identifying information (to establish who uses the computer) or the location of the computer (and thereby, the user). It might be seen as a digital sneak-and-peek operation.[47]

B. **Remote search of stored data**. This involves the remote and covert search of existing data, stored on the infected target computer or stored on a service provider's server (possibly in the cloud). The search may be targeted at certain data, but also involve making a mirror image of the hard disk. This is functionally equivalent to a traditional search of a place, such as a dwelling, and the seizure or mirror-imaging of computers found during the search, but a crucial difference is that the hacking-based remote search is covert: it remains unknown to the persons affected by the search. It shares, however, the characteristics of the traditional search in being a one-off search of existing data, which distinguishes it from the following functionality: remote monitoring.[48]

---

[46] *See infra*, Part II(C). In addition to these, Torre, *supra* n 18, at 18 also mentions "circumventing commercial anti-virus software" as a functionality of police hacking, but we consider this a system requirement of policeware rather than a purpose in itself.

[47] *Kamerstukken II* 2015/16, 34 372, no. 3 at 20.

[48] Dutch law treats the functionalities of a remote search (B) and remote monitoring (C) together as a single purpose (art. 126nba(1)(d) Dutch CCP), but we distinguish them as two separate functions to emphasize the important dogmatic difference between searching existing data (one-off and backward-looking) and monitoring computer use (periodic and forward-looking).

C. **Remote monitoring of computer use**. This is one of the most comprehensive functionalities, enabling the capture of data that come into existence after the malware infection during a certain period. It can take the form of a repeated remote search at certain intervals (for instance, at the end of each day searching for newly stored data) or real-time monitoring—for example, using the keylogger function to transmit in real-time what the user types or clicks. This can be combined with taking screenshots or screencasting. Thus, this functionality has a hybrid character. On the one hand, it can resemble a (repeated) search, focusing on acquiring stored data, with the atypical element that it is not only targeted at historic data but also at data that will come into existence after the order for hacking has been given. On the other hand, it can resemble real-time surveillance, virtually an equivalent of an invisible police officer looking over your shoulder at whatever you do with your computer.

D. **Intercepting communications**. With this functionality, policeware is used as an alternative means of (or as a way to implement) intercepting communications. As with traditional interception, there are two different modalities.

   1) Intercepting *electronic communications content*, such as email, texting, chatting, Skyping, or FaceTiming. Since most of these services nowadays use end-to-end encryption, and interception through the service provider is often not possible, interception at the source before encryption (or at the destination after decryption) may be the only way to capture the contents of online communications.
   2) Intercepting *oral communications*. This can be done by, e.g., using the malware to turn on the computer's microphone, which enables recording the sounds and conversations taking place with, or in the vicinity of, the device. Here, hacking functions as a means to implement oral interception, similar to placing a bug in a computer or other object in use by the suspect.

E. **Visual observation**. This functionality is served by turning on the computer's webcam, which can be used to identify the user or the computer's location, or to observe the behavior of the user or people in its environment. Here, police hacking is a functional equivalent to installing a hidden camera in the suspect's environment.

F. **Remotely deleting (unlawful) data**. This functionality—only encountered in Dutch law—enables the police to remotely remove or delete unlawful data, such as child pornography or botnet infection software, from a targeted computer. It complements the functionality of a remote search, so that, similarly to situations of a traditional search,[49] police can remove unlawful data they find on a hard disk (or in an account) from the suspect's control. It also might enable the police to remotely disinfect computers that have fallen victim to a botnet, although such interference with the computers of non-suspects would be highly controversial.

As is clear from this list, police hacking is quite varied in nature. Nevertheless, it is possible to classify the different purposes into two main categories: (1) search and (2) surveillance.[50] This grouping matches a classic distinction in criminal investigation powers, namely between investigations that are generally overt and backward-looking (i.e., looking for existing evidence)—as in search and seizure powers—and investigations that are generally covert and forward-looking (i.e., looking for evidence yet to come into existence)—through the special investigation powers of surveillance. Functionalities A, B and F (and perhaps part of C), can be classified in the category of search, while the functionalities of C, D and E fall within the category of surveillance.

II. BROAD OVERVIEW OF LAWS ON POLICE HACKING

Since the different functionalities of police hacking are usually covered by the same (or a small number of) provisions in the procedural criminal law in each of the countries we studied, we first give a high-level overview of the most relevant provisions, per country. This overview introduces the main provisions regulating police hacking powers, the functionalities allowed, and the main safeguards placed on the exercise of this power, including the authorization requirements, types of offenses for which police hacking is allowed, necessity requirements, temporal limitations, and other safeguards, where relevant.

---

[49] *Cf.* Convention on Cybercrime, art. 19(3)(d), Nov. 23, 2001, C.E.T.S. 185 (requiring Parties to adopt measures to seize or similarly secure computer data, including the power to "render inaccessible or remove those computer data in the accessed computer system").

[50] Torre, supra n 18, at 18-19 (referring to Roberto Flor, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung*, 22 RIV. TRIM. DIR. PEN. EC. 695, 697 *et seq.* (2009).

A. Germany

In Germany, police hacking has until recently only been regulated in various federal and state-level police laws in the context of preventive police activities. Only recently has the Code of Criminal Procedure (*Strafprozessordnung*, hereafter: German CCP) been amended to provide a legal basis for police hacking for criminal investigation in Sections 100a and 100b German CCP. The way in which the amendment came about has been criticized in literature[51] as well as by the experts invited to the parliamentary expert hearing.[52] The amendment was inserted into the draft of the Criminal Procedure reform rather late in the legislative process and the bill was adopted only five weeks later. This meant that a proper parliamentary and societal debate about the proposed, and highly intrusive, investigation measures could not be conducted.[53]

German regulation of police hacking is split into two provisions. Section 100a regulates the so-called source interception of telecommunications (*Quellen-TKŰ*) and Section 100b regulates the so-called online search (*Online-Durchsuchung*), which is subject to considerably stricter procedural safeguards. The origin of the split can be traced back to the landmark decision of the Federal Constitutional Court from 27 February 2008,[54] which interpreted the German Basic Law as protecting the right to integrity and confidentiality of computer systems. This new right especially protects citizens from covert interventions into their computers and can only be restricted in extremely selective circumstances. However, as an exception, if such covert intervention is restricted to obtaining the content or metadata of ongoing communications, the protection of integrity and confidentiality of computer systems does not apply and the less-weighty requirements of constitutional protection of communications must be observed. This distinction allowed the legislator to regulate source interception of communications as a special form of police hacking, essentially an extension of the existing telecommunications interception powers.

Thus, Section 100a German CCP (regulating the monitoring and recording of telecommunications) was supplemented to provide a legal basis for the source interception of telecommunications:

---

[51] Beukelmann, *supra* note 29, at 440; Tobias Singelnstein & Benjamin Derin, *Singelnstein/Derin: Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens*, NEUE JURISTISCHE WOCHENSCHR. 2646, 2646 (2017). Freiling et al., *supra* note 7, at 9-10.

[52] Bundestag, *supra* note 6.

[53] Singelnstein & Derin, *supra* note 51, at 2646.

[54] BVerfG, 1 BvR 370/07, Feb. 27, 2008 (Ger.).

> The monitoring and recording of telecommunications may also be carried out by intervening with technical means in information technology systems used by the data subject, if this is necessary, to enable monitoring and recording, in particular in unencrypted form. Content and circumstances of the communication stored on the information technology system of the person concerned may be monitored and recorded, if they could have been monitored and recorded in encrypted form in the public telecommunication network during the current transmission process.[55]

Section 100a, therefore, allows two functionalities of police hacking: monitoring and recording ongoing telecommunications and obtaining stored data if the data relate to past telecommunications that could have been monitored under the existing judicial order. The latter functionality seems to go beyond the limitation imposed by the Federal Constitutional Court.

While Section 100a merely extends the existing powers of interception of communications, Section 100b enters completely new territory, differing not so much in the means by which interception is conducted, but by the extent of the data which can be collected.[56] Section 100b reads:

> Even without the knowledge of the person concerned, technical means may be used to intervene in an information technology system used by the data subject and data may be collected therefrom (online search) . . .

This provision gives law enforcement a potentially very wide access to data in information systems, including not only past data, but also future data that becomes available in the duration of a police hacking measure. Unlike the measure under Section 100a, past data available to the investigators also include data originating from before the ordering of the measure. However, according to the prevalent opinion in doctrinal literature, the measure does not permit independent generation of data by the investigators or making changes to the data. Therefore, police are not allowed, for instance, to secretly turn on the camera or the microphone, or to delete unlawful data from the information system.[57]

Authorization requirements for both measures are regulated in Section 100e German CCP. Source interception of telecommunications under Section

---

[55] StPO §100a(1) (Ger.).

[56] Fredrik Roggan, *Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung: Elektronische Überwachungsmaßnahmen mit Risiken für Beschuldigte und die Allgemeinheit*, STV - STRAFVERTEIDIGER 821, 825 (2017).

[57] Singelnstein & Derin, *supra* note 51, at 2467; *see also* Niedernhuber, *supra* note 39, at 172.

100a must be ordered by a court upon request of the public prosecutor. The measure may be ordered by the public prosecutor in case of imminent danger (of losing evidence), provided a court confirms the claim of imminent danger within three working days. The order is valid for three months, which can be extended as long as the conditions of the order persist.

The so-called online search under Section 100b may only be ordered by the chamber of a *Landgericht* (mid-level district court). In case of imminent danger, the chamber's chairman may order the measure, but the chamber must confirm it within three working days. This order is limited to a maximum of one month, although it can be extended; any extension beyond a total of six months must be decided by the Higher Regional Court.

Both measures are restricted to a particular set of criminal offenses, where the act weighs heavily in the individual case and hacking is considered necessary. Source telecommunications interception can be ordered if there are particular grounds to suspect a perpetrator has committed a serious crime or, where punishable, attempted or prepared to commit such an act. The same standard of suspicion is required for ordering an online search, but this is further restricted to particularly serious crimes, which nevertheless comprise a rather extensive list of not only violent offenses but also particularly serious economic crimes. Police hacking thus becomes a tool available for a significantly broader set of activities than under previous police laws, where it is limited to counter-terrorism activities.[58] Both measures may be only be ordered, if the determination of the facts or the whereabouts of the perpetrator could not otherwise be obtained and may only target the suspect or persons who communicate with the accused or use the same devices.

A further limitation, particular to the German legal system, are the requirements for the protection of the core area of private life (*Kernbereich privater Lebensgestaltung*), which guarantees a highly private sphere that is free from surveillance in order to protect human dignity. This sphere consists of inner processes, such as impressions and feelings, as well as reflections, views, and experiences of a highly personal nature.[59] The core area is relevant both during data collection (avoiding intrusion as much as possible) and during data analysis and use (minimizing the intrusion by excluding all accidentally collected data that fall into the core area).[60] As data relevant to the core area cannot be adequately excluded during data collection, safeguards must be put in place at the levels of analysis and use, such as using

---

[58] *See, e.g.*, §49 Bundeskriminalamtgesetz, which permits police hacking in order to protect the body, life and freedom of persons, or such public goods on which the foundations of the state or human existence depend.

[59] BVerfG, 1 BvR 966/09, Apr. 20, 2016, Rn. 120-121 (Ger.).

[60] *Id.* Rn. 216-217.

an independent examiner to screen the information and filter out information relevant to the core area prior to making the information available to the investigating law enforcement authority.[61]

B. Italy

Police hacking is generally discussed under the moniker of "informatic sensors" (*captatori informatici*). Sometimes these "sensors" are—inspired by the German Bundestrojaner—referred to as "state viruses" (*virus di Stato*). The use of hacking for remote searches is usually referred to as an "online search" (*perquisizione online*). Although the technique appears to be massively used in practice, it is largely unregulated and there are relatively few court cases on its lawfulness as an investigation power or on the use of resulting evidence.[62] Only one proposal, regulating the functionality of oral interception, has so far been successful in the legislature, despite a number of efforts to regulate covert online investigations.[63] The under-regulation of police hacking is severely criticized in doctrinal literature, given that it is used in practice but without specific safeguards associated with constitutional privacy protection.[64]

Nevertheless, Italian courts have been rather permissive in allowing various practices of police hacking under existing legal provisions. Covertly installing a device on a computer to acquire files stored on it was held by the Supreme Court to be governed by art. 189 Italian CCP (atypical means of searching for evidence), for which a motivated order from the Public Prosecutor suffices.[65] In contrast, in the 2012 *Ryanair* case, the Supreme Court ruled out using a Trojan to monitor data flows to and from a computer on the basis of traditional search and seizure powers.[66] In relation to electronic communications interception, in the *Occhionero* case, the Supreme Court found that there was no general principle disallowing the use of Trojans under interception provisions.[67]

---

[61] *Id.* Rn. 220.

[62] Vaciago & Ramalho, *supra* note 40, at 91.

[63] *See* the overviews in Vaciago & Ramalho, *supra* note 40, 92-93 and Cass., Sez. Un., 28 aprile 2016, n. 26889, ARCH. NUOVA PROC. PEN. 2017, 76, §2 ('Scurato') (It.). The situation with respect to covert online investigations has not changed since 2016.

[64] *See* Palmieri, *supra* note 45, at 60, 65-66; Iovene, *supra* note 28, at 341.

[65] Cass., Sez. V, 14 ottobre 2009, n. 16556, CED CASSAZIONE ('Virruso') (It.), confirmed in Cass., Sez. VI, 27 novembre 2012, n. 254865 ('Bisignani') (It.), mentioned in Vaciagio & Ramalho, *supra* note 40, 92.

[66] Torre, *supra* n 18, 48.

[67] Cass., Sez. V, 20 ottobre 2017, n. 15512 ('Occhionero') (It.). *See also* Carola Frediani, *Trojan per intercettazioni nelle indagini, via libera dalla Cassazione*, LA STAMPA (Oct. 25, 2017), http://www.lastampa.it/2017/10/25/italia/trojan-per-intercettazioni-nelle-indagini-

The use of Trojans for intercepting communications, particularly oral interception through turning on the computer's microphone, has triggered more case law. In the *Bisignani* case, the investigatory judge authorized this on the basis of art. 266(2) Italian CCP (interception of oral communications).[68] In the *Musumeci* case, the Supreme Court found that installing spyware (*programma spia*) on a portable device that turned on the microphone was a form of oral interception, and that this can only take place "in clearly circumscribed places, identified at the outset, and not wherever the subject might be."[69] However, this judgment was overturned in 2016 by the United Sections of the Supreme Court in the *Scurato* case,[70] according to which such use of a Trojan is effectively not allowed at all except in organized-crime investigations.[71]

In statutory law, only the use of Trojans for oral interception targeting mobile devices has been specifically regulated. In 2017, a law was passed to amend article 266(2) Italian CCP so that oral interception (in Italian terms: interception of communications "between people present") can also be conducted by inserting an informatic sensor on a mobile electronic device.[72] An investigative judge must authorize the measure upon a prosecutor's request. The decree authorizing the hacking must mention why this measure is necessary, as well as—if the crime is not one of the listed serious crimes—"the places and the time, also indirectly determined, in relation to which the activation of the microphone is permitted."[73]

C. Netherlands

Until recently, a police power to access computers remotely and covertly was very limited.[74] Police could covertly access computers in two specific situations,[75] but only to intercept communications, not to search the (data

---

via-libera-dalla-cassazione-R0jMpFvJJZAq33P4a9oZII/pagina.html.

[67] Cass., Sez. V, 20 ottobre 2017, n. 15512 ('Occhionero') (It.).

[68] Cass., Sez. VI, 27 novembre 2012, n. 254865 ('Bisignani') (It.).

[69] Cass., Sez. VI, 26 maggio 2015, n. 27100 ('Musumeci') (It.).

[70] Cass., Sez. Un., 28 aprile 2016, n. 26889 ('Scurato') (It.).

[71] *Id.* at §§6, 7. For a more detailed discussion of the Italian case law, *see infra*, Part III.

[72] Law of 29 December 2017, no. 216. Note that the law's entry into effect has been postponed to March 2019.

[73] Art. 267(1) Italian CCP.

[74] Bert-Jaap Koops & Jan-Jaap Oerlemans, *Formeel strafrecht en ICT*, *in* STRAFRECHT EN ICT 117, 175 (Bert-Jaap Koops & Jan-Jaap Oerlemans eds., 2019).

[75] One situation is entering a dwelling to place a bug for oral interception; the other is accessing a computer as a technical means to execute an order for intercepting telecommunications. *See* Bert-Jaap Koops, *Criminal Investigation and Privacy in Dutch Law* at 17, 38 (2016), http://ssrn.com/abstract=2837483.

stored on the) computer. In June 2018, however, a law was passed to enable legal hacking. The Computer Crime III Act (*Wet computercriminaliteit III*) will introduce legal hacking as a special investigatory power in the Dutch Code of Criminal Procedure (Dutch CCP).[76] The Act is expected to enter into force in early 2019.

The provisions introduced by the Computer Crime III Act involve a far-reaching and broad set of powers combined within one single provision. The basic idea is that computers can be covertly accessed remotely, in order to perform a variety of follow-up investigatory activities. These follow-up activities (which thus indicate the purposes for which remote covert access is allowed) are exhaustively mentioned in art. 126nba(1) Dutch CCP:

A. Determining certain characteristics (especially the identity or location) of the computer or the user.
B. Recording confidential communications (both telecommunications and oral interception).
C. Systematic observation, where the remote access facilitates observation.[77]
D. Securing data (both data stored on the computer and data that enter the computer after the remote access) for the period authorised in the order.
E. Rendering data inaccessible, for example to delete unlawful data from the user's computer (usually after copying the data for evidential purposes).

This power can be applied for a period of four weeks, which can be prolonged repeatedly, each time for four weeks. It requires authorization from an investigatory judge and from the Council of Procurators-General after advice from a technical-legal advisory body (Central Examination Committee).[78] It can be used for investigating serious crimes: remote access for the goals mentioned under A, B, and C is possible for pre-trial detention crimes (generally, crimes carrying a maximum of at least four years' imprisonment) that seriously breach the rule of law; access for the goals mentioned under D and E is only possible for crimes carrying a maximum penalty of at least eight years' imprisonment, and for specially designated felonies.[79]

Only computers "in use with the suspect" can be investigated remotely.

---

[76] See *Kamerstukken I*, 2016/17, 34 372, A. While the Act has been accepted by Parliament, it has not yet (as of January 2019) been published in the official journal (*Staatsblad*) or entered into force.

[77] Art. 126g Dutch CCP.

[78] *Kamerstukken II* 2015/16, 34 372, no. 3, at 37.

[79] This particularly involves felonies where "there is often no other clue" than to use the present power, such as botnet infections, child pornography, grooming, and other computer-related crimes. *Kamerstukken II* 2015/16, 34 372, no. 3, at 29.

Depending on the circumstances, this might involve the laptop or smartphone of the suspect's co-inhabitants, friends, or relatives, if the suspect (more or less regularly, e.g., more than just once or twice) uses these devices.

Various safeguards are in place. For example, the order should specify the way the power is to be used and, for prolongation of use, the investigatory judge must give renewed authorization. The software used for remotely infecting computers should also conform to certain technical requirements.[80] The power is to be executed by specifically designated technical investigation officers, while the collected data will be analyzed by officers investigating the case; this functional separation between technical and tactical investigation officers is an important safeguard.[81] Afterwards, the software used should, in principle, be removed from the user's computer unless that is too difficult or risky; in the latter case, the infected computer's administrator should be notified so that they can (try to) remove the software on their own.[82] Also, relevant subjects (*betrokkenen*) should be notified, unless this damages the investigation.[83]

D. United Kingdom

The framework that regulates interference with computers and other electronic devices ("equipment interference") in the United Kingdom is found in set of relatively complex provisions that, together, comprise Part 5 of the Investigatory Powers Act 2016 ("the IPA"). This part of the Act is supplemented by a statutory Code of Practice (hereafter "the Code").[84] This is intended to be read in conjunction with the primary legislation and provides guidance to public authorities responsible for authorizing interference. Such codes have become an increasingly common means of regulating investigatory powers in the United Kingdom. They have an unusual legal status. The requirement to issue them is usually set out in the primary legislation that confers the investigatory powers to which they relate,[85] but the codes do not themselves constitute primary legislation. Nevertheless, codes for traditional investigatory powers have been the subject of the kind of interpretive inquiry usually reserved for primary legislation.[86]

---

[80] *Kamerstukken II* 2015/16, 34 372, no. 3, at 31.

[81] *Kamerstukken II* 2015/16, 34 372, no. 3, at 31.

[82] Art. 126nba(6) Dutch CCP.

[83] Art. 126bb Dutch CCP.

[84] Code of Practice, *supra* note 24.

[85] Section 241 and Schedule 7 Investigatory Powers Act 2016, c. 25, §272, sch. 10 (Eng.) requires the Secretary of State to issue codes of practice about the exercise of powers and functions conferred by the Act.

[86] See for example, R v. Forbes [2001] 2 WLR 1 (UK), in which the House of Lords—

The Code's preamble states that its provisions are admissible as evidence in any civil or criminal proceedings, and that any court or tribunal considering such proceedings "may take the provision of the codes of practice into account."[87] Courts have taken breaches of codes of practice regulating more traditional investigatory powers into account in determining the admissibility of evidence.[88] If, as appears to be the case, the Code relating to equipment interference enjoys a similar status, breaches of its provisions might also affect the admissibility of evidence acquired through equipment interference. Unlike any internal guidance that might be published by public bodies exercising powers to interfere with equipment, the Code is a significant legal instrument extending to some 140 pages.

The powers conferred by the IPA are very broad. In contrast to traditional warrants for the search of physical premises, which are judicially issued, equipment interference warrants are issued by the chief officer of a police area. Judicial oversight is maintained, however, by the requirement—except in urgent cases—that a chief police officer's decision to issue a warrant should be approved by a Judicial Commissioner.[89] A warrant will either authorize or require the persons to whom it is addressed to secure interference with any "equipment" for the purpose of obtaining communications, equipment data, or any other information. "Equipment" is defined in very broad terms, as "any equipment producing electromagnetic, acoustic, or other emissions, or any device capable of being used in connection with such equipment."[90] Any device with components powered by an electrical charge will generate electromagnetic emissions. The Code provides as examples "desktop computers, laptops, tablets, smartphones, other internet-enabled or networked devices and any other devices capable of being used in connection with such equipment. Cables, wires and storage devices (such as USB storage devices, CDs or hard disks [sic] drives)."[91]

Any interference authorized by a warrant must be for the purpose of obtaining "communications," "equipment data," or "any other information."[92] Clearly, there is no significant restriction here. In common

---

at the time, the highest appellate court in England and Wales—had to determine whether a literal or purposive approach to construing the words of a key provision of the code of practice on identification procedures was required.

[87] Investigatory Powers Act 2016, Code of Practice, *supra* note 84.

[88] In criminal trials, judges have a broad discretion to exclude prosecution evidence where its reception would have an adverse effect on the fairness of the trial; section 78 Police and Criminal Evidence Act 1984, c. 60, §122, sch. 7.

[89] §106(1)(d) Investigatory Powers Act 2016.

[90] §135(1) Investigatory Powers Act 2016.

[91] Code of Practice, *supra* note 84, para. 2.2.

[92] §99(2) Investigatory Powers Act 2016.

with other definitions in Part 5 of the IPA, the concept of a "communication" is very broad. It includes any files that comprise speech, music, sounds visual images "or data of any description," as well as "signals" that impart anything between persons, or between person and things, or that enable any apparatus to be operated.[93] "Equipment data" that may be obtained using a targeted interference warrant can include "system data" and "identifying data." The former encompasses information router configurations and firewalls, the software operating system, account identifiers such as email and IP addresses, and information about the period in which a router has been active on a network.[94] "Identifying data" is any data that can be used to identify or assist in identifying any person, apparatus, system service, event, or the location of a person, a thing or an event.[95] The Code envisages that such data might include the location of a meeting in a calendar appointment, information relating to the date, time and location that a photograph or image was taken, and contact addresses to which mail has been sent via a webpage. Thus, some forms equipment interference—taking control of a computer and tracking keystrokes or activating a webcam, for example—make it possible to monitor, observe or listen to a person's communications, and to record anything that is seen, heard or discovered.

The potential scope of an equipment interference warrant also depends on the number of devices covered by the warrant. The IPA envisages warrants of varying scope, and the Code refers to two categories. A non-thematic warrant is narrower, authorizing interference with equipment belonging to a particular person or organization, or with equipment at a particular location. A thematic warrant will be considerably broader, as it relates to equipment that is linked by a common theme; it may "cover a wide range of activity, cover a wide geographical area, or involve the acquisition of a significant volume of data."[96] An interference warrant will be valid initially for six months, and can subsequently be renewed for a further six months.

The statutory regime for equipment interference not only enables hacking by police themselves; it also confers power to co-opt communications providers in this endeavor by serving the warrant on any person who may be able to provide assistance—telecommunications operators, for example. The Code suggests that law enforcement officers should attempt to work co-operatively with those who might provide assistance, but they have a power—subject to approval by the Secretary of State—to "impose a duty" to

---

[93] §135(1) Investigatory Powers Act 2016.

[94] The general definition is set out in sections 100,177 Investigatory Powers Act 2016. Examples are provided in HOME OFFICE, *supra* note 37, para. 2.4.

[95] §§263(2)-(3) Investigatory Powers Act 2016.

[96] HOME OFFICE, *supra* note 37, para. 5.12.

assist.[97] The Code also explains that the assistance sought will usually be the provision of infrastructure (though no indication is given as to the nature of such infrastructure) or information about the technical specification of relevant equipment.

The concept of privacy is central to the structure and rationale of the legislation. Section 1 of the Act explains that the purpose of the legislation generally, is "to set out the extent to which certain investigatory powers may be used to interfere with privacy."[98] Section 2 of the Act requires those issuing and renewing warrants to have regard to several broad considerations:

- whether what is sought to be achieved by the warrant, authorization, or notice could reasonably be achieved by other less intrusive means,
- whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorization or notice is higher because of the particular sensitivity of that information,[99]
- the public interest in the integrity and security of telecommunication systems and postal services, and
- any other aspects of the public interest in the protection of privacy.

Section 1 goes on to state that, protections for privacy can be found in various parts of the IPA. The part that regulates equipment interference requires the person issuing a warrant—the chief police officer—to justify the application in terms that mirror the justificatory grounds for interference with the right to privacy under Article 8(2) of the European Convention on Human Rights. They must consider the warrant necessary for preventing or detecting serious crime[100] and proportionate to the purpose of the interference.[101] In relation to proportionality, the Code explains[102] that, in considering whether this condition is met, the following should be considered:

- the extent of the proposed interference with privacy against what is sought to be achieved;

---

[97] §128 Investigatory Powers Act 2016; HOME OFFICE, *supra* note 37, paras. 7.4, 7.9.

[98] §1(1) Investigatory Powers Act 2016.

[99] §2(5) and sch. 7 para. 2(4), state that 'sensitive information' includes items that are subject legal privilege, information that might identify the source of journalistic information, and information held in confidence by a member of a professional, e.g. medical records.

[100] A "serious crime" is defined in §263(1) Investigatory Powers Act 2016, as one for which a person aged 18 or over who has no previous convictions could reasonably expect to be sentenced to imprisonment for a term of three years or more, or which involves the use of violence, results in substantial financial gain, or is conduct by a large number of persons in pursuit of a common purpose.

[101] Investigatory Powers Act 2016 §§106(1)(a)-(b).

[102] HOME OFFICE, *supra* note 37, at para. 4.20.

- how and why the methods to be adopted will cause the least possible interference with the privacy of the person and others;
- whether the activity is an appropriate use of the Act and a reasonable way, having considered all reasonable alternatives, of achieving what is sought to be achieved;
- what other methods, where appropriate were either not implemented or have been employed but which are assessed as insufficient to fulfil operational objectives without the use of the proposed investigatory power;
- whether there are any implications of the conduct authorized by the warrant for the privacy and security of other users of equipment and systems, including the internet, and an explanation of why (if relevant) it is nevertheless proportionate to proceed with the operation.

There are further protections for privacy in the form of a condition that limits the collection, copying, and dissemination of information and material that which is necessary for a number of purposes prescribed in the Act.[103] The legislation also sets out specific protections in relation to material that is subject to legal privilege,[104] confidential journalistic material,[105] information that identifies the sources of journalistic material,[106] and communications sent by or intended for members of the legislature and the private information of such persons.[107]

E. United States

In the United States, scholars have begun to address police malware—frequently referred to as a "network investigative technique"[108] (NIT) or "government hacking"[109]—in a variety of contexts. Federal courts have addressed government hacking questions, most notably since 2016.[110] Most of these cases stem from FBI deployment of malware as part of two major

---

[103] §129 Investigatory Powers Act 2016.

[104] *Id.* §112.

[105] *Id.* §113.

[106] *Id.* §114.

[107] *Id.* §111.

[108] *See, e.g.*, Kerr & Murphy, s*upra* note 25, at 59 (referring to NITs as presumably referring to "software used to bypass security features controlling access to a computer." *Id.*, at 59 n. 7); United States v. Matish, 193 F. Supp. 3d 585, 592 (E.D. Va. 2016).

[109] Mayer, *supra* note 5, at 580; Ohm, *supra* note 5, at 304; Kerr & Murphy, *supra* note 25, at 58.

[110] Mayer, *supra* note 5, at 578 (noting that, "[t]hrough 2015, there were only a few federal opinions on the practice. In 2016 and 2017, there were nearly a hundred").

online sting operations beginning in 2011[111] and 2014,[112] although another major investigation of 23 additional hidden websites was also mounted in 2013.[113] However, there is clear evidence that the FBI has been using malware to support its investigations since at least 2001.[114] These investigations have led to criminal charges not just in the United States, but also in other countries.[115]

In the earliest known judicial decision involving hacking by the FBI, the FBI physically installed a keylogger onto a suspect's computer in an effort to discover the suspect's passwords.[116] In another pre-2012 investigation, FBI agents posed as journalists, writing a fake Associated Press article and sending a link to the suspect's social media account.[117] When the suspect clicked the link, his computer was infected with malware, reporting his IP address to the FBI.[118] In the 2013 "Freedom Hosting" investigation, the FBI took control of a Tor hidden service (aka "Freedom Hosting") to deliver malware to specific users under a warrant that authorized them to access the following information: IP address, operating system, whether the NIT had already been delivered to the computer, host name, and MAC address.[119]

Generally, the FBI has relied on the authority of Rule 41 of the Federal

---

[111] *See, e.g.*, United States v. Welch, 811 F.3d 275, 276 (8th Cir. 2016).

[112] United States v. Horton, 863 F.3d 1041, 1045 (8th Cir. 2017); *see also* Ohm, *supra* note 5, at 304 (describing the Playpen investigation).

[113] Affidavit in Support of Application for a Search Warrant, In re Search of Computers that Access Websites 1-23, No. 8:13-mj-01744-WGC (D. Md. July 22, 2013); Affidavit in Support of Application of Search Warrant, In re Search of Computers that Access Websites 1-23, No. 8:13-mj-01744-WGC (D. Md. Oct. 31, 2016) (hereinafter "In re Search, 2016 affidavit").

[114] *See* Mayer, *supra* note 5, at 574-576 ("The earliest reported case is from 2001, when FBI agents snuck into a mafioso's office and installed a system for recording keystrokes"), *citing* United States v. Scarfo, 180 F. Supp. 2d 572, 574 (D.N.J. 2001); *see also* OFF. OF THE INSPECTOR GEN., A REVIEW OF THE FBI'S IMPERSONATION OF A JOURNALIST IN A CRIMINAL INVESTIGATION, U.S. DEP'T JUST. (Sept. 2016), https://oig.justice.gov/reports/2016/o1607.pdf (detailing the FBI's use of malware to identify the source of bomb threats to a school in the summer of 2007). The Electronic Frontier Foundation also released FBI documents pertaining to government use of malware referred to as a "web bug" or "Computer and Internet Protocol Address Verifier" (CIPAV). *See Endpoint Surveillance Tools (CIPAV)*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/cases/foia-endpoint-surveillance-tools-cipav (last visited Jan. 28, 2019).

[115] Ohm, *supra* note 5, at 303; Joseph Cox, *Child Porn Sting Goes Global: FBI Hacked Computers in Denmark, Greece, Chile*, VICE: MOTHERBOARD (Jan. 22, 2016, 2:01 PM), https://motherboard.vice.com/enus/article/qkj8q3/child-porn-sting-goes-global-fbi-hacked-computers-in-denmark-greece-chile.

[116] *Scarfo*, 180 F. Supp. 2d at 574.

[117] Mayer, *supra* note 5, 574-76; OFF. OF THE INSPECTOR GEN., *supra* note 114.

[118] Mayer, *supra* note 5, 574-76; OFF. OF THE INSPECTOR GEN., *supra* note 114.

[119] Mayer, *supra* note 5, at 588; In re Search, 2016 affidavit, *supra* note 113 at 89-90.

Rules of Criminal Procedure to apply for judicial warrants authorizing their deployment of NITs.[120] However, according to one recent analysis,

> about half of the district courts that have considered the issue have—surprisingly—concluded that law enforcement hacking is not necessarily a Fourth Amendment search, and that the most common configuration of government malware is exempt from ex ante judicial supervision.[121]

Prior to 2016, defendants would challenge these warrants, arguing that magistrate judges in other districts did not have jurisdiction to issue warrants covering searches outside their districts (i.e., in other parts of the country).[122] However, effective December 1, 2016, Rule 41 was amended to explicitly allow magistrate judges "with authority in any district where activities related to a crime may have occurred" to issue warrants encompassing the use of malware or "remote access" software "to search electronic storage media and to seize or copy electronically stored information located within or outside that district if the district where the media or information is located has been concealed through technological means."[123] (The 2016 amendments also allow a single magistrate judge to authorize the search of computers located in "five or more districts"[124] that have been damaged by malware (e.g., in cases of "botnets") in violation of the Computer Fraud and Abuse Act (18 U.S.C. §1030(a)(5)).

In the dark web context, or whenever police do not know the location or identity of a device or suspect (when investigatory techniques are being used to identify the device's or data's location and ownership), the "government's best chance of identifying who is behind the crime and where he is requires tricking the target into downloading malicious code."[125] This has led, for example, the FBI to seek warrants authorizing them to remotely install software onto target computers that have

---

[120] Indeed, as noted by one scholar, "It is not apparent whether federal law enforcement agents have ever deployed malware without obtaining a search warrant." Mayer *supra* note 5, at 599.

[121] *Id.* at 582.

[122] However, federal courts frequently held that suppression of the evidence obtained through use of the malware in these cases was not necessary, even when the searches violated the Fourth Amendment, under the exclusionary rule or the good faith exception established in United States v. Leon, 468 U.S. 897, 920 (1984). United States v. Jones, 230 F.Supp.3d 819, 823 (S.D. Ohio 2017).

[123] FED. R. CRIM. P. 41(b)(6).

[124] *Id.* 41(b)(6)(B).

[125] Kerr & Murphy, *supra* note 25, at 59.

> the capacity to search the computer's hard drive, random access memory, and other storage media; to activate the computer's built-in camera; to generate latitude and longitude coordinates for the computer's location; and to transmit the extracted data to FBI agents.[126]

As of November 5, 2018, there were seventeen federal appellate court decisions involving a "network investigative technique", as well as numerous federal trial court decisions in hundreds of different individual prosecutions.[127] All of these decisions arose within the context of just two federal child pornography investigations, "Operation Torpedo" (2011–12) and "Operation Pacifier" (2014–15), both part of the Department of Justice's "Project Safe Childhood Initiative."[128] Of the seventeen appellate decisions, thirteen arose from the FBI's investigation into a popular child pornography website within the Tor network (upf45jv3bziuctml.onion, or "Playpen") as part of Operation Pacifier. The remaining four appellate cases stemmed from Operation Torpedo, involving the investigation of other dark web sites (including "PedoBoard" and "PedoBook").

Aside from the investigations into PedoBoard/PedoBook and in the *Scarfo* and *In re Warrant To Search a Target Computer at Premises Unknown* cases, all other reported cases noted above appear to have involved government hacking operations limited to Functionality A (described *supra*, in Part I.C)—that is, *capturing specific types of data*, largely limited to information useful in identifying and locating computers allegedly associated with accessing or distributing child pornography. In *Scarfo*[129] and the PedoBoard/PedoBook investigation, the installation of a keylogger presents an example of Functionality D.1, or *intercepting online communications*—specifically, any typed commands inputted by the computer's user (and, in the PedoBoard/PedoBook investigation, the issued warrants also extended to capturing various other forms of online communication).

In the *In re Warrant to Search a Target Computer at Premises*

---

[126] In re Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013).

[127] We have identified 102 of these cases through a manual search and reading of federal cases in Westlaw using the search terms: [adv: "network investigative technique"], [adv: "Website A" & FBI & 2015], [adv: "child pornography" & (playpen OR "play pen" OR pedobook OR pedoboard)], [adv: "child pornography" & NIT], and [adv: NIT & FBI]. *See also* Mayer, *supra* note 5, at 578 (noting that, "[t]hrough 2015, there were only a few federal opinions on the practice. In 2016 and 2017, there were nearly a hundred").

[128] U.S. DEP'T OF JUST., PROJECT SAFE CHILDHOOD, https://www.justice.gov/psc (last visited Jan. 28, 2019).

[129] *Scarfo*, 180 F. Supp. 2d 572.

Unknown[130] case, the FBI's intended (but not authorized) hacking activities extended to basically all functionalities A through E. The judge ruling on the FBI's warrant application denied the warrant because it did not 1) meet the particularity requirement of the Fourth Amendment,[131] or 2) meet the heightened requirements for warrants authorizing video surveillance.[132] The court noted that video surveillance was "a potentially indiscriminate and most intrusive method of surveillance," requiring additional safeguards under Fifth Circuit precedent.[133]

Federal courts have issued contradictory opinions about the applicability of the Fourth Amendment in many of these cases, particularly those involving only the capture of specific types of data about a computer and its location (Functionality A). While the delivery and execution stages in the malware utilization process may also implicate the Fourth Amendment in some circumstances, the bigger question is whether the exploitation (electronic access to a suspect's device) or reporting (sending information back to the government) stages ought to implicate Fourth Amendment concerns.[134] Importantly, the Supreme Court has held that merely *touching* a suspect's physical property can constitute a Fourth Amendment search, and some circuit courts have analogized these physical "closed container" searches to those conducted of electronic devices.[135] On the other hand, metadata,[136]

---

[130] 958 F. Supp. 2d 753.

[131] *Id.* at 758-59 (The judge so found for the following reasons: 1) "The Government's application contains little or no explanation of how the Target Computer will be found," and 2) "The Government's application offers nothing but indirect and conclusory assurance that its search technique will avoid infecting innocent computers or devices.").

[132] *Id.* at 759-61 (elaborating requirements for video surveillance warrants within the Fifth Circuit).

[133] *Id.* at 759-60, *quoting* United States v. Cuevas–Sanchez, 821 F.2d 248, 250 (5th Cir. 1987).

[134] Mayer, *supra* note 5, at 589 (finding that, "If there is any constitutional privacy protection associated with this form of malware, it must reside in the exploitation and reporting steps").

[135] *Id.* at 590-92; United States v. Andrus, 483 F.3d 711, 718-19 (10th Cir. 2007) ("it seems natural that computers should fall into the same category as suitcases, footlockers, or other personal items that command a high degree of privacy" (internal citation omitted)). *See also* United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers."); Trulock v. Freeh, 275 F.3d 391, 402-04 (4th Cir. 2001); Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001).

[136] Bryce Clayton Newell, *The Massive Metadata Machine: Liberty, Power, and ~~Secret~~ Mass Surveillance in the U.S. and Europe*, 10 ISJLP 481, 487 (2014) (defining metadata as including "information about the time, duration, and location of a communication as well as the phone numbers or email addresses of the sending and receiving parties. It also may include information about the device used, for example, the make/model and specific device identification number.").

which is essentially the type of information obtained under Functionality A, is generally not protected by the Fourth Amendment.[137] Hence,

> [l]aw enforcement hacking thus poses a Fourth Amendment conundrum. It shares a key feature of physical device searches: the government obtains data directly from the suspect's device. But it also shares key features of compelling data from a service provider: there is no physical contact with the suspect's property, and the data that the government obtains can be conceptually divided into content and metadata categories.[138]

Mayer has argued that law enforcement "unambiguously engage in a Fourth Amendment search" when they deliver malware to a suspect's device because it "involves law enforcement officers physically interacting with a suspect's device," or, separately, when a piece of malware captures and "transmits the contents of a communication or a file."[139] However, in most Functionality A cases, at least those dealing with the capture of information like IP addresses, it is not clear that either of these conclusions would apply.[140] With this limited functionality, has the device been touched or accessed by law enforcement?

III. HACKING FUNCTIONALITIES AND PRIVACY INTERESTS

In this Part, we discuss how law-makers and courts have framed the privacy interest(s) at issue when allowing certain functionalities of police hacking for investigatory purposes. What were law-makers' primary concerns, and which constitutionally guaranteed privacy types, if any, did they apply? Does legislative history indicate whether law-makers felt that existing constitutional frameworks sufficiently addressed the intrusiveness of police hacking? In the subsections that follow, we examine how privacy considerations have arisen in connection to the functionalities of police hacking identified above in Part I.C.[141]

---

[137] *See id.* at 492-93 (discussing limited privacy protections for non-content information under the Fourth Amendment). An exception is cell-site location data held by a wireless service provider, which has received Fourth Amendment protection; *see* Carpenter v. United States, 138 S.Ct. 2206 (2018). Possibly, the Supreme Court may craft other future exceptions to the general rule that metadata does not acquire Constitutional protections.

[138] Mayer, *supra* note 5, at 594.

[139] *Id.*

[140] *Id.* at 596 (noting that "Courts have consistently held that an IP address is constitutionally unprotected metadata, much like a telephone number").

[141] We will not discuss functionality F—remotely deleting unlawful data—since this is only encountered in Dutch law and involves risks for the integrity and availability of computer data rather than privacy risks to confidentiality of data.

A. Capturing specific types of data

Some of the jurisdictions we studied regulate the capture of certain specific types of data separately from, or differently than, more comprehensive searches of data. This is perhaps based on the idea that such targeted use of police hacking powers, limited to specific types of data necessary for an investigation, is less intrusive than more comprehensive access to various types of data.

This distinction is seen in the content/non-content distinction in US Fourth Amendment law (although, as discussed above, police hacking does challenge this general rule). If the application is to acquire non-content (metadata) information about electronic or wire communications, the federal Pen Registers and Trap and Trace Devices chapter of Title 18[142] (the "Pen/Trap Statute") applies, providing statutory rules that govern in place of the standard Rule 41 warrant requirements. A pen-register order allows law enforcement to acquire "dialing, routing, addressing, or signaling information,"[143] while a trap-and-trace order allows them to capture "incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication."[144] Neither of these orders can authorize the collection of the "contents of any communication."[145] In practice, it appears the FBI may have (at least at one time) settled on a two-part process for deploying what has been referred to as a Computer and Internal Protocol Address Verifier (CIPAV) in conjunction with additional measures designed to collect additional information, acquiring an initial "search warrant to authorize intrusion into the computer" followed by an application for an order under the Pen/Trap Statute "to authorize the surveillance done by the spyware."[146]

FBI hacking techniques often implicate this functionality (capturing specific types of information). In the *PedoBook/PedoBoard* cases,[147] FBI agents had taken control of an illicit child pornography site and had inserted malware into the code of the site that would infect users' computers and

---

[142] 18 U.S.C. §§3121-27.

[143] *Id.* §3127(3).

[144] *Id.* §3127(4).

[145] *Id.* §3127(3)-(4).

[146] Jennifer Lynch, *New FBI Documents Provide Details on Government's Surveillance Spyware*, ELECTRONIC FRONTIER FOUND. (Apr. 29, 2011), https://www.eff.org/deeplinks/2011/04/new-fbi-documents-show-depth-government.

[147] *Welch*, 811 F.3d 275; United States v. Cottom, 679 Fed.Appx 518 (8th Cir. 2017); United States v. Huyck, 849 F.3d 432 (8th Cir. 2017); United States v. DeFoggi, 839 F.3d 701 (8th Cir. 2016).

instruct them to report the "user's IP address, the date and time the user accessed the content, and his or her computer's operating system."[148] The technique used by the FBI exploited the user's computer by exploiting a vulnerability within the Adobe Flash plugin.[149] In investigating the creator of the site, Aaron McGrath, the FBI also acquired a warrant allowing them to install keylogging software in order to "allow law enforcement to obtain the passwords and pass-phrases necessary to access McGrath's computers and the electronic files stored on those computers and to access communications between McGrath and others currently unknown to law enforcement."[150] Subsequently, the FBI obtained additional warrants allowing them to intercept private messages and other electronic communications sent through the hidden service, for as long as needed to "fully reveal" the "identity of the target subjects or information that may be useful in establishing their identity."[151]

In the *Playpen* cases,[152] the FBI was investigating users of a popular child pornography website hosted on the "dark web"[153] within the Tor network.[154] The FBI gained control of the site's servers and "relocated the website content to servers in a secure government facility" in Virginia.[155] Next, in order to identify users, who were "still cloaked by the Tor encryption technology," agents acquired a warrant that permitted them to use malware to infect the computers of any "user who logged into the target website."[156] The malware infected any computer that logged into the Playpen website, causing the users' computers to transmit "seven pieces of identifying information"[157] back to the government, including:

---

[148] *Welch*, 811 F.3d 275, 278 (8th Cir. 2016).

[149] United States v. Cottom, 2015 WL 9308226, *3 (D. Neb. 2015) (describing the technique); Mayer, *supra* note 5, at 587.

[150] United States v. Laurita, No. 8:13CR107, 2016 WL 4179365, at *3 (D. Neb. Aug. 5, 2016).

[151] *Id.*

[152] United States v. Horton, 863 F.3d 1041 (8th Cir. 2017); United States v. Workman, 863 F.3d 1313 (10th Cir. 2017); United States v. Levin, 874 F.3d 316 (1st Cir. 2017); United States v. McLamb, 880 F.3d 685 (4th Cir. 2018); United States v. Henderson, 2018 WL 5260851 (9th Cir. 2018); United States v. Werdene, 883 F.3d 204 (3rd Cir. 2018); United States v. Jean, 891 F3.3d 712 (8th Cir. 2018); United States v. Randolph, 725 Fed.Appx. 249 (Mem) (4th Cir. 2018); United States v. Hammond, 2018 WL 5278939 (Mem) (9th Cir. 2018); United States v. Torres, WL 4998156 (Mem) (5th Cir. 2018); United States v. Kienast, WL 5262735 (7th Cir. 2018); United States v. Lough, 721 Fed.Appx. 291 (Mem) (4th Cir. 2018); United States v. Tagg, 886 F.3d 579 (6th Cir. 2018).

[153] *McLamb*, 880 F.3d at 686.

[154] *Henderson*, 2018 WL 5260851 at *1.

[155] *Horton*, 863 F.3d at 1045.

[156] *Randolph*, 725 Fed.Appx. at 250.

[157] *Henderson*, 2018 WL 5260851 at *2.

> (1) the computer's IP address and the date and time that it was determined; (2) a unique identifier to distinguish data from that of other computers accessing Playpen; (3) the computer's operating system; (4) information about whether the NIT had already been delivered to the computer; (5) the computer's host name; (6) the operating system's username; and (7) the computer's media access control [MAC] address.[158]

Across the Atlantic, the Dutch regulation of police hacking regulates the collection of certain characteristics of the computer or its user, such as the computer's location or the user's identity, as a separate functionality of police hacking (considered a digital variant of the physical sneak-and-peak operation[159]). These types of searches are subject to less strict procedural requirements than remote searches or the deletion of data (functionalities B, C, and F), but have the same requirements as hacking to facilitate interception or observation (functionalities D and E).

The use of police hacking for the purpose of locating offenders is also discussed in German doctrine, although it is not regulated as a separate functionality. Rather, it is discussed as one of the few cases where the use of police hacking is justifiable from the perspective of the necessity requirement. A number of German scholars are critical of the wide scope[160] and intrusiveness of the newly introduced provisions[161] and question the proportionality and necessity of the regulation.[162] The determination of the location of perpetrators who use advanced anonymization technology to hide their IP address is recognized as an exception in this sense, since it can hardly be pursued otherwise than through the use of police hacking.[163]

B. Remote search of stored data

In the US, as mentioned earlier, there is little doctrine or case law directly covering the legality of remote searches of stored data using police hacking techniques, although it seems clear that these would generally amount to Fourth Amendment searches, at least insofar as the search might extend

---

[158] *Kienast*, 2018 WL 5262735 at *1.

[159] *Kamerstukken II* 2015/16, 34 372, no. 3, at 19.

[160] Lisa Blechschmitt, *Blechschmitt: Strafverfolgung im digitalen Zeitalter*, MULTIMED. RECHT 361–366, 365 (2018).

[161] *See, e.g.*, Roggan, *supra* note 56, at 827; Freiling et al., *supra* note 7, at 19; Michael Soiné, *Die strafprozessuale Online-Durchsuchung*, NEUE Z. FÜR STRAFR. 497–504, 497 (2018).

[162] Roggan, *supra* note 56, at 828; Freiling et al., *supra* note 7, at 19.

[163] Freiling et al., *supra* note 7, at 19.

beyond merely acquiring non-content data.[164] In the FBI's ill-fated application for a warrant in the *In re Warrant To Search a Target Computer at Premises Unknown*[165] case, the FBI had sought the ability to remotely search the hard drive and RAM of the suspect's computer. This sort of request (or hacking) may be occurring (indeed, it is the specific type of functionality addressed in the 2016 changes to Rule 41), but its occurrence is not (yet) otherwise apparent in available case law.

In the promulgation of the 2016 amendments to Rule 41, the Advisory Committee on Criminal Rules (which developed the amendments), promoted the expanded magistrate powers to explicitly authorize "remote access to search electronic storage media," at least in part, as a response and remedy (rather than a threat) to the invasion of privacy experienced by computer users who had had their computers infected with illegal malware under 18 U.S.C. §1030(a)(5). In advocating for rules that allow for more efficient investigations of botnet-related crimes, the committee stated that, "Botnets are used to steal personal and financial data, conduct large-scale denial of service attacks, and distribute malware designed to invade the privacy of users of the host computers."[166]

The most common public comments in opposition to the proposed rule changes were related to privacy and the Fourth Amendment, including comments arguing that remote searches would run afoul of the Fourth Amendment's particularity requirement.[167] However, the committee (excepting one dissenting member) explicitly defended its changes as procedural, not substantive, thus outside the remit of Fourth Amendment concerns.[168] The comments in opposition to the changes, in the committee's view, did not consider "the real need for amendment to allow the government to respond effectively to the threats posed by technology . . . [including] individual privacy."[169] The committee was "confident that judges will address Fourth Amendment requirements on a case-by-case basis both in issuing warrants under these amendments and in reviewing them when

---

[164] Of course, law enforcement resort to utilizing orders available under the Stored Communications Act (18 U.S.C. §§2701-2713) is another way for investigators to acquire stored communications data, but this process does not involve police hacking.

[165] 958 F. Supp. 2d 753.

[166] HON. REENA RAGGI, ADVISORY COMM. ON CRIMINAL RULES, REPORT OF THE ADVISORY COMMITTEE ON CRIMINAL RULES 9 (May 6, 2015), https://www.uscourts.gov/sites/default/files/2015-05-criminal_rules_report_0.pdf. Notably, however, the amendment and supporting documentation do not explicitly authorize law enforcement to disinfect computers or otherwise delete data.

[167] *Id.* at 11-12.

[168] *Id.* at 9-10, 13-14.

[169] *Id.* at 13.

challenges are made thereafter"[170] and that "Judicial review of warrant applications better ensures Fourth Amendment rights and enhances privacy."[171] In response to the dissenting view of one member of the committee that, "For many people, computers are their lives, and that these privacy concerns should be considered in the first instance by Congress," the rest of the committee argued that "computers are no more sacrosanct than homes, and search warrants for homes have long been issued ex parte and reviewed in back-end litigation."[172] Subsequently, the Committee on Rules of Practice and Procedure recommended that the Judicial Conference of the United States (the national policy-making body for the US federal courts) adopt the amendments as proposed by the advisory committee, only briefly noting the privacy-related concerns.[173]

Elsewhere, the German regulation of so-called online searches in Section 100b German CCP includes a wide-spread and rather indefinite permission for law enforcement to intervene and collect information from computers. By not limiting the scope of data collection to concrete types of data, it potentially allows the collection of all types of data, either by making a bitstream copy of the discs or enabling complete external control of the system.[174] The provision enables comprehensive monitoring of the use of the computer, including reading the storage media, and access to data generated prior to the order allowing the investigatory conduct (unlike source telecommunications interception) as well as future data generated during the duration of the measure.[175] However, the measure must always be limited to data relevant to the ongoing criminal proceedings and data that can be assumed to be evidence-related. Therefore, the comprehensive investigation of the whole computer system is fundamentally precluded.[176]

The measure must also be subsidiary to other investigative means and may only be used if other techniques, such as an overt search do not suffice.[177] This principle has also been expressed by the Federal Constitutional Court, which stated that overt access to such data must take priority over secret infiltration, and it must be demonstrated why an overt search does not

---

[170] *Id.*

[171] *Id.* at 14.

[172] *Id.*

[173] COMMITTE ON RULES OF PRACTICE AND PROCEDURE, SUMMARY OF THE REPORT OF THE JUDICIAL CONFERENCE COMMITTEE ON RULES OF PRACTICE AND PROCEDURE 26 (Sept. 2015), https://www.uscourts.gov/sites/default/files/st09-2015_0.pdf.

[174] Freiling et al., *supra* note 7, at 18.

[175] Niedernhuber, *supra* note 39, at 171.

[176] Singelnstein & Derin, *supra* note 51, at 2646–2647.

[177] *Id.* at 2647.

promise success, before an online search can be authorized.[178] Considering this, some authors express confusion as to which gaps in existing powers the new regulation is supposed to fill, since in most cases access to data is readily available in the context of overt seizure of the data carriers. Other than determining locations, discussed in the previous subsection, the area of application related to the presence of full-disk encryption is suggested, although the provision itself makes no reference to encryption technology.[179] Perhaps the main advantage for law enforcement in comparison to overt searches is the covert character of online searches. However, if this is the motivation for the new measure, then it is creating a new type of power exclusively related to computer investigations that does not have an equivalent in traditional searches, since there are no comparable provisions to covertly seize objects in the Code of Criminal Procedure.

The newly introduced online search is widely considered the most intrusive investigation measure in the German CCP. Contemporary computers and smartphones process and store a large variety of data from all walks of life which potentially allow secretive creation of comprehensive personality profiles.[180] Recognizing these risks (in the context of preventive police powers), the German Constitutional Court considered it particularly necessary to protect citizens from such interference. It considered existing provisions of the Basic Law, including the protection of informational self-determination, the inviolability of the home and the secrecy of communications, but found these existing protections insufficient. Therefore, it interpreted the Basic Law, on the basis of the protection of human dignity[181] and the protection of the free development of individual personality[182] to protect the (newly created) fundamental right to confidentiality and integrity of information technology systems. All covert infiltrations of computers with the aim to obtain data stored in them must be measured against this standard, which places particularly high demands on the justification of such interventions.[183]

The German Constitutional Court compared the intensity of fundamental rights interference of the secret infiltration of computer systems to the interference with the inviolability of the home.[184] Due to this, the legislator designed the procedural requirements for online searches to be identical to

---

[178] Freiling et al., *supra* note 7, at 22.

[179] *Id.* at 19.

[180] Singelnstein & Derin, *supra* note 51, at 2647.

[181] Art. 1, GRUNDGESETZ [GG] [BASIC LAW], *translation at* https://www.gesetze-im-internet.de/englisch_gg/index.html (Ger.).

[182] Art. 2, GG.

[183] Singelnstein & Derin, *supra* note 51, at 2647.

[184] Freiling et al., *supra* note 7, at 21.

those of the acoustic surveillance of the home.[185] Therefore, the integrity and confidentiality of computer systems and the inviolability of the home are considered to be of equal importance,[186] although they remain separate legal goods. Online searches are, thus, not measured against the constitutional standard protecting the inviolability of the home (even when the computer system is located inside a home) and are not allowed to breach the protection of the home by, for example, secretly entering the home to infiltrate a computer system.[187]

Interestingly, the Dutch regulation of remote computer searches, which allows the authorities to secure data stored on the computer (in art 126nba Dutch CCP) also seems to be inspired by the provisions on oral interception inside a dwelling. Since the remote search is considered the most privacy-intrusive form of remote access, the procedural requirements have been set up to be identical to oral interception inside the home.[188] However, not much specific attention has been paid to the protection of the home in the legislative history of article 126nba Dutch CCP.[189] Since the safeguards for using legal hacking are high compared to most other investigation powers, it apparently is not very relevant whether remotely accessed computers are located in a dwelling or elsewhere—it is the computer itself that is being protected against intrusions through the relatively high safeguards.

In Italy, the primary judgment on using a Trojan to covertly copy data from computers dates from 2009, in which the Supreme Court held that covertly installing a device on a computer to acquire the files stored on it was an atypical means of searching for evidence, and thus governed by art. 189 Italian CCP, for which a motivated order from the Public Prosecutor suffices, which in this case was given on the basis of article 234 Italian CCP to acquire documents (*prova documentale*).[190] According to the Court, the secrecy of communications is not at issue because the program does not intercept a flow of communications (which implies a dialogue with other persons), but merely targets the unidirectional flow of data inside the computer's circuits.[191]

---

[185] Niedernhuber, *supra* note 39, at 171.

[186] Part of the literature considers the intensity of intervention in case of police hacking to be even higher than in the case of acoustic monitoring of the home. *See* Singelnstein & Derin, *supra* note 51, at 2647; Freiling et al., *supra* note 7, at 18–19.

[187] Niedernhuber, *supra* note 39, at 171.

[188] *Kamerstukken II* 2015/16, 34 372, no. 3, at 29.

[189] Significantly, the lengthy discussion in the Explanatory Memorandum of the protection of constitutional rights in relation to art. 126nba Sv (*Kamerstukken II* 2015/16, 34 372, no. 3, at 50-56) is limited to the general right to privacy and the right to secrecy of communications; nothing is said on a possible violation of the right to inviolability of the home.

[190] Cass., Sez. V, 14 ottobre 2009, n. 16556 ('Virruso').

[191] *Id.*, as referred to in Mauro Trogu, *Sorveglianza e "perquisizioni" on-line su*

Moreover, the Court did not consider the inviolability of the home to be infringed, because the computer was located in a public office, open to a "community of people that was not particularly extensive, but neither limited or a priori determinable on the basis of a personal decision by the accused," and hence not a constitutionally protected type of place.[192] Thus, unlike in Germany and the Netherlands, where the location of the computer does not appear to be of importance, computers in Italy appear to be more strongly protected when located in constitutionally protected places. This has been criticized in the literature: it misunderstands the intrinsic place-independence of computers, in relation to the (doctrinally-constructed) protected legal good of "informatic home" or "informatic privacy." The court's argument leads to "protecting the data contained in a computer when this is located inside a home, but not when it is located in public places, completely ignoring the factual circumstance that—for instance through accessing the *cloud*—the subject can in both cases conduct in both places activities with the same level of sensitiveness."[193] A considerable part of Italian doctrine considers online covert searches for data retrieval to be unconstitutional, for lack of specific legal rules stipulating the conditions and modes of operation and lack of necessary safeguards to limit the privacy infringement to what is necessary.[194] Nevertheless, the 2009 judgment was confirmed in the 2012 Bisignani case by the Supreme Court.[195] Interestingly, the prosecutor had requested the investigatory judge to authorize an "online search," alongside an authorization for oral interception, both on the basis of article 266 Italian CCP (interception of communications), but the judge had not considered such authorization necessary for the online search, as, according to the 2009 judgment, a motivated order from the prosecutor would suffice. This was upheld by the Supreme Court.[196]

---

materiale informatico, *in* LE INDAGINI ATIPICHE 431, at 448 (Adolfo Scalfati ed., Giappichelli Editore, 2014).

[192] *Id.* at 448.

[193] Giulia Lasagni, *L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"*, DIRITTO PENALE CONTEMPORANEO, §4 (2016), https://www.penalecontemporaneo.it/d/4995-luso-di-captatori-informatici-trojans-nelle-intercettazioni-fra-presenti. *See also* Trogu, *supra* note 191, at 448 (observing that this reasoning would lead to "the individual who uses his portable personal computer on the public street would lose the right to privacy on its contents, thus legitimating any public or private intrusion").

[194] Stefano Marcolini, *Le cosiddette perquisizioni on line (o perquisizioni elettroniche)*, 7/8 CASSAZIONE PENALE 2855, at 2866-67 (2010); Iovene, *supra* note 28, at 341-342 (2014); Lasagni, *supra* note 193, §4.

[195] Cass., Sez. VI, 27 novembre 2012, n. 254865 ("Bisignani"), mentioned in Vaciagio & Ramalho, *supra* note 40, at 92.

[196] As reported in Lasagni, *supra* note 193, §4, referring to Marco Torre, *Il virus di Stato*

The UK legislation neither prescribes nor proscribes any particular form of equipment interference. An equipment Interference warrant will specify the object of the warrant—equipment controlled by a particular person, installed at particular locations, forming part of a network etc.—but will not impose conditions relating to the particular functionality of interference. The legislation merely states that the "obtaining of communication or other information" that is authorized *includes* "monitoring, observing or listening to a person's communications or other activities."[197] A warrant authorizes "any conduct which it is necessary to undertake to do what is expressly authorised or required by the warrant."[198] The Code of Practice explains that equipment interference warrants authorize both physical interference with equipment and remote interference.[199] Thus, the UK legislation authorizes, prima facie, each of the forms of hacking functionalities dealt with in this Part of the Article. However, the requirement that those issuing interference warrants consider the necessity and proportionality of the authorization sought, might act as a constraint on the form and functionality of interference that can be employed. The Code of Practice explains that proportionality, on which the issue of a warrant depends, will not be met if the material that is sought could be obtained by less intrusive means. An assessment of proportionality requires consideration of "how and why the methods to be adopted will cause the least possible interference with the privacy of the person and others."[200]

C. Remote monitoring of computer use

Although the legal provisions in some jurisdictions generally do not distinguish between a one-off remote search of data stored in a computer and longer-term monitoring of computer use, the latter is recognized as significantly more intrusive in literature and case law of other jurisdictions. In the US, ongoing searches (e.g., location tracking or wiretapping warrants) must typically be explicitly allowed in the legitimating warrant or court order. Likewise, police hacking operations that extend prospectively for a period of time should also be explicitly approved under ongoing warrants.[201] Importantly, if the remote monitoring encompasses the collection of electronic communications content (including the capture of text-based

---

nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali, 9 DIR. PEN. PROC. 1163, at 1167 (2015).

[197] §99(4)(a) Investigatory Powers Act 2016.

[198] §99(5)(a) Investigatory Powers Act 2016.

[199] Code of Practice, supra n.90, para. 3.11.

[200] Code of Practice, supra n.90, para. 4.20.

[201] Mayer, *supra* note 5, at 628-29.

communications), police must acquire a "continuously valid super-warrant" under the federal Wiretap Act[202] (this requirement is mostly relevant to functionality D, discussed in the following subsection, but would also apply here in appropriate cases). Remote monitoring of computer use was also one of the functionalities requested by the government in *In re Warrant to Search a Target Computer at Premises Unknown*.[203]

In Germany, some authors point out that the official legal term used for police hacking—"online search"—is misleading. Whereas a classic search is a one-off, limited measure, from the wording of Section 100b Germany CCP it is evident that by means of the "online search" data may be continuously collected over an extended period.[204] Consequently, police could access data already existing at the time of ordering the measure as well as newly created data, including (future) stored emails, text messages, photographs, video files, social media contacts, etc. Furthermore, the measure can also be used to give law enforcement "live access" to data which is only plainly visible on the computer system temporarily. This can be compared to secretly glancing over the shoulder of the computer user to monitor all of their digital activities.[205] As such, rather than a search, this constitutes comprehensive covert surveillance of the computer.[206]

Naturally, such collection must be restricted to data relevant to the investigation at hand and should be described as precisely as possible in the court order to comply with the proportionality principle. Therefore, truly comprehensive monitoring should not be permissible in most cases.[207] Nevertheless, the online search is a considerably more serious violation of fundamental rights than telecommunications surveillance or overt searches and seizures because it takes place covertly and can extend over a longer period, monitoring the entire usage of a computer system.[208] Therefore, *duration* contributes to the infringement of fundamental rights. Since such monitoring potentially gives law enforcement agents access to an extremely large and meaningful set of data, such collection carries a heavy weight on the personality of the person concerned, which goes beyond the individual data collections protected by the right to informational self-determination.[209] The German Constitutional Court compares the intensity of an online search

---

[202] *Id.* at 629; 18 U.S.C. §§2510-2511, 2518.
[203] 958 F. Supp. 2d 753.
[204] Freiling et al., *supra* note 7, at 13.
[205] Roggan, *supra* note 56, at 825.
[206] Freiling et al., *supra* note 7, at 13.
[207] *Id.*
[208] Roggan, *supra* note 56, at 826.
[209] *Id.*

to the intensity of secret surveillance of the home.[210] Yet, the surveillance of the home under Section 100c German CCP is limited to acoustic surveillance, while the diversity and volume of data accessed during online searches facilitate more far-reaching conclusions about the personality of the affected individual. This would make it more comparable to repeated covert home searches and monitoring, which are not allowed under the German Basic Law.[211]

The difference between one-time searches and extended monitoring has also been recognized in Italian doctrine. Although corresponding powers have not yet been incorporated into statutory law, some guidance can be found in existing case law. Various authors criticize the lack of statutory regulation, arguing that these forms of hacking significantly infringe constitutional rights (secrecy of communications, inviolability of the home and/or the right to privacy).[212] According to Palmieri, rather than "violation," it would be more correct to speak of an "attack" on the fundamental right to privacy.[213]

Discussing a 2009 Supreme Court judgment that involved a Trojan that was used to monitor a computer for eight months, some authors held that the Trojan at issue did not constitute a form of a search, because it did not aim to find existing information, but also to find future information, which is intrinsically different.[214] In the 2012 *Ryanair* case, the police used spyware to capture real-time traveler data in an online booking system.[215] The court found this use of spyware distinguishable from traditional search and seizure, which takes place on the basis of existing suspicion, as it was targeted at finding new information that might lead to a concrete suspicion; this turns the Trojan into an exploratory surveillance measure, which, in that respect, is similar to interception of communications, and this is not allowed under current law.[216] This may suggest that there is a difference between using a Trojan to covertly copy existing data (which would be allowed on the basis of acquiring documental evidence or, possibly, a search) and using it to monitor future data entered into a system (which would not be allowed in the absence of specific legal rules for this form of surveillance). In the *Occhionero* case,[217] the defense argued that a Trojan had been used to capture real-time data on the screen or on the device—for example, taking

---

[210] BVerfG, 1 BvR 966/09, Apr. 20, 2016, Rn. 210 (Ger.).
[211] Roggan, *supra* note 56, at 826.
[212] *See, e.g.*, Palmieri, *supra* note 45, at 60; Torre, *supra* note 18, at 18, 20.
[213] Palmieri, *supra* note 45, at 60.
[214] Iovene, *supra* note 28, at 339.
[215] Torre, *supra* note 196, at 48.
[216] Cass., Sez. IV, 17 aprile 2012 no. 19618 ("Ryanair") (It.).
[217] Cass., Sez. V, 20 ottobre 2017, n. 15512 ('Occhionero').

screenshots—but not (only) to capture data flowing from a computer to the web. The court merely ruled that the former might lead to exclusion of evidence, but that it is up to the defense to specify which captured data exactly are unusable.[218]

Although the courts in Italy have been relatively permissive in relation to remote searches, authors tend to conclude that legislative intervention is required before Trojans can be employed, based on what they perceive as the main legal goods at stake. According to Trogu, the primary legal good is the "informatic home" (which has been conceptualized in law and doctrine on the hacking offense[219]). The informatic home is a constitutionally protected virtual space (but also physical space in which the informatic data are contained) over which the owner can exercise the *jus prohibendi* and *jus admittendi* towards third persons, with a legitimate expectation of privacy.[220] And since it is the informatic home that is at stake, covert remote investigations of computers are most similar to making video recordings (of non-communicative behavior) inside the home, which is not allowed.[221] For a more detailed discussion of the concept of informatic home see *infra* Part IV(B)(1).

Other authors offer further reflection in Italian doctrine on the legal good at issue in remote monitoring. Iovene argues that what is at issue is no longer a matter only of data protection or informational self-determination, but more fundamentally one of the right to personality. It is necessary, she argues, "to protect the informatic system as a space in which the individual expresses his personality, regardless of the nature of the information entrusted to it."[222] Finding the concept of informatic home insufficient, she proposes the concept of *informatic privacy* to enable controlling what happens with information. Thus, it is "informatic privacy" (*riservatezza informatica*) that is the legal good to be protected, which can be described as the "exclusive interest, legally recognised, to enjoy, dispose, and control the digitized information, processes, systems and 'spaces,' and their uses."[223] For more on the concept of informatic privacy see *infra* Part IV(B)(2).

Torre, seeing that the computer functions nowadays as an actual

---

[218] *Id.* at 7-8.

[219] See Bert-Jaap Koops, *Criminal Investigation and Privacy in Italian Law*, §3.2.2 (TILT Law & Technology Working Paper Series, December 2016), https://ssrn.com/abstract=2888422, for a brief discussion.

[220] Trogu, *supra* note 191, at 434, with reference to Cass., Sez. VI, 4 ottobre 1999, n. 3067 (It.).

[221] Trogu, *supra* note 191, at 447.

[222] Iovene, *supra* note 28, at 334.

[223] *Id.* at 335, quoting Roberto Flor, *Phishing, identity theft, e identity abuse. Le prospettive applicative del diritto penale vigente*, RIV. IT. DIR. PROC. PEN. 899 (2007).

"appendix" of the person and his most fundamental self, argues that police hacking enables an infringement of individual intimacy that touches upon the inviolability of the mind, and therewith triggers human dignity. After all, the real-time monitoring that police hacking implies that "also that what is being written in a file and subsequently erased can be captured."[224] Thus, it seems that Torre ultimately considers human dignity to be the core legal good at issue and recommends treating this as a constitutional right associated with proper constitutional safeguards to regulate infringements of this right. The Italian focus on the protection of individual personality and its free expression[225] and human dignity of the individual[226] resembles the German constitutional case law in which the right to confidentiality and integrity of computer system are held to be an expression of precisely these two values.

D. Intercepting communications

1. Intercepting Electronic Communications (Wiretapping)

One of the most-cited reasons for introducing police hacking has been the inability of law enforcement to access the content of encrypted communications. The main solution proposed and adopted in several jurisdictions is source telecommunications interception. From a technical point of view, source telecommunications interception is also similar to other functionalities of police hacking, since it also requires secret intrusion into the computer system. The difference lies in the scope of the collected data.[227]

In the US, the interception of oral, electronic, and wire communications is governed by Title III of the Omnibus Crime Control and Safe Streets Act of 1968[228] (the "Wiretap Act," codified in sections 2710-2722 of the US Code), as amended by the Electronic Communications Privacy Act of 1986 (ECPA),[229] requiring a "super warrant" with heightened application requirements for law enforcement. These heightened requirements generally apply to (wireless) network interception, keystroke logging, and a variety of

---

[224] Torre, *supra* note 18, at 87. Also, Palmieri emphasises that the use of Trojans "borders on controlling the mind," touching upon "opinions and thoughts" rather than "actions and behaviors." *See* Palmieri, *supra* note 45, at 60-61, referring to Paolo Tonini & Carlotta Conti, IL DIRITTO DELLE PROVE PENALI at 482 (Giuffrè Editore 2014) *and* Alfredo Gaito & Sandro Furfaro, *Intercettazioni: esigenze di accertamento e garanzie della riservatezza*, *in* I PRINCIPI EUROPEI DEL PROCESSO PENALE at 364 (Alfredo Gaito ed., Giuridica Editrice 2016).

[225] Iovene, *supra* note 28, at 334.

[226] Torre, *supra* note 18, at 87. Similarly Torre, *supra* note 196, at 28.

[227] Singelnstein & Derin, *supra* note 51, at 2647.

[228] P.L. 90-351, 82 Stat. 197.

[229] P.L. 99–508, 100 Stat. 1848.

other forms of interception.[230] Congress updated the Wiretap Act in 1986 to cover electronic communications[231] (alongside existing regulations for interception of oral and wire communications), explicitly doing so as a response to the "development of new methods of communication and devices for surveillance" as well as dramatic expansion in "the opportunity for such intrusions" and "the arbitrary use of Government power to maintain surveillance over citizens."[232] The drafting of the legislation was spurred by the idea that determining whether a reasonable expectation of privacy existed in any given case, the Fourth Amendment standard, was "not always clear or obvious" in the context of communications interception.[233] According to the Senate Report on the ECPA,

> tremendous advances in telecommunications and computer technologies have carried with them comparable technological advances in surveillance devices and techniques. Electronic hardware making it possible for overzealous law enforcement agencies, industrial spies and private parties to intercept the personal or proprietary communications of others are readily available in the American market today.[234]

Additionally, the Senate reported that the ECPA represented "a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies," and that "[p]rivacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances."[235] As such, "Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this

---

[230] *See* Mayer, *supra* note 5, at 639-40, *citing* Joffe v. Google, Inc., 746 F.3d 920, 926-36 (9th Cir. 2013) (applying the Wiretap Act to wireless network interception); United States v. Councilman, 418 F.3d 67, 69-85 (1st Cir. 2005) (holding that email interception is covered under the Wiretap Act), Luis v. Zang, No. 1:11-cv-884, 2013 WL 811816, at *4-9 (S.D. Ohio Mar. 5, 2013) (reviewing litigation on keyloggers and concluding that, if malware reports keystrokes to a remote party, it implicates the Wiretap Act); Shefts v. Petrakis, No. 10-cv-1104, 2012 U.S. Dist. LEXIS 130542, at *37-44 (C.D. Ill. Sept. 12, 2012) (holding that screen capture software that recorded email activity was covered by the Wiretap Act).

[231] The law defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce" with some exceptions, including "any wire or oral communication" as defined in the same section. 18 U.S.C. §2510(12).

[232] S. REP. NO. 99-541, at 1-2 (1986).

[233] S. REP. NO. 99-541, at 4 (1986) (quoting a statement made by the Criminal Division of the U.S. Department of Justice in response to a letter from Senator Leahy).

[234] S. REP. NO. 99-541, at 3 (1986).

[235] *Id.* at 5.

precious right."[236]

The Wiretap Act covers the collection of the *contents* of communications as they are in transit rather than the metadata covered by the Pen/Trap Statute (or after they are relegated to electronic storage, in which case they would be covered by Rule 41 or the Stored Communications Act,[237] depending on the context and type of search at issue). It authorizes judges to issue warrants for police interception of wire, oral, or electronic communications, with some limitations. Specifically, judges may order wiretapping only "within the territorial jurisdiction of the court in which the judge is sitting" as well as "outside that jurisdiction but within the United States in the case of a mobile interception device."[238] The definition of "mobile interception device" has been met with some disagreement by federal courts.[239] The Tenth Circuit has held that "mobile interception device" refers to a "mobile device for intercepting communications,"[240] while the Seventh Circuit has defined it as "a device for intercepting mobile communications."[241]

Because many instances of police hacking involve searches of computers in unknown locations, and because communications interception is not subject to the expanded venue provisions provided for under the 2016 amendments to Rule 41, this makes authorizing the interception of communications as part of hacking operations complicated. In either case, police applying for an interception warrant must know that the target device is within the court's jurisdiction or, in the case of a mobile interception device, at least within the US. And, considering the differing definitions of mobile interception device across circuits, it may not always be clear whether that provision applies to the mobility of the interception device or of the targeted device. Thus, in some contexts and in some circuits, it may be difficult (or unlikely) that a wiretap warrant could be issued prior to additional information being collected about the target device, including its location. As such, these measures might be employed only as a secondary hacking technique, only after other functionalities have revealed the prerequisite information.

In Germany, this functionality has been regulated separately, as a less intrusive form of police hacking. The measure is subsidiary to the traditional

---

[236] *Id.*

[237] 18 U.S.C. §§2701-2713.

[238] *Id.* §2518(3).

[239] Michael Koch, *If Technology is the Hare, is Congress the Tortoise? Split Circuits in the Wake of* Dahda, 59 B.C. L. REV. E-SUPP. 45, 45-46 (2018); *contra* United States v. Dahda, 853 F.3d 1101 (10th Cir. 2017) *with* United States v. Ramirez, 112 F.3d 849 (7th Cir. 1997).

[240] *Dahda*, 853 F.3d at 1114.

[241] *Ramirez*, 112 F.3d at 853.

telecommunications interception and only possible when the traditional form of wiretapping along the line is not possible.[242] It is limited to ongoing communications from the time of the order[243] and it is neither permissible for the police to access communications from before that period nor, for example, draft emails or draft messages not yet transmitted.[244] Since it can only be used when traditional interception is not possible, it is, in practice, limited to communications that are encrypted in transit. By infiltrating the terminal equipment, law enforcement can gain access before the communication is encrypted or after it has been decrypted by the recipient.[245]

One of the main reasons why this functionality of police hacking is regulated separately is that the German Constitutional Court has exempted ongoing communications from the strict regime of protection that is afforded the right to confidentiality and integrity of computers. Access to current communications, even by means of police hacking, is protected by Art. 10 of the Basic Law, which protects the secrecy of communications and can be interfered with under less stringent requirements.[246] Art. 10 is the sole fundamental rights standard for source telecommunications surveillance. However, technical and legal precautions must ensure that monitoring is limited to data from ongoing telecommunications processes, and if such restrictions fail, the measure violates the right to confidentiality and integrity of computer systems.[247] The reason for excluding ongoing telecommunications from the stricter regime is that it is coherent with the social function of telecommunications and the expectations of users, who make no detailed distinctions between traditional telephony and mobile or internet communications, and thus accessing ongoing communications through the terminal device can be seen as functionally equivalent to traditional forms of interception.[248]

In Italy, although source telecommunications interceptions are not regulated in statutory law, it appears that they are also considered less intrusive, at least in comparison to oral interception of communications. In the *Occhionero* case, a Trojan had been installed in the (fixed) personal computer of the accused, ostensibly to intercept telecommunications, and the Court found this admissible, pointing out that previous case law (the *Scurato* case) only concerned oral interception, which was considered to be more invasive.

---

[242] Singelnstein & Derin, *supra* note 51, at 2648.
[243] Niedernhuber, *supra* note 39, at 170.
[244] Singelnstein & Derin, *supra* note 51, at 2648.
[245] Freiling et al., *supra* note 7, at 10.
[246] Singelnstein & Derin, *supra* note 51, at 2647.
[247] Roggan, *supra* note 56, at 821–822.
[248] Freiling et al., *supra* note 7, *supra* note 6 at 21.

In the Netherlands, unlike Italy and Germany, police hacking to intercept telecommunications is considered equivalent to oral interception, judging by the fact that they are regulated together as one functionality of police hacking.

2. Intercepting Oral Communications

Unlike telecommunications interception, which essentially aims to get access to technically mediated (oral or electronic) communications, oral interception aims to use the peripheral equipment (microphones) of the computer to hear or record communications taking place in the environment surrounding the device. In the US, interception of oral communications is regulated under the Wiretap Act, described in the previous subsection. Under the Act, "'oral communication' means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation."[249] In other respects, oral interception is essentially treated the same as other forms of wiretapping, and might be accomplished by a variety of technical means, although the computer intrusion necessary to deploy software capable of activating a device's microphone might also need to be supported by a separate (e.g., Rule 41) warrant authorizing a broader search and infiltration of the device.

In the Netherlands, both telecommunications and oral interception are regulated as one functionality. Here, the remote access facilitates intercepting electronic communications[250] (e.g., intercepting Skype conversations or in- or out-going email) or oral interception[251] (e.g., through a keylogging device intercepting communication typed on the keyboard or to turn on the computer's microphone). One reason for introducing police hacking was the fact that current law allows placing a bug in a computer for oral interception purposes, but only by physical means (entering a place and installing a bug in the keyboard or computer). The law did not include the option of installing a bug remotely, which hindered the investigation if the location of the computer is unknown or if physical installation is too risky. By allowing remote access for this purpose, the advantage is that it is not necessary to enter a dwelling to install the device, so that article 12 Dutch Constitution (protecting the home) does not have to be infringed.[252] It therefore appears that, at least in this context, the protection of the inviolability of the home is

---

[249] 18 U.S.C. §2510(2).

[250] Art. 126m Dutch CCP.

[251] Art. 126l Dutch CCP.

[252] *Kamerstukken II* 2015/16, 34 372, no. 3, at 13. Similarly, *Kamerstukken II* 2016/17, 34 372, no. 6, at 24.

given priority over the protection of the integrity of computers, since the intrusion into computers is considered justified by avoiding infringement of the home. However, it may also merely reflect practical considerations, such as the ability to conduct the investigation undetected, which would be potentially compromised in the case of a physical intrusion.

In Italy, the use of Trojans for intercepting communications, particularly oral interception through turning on the computer's microphone, has triggered most legal discussion. In the *Bisignani* case, the investigatory judge authorized this on the basis of article 266(2) Italian CCP.[253] However, since this stipulates that if communications among people present (*communicazioni tra presenti*) take place in homes and places of private abode (the places mentioned in article 614 Criminal Code on trespass), this is only allowed if there is motivated reason to believe that the criminal activity is taking place there. In the 2015 *Musumeci* case, the Supreme Court found that installing spyware on a portable device that turned on the microphone was a form of oral interception, and that this can only take place "in clearly circumscribed places, identified at the outset, and not wherever the subject might be." It continued:

> At issue is a technique . . . that presents specific characteristics and that adds something with respect to the ordinary potential of interception, constituted precisely by the possibility to capture conversations between people present not only in a number of places, according to the subject's movements, but—and this constitutes the problematic fulcrum of the issue—without limitation of place. This is prohibited by the constitutional requirements of article 15 Constitution even more so than by the current statutory law.[254]

However, this judgment was overturned in 2016 by the *Scurato* decision.[255] The court observed that the requirement to specify in advance the places where the interception was to take place was not required in statutory law nor by ECHR case law. The *Musumeci* judgment had confused the term colloquially used for oral interception, namely "environmental interception" (*intercettazione ambientale*), which historically assumes that oral interception takes place in a particular environment in which a bug is to be placed, with the term that the law actually uses, which is interception of "communications between persons present." The first sentence of article 266(2) Italian CCP, saying that communications between persons present can

---

[253] Cass., Sez. VI, 27 novembre 2012, n. 254865 ('Bisignani').
[254] Cass. Sez. VI, 26 maggio 2015, n. 27100 ('Musumeci').
[255] Cass., Sez. Un., 28 aprile 2016, n. 26889 ('Scurato').

be intercepted in the cases listed in article 266(1), does not contain a requirement to specify the place for such interception. It is only in the second sentence that protected places are mentioned; however, this does not constitute a requirement to *specify* the place of interception beforehand as a condition of authorized interception. Rather, it exists as a requirement to motivate why it is necessary to install a bug in a protected place, for the purposes of specifying how oral interception is to be executed. Such necessity is absent in the case of interception through "informatic viruses," which is irrespective of place and by its nature a form of "itinerant" environmental interception.[256]

The import of this, according to the United Sections of the Supreme Court, is not that oral interception with Trojans in mobile devices is allowed, as the *Musumeci* judgment suggested, when the authorization order *would* describe ex ante the protected places in which the interception was (expected) to take place (and motivating that crime takes place there). Rather, such use of a Trojan is effectively not allowed at all, because the legislative requirement that oral interception can only take place in places of private abode if there is motivated reason to believe criminal activity takes place there does not allow for exceptions, while the judge cannot foresee and predetermine in which places of private abode the bugged portable device will be used, making it impossible for the judge to effectively supervise that the legal requirement be respected.[257]

There is, however, a major exception, which applies in the *Scurato* case (and which had not been considered in *Musumeci*). Article 13 of Decree-Law no. 152 of 1991 (enacted by law no. 203/91) on combatting organized crime allows for interception under broader conditions in investigations concerning organized crime or threat by telephone. The law stipulates that in organized-crime investigations, oral interception is allowed in protected places, even if there is no ground to believe that crimes are taking place in such places. Therefore, in organized-crime investigations, an indication of the places in which interception is to take place is irrelevant.[258]

The use of Trojans for oral interception is also the only functionality of police hacking that the legislator has taken up and is now regulated by statutory law. This suggests that the law-maker considers oral interception, particularly in constitutionally protected places (homes and places of private abode), the most intrusive usage of police hacking.[259]

---

[256] Cass., Sez. Un., 28 aprile 2016, n. 26889, §5 ('Scurato').

[257] *Id*. §6.

[258] *Id*. §7.

[259] In doctrinal literature, however, it is emphasized that other functionalities can also be very—equally or perhaps even more—intrusive. *See* text accompanying fn. 212 *supra*.

By law of 29 December 2017, no. 216 (effective date postponed until March 2019), article 266(2) Italian CCP has been amended to the effect that oral interception can also be effected "through the insertion of an informatic sensor [*captatore informatico*] on a mobile electronic device. However, if this occurs in the places indicated in article 614 Criminal Code, the interception is allowed only if there is motivated reason to believe that the criminal activity is taking place there."[260] For certain serious crimes,[261] however, oral interception through informatic sensors is always allowed (also in protected places without indications of criminal activity).[262] The decree authorizing the hacking must mention the reasons that make this measure necessary, as well as (if the crime is not a listed serious crime) "the places and the time, also indirectly determined, in relation to which the activation of the microphone is permitted."[263] These requirements suggest that the oral interception through hacking will usually (or only) be possible if combined with other investigation measures, such as visual observation or location tracking, in order to determine the right moments for turning the microphone on or off.

It should be noted that the statutory law only applies to hacking *mobile* devices; hacking fixed devices (such as desktop computers) for the purposes of oral interception therefore falls under the regime previously determined in case-law, in particular the *Scurato* judgment. Consequently, the legal goods considered to be most at issue in this stream of law are the secrecy of communications (particularly communications between people present, which are more strongly protected than telecommunications in this context) and the inviolability of the home. The latter receives particular emphasis in the fine-grained patchwork of situations in which it is allowed to conduct oral interception in protected places (dwellings and places of private abode), primarily through a requirement that conversations in these places can only be intercepted if there are grounds to believe that criminal activity is taking place there. Only for certain designated crimes does this limitation not apply. This suggests that the home is, in this context, particularly seen as a place where people should be able to freely converse and speak their minds.

In Germany, the functionality of oral interception does not appear to be permissible. The online search is limited to collection of data; using the

---

[260] Art. 266(2) Italian CCP. Art. 614 Criminal Code refers to the places protected by art. 14 Costituzione [Cost.] (It.) (inviolability of the home), namely dwellings, places of private abode, and appurtenances.

[261] The crimes mentioned in art. 51, paras. 3-bis and 3-quater Italian CCP (briefly put, conspiracy to, e.g., abduction, illegal immigration, or underage sex trafficking, and terrorist crimes).

[262] Art. 266-bis(2-bis) Italian CCP.

[263] Art. 267(1) Italian CCP.

infiltrated computer system for the independent generation of data is inadmissible. Therefore, an independent activation of the microphone is not allowed. This can be deduced from the wording of the provision as well as its title (search).[264] Furthermore, the literature questions the permissibility of using incidental oral interception, for example when the connected microphone intercepts conversations without being activated by law enforcement. Such interception could meet the conditions of acoustic surveillance of the home (subject to the same requirements as the online search), but since the order for such measure would not exist in case of incidental interception, it will usually not be usable.[265]

E. Observation

Observation encompasses turning on a webcam (or another camera), to identify the user or location of a device or to observe behavior of the user or people in their environment. In the US, multiple federal appellate courts have held that the heightened "super-warrant" requirements outlined in the Wiretap Act apply to video surveillance[266] (although these requirements technically apply by virtue of the Supreme Court's decision in *New York v. Berger*[267] rather than as a direct application of the Wiretap Act itself[268]). Thus, in *In re Warrant To Search a Target Computer at Premises Unknown*, the federal magistrate judge borrowed the Wiretap Act's heightened standard to reject a warrant application from the government covering the remote activation of the target computer's webcam.[269] In that application, the

---

[264] Singelnstein & Derin, *supra* note 51, at 2647; Niedernhuber, *supra* note 39, at 172.

[265] Graf, *supra* note 41, Rn. 55.

[266] *See* United States v. Cuevas-Sanchez, 821 F.2d 248, 250 (5th Cir. 1987); United States v. Biasucci, 786 F.2d 504, 510-11 (2nd Cir. 1986) *cert. denied*, 479 U.S. 827 (1986); United States v. Torres, 751 F.2d 875 (7th Cir.1984), *cert. denied*, 470 U.S. 1087 (1985); United States v. Mesa-Rincon, 911 F.2d 1433, 1436-46 (10th Cir. 1990); United States v. Koyomejian, 970 F.2d 536, 538-42 (9th Cir. 1992); United States v. Falls, 34 F.3d 674, 679-83 (8th Cir. 1994); United States v. Williams, 124 F.3d 411, 416-20 (3d Cir. 1997). *See also* In re Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d at 759-60 (applying Title III wiretap standards for warrant applications to a request for video surveillance).

[267] 388 U.S. 41, 58-60 (1967).

[268] *See* Mayer, *supra* note 5, at 639-40 ("The unanimous conclusion among federal appellate courts has been that the Wiretap Act does not apply, but the Berger doctrine does. Courts must, consequently, borrow the core super-warrant protections from the Wiretap Act when authorizing video surveillance. The result for law enforcement malware is clear guidance: if agents seek to enable a computer's camera, they must obtain a super-warrant in advance.").

[269] *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d at 759-60.

government sought to get around the "super-warrant" requirements by claiming that they only intended to "snap photographs sufficient to identify the persons using the computer," a form of surveillance they described as "photo monitoring, as opposed to video surveillance"[270] (meaning they would not acquire the contents of any oral, wire, or electronic communications). However, the magistrate found that, "this is a distinction without a difference. In between snapping photographs, the Government will have real time access to the camera's video feed. That access amounts to video surveillance."[271]

In the Netherlands, systematic observation, where the remote access facilitates observation is regulated in art. 126g Dutch CCP. In contrast to the regular power for systematic observation, a technical device (i.e., the software used to infect the target's smartphone) may be placed on a person without their consent. An example would be a secretly installed GPS tracker that maps the smartphone's movements with high accuracy.[272]

It is relevant to note that the current prohibition of "permanent" visual observation in the home remains in place. Since article 126nba(1)(c) Dutch CCP refers to using hacking for the purpose of conducting systematic observation as regulated in article 126g, the latter's legal conditions also apply, which include prohibition of in-home recordings by installed cameras.[273] Thus, "*permanent* observation of what happens inside a dwelling through remotely turning on the webcam of, for instance, a smartphone or laptop, must be considered equally intrusive as entering a dwelling; that is not allowed in the context of criminal investigation."[274] As before, the law-maker here leaves open some form of incidental observation inside the dwelling from the outside: the prohibition explicitly sees to "permanent" recordings, which likely refers to indiscriminate recording of everything over a certain period of time. The recording of webcam images for a short period might be allowed. Possibly, the real-time watching of webcam images—without recording them—might also be allowed if this is done with a view to start recording webcam footage when something happens that is relevant for the investigation (and stopping the recording as soon as the investigation-relevant activity ends). Such real-time observation might be compared with a police officer hiding in the bushes and taking snapshots of relevant in-home activities, which is allowed.[275] In any case, using the webcam for covertly making in-home recordings over a period of time is not allowed.

---

[270] *Id.* at 759.
[271] *Id.*
[272] *Kamerstukken II* 2015/16, 34 372, no. 3, at 26.
[273] *Id.*
[274] *Kamerstukken II* 2015/16, 34 372, no. 3, at 27 (emphasis added).
[275] *Kamerstukken II* 1997/98, 25 403, no. 7, at 66.

In Italy, for video recordings (using spyware to turn on the computer's or phone's camera), the norms for visual recordings apply, according to the *Musumeci* case.[276] Briefly put, such use of Trojans are allowed, as atypical means of searching for evidence, if visual recordings are made in public places or places exposed to the public, but not in places of private abode or in situations where personal privacy needs to be protected (such as public toilets). Images made in the latter cases have to be excluded from evidence.[277] Therefore, since visual recordings inside protected places is not allowed at all, it can arguably be concluded that, despite the *Musumeci* case, visual observation through Trojans in mobile devices is not allowed, since it may not be possible to determine in advance whether they are not located in a protected place. Only fixed computers in public or publicly accessible places might be infected with malware to turn on a webcam.

In Germany, although some authors mention visual observation as one of the possibilities enabled by police hacking,[278] most of the literature rejects this.[279] As we already discussed with regard to oral interception, German online search provisions only allow collection of data, not their active generation by, for example, activating the webcam. Even when the camera is activated by the user themselves, this would be quite problematic. If the user is inside a dwelling, this would constitute visual surveillance of living space, which is invariably unacceptable under the German Basic Law.[280] The potential use of this functionality would therefore have to be limited to incidental cases when the user turns on their camera in a public place.

Although the functionality of turning on a computer's webcam is little discussed in the context of police hacking, the general prohibition of visual observation inside the home in several jurisdictions (Germany, Italy, Netherlands) suggests an additional emphasis on protection of the home as a shelter for behavioral freedom: people should not feel inhibited to do what they want without fear of being observed in the security of their home. The fact that visual observation is prohibited, while oral interception is allowed (albeit under strict conditions), might suggest that behavioral freedom is valued even more highly than the freedom to speak one's mind inside the home. However, this legal constellation might also be explained by the generally higher relevance of interception for criminal investigation purposes over visual observation, so that the balance of interests weighs somewhat

---

[276] Cass. Sez. VI, 26 maggio 2015, n. 27100, §3 ('Musumeci').

[277] *Id*.

[278] Beukelmann, *supra* note 29, at 440.

[279] Singelnstein & Derin, *supra* note 51, at 2647; Niedernhuber, *supra* note 39, at 172; Roggan, *supra* note 56, at 826.

[280] Roggan, *supra* note 56, at 826.

more towards criminal investigation in the case of in-home interception, while it weighs more towards privacy in the case of in-home observation.

IV. ANALYSIS AND DISCUSSION

In this Article, we are particularly interested with the way in which law-makers and courts assess the intrusiveness of police hacking, given that this multifunctional new power can impact on a wide variety of interests and rights. A computer, alone or in combination with cloud storage, is a functional equivalent of many traditional spaces in which social life is enacted (such as living rooms, bedrooms, cafés, libraries, hospital rooms, and public squares), and essentially collapses these into a single complex digital environment.[281] This makes police hacking a power that potentially intrudes upon various privacy interests in a manner and degree that may resemble traditional offline investigation to greater or lesser extents, depending on the functionalities and application. We are particularly interested in examining whether law-makers and courts rely on traditional privacy frameworks in regulating police hacking or, alternatively, whether they resort to new privacy frames in order to determine its intrusiveness. In this Part, we first summarize the classic privacy frameworks that emerged in our analysis, and then focus on new privacy frames that emerge in the regulation of police hacking.

A. Classic Privacy Frames

During our comparative research, we identified two classic privacy frames which are relevant in all five jurisdictions to some extent. These are the *inviolability of the home* and *secrecy of communications*. Additionally, *protection of personal data* is a classic framework in Italy and Germany, as is protection of a *core of privacy* in Germany. It is also worth mentioning that certain privileged information, related, for instance, to legal privilege or the protection of journalistic sources, enjoys special protection in most jurisdictions, although it is often not regulated specifically in the context of police hacking.[282]

1. Inviolability of the home

---

[281] *See* Bert-Jaap Koops, *Privacy Spaces*, 121 WEST VIRGINIA LAW REVIEW (forthcoming 2018).

[282] Protecting privileged information plays an important role in police hacking regulation in the UK. *See supra*, Part II(D).

In the continental jurisdictions (and in the United States[283]), constitutional protection of the inviolability of the home forms a key traditional form of privacy protection. The protection is given to a spatially delimited sphere which is under control of the individual, and which can only be intruded upon in a limited set of circumstances in which relatively high safeguards have to be met, typically requiring a judicial order. It offers container-type protection, not protecting private life directly, but protecting this physical space as a proxy for where private life is presumed to take place.

The limitations of such a form of protection to effectively protect computers are apparent. One reason is that current computers (understood broadly) are not necessarily always kept at home and are commonly carried by their users wherever they go. Additionally, even computers that typically remain physically inside the home are interconnected with other computers. Data are also increasingly stored remotely, which makes data susceptible to being collected either in transit or at the place of remote storage (where protections based on traditional notions of "home" will not typically apply[284]). The significance of this limitation is moderated to some extent in the US by a similar focus on protecting privacy (by proxy) through the protection of closed containers and the application of this doctrine to computers,[285] but that does not apply to the European jurisdictions in our study.

Therefore, even though commitments to and theories of the inviolability of the home potentially offer robust protection for private life, our research reveals that its relevance in relation to police hacking activities is limited and partial. We can distinguish between two principal types of police hacking activities when it comes to the importance of home protection: measures using covert access to a computer as a tool to monitor behavior in the physical space in which it is located and measures targeting the computer itself in order to access stored data. The role of home protection appears to remain very strong in the first type, where the police hacking does not target the computer

---

[283] *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001) ("the interior of homes [are] the prototypical and hence most commonly litigated area of protected privacy"); United States v. U.S. Dist. Court (Keith), 407 U.S. 297, 313 (1972) ("physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed"). Note, however, the text accompanying fn. 172 *supra* (advisory committee finding that "computers are no more sacrosanct than homes").

[284] This is particularly evident in the provisions of the Stored Communications Act in the US, which provides a very different (and less restrictive) regulatory regime for access to stored communications-related data than, for example, a search of a person's house for communication-related evidence, a search of a smartphone, or the wiretapping of communications occurring within a person's place of residence.

[285] *See supra* note 135 (references and text accompanying the note).

itself but rather the physical environment by, e.g., turning on the microphone or the webcam. The inviolability of the home remains the main constitutional standard in relation to these functionalities. In the US, the Fourth Amendment clearly covers this form of covert surveillance.[286]

Dutch regulation of the functionality of oral interception has been justified by the fact that it avoids the need to physically enter the home.[287] In Italy, communications taking place in homes and places of private abode can only be monitored if there is motivated reason to believe criminal activity is taking place there, and since it cannot be foreseen beforehand and effective judicial supervision would be impossible, police hacking for the purposes is generally not allowed under existing case law.[288] The forthcoming statutory regulation of police hacking into mobile devices for the purpose of oral interception also suggests that oral interception in constitutionally protected places (homes and places of private abode) is considered the most intrusive form of police hacking.[289]

In German doctrine we also found considerations for the protection of the home being used as an argument against the possibility of using police hacking for oral interceptions.[290] The UK legislation makes no specific provision for the monitoring of activity in the home. However, the extent to which equipment interference reveals such activity will be considered under the proportionality assessment by the authority issuing an interference warrant.

The protection of the home features even more strongly in case of visual observation. In the Netherlands, permanent visual observation in the home is generally prohibited, which applies also to police hacking.[291] Similarly, in Italy, use of Trojans to make visual recordings of public places is allowed,

---

[286] Indeed, as the Supreme Court stated in *United States v. Karo*, the Fourth Amendment's protections for the privacy of the home apply to the mere use of tracking technology to determine "whether a particular article—or a person, for that matter—is in an individual's home at a particular time," something the Court noted would "reveal a critical fact about the interior of the premises that the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant." United States v. Karo, 468 U.S. 705, 716 (1984). *See also Kyllo*, 533 U.S. at 34 ("obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area . . . constitutes a search") (internal citations omitted).

[287] *Kamerstukken II* 2015/16, 34 372, no. 3, at 13. *See also Kamerstukken II* 2016/17, 34 372, no. 6, at 24.

[288] Cass., Sez. Un., 28 aprile 2016, n. 26889, §6 ('Scurato').

[289] D.Lgs. 29 dicembre 2017, n. 216, G.U. Jan. 11, 2018, n.8 (It.) (the entry into effect of which, as observed, has been postponed to March 2019); art. 266 para. 2 Italian CCP.

[290] Graf, *supra* note 36 Rn. 55.

[291] *Kamerstukken II* 2015/16, 34 372, no. 3, at 27 (emphasis added).

but monitoring places of private abode or in situations where personal privacy needs to be protected is not.[292] Visual surveillance of dwellings is also not permitted under German Basic Law in the criminal procedure context.[293] In the US, heightened warrant standards would apply to video surveillance inside the home.[294]

In contrast, when either data stored on a computer or a user's computer behavior is the target of the investigation (functionalities B and C), constitutional home protection appears to be less relevant as the standard of protection. An exception is Italy, where case law suggests that, in cases of remote access, computers located inside the home should be protected more strongly than computers located elsewhere, such as in public offices that can be accessed by a larger number of people.[295] However, this has been criticized in the literature as misunderstanding the intrinsic place-independence of computers; Italian authors therefore point to different legal goods, such as "informatic home" or "informatic privacy," as the proper yardstick, instead of traditional home protection.[296]

Explicit place-based distinctions are not found in the German, Dutch, UK, or US regulation of remote computer searches. Dutch, UK, and US safeguards for this form of police hacking are equally high regardless of the location of the computer (although, in practice, US judges might choose, at their discretion, to apply stricter rules for searches conducted within homes than for searches conducted in less privacy-sensitive places). The UK approach is illustrative, in that its statutory scheme regulating equipment interference corresponds with the place-independent criminal offense of hacking, which criminalizes unauthorized access to a computer, or any data stored on it, regardless of its place.

Computers thus appear to be worthy of protection themselves, protected through very high safeguards, thus making home protection irrelevant.[297]

German provisions on the online search also make no mention of home protection. The applicability of home protection to police hacking has been

---

[292] Cass. Sez. VI, 26 maggio 2015, n. 27100, §3 ('Musumeci').

[293] Roggan, *supra* note 56, at 826.

[294] *See supra*, Part III(E).

[295] Cass., Sez. V, 14 ottobre 2009, n. 16556 ('Virruso') (It.), as quoted in Trogu, *supra* note 191, at 448.

[296] *See supra* Part III(B) and *infra* Part IV(B)(1)-(2).

[297] *See supra* Part III(B). Analogies to the constitutional protection of the home are found, however, quite often in judicial decisions related to the regulation of police searches of digital devices. *See, e.g.*, Riley v. California, 134 S.Ct. 2473, 2491 (2014) ("a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is").

examined at some length by the German Constitutional Court, identifying significant loopholes in the protection offered to computers.[298] According to the Constitutional Court, the protection of the home applies to both physical penetration of the dwelling and to measures by which the state agencies obtain an impression of events within the dwelling that are removed from natural perception.[299] Thus, police hacking to monitor events in the dwelling by using peripherals of the system are covered by the constitutional home protection.[300] We see the same result in the US.[301] However, constitutional protection of the home, in Germany,

> does not confer on the individual any across-the-board protection regardless of the access modalities against the infiltration of his or her information technology system, even if this system is located in a dwelling. The encroachment may take place regardless of location, so that space-oriented protection is unable to avert the specific endangerment of the information technology system. Insofar as the infiltration uses the connection of the computer concerned to form a computer network, it leaves spatial privacy provided by delimitation of the dwelling unaffected. The location of the system is in many cases of no interest for the investigation measure, and frequently will not be recognizable even for the authority.[302]

The latter is an important point for consideration by jurisdictions that stick to place-based protection: laws that allow police hacking outside the home but not inside the home for certain functionalities will be difficult to enforce in practice due to the place-independence of modern computing devices. From the legislative documents we studied, in jurisdictions that (for some functionality, such as oral interception or visual observation) apply a place-based distinction, the law provides very little guidance to police how they should determine when the hacking takes place inside or outside a home (indeed, knowing this might reasonably necessitate some form of *a priori* police hacking, à la Functionality A). The most meaningful way to operationalize a place-based distinction is to distinguish between fixed computers (where non-home-based fixed computers might be hacked under lower conditions than in-home fixed computers) and mobile computers (where the practical difficulties of determining their actual location would imply that mobile computers should not be hackable, if home protection is to

---

[298] BVerfG, 1 BvR 370/07, Feb. 27, 2008, Rn. 191 (Ger), http://www.bverfg.de/e/rs20080227_1bvr037007en.html.

[299] *Id.* Rn. 192.

[300] *Id.* Rn. 193.

[301] See discussion *supra* at note 286.

[302] *Id.* Rn. 194 (official translation).

be respected).

However, as ever more people are using mobile computers rather than fixed desktop computers, it will make less sense to base protection on computers' locations. This is where the German approach is innovative and seems prescient: it determines the intrusiveness of covert online searches not through the lens of home protection (even if a hacked computer would happen to be inside a home),[303] but solely through the lens of the new standard of the confidentiality and integrity of computers.

Nevertheless, it is interesting to note that even though the protection of the home does not appear to be a relevant standard of protection in cases of covert remote searches in Germany, the Netherlands, and the US (to a great extent, excepting *sua sponte* judicial determinations when reviewing warrant applications), it does appear to have served as a role model for the level of procedural safeguards that should be put in place. Since the German Constitutional Court considers secret infiltration of computer systems to be comparably intrusive to acoustic surveillance of the home, the legislator designed the procedural safeguards for the two measures identically.[304] The same is true for the Dutch statutory regulation, where oral interception in the dwelling and remote computer searches are arguably considered equally intrusive by the law-maker.[305]

2. Secrecy of communications

Most contemporary computers serve, at least in part, as communication devices. Computers that can be the target of remote police hacking must be in some way connected to other devices and, thus, capable of communication. Mobile phones, the most commonly used type of personal computing device (at least in the US[306]), originated primarily as communication devices, but have assumed additional computing functions over time.

In the US, at least at the federal level, the privacy of communications is protected under a variety of statutory regimes, with varying levels of protection based on 1) whether police seek the content of a communication or only related non-content information (metadata); or, for searches related to the content of communications, 2) whether police seek to intercept the communication in transit (wire and electronic communication),

---

[303] *Id.* Rn. 195.

[304] Niedernhuber, *supra* note 39, at 171.

[305] *See supra* Part III(B).

[306] According to the Pew Research Center, 95% of Americans own some type of cellphone (with smartphone ownership at 77%), while 73% own a laptop or desktop computer and only 53% own a tablet computer (as of January 10, 2018). Pew Research Center, *Mobile Fact Sheet* (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile/.

contemporaneously with oral utterance (oral communication), or after evidence of the communication has been saved to electronic storage. Contemporaneous (or nearly contemporaneous[307]) wire, oral, and electronic communication is protected against unlawful interception by the heightened authorization requirements contained within the Wiretap Act, while police access to electronically stored communications information is subject to the requirements of either Rule 41 or the Stored Communications Act (depending on the nature of the proposed search).[308]

In most continental European jurisdictions, the constitutional protection of the secrecy of communications traditionally protects only mediated communications, such as letters, phone calls, or various electronic communications. Since it only protects information *in transit*, it essentially protects the communication channel itself from interference (interception) or, more precisely, it protects the trust of communicating parties in the confidentiality of the communication channel.[309] Such protection is supposed to avert the dangers of spatially distanced communication.[310] Thus, the standard of secrecy of communications should normally not apply to police hacking activities, since these activities do not target the communications channel, but the terminal device itself, and thus concern the trust of users in the integrity of their terminal equipment and not in the communication channel.[311]

However, we observe a departure from the traditional framing of secrecy of communications, especially in German law. The German Constitutional Court recognizes that the constitutional guarantee of the secrecy of telecommunication protects the non-physical transmission of information to individual recipients, regardless of the method of transmission, but does not protect the confidentiality and integrity of computer systems.[312] Yet, the Court stated that

> insofar as an empowerment is restricted to a state measure by means of which the contents and circumstances of the ongoing

---

[307] *See* Mayer, *supra* note 5, at 640 n.176 ("Courts have generally not required that the transmission of recorded activity be precisely contemporaneous with the activity," *citing* Williams v. Stoddard, No. PC 12-3664, 2015 R.I. Super. LEXIS 58, at *19-30 (R.I. Super. Ct. Feb. 11, 2015)).

[308] *See supra*, Part III(D)(1).

[309] Italian law is an exception here, since art. 15 Cost. protects the secrecy "of correspondence and of any other form of communications," which includes non-mediated (i.e., oral) conversations. Filippo Donati, *Commento all'art. 15*, *in* COMMENTARIO ALLA COSTITUZIONE §2.2 (Raffaele Bifulco, Alfonso Celotto & Marco Olivetti eds., Utet 2006).

[310] BVerfG, 1 BvR 370/07, Feb. 27, 2008, Rn. 185.

[311] Freiling et al., *supra* note 7, at 20.

[312] BVerfG, 1 BvR 370/07, Feb. 27, 2008, Rn. 182-183.

> telecommunication are collected in the computer network, or the data related thereto is evaluated, the encroachment is to be measured against Article 10(1) of the Basic Law (secrecy of communications) alone. The scope of protection of this fundamental right is affected here regardless of whether in technical terms the measure targets the transmission channel or the terminal used for telecommunication.[313]

The protection of secrecy of communications, however, only applies to communications *in transit*; it does not apply to stored communications, nor to stored (non-communicative) data that are in transit (e.g., access by users to their own data in the cloud).[314] Thus, according to the Constitutional Court, the so-called source telecommunications surveillance (Functionality D.1) is to be solely measured against the standard of constitutional protection of secrecy of communications. This implies that access to such communications is allowed under less strict safeguards than an online search (Functionality B), as long as it can be technically ensured that access to non-communications data is precluded.[315]

In Italy, the secrecy of communications has not been found at issue by the Supreme Court when the program does not intercept a flow of communications (which implies a dialogue with other persons), but merely targets the unidirectional flow of data inside the computer's circuits.[316] In the UK, the interception of communications and the acquisition of communications data stored on a computer or other device are covered by separate regulatory regimes; still, they afford similar levels of protection to comply with the right to private life under Article 8 of the European Convention on Human Rights.

3. Data protection

Protection of personal data, as used in this subsection, refers to a variety of content-based approaches of privacy protection in our jurisdictions. As opposed to the protection of the home which protects the physical place as a container, and the secrecy of communications which traditionally protects the communication *channel*, data protection aims to protect personal data itself, as something worthy of distinct protection.

In Germany, this content-based protection is expressed as the standard of informational self-determination which is one manifestation of the general

---

[313] *Id.* Rn. 184.
[314] *Id.* Rn. 185-186.
[315] *Id.* Rn. 190.
[316] Cass., Sez. V, 14 ottobre 2009, n. 16556 ('Virruso') (It.), as referred to in Trogu, *supra* note 191, 448.

right of personality.[317] As with protections for home and communication, the Constitutional Court finds that informational self-determination offers insufficient protection to computer users. This manifestation of privacy protection confers on the individual, in principle, the power to determine for themselves the disclosure and use of their personal data.[318] The Court, however, finds that the

> need for protection of the user of an information technology system is however not solely restricted to data to be allotted to his or her privacy. Such an attribution also frequently depends on the context in which the data came about and into which it is brought by linking with other data. In many cases, the data itself does not reveal what significance it has for the person concerned and which it may gain by inclusion in other contexts.[319]

A similar argument is advanced in the Italian debate, where Iovene determined that article 7 of the EU Charter of Fundamental Rights (the right to privacy), rather than article 8 (the right to data protection), is at stake:

> It is not so much to guarantee to the affected person the control of the ways in which his personal data are processed; rather, more fundamentally, to protect the person in a context in which the most varied aspects of his private life are translated into data, which are susceptible to informatic processing. In an environment in which it is no longer possible to distinguish between intimate, reserved, and social data, article 8 Charter turns out inapplicable and one should turn to the wide protection offered by article 7 to protect private life.[320]

In other jurisdictions, we have not encountered the application of a data-protection-oriented lens in discussions of police hacking. Thus, we conclude that law-makers and courts do not consider the protection of personal data to be a significant normative framework by which to evaluate the intrusiveness of police hacking, even if personal data are constitutionally protected (e.g., in the EU Charter).

B. New Privacy Frames

As the previous discussion shows, jurisdictions resort to classic privacy frames (in particular, the home and secrecy of communications), but the

---

[317] BVerfG, 1 BvR 370/07, Feb. 27, 2008, Rn. 196.
[318] *Id.* Rn. 198.
[319] *Id.* Rn. 197 (official translation).
[320] Iovene, *supra* note 28, at 338.

adequacy of these frames in assessing the intrusiveness of police hacking is limited to certain functionalities (such as visual observation and interception). As computers contain so much information that a computer search can reveal significantly more than could a search of a person's home,[321] new privacy frames may be needed to assess the intrusiveness of police hacking. Across our jurisdictions, we observe the contours of two such new frames emerging: a container-based approach focusing on the computer as protection-worthy in itself and a content-based approach focusing on the data.

1. Inviolability of the computer

Since traditional privacy frames of home, communications, and data protection seem no longer sufficient to protect the privacy of computer users in the context of police hacking, some jurisdictions have taken a new approach: recognizing, explicitly or implicitly that computers are protection-worthy in themselves. Thus, a new form of container-based protection, in which the computer serves as a proxy for protected privacy values is emerging in several legal systems.

Importantly, the property-based approach to constitutional privacy protections under the Fourth Amendment has long regarded "closed containers" as worthy of some protection. In more recent years, the Supreme Court has held that the police may engage in a Fourth Amendment search when they merely touch a suspect's physical property (including a computer), analogizing these physical "closed container" searches to those conducted of electronic devices.[322] As such, this line of reasoning continues the long-running US approach to protecting privacy through proxies (often relying on notions of real or personal property).

In Germany, the Constitutional Court found, as early as 2008, that the existing constitutional safeguards protecting the inviolability of the home, the secrecy of communications, and informational self-determination were not sufficient to protect individuals against secret infiltration of their computers. The Court recognized that the use of computers, their omnipresence and centrality in the lives of individuals, and the significance they hold for developing individual personalities, provides individuals with many new

---

[321] *See supra*, note 297.

[322] *See supra* note 135 (references and text accompanying the note). *See also* United States v. Jones, 565 U.S. 400, 404-405 (2012) (holding that that the physical placement of a GPS tracking device under an automobile's rear bumper constituted a search for Fourth Amendment purposes, at least insofar it as was connected to collecting information about the location of the vehicle, as "[t]he Government physically occupied private property for the purpose of obtaining information").

opportunities, but also presents previously unforeseen dangers.[323] Consequently,

> a large amount of data can be accessed in the working memory and on the storage media of such systems relating to the personal circumstances, social contacts and activities of the user. If this data is collected and evaluated by third parties, this can be highly illuminating as to the personality of the user, and may even make it possible to form a [personality] profile.[324]

In response, the Court interpreted the articles of the Constitution protecting human dignity and the free development of personality as encompassing a fundamental right to the guarantee of the confidentiality and integrity of information technology systems.[325] This right protects against encroachments to computers insofar as protection is not guaranteed by other fundamental rights.[326] This fundamental right is not absolute and encroachments may be justified for both preventive and criminal prosecution purposes, but these encroachments must meet very high standards in terms of both the conditions for their authorization and other procedural safeguards.[327]

Although not as explicit as in Germany, the Dutch regulation also seems to find computers as highly protection-worthy in themselves in the context of police hacking, since the preconditions for covert remote searches are among the strictest in the criminal procedure system, on par with the requirements set for acoustic surveillance inside private dwellings.

Both Germany and the Netherlands therefore recognize a form of *sui generis* protection of computers in the context of police hacking.[328] In Italian law, computer systems are more broadly recognized as protection-worthy in themselves, in an attempt to make a conceptual connection between the home as a physical space and a computer or cyberspace as an informatic equivalent of the home, which is a legal good recognized in the law on the offense of hacking.[329] The informatic home needs to be protected,

> as the virtual space (but also physical space in which the informatic data are contained) relating to the individual sphere, which is also constitutionally protected, over which the owner can exercise

---

[323] BVerfG, 1 BvR 370/07, Feb. 27, 2008, Rn. 170-171.

[324] BVerfG, 1 BvR 370/07, Feb. 27, 2008, Rn. 178 (official translation).

[325] *Id.* Rn. 166.

[326] *Id.* Rn. 167.

[327] *Id.* Rn. 207.

[328] Such protection of computers (at least in the manifestation of cell-phones) has also been recognized in US law, but in a different context, namely search of smartphones incident to arrest. *See supra* note 297.

[329] *See supra* note 219 and surrounding text.

> towards third persons both the *jus prohibendi* and the *jus admittendi*, with a legitimate expectation of privacy.[330]

Torre observes that the concept of "informatic home" has been recognized by the legislator as a virtual extension of the physical home protection under article 14 of the Italian Constitution. This has also been confirmed by the Italian Supreme Court.[331] Although

> a notion of home disconnected to spatio-temporal coordinates was inconceivable at the time the Constitution was drafted, the rationale of the norm of article 14 should today direct us not only to protect the physical home, but also and ever more towards defending those virtual spaces that represent, by now, a fundamental conjugation of the individual's life.[332]

Importantly, Torre argues that the informatic home is even more personal and intimate than the traditional home, since the latter may contain documents or personal effects, but

> the informatic home, be it a depository of the individual's work activities or of his private life, preserves an extension of our mind itself, because the user, 'working' with the machine, and inserting his own information into it, entrusts to it his work and/or private plans, his thoughts, his projects (past, present or future): all those data represent traces and expressions of our daily life and of our personality; hence, from this perspective, the necessity to protect the privacy of the informatic home would prove even more relevant and important than the physical home itself, going beyond the mere aspect of protecting the privacy of the places of a person's life, and embracing the protection of the individual's personality itself.[333]

According to Iovene, it is now necessary to "reaffirm the existence of that sphere of privacy, whose classic boundaries, linked to the physical spaces and to the type of information that one wants to keep others from knowing, are blurring and dissolving."[334] This can be done by recognizing a new legal good, worthy of constitutional protection. While the "informatic home" seems a good candidate for that, it is not sufficiently precise, since the home

---

[330] Trogu, *supra* note 191, at 434, with reference to Cass., Sez. VI, 4 ottobre 1999, n. 3067, CED Cass (It.).

[331] Cass. Sez. V, 26 ottobre 2012, n. 42021, as quoted in Torre, *supra* note 18, at 85.

[332] Torre, *supra* note 18, at 85-86.

[333] Torre, *supra* note 18, at 86, quoting G. PICA, DIRITTO PENALE DELLE TECNOLOGIE INFORMATICHE 66 (Torino 1999).

[334] Iovene, *supra* note 28, at 335.

serves the interest of the *jus excludendi alios* (the right to exclude others) from a pre-eminently personal or intimate sphere, while computer systems involve a broader range of activities in which people express their personalities, also in developing social relations online or in other "informatic" spaces.[335] The concept of informatic privacy, which Iovene proposes will be discussed in the following subsection.

2. Informatic privacy and the mosaic theory

In the previous subsection, we discussed new approaches to protecting individuals in the context of covert access to their computer which attempt to do so by protecting the computers or a metaphorical informatic home, as a proxy for the values that are sought to be protected. At the same time, and often interconnected with the first approach, we observe a second approach, which attempts to protect *content* itself rather than the container, as a proxy for the values that are sought to be protected.

In Italian doctrine, this protection-worthy content idea is expressed as informatic privacy (*riservatezza informatica*). The concept is in a way a critique of the informatic home concept, stressing that computer systems involve a broader range of activities in which people express their personalities, also in developing social relations online or in other "informatic" spaces.[336] In other words, since informatic systems collapse the personal and the social spheres of life, the interest at stake is not so much in protection of an informatic "home" to enable controlling access to information as such, but in protection of informatic privacy to enable controlling what happens with information. Thus, part of Italian doctrine emphasizes that "informatic privacy" is the legal good to be protected, which can be described as the "exclusive interest, legally recognized, to enjoy, dispose, and control the digitized information, processes, systems and 'spaces', and their uses."[337] The focus on what happens with the information as opposed to merely controlling the access to it, is also reflected by the German Constitutional Court in the context of core area protection.[338]

Some Italian authors reach beyond informatic privacy and resort to human dignity as the ultimate normative frame to apply to police hacking. Torre argues that the computer can now function as an actual "appendix" of the person and their most fundamental self, so that police hacking touches upon the inviolability of the mind, and thereby triggers considerations of

---

[335] *Id.* also referring to Flor, *supra* note 50.
[336] *Id.*
[337] Iovene, *supra* note 28, at 335, quoting Flor, *supra* note 223.
[338] *See supra*, Part II(A).

human dignity. After all, through real-time monitoring of computer use, police hacking implies that police can not only acquire finished or stored documents, but also expressions that people type but, on second thoughts, erase before storing the document in some durable form. Thus, police hacking enables an unprecedented perception of people's thoughts.[339] Therefore, it seems that Torre ultimately considers human dignity to be the core legal good at issue and recommends treating this as a constitutional right associated with proper constitutional safeguards. However, his argument remains somewhat ambiguous since, at the end, he jumps from human dignity to "informatic privacy" as the legal good that is at issue in the regulation of police hacking, perhaps because he considers this more realistically achievable as a constitutionally protected right.

The German protection of the confidentiality and integrity of computer systems[340] also contains elements of the content type of protection. This computer-focused protection is based on the observation that computers process a wide variety of data, which together can tell a lot about someone, without individual pieces of data necessarily being privacy-relevant. The Court argued as follows:

> In many cases, the data itself does not reveal what significance it has for the person concerned and which it may gain by inclusion in other contexts. The consequence of this is that, inevitably, not only private data is collected by the infiltration of the system, but access to all data is facilitated, so that a comprehensive picture of the user of the system may emerge.[341]

The notion that computers may contain so many and such varied data that computer searches can result in highly intrusive pictures of people's private lives, leads to an important limitation in the scope of the new right to integrity and confidentiality of computers. According to the Constitutional Court,

> not all information technology systems which are able to create, process or store personal data require the special protection of a separate guarantee of personality rights. Insofar as such a system by its technical construction only contains data with a partial

---

[339] Torre, *supra* note 18, at 87. Similarly Torre, *supra* note 196, at 28 (observing that the 'inviolability of the mind' (*inviolabilità della psiche*) is infringed, if the Trojan captures whatever the investigated person writes, also if he decides to immediately delete what he has just written'). Also, Palmieri emphasises that the use of Trojans 'borders on controlling the mind', touching upon 'opinions and thoughts' rather than actions and behaviours'. *See* Palmieri, *supra* note 45, at 60-61, referring to Tonini & Conti, *supra* 224, at 482, and to Gaito & Furfaro, *supra* 224, at 364.

[340] *See supra* Part IV(B)(1).

[341] BVerfG, 1 BvR 370/07, Feb. 27, 2008, Rn. 197 (official translation).

> connection to a certain area of life of the person concerned – for instance non-networked electronic control systems in household appliances –, state access to the existing data is no different in qualitative terms than other data collections. In such a case, the protection of the right to informational self-determination is sufficient to guarantee the justified interests of the person concerned in confidentiality. (…) The fundamental right to the guarantee of the integrity and confidentiality of information technology systems is to be applied, by contrast, if the empowerment to encroach covers systems which alone or in their technical networking can contain personal data of the person concerned to such a degree and in such a diversity that access to the system facilitates insight into significant parts of the life of a person or indeed provides a revealing picture of the personality.[342]

The Court here recognizes a special status of computers, which deserve to be protected not necessarily because they contain bits of very intimate data, such as those protected by the core area of private life, but because they process a large quantity and diversity of data relating to many spheres of life of the user. Even if the individual bits of information are not in itself very revealing, putting them together might provide a revealing image of the personality and thus constitute a significant intrusion.

The German Court therefore seems to implicitly recognize a mosaic framework resembling the considerations that led to the formulation of the so-called mosaic theory in the United States. The basic idea of the mosaic theory, particularly in the criminal procedure context, is that the aggregation of numerous individual data points about a person can, in their composite, reveal substantially more about a person than any of the individual pieces of data can on their own. The (potential) application of the mosaic theory to the regulation of police investigatory conduct in the United States has provoked quite a significant response from legal scholars in recent years,[343] including a number of critical responses.[344] The theory has, thus far, been influential in some recent Supreme Court decisions, most notably *United States v. Jones*, in which Justice Sotomayor expressed concern about the implications of

---

[342] *Id.* Rn. 202-203 (official translation).

[343] *E.g.*, David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381, 402-11 (2013); Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1, 12-13 (2012).

[344] *E.g.*, Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 315 (2012) ("[A]s a normative matter, courts should reject the mosaic theory").

police use of GPS tracking technologies: "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[345] Additionally, Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, made a similar argument, namely, that the duration of surveillance (data collection) and amount of data collected would ultimately implicate constitutional privacy concerns, even if the initial search would not on its own.[346]

The mosaic theory has also featured in Dutch law-making, not in the context of police hacking specifically but for digital criminal investigations more in general. A committee advising the Dutch law-maker on the regulation of digital investigations in the new Code of Criminal Procedure (envisioned to enter into force around 2024) proposed a general criterion to measure the intrusiveness of criminal investigation powers. This criterion builds on an existing Dutch standard of so-called "systematicness," which involves the question whether it is reasonably foreseeable in advance that "a more or less complete picture of certain aspects of a person's private life may arise."[347] If so, particular safeguards apply. The committee's advice added a second layer to the standard—triggering still higher safeguards—of "far-reaching systematicness," which is the case if it is reasonably foreseeable in advance that "a far-reaching picture of someone's life can be created."[348] With its emphasis on the image of someone's private life that results from the collection of data, this criterion seems a direct application of the mosaic theory.

To conclude, content-based frameworks to evaluate the intrusiveness of police hacking have been used in Italian doctrine (the framework of informatic privacy) and German case law (an implicit form of the mosaic theory). Although this seems rather minimal, it might be useful to focus on the content of computers—the multitudinous and multifarious data stored and processed in computers—as a proxy for privacy protection; this approach could be a fruitful alternative or complementary normative framework to the container-based approached of protection computers as the new bastion of

---

[345] *Jones*, 400 U.S. at 415-16.

[346] *Id.* at 430 (". . . the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period").

[347] COMMISSIE MODERNISERING OPSPORINGSONDERZOEK IN HET DIGITALE TIJDPERK, REGULERING VAN OPSPORINGSBEVOEGDHEDEN IN EEN DIGITALE OMGEVING 37-38 (s.l., 2018).

[348] *Ibid*. at 39.

privacy. The content-based approach of protecting computers' contents, combined with a mosaic framework, resonates with the mosaic theory that emerges more broadly as a framework to assess the intrusiveness of investigation powers in a digital context, primarily in the context of police location tracking,[349] but also in the Dutch proposal to formulate more broadly a general, mosaic-based, criterion for assessing the intrusiveness of digital investigations.

CONCLUSION

Our analysis has highlighted two different approaches in updating legal frameworks to enable an assessment of the intrusiveness of investigation powers that is sensitive to the specifics of an era in which much if not all private life resides in data and mobile computers.

First, a container-based approach uses computers as the primary proxy of protection, which can be seen as an extension or analogy of the traditional emphasis in legal systems on protecting the home as the key container of private life. Particularly Italian law and doctrine provide valuable insights in how computer protection can be conceptualized as a new form of home protection, in the form of an "informatic home." Also, German law focuses on computer protection, not as an extension of home life but as a new, sui generis object of legal protection. Interestingly, US law with its Fourth Amendment doctrine of containers easily combines traditional homes and mobile computers as protection-worthy containers of private life.

Second, a content-based approach uses data as a proxy of protection, in the form of a general concept of "informatic privacy" (covering all data in digital environments to which individuals have, or should have, some form of control in terms of its accessibility or use) or in the form of the mosaic theory that applies the concept of a mosaic picture constituted by the set of data that the police are collecting.

Both approaches apply proxies: they protect computers or data as such, without specifically requiring that a privacy interest is at issue. The law can hardly avoid using proxies, since legal protection focusing on the underlying interests as such will often be too vague to be workable in practice. Investigation officers need some guidance what they can do to collect data, without having to make abstract normative evaluations all the time. The core challenge for legal systems is to apply proxies that are sufficiently workable in practice (hence, concrete enough for investigation officers to work with) as well as sufficiently fine-tuned to the protected interest (hence, containing sufficient normative thrust as to guide the legal interpretation towards the

---

[349] *See* Koops, Newell & Škorvánek, *supra* note 16 at Part III(B)(3)(b).

intended type and level of protection).

Using computers as a proxy for protection is attractive because it is easy to apply: investigating officers can easily recognize computers or smartphones as protected objects, and hence apply for the required authorization before starting to investigate them. However, the container-based approach is crude because it treats all computing devices alike, whereas the privacy interest can diverge significantly depending on the type of computer and the way it is used. Many laptops, desktops, and cell-phones will contain "the privacies of life,"[350] but some laptops and cell-phones will contain only relatively few or non-privacy-sensitive data (e.g., a cell-phone bought and used only to communicate for some particular drug transactions, or a cell-phone used purely for work purposes). The container-based approach is also limited in guiding the investigation *within* the container: it is useful to determine the conditions for accessing containers, but not to distinguish between levels of intrusion of the investigation of their contents. Here, the content-based approach appears as another approach with roughly mirroring advantages and drawbacks. The content-based approach offers a more nuanced guidance of the investigation of computer data, since it focuses on the types of data and the intrusiveness of the data set that are actually (intended to be) investigated. The downside of the content-based approach is that it is more abstract than the container-based approach, and thus less workable in practice. How is an investigation officer to determine when a "mosaic picture" arises that triggers specific levels of protection? This can be determined by additional proxies, such as the number and type of data, the way they are combined, and the data's impact on someone's private life, but such a list of factors still requires a fairly complex assessment that is difficult to perform for street-level police officers.

Since both approaches have valuable benefits but also drawbacks, we think that both frames emerging from our analysis—inviolability of computers and informatic privacy/mosaic theory—should not be seen as alternatives but as complementary frameworks. A combination of both might work best to offset the drawbacks of each new framework and to capitalize on their combined advantages over traditional frameworks that no longer work well to assess the intrusiveness of police hacking.

Some combination of the two frames can be seen in German and UK law. The German approach is to primarily adopt the container-based protection of computers, but to then qualify this protection by limiting it to computers that process data in such a way that mosaic pictures of individuals' private lives are likely to arise from the investigation of their contents.[351] In the UK, the

---

[350] *Riley*, 134 S.Ct. at 2495.

[351] *See supra* sections IV(B)(1) and (2).

relevant legislation establishes a framework for issuing warrants for equipment interference, but limiting this by a proportionality condition that requires consideration of the nature of the material sought and the proposed means of obtaining it. Interestingly, the combination seems flipped around in Italian doctrine, where scholars emphasize that primarily the contents of computers are protection-worthy, while recognizing that such protection is needed to supplement the dominant spatial approach of protecting traditional and "informatic" homes. In their view, protecting "informatic privacy" is necessary because computers are more than just "informatic homes."[352] "Informatic privacy," however, remains a very general, and therewith abstract, normative frame, which lacks the attractive concreteness of designating certain data-carriers as containers worthy of protection in themselves.

We conclude that the container-based approach and the contents-based approach can best be seen as two sides of a coin. They complement each other in their capacity to serve as a yardstick to assess the intrusiveness of police hacking (and, perhaps, more generally of criminal investigation powers in digital contexts). Choosing one or the other seems unwise: designating computers as protection-worthy in themselves ("my computer is my castle") is attractive but crude; focusing on informatic privacy and/or the mosaic theory makes normative sense but lacks practical foothold. We think that a combination of both is likely to be the most suitable new framework for evaluating the intrusiveness of police hacking. German law goes a long way in this direction, but probably still puts too much emphasis on the container-based approach: the limitation to computers that process many and diverse personal data, and safeguarding the core area of private life, are helpful to fine-tune the protection to what is really protection-worthy. However, the framework lacks guidance to assess the intrusiveness of the investigation once conditions are fulfilled to enter a protected computer and to guide the investigation of the contents. With some supplementary protection derived from the contents-based approach, we think the German framework could serve as a useful model for other countries to apply as normative frame when regulating police hacking.

---

[352] *See supra* section IV(B)(2).