FH | JOANNEUM
University of Applied Sciences

Incidental Data: Detect and Process Personal Information from Social Media Platforms

Master Thesis
submitted in conformity with the requirements for the degree of
Master of Arts in Business (MA)
Master's degree programme **IT-Law & Management**

FH JOANNEUM (University of Applied Sciences), Kapfenberg

supervisor: DI(FH) Michael Brickmann, MA
submitted by: Stefan Kutschera, BSc MSc
personal identifier: 1910472016

May 2021

Formal declaration

I hereby declare that the present master's thesis was composed by myself and that the work contained herein is my own. I also confirm that I have only used the specified resources. All formulations and concepts taken verbatim or in substance from printed or unprinted material or from the Internet have been cited according to the rules of good scientific practice and indicated by footnotes or other exact references to the original source.

I understand that the provision of incorrect information may have legal consequences.

Kapfenberg, Austria, May 2021

Stefan Kutschera, BSc MSc

SIGNATURINFORMATIONEN	**Unterzeichner**	BSc Stefan Kutschera
	Datum/Zeit-UTC	2021-06-07T11:06:42+02:00
	Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 ("eIDAS-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument.	

Abstract

Social media is often only one click away. Now more than ever, it is entangled with our everyday life. To put it another way, what happens if social media does not stop when we leave the site or delete the post we no longer want to share with the world? What if our social media posts are used unintentionally, furthermore, contain incidental data? Thus, data or information we - did not - intend to share with the world but can be found within our social media posts. What if this incidental data can be used to harm our beloved ones or ourselves? Moreover, such data combined with publicly free available governmental databases, such as the company register, can be used to compromise privacy even further. Within this master's thesis it was analyzed how incidental data can be found, what are the legal obligations and the monetary value behind it. Moreover, it was possible to gain interview partners such as the Criminal Intelligence Service Austria or the owner of Techlore, a company that specializes in privacy for the masses. As methodology, Open Source Intelligence Methods were used to gather incidental data. During each case, the time to search for information was limited to 2 hours. Interestingly it was possible to show that incidental data can also be found among web security experts such as Troy Hunt. With the input of such cases, an abstract fictive scenario was created to evaluate the legal implications of gathering incidental data. Further, the monetary value of incidental data using expert interviews was tried to be evaluated. In the end, the results have shown that privacy needs to be more emphasized on a governmental as well as on a private level. For this reason, a change of law is proposed as one of the results of this master's thesis.

Acknowledgement

This is for M & V

01110011 01101101 01110011 01101110 01100010 00100000 01100110 01110000
01110101 01110111 01100111 00100000 01100001 01101000 01111001 01110110
01110000 00100000 01110010 01100011 01110100 01110000 01110111 00100000
01101100 01100100 01101011 01100110 01101101 00100000 01101111 01101010
01100001 01110010 01110101 00100000 01111001 01110101 01110011 01101110
01101100 00100000 01110010 01110001 01101110 01100111 01101110 00100000
01100001 01110010 01101000 01101110 01100110 00100000 01101111 01100100
01110010 01101110 01100111 00100000 01100010 01100111 01100010 01100110
01110001 00100000 01101000 01111001 01100111 01111000 01101011 00100000
01110110 01110000 01110010 01111001 01101110 00100000 01100010 01110001
01111000 01101010 01110100 00100000 01101100 01101001 01110111 01100001
01111010 00100000 01111001 01110100 01101000 01100010 01101110 00100000
01110011 01100111 01100101 01101100 01110101 00100000 01100011 01110001
01111000 01101000 01101110 00100000 01111000 01100010 01100100 01101001
01110010 00100000 01101000 01100110 01111010 01101010 01100011 00100000
01100010 01101001 01110010 01100110 01101111 00100000 01110101 01110101
01110100 01101101 01100001 00100000 01100101 01101001 01100101 01110010
01110100 00100000 01101100 01100100 01111010 01100100 01110111 00100000
01110010 01110001 01100110 01110000 01100011 00100000 01100101 01101000
01101110 01101111 01101110 00100000 01110101 01101101 01100100 01110000
01110000 00100000 01110010 01100111 01110011 01110110 01100110 00100000
01101011 01101001 01101000 01100010 01111000 00100000 01110111 01100110
01110001 01110101 01101111 00100000 01101001 01110101 01110011 01100110
01100111 00100000 01110010 01100100 01110001 01111010 01101011 00100000
01110100 01100110 01101101 01110010 01100100 00100000 01100001 01101111
01100111 01110000 01101111 00100000 01100111 01100100 01110100 01100110
01100100 00100000 01110000 01111001 01111010 01110000 01110110 00100000
01111001 01100111 01110110 01101100 01100111 00100000 01100010 01111010
01101101 01110011 01110110 00100000 01101111 01101110 01100001 01101110
01101110 00100000 01100101 01110010 01111000 01100001 01101010 00100000
01100110 01101110 01100010 01110001 01100001 00100000 01101001 01110100
01100111 01100110 01101110 00100000 01111010 01101111 01100101 01110100
01110110 00100000 01110111 01100011 01110010 01100010 01110110 00100000
01100101 01101110

Contents

List of Figures **ii**

List of Tables **ii**

1 Introduction **1**
1.1 Problem Statement 1
1.2 Research Questions 2
1.3 Hypothesis 2
1.4 Method 3
1.5 Previous Results & Conclusions 3
1.6 Manual Gathering Process 6

2 Related Work **16**
2.1 Incidental Data 16
2.2 Open Source Intelligence - OSINT 16
2.3 Value of Personal Data 26
2.4 Mock-Up Case Austria-Austria 27
2.5 Academic Freedom 32
2.6 Human Rights Convention 33

3 Implementation **36**
3.1 Off-the-Grid 36
3.2 VPN Service Provider 39
3.3 Attack Vectors using Incidental Data 42
3.4 Interviews & Statements 43
3.5 Problems 56

4 Conclusion and Outlook **68**
4.1 Security Measures 68
4.2 Awareness 71
4.3 Conclusion 73
4.4 Outlook 75

A Proposed Change of Law **76**

B Statement **79**

C Request for Comment **86**

D Transcript **88**

E Ethics Self Assessment Test **94**
E.1 Human Embryos 95
E.2 Humans 95
E.3 Human Cells / Tissues 96
E.4 Protection of Personal Data 97
E.5 Animals 98
E.6 Third Countries 99
E.7 Environment & Health and Safety 100
E.8 Dual Use 100
E.9 Misuse 100
E.10 Other Ethical Issues 101

List of Figures

1.1 Left side of surroundings, revealing the shape and colour of the house. (LiveEachDay, 2018) . . . 6
1.2 Right side of surroundings, revealing the shape and colour of the house. (LiveEachDay, 2018) . . . 6
1.3 Screenshot of the video showing a smartphone revealing the GPS location. (LiveEachDay, 2018) . . . 7
1.4 A screenshot from Google Maps showing the city Tulsa, Oklahoma, United States of America. (Google Inc., 2019) . . . 8
1.5 Showing a zoomed and rotated version of the map from the mobile phone visible in the uploaded video. (LiveEachDay, 2018) . . . 8
1.6 Modified overlay of the revealed GPS location with the map of Tulsa, Oklahoma. (Google Inc., 2019) (LiveEachDay, 2018) . . . 8
1.7 Showing the matching object on Google Maps and using the "What's Here" feature. (Google Inc., 2019) . . . 8
1.8 Showing the found address search within other available satellite images on Bing Maps. (Microsoft, 2019) . . . 8
1.9 A screenshot from Google Maps showing the found address within Tulsa, Oklahoma. (Google Inc., 2019) . . . 9
1.10 Showing an overlay of the map from the mobile phone and the map including the hit. (Google Inc., 2019, LiveEachDay, 2018) . . . 9
1.11 Modified and zoomed view of Google Streetview service showing a vage representation of the housenumber. (LiveEachDay, 2018) . . . 10
1.12 Price curve before the owner of the YouTube channel LiveEachDay bought the property. (Trulia Group, 2019) (Zillow, LLC., 2019) . . . 11
1.13 Showing general information of the property from the public register. (Wright, 2015) . . . 12
1.14 Showing tax information of the property from the public register. (Wright, 2015) . . . 12
1.15 Showing document listings on the property from the public register. (Wright, 2015) . . . 12
1.16 Stating the Twitter profile description of Mr.Troy Hunt. (Hunt, 2021) . 13

1.17 A social media post stating, that one should not post pictures of an ongoing vacation as it increases the likelihood of a burglary during the absence. (Polizei Hagen Nordrhein-Westfalen, 2015) 13
1.18 Announcement of an upcoming roadtrip through Australia including the route as Google Maps link as shown in Figure 1.19. (Hunt, 2020c) 14
1.19 Shows the detailed itinerary of the planned road trip through Australia, as shown in Figure 1.18. (Google Maps, 2021b) 14
1.20 A status update of Mr. Troy Hunt of the destination Barmoya, Queensland on his itinerary. (Hunt, 2020a) 15
1.21 Shows the posting of Mr. Troy Hunt announcing his road trip through Southern Territory, AU. (Hunt, 2020b) 15

2.1 Workflow chart showing the methodology on the OSINT process for Email addresses. (Bazzell, 2021) 18
2.2 Workflow chart showing the methodology on the OSINT process for the Location. (Bazzell, 2021) 19
2.3 Workflow chart showing the methodology on the OSINT process for domains. (Bazzell, 2021) 20
2.4 Workflow chart showing the methodology on the OSINT process for real names. (Bazzell, 2021) 21
2.5 A collage with 9 out of 30 pictures from the alleged home of Mr. Troy Hunt. (RP Data Pty Ltd, 2020) 24
2.6 K-Index table exported and redacted from the dedicated relational database PostgreSQL. 25

3.1 A simplification of the Setup used in order to gain anonymity. 37
3.2 Displays the desired network setup including the chosen VPN service provider. 39
3.3 Shows a screenshot of the GIS-Kataster with the deactivated ownership information pop-up window. 55
3.4 Shows the No-Log policy of ProtonVPN. (Proton Technologies AG, 2021) 61
3.5 Shows the Privacy-Policy of ProtonVPN Version: March 11th, 2020. (Proton Technologies AG, 2021), (Internet Archive, 2021) 61
3.6 Statement out of the correspondence with ProtonVPN in regards to my request for comment. 63
3.7 Shows the current IP address which is obtained through the router with an active VPN connection. 64
3.8 Last entries from the export of all logs as of 26th of April 2021. 64
3.9 Authentication logs as mentioned in the statement of ProtonVPN. . . 64
3.10 Authentication logs of a newly created, thus plain account, with several correct and failed logins, that stand in contradiction with the statement of ProtonVPN as can be seen in Figure 3.11. 65
3.11 One response of the correspondence with ProtonVPN stating that logs do not contain a users IP address and that each successful login shall overwrite the previous timestamp. 65

4.1 Images from a social media post that were used and processed to identify a location. (Google Maps, 2021a) (Youtube, 2021) 69
4.2 Matching features from a social media post compared with Google Street View to verify an address. (Google Maps, 2021a) (Youtube, 2021) 70

List of Tables

1.1 This table gives an overview of how the questions from the ethical self-assessment test were answered and how the overall ratio of Yes/No is. As in this case, the ratio is 9/11. 5
1.2 List of property price and operation type. (Trulia Group, 2019), (Zillow, LLC., 2019) 11

2.1 Shows the redacted information collected from various public free available sources. 23
2.2 List and properties of the owned accounts by the plaintiff. 27

3.1 Quick facts on various VPN service providers. 42
3.2 Pricing table of various VPN service providers. Prices in EUR, 1 USD : 0.900495 EUR as for the 29th of May 2020. 42
3.3 Shows all sent requests to a person or organisations with date, contact, response and whether or not the person or organisation was an acquaintance. 59
3.4 Breaks down the response rate of sent requests for acquaintances and non-acquaintances. 60
3.5 Breaks down the response rate of sent requests for non-acquaintances. 60
3.6 Shows which information is stored for a specific ProtonVPN setting. . 66

Chapter 1

Introduction

The master's thesis at hand discusses the detection and processing of information gathered from social media from an interdisciplinary perspective and a technical, economical, and legal perspective. However, the different fields of expertise interact strongly with each other. In order to gain more value of synergies of those expertise fields, they are not separated within this thesis. The following chapter lays out the problem and methodology and states out why it was inevitable to choose this polarizing[1] topic.

1.1 Problem Statement

We live in an era in which most of the earth's population has access to digital devices. A subset of the population with such access is connected to the internet and consumes the available information. Another subset of those users contribute actively to the available data on the internet, in other words: they add data.

It is very simple to contribute, in fact, it is even possible to have semi-professional television shows as a single person[2]. But the simplicity of contributing has its costs in terms of privacy, safety and security. Not everyone who contributes has the time or awareness to do a proper check of what they release. The released material may harm the contributor itself or someone else. For example, the contributor of a video may intend to show how well, big and red their tomatoes are growing. However, they are unaware of the fact that the mountain, the very high building and the shape of the swimming pool that are also visible in the video might reveal their location.

[1] The interviews in Chapter 3.4 show different personal views from experts and/or affected persons.
[2] https://www.kek-online.de/service/pressemitteilungen/meldung/news/ergebnisse-233-sitzung-der-kek/

The information about the location can reveal even more data such as previous owners, cost of recent renovations, property tax, telephone number and date of birth. Criminals may use the combination and quantity of personal information for online asset scouting without the danger of getting caught during the observation on-site or forged phishing attacks either online or via postal service. For example, a burglar could make a guess on the address and collect a floor plan from real estate websites. The burglar can then plan the coup by having information on the hand without ever leaving the comfort of his or her home.

However, as Kutschera, 2021, states, this is not only a problem for single person contributions[3] but even big television companies can make such mistakes as Schmid, 2019, the documentary of an Austrian politician has shown. In contrast, if the personal data has no or very little value to a criminal or criminal organization, the risk of being a target may also be considered as low.

1.2 Research Questions

Within this master's thesis at hand the following research questions will be answered.

1. What is the legal aspect of unveiling personal information found in videos?
2. To which extend is the gathered information valuable to a criminal individual or organization?
3. What are the possibilities to extract incidental data that either identifies or verifies a home address within maximal 2 hours using OSINT methods?
4. What are technical options to blur a trace when exploiting and selling the gathered information?

1.3 Hypothesis

People who upload content to social media platforms are often unaware of uploading incidental data at the same time which could lead to severe damage. Incidental data is valuable for criminals or can harm a person physically or financially.

[3] Single person contribution where the owner of the social media account is also the creator and editor of the pictures and/or videos posted online.

1.4 Method

This master's thesis shows that personal data can be published unintentionally by the person themselves without them being aware of the data that is posted. This unaware posted data, hence incidental data, can be used in further steps to gather more information about a person by using only freely available information or information services. The amount of time to gather information shall not exceed 2 hours either through random search or selected individuals. In order to get a popular view, expert interviews shall be conducted to get an overview of the current situation of incidental data. The interviews should also show if persons were aware that such data exists and if there are certain measures taken to reduce or eliminate them.
Manually gathered incidental data shall be evaluated in terms of the potential economic impact, hence on the direct or indirect monetary effect on a person and/or the usage for criminal purposes. The gathering process shall be reviewed and evaluated from a legal point of view with the usage of a mock-up[4] case. Technical aspects regarding staying anonymous during the gathering process and potential criminal monetization shall be evaluated.

1.5 Previous Results & Conclusions

This master's thesis used research conducted from previous term papers, namely "Projektarbeit 1 - Rechtlich"[5] & "Projektarbeit 2 - Wirtschaftlich"[6]. Whenever research results are used from those previously conducted research they will be correctly referred as follows "Kutschera, 2020" & "Kutschera, 2021". The following is a comprehensive summary of the previous results and conclusions. Moreover, those results shall be discussed in more detail in the upcoming chapters. In any case, correct citations shall be used.

1.5.1 Ethics & Moral

Personal data is valuable not only because a big legal and illegal industry is interested in it but it can also be used to harm people. Therefore, it needs to be emphasized that it is - not - the intention of this master's thesis to harm any people or organizations but to raise awareness without causing any harm. As a result, measures will be taken to minimize the risk that this master's thesis will spread information that could harm a

[4] A case out of pure imagination but within its core concept based on real-world examples.
[5] Translated: "term paper 1 - legal".
[6] Translated: "term paper 2 - economical".

natural or legal person. During the ethics self-assessment test Kutschera, 2021 found out that this master's thesis needs to be written carefully. Furthermore, it turned out that Kutschera, 2020 has uncovered incidental data that is highly dangerous to the currently and future affected persons. In brief, it was decided to completely remove those chapters from this master's thesis. However, the abstract and anonymized idea of those threats will be included in the guideline found in Chapter 4.1. Within the previous research in Kutschera, 2020 and Kutschera, 2021 it was intended to gather incidental data and contact most of the affected persons, provide questionnaires and ask for permission. During the ethical self-assessment test and review of my redacted work, the initial approach has changed. The final analysis had the outcome that it is best to ask for permission before the gathering process even though the gathering process is conducted within 2 hours at maximum and done manually.

1.5.1.1 Ethics Self-Assessment & Moral

To ensure whether or not research on such data can be justified, a look into the ethical aspects of the research in question was necessary. A good approach for such ethical evaluation is the European Granting Program, *Horizon 2020 Program* of the *European Commission Directorate-General for Research & Innovation* as it provides an ethics self-assessment test. The ethics self-assessment test does not provide a binary answer. This is also the reason why the ethics self-assessment test, which is attached to the grant application, has to undergo a review process. However, the how-to documentation for the ethics self-assessment test, on the one hand, lists all questions of the test and, on the other hand, gives suggestions to deal with certain issues and provides further documents and related material (EUROPEAN COMMISSION Directorate-General for Research & Innovation, 2019). Correspondingly, this ethics self-assessment test can be used as a final or a dynamic review process in order to minimize the risk of violation of fundamental ethical guidelines (European Research Council Executive Agency, 2018).

However, there is no grading tool existent to use on this assessment. Furthermore, this assessment will be evaluated individually upon applying for funding. The self-assessment has 20 main questions and 24 side questions. With the exception of the question E.6.4, an answered 'Yes' implies a certain risk. Therefore, counting the Yes/No ratio provides quick feedback on how many ethical critical topics are crossed. However, out of the 20 main questions, 9 had to be answered with 'Yes', 11 were answered with 'No', see Table 1.1. This indicates that the chosen research topic for my master's thesis implies a greater ethical risk in certain areas. In addition, certain measures to protect involved people and the environment have to be made.

Section of Question	1	2	3	4	5	6	7	8	9	10	
Main Questions	3	2	1	2	1	5	3	1	1	1	∑20
Answered YES	0	1	0	2	0	2	2	1	1	0	∑9
Answered NO	3	1	1	0	1	3	1	0	0	1	∑11

Table 1.1: This table gives an overview of how the questions from the ethical self-assessment test were answered and how the overall ratio of Yes/No is. As in this case, the ratio is 9/11.

1.5.2 Lawfullness

During the examination of a fictive case scenario, it turned out that violations of several terms and conditions are done. However, considering the *freedom of science*, it will be without consequences for this research. In contrast, even though the information used for geolocation was posted by the person themself, it would violate Art. 8 ECHR (Right to respect for private and family life) and not withstand a balancing between Art. 10 ECHR (Freedom of expression). Moreover, the Austrian law § 365e Gewerbeordnung 1994 (Trade Code) has a measure to protect the private details of business owners as interested persons must provide a legitimate interest beforehand. However, for small businesses that have the same private address as their business address, this measure fails. For this I propose a change of § 365e Gewerbeordnung 1994 (Trade Code), to implement the following: “If the private address matches the business address, the business owner - must - decide if his or her address is protected by the proof of legitimate interest.” The resulting proposed change of law can be found in Appendix A.

1.5.3 Economical

The economic value for a criminal individual or organization is low, as there is no market for such incidental data (See Chapter 2.3). Nonetheless, there is a chance that such information gathering is provided as a service, thus “Crime as a Service”. However, during the research of this topic, it was made evident that the incidental data might negatively impact the person itself. This negative impact can be repair bills after a burglary or, worse, reputation damage and/or the loss of a job (See Chapter 2.3). (Kutschera, 2021)

1.6 Manual Gathering Process

Within this section, two examples of manual findings will be discussed in order to get an insight into how incidental data can be gathered. Hence, it will be explained how it would be possible to gather personal information from a single posting or multiple postings on social media platforms. This process can be supported with resources from other publicly available databases or social media accounts. Moreover, those examples will help to write a comprehensive guideline to avoid common mistakes within Chapter 4.1.

1.6.1 Youtube Video

A video from the YouTube-Channel “LiveEachDay” with the title “Wild Oklahoma Weather” reveals a scene in which the surroundings of their home can be seen. As a matter of fact, the home that was shown has a very specific shape as it is formed in a U-shape with a U.S. flag in the middle of the backyard. In addition, the title also indicates the state of Oklahoma.

Figure 1.1: Left side of surroundings, revealing the shape and colour of the house. (LiveEachDay, 2018)

Figure 1.2: Right side of surroundings, revealing the shape and colour of the house. (LiveEachDay, 2018)

Nevertheless, it still would not be feasible to search through the whole state of Oklahoma using satellite images. However, within the same video, the smartphone is held directly into the camera, and the person who is recording shows the audience the rain radar of a weather app. The weather app also reveals the GPS location of the recording person as it is a feature of the weather app to show the user his or her current location.

Knowing the more or less exact GPS location and the overall uncommon shape of the house makes it much easier to track the exact location down. Figure 1.4 to Figure 1.6 show how the revealed GPS location reduced the searched area.

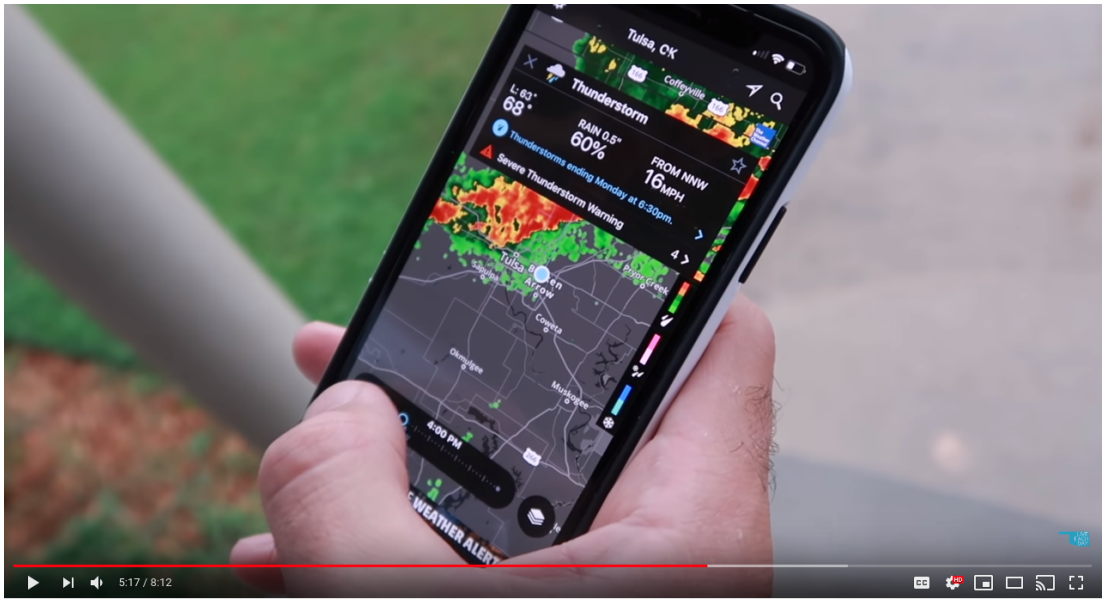


Figure 1.3: Screenshot of the video showing a smartphone revealing the GPS location. (LiveEachDay, 2018)

Figure 1.4 shows a plain map of the city Tulsa in Oklahoma whereas Figure 1.5 shows the map visible from the screenshot of the video, see Figure 1.3, but digitally modified. Digitally modified within this context means that in order to match the orthographical correct map from Google Maps, the screenshot from the video had to be zoomed, rotated and cropped. The overlay of those two maps is visible in Figure 1.6. The process to create such an overlay can be called morphing and feature mapping. Morphing originally means the animated transition of two pictures, whereas feature mapping identifies certain marks within a picture that are within the other picture as well. Due to the fact that streets may have very unique patterns, it is very easy to feature-map and morph pictures from maps. The blue dot visible in the overlay of these two maps is the starting point for a manual search with satellite images from any map provider, see Figure 1.6.

As it turned out, the GPS location is very accurate and searching for the alleged home of the YouTube channel owner took about 10 minutes. During the search process, the so-called service “What’s here”, provided by Google Maps, can help to get the exact address of the property. However, in this case, the “What’s here” functionality of Google Maps does not work. The address can be detected by another service of Google Maps called “Street View”. By reading the house number on the mailbox and the street sign using the service “Street View” by Google Maps, it is possible to make an educated guess on the exact address. However, Kutschera, 2020, was able to locate the address.

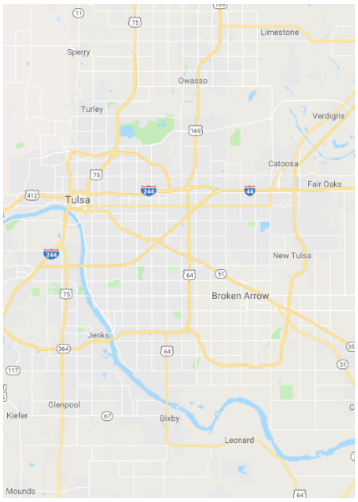


Figure 1.4: A screenshot from Google Maps showing the city Tulsa, Oklahoma, United States of America. (Google Inc., 2019)

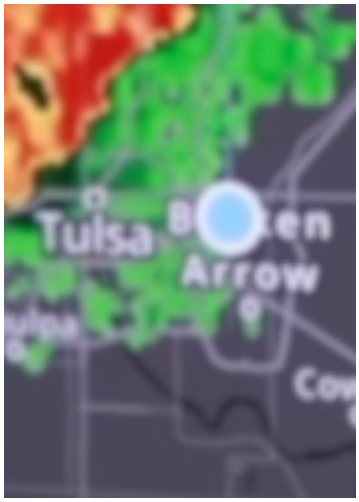


Figure 1.5: Showing a zoomed and rotated version of the map from the mobile phone visible in the uploaded video. (LiveEachDay, 2018)

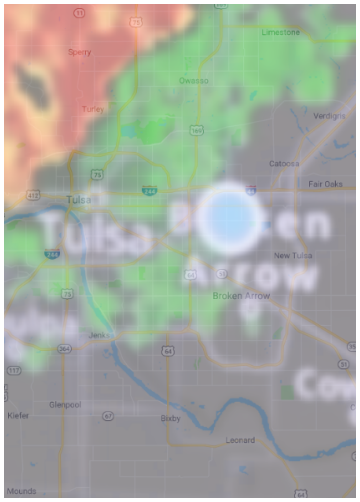


Figure 1.6: Modified overlay of the revealed GPS location with the map of Tulsa, Oklahoma. (Google Inc., 2019) (LiveEachDay, 2018)

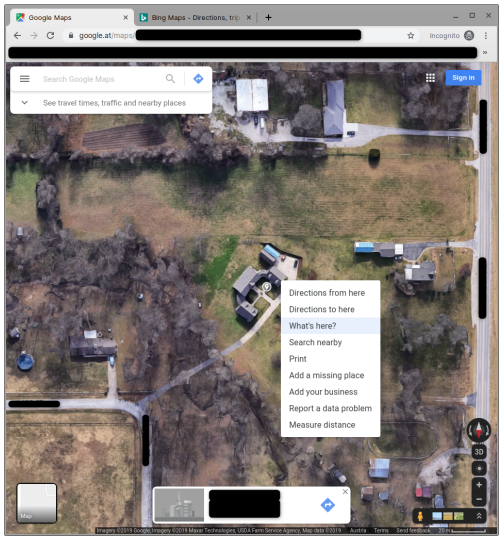


Figure 1.7: Showing the matching object on Google Maps and using the "What's Here" feature. (Google Inc., 2019)

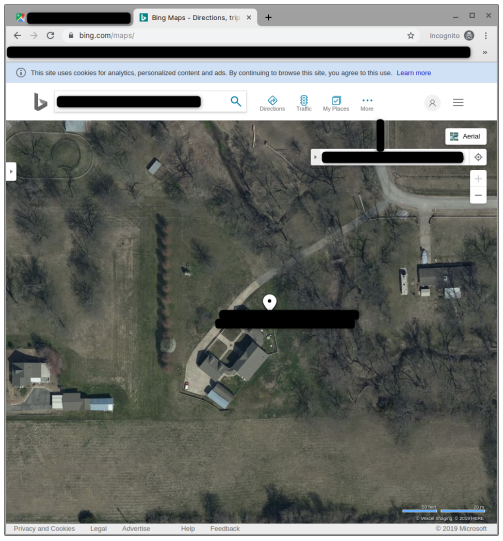


Figure 1.8: Showing the found address search within other available satellite images on Bing Maps. (Microsoft, 2019)

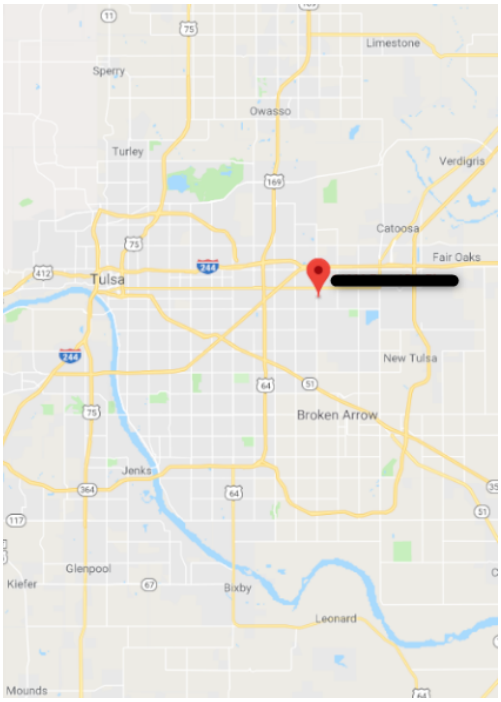


Figure 1.9: A screenshot from Google Maps showing the found address within Tulsa, Oklahoma. (Google Inc., 2019)

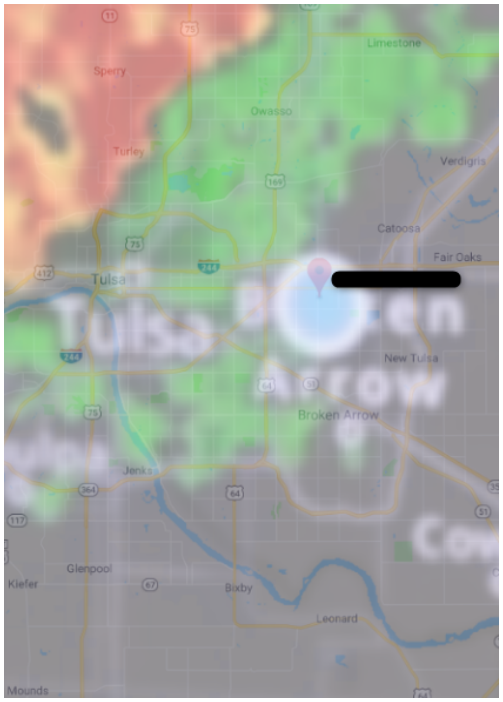


Figure 1.10: Showing an overlay of the map from the mobile phone and the map including the hit. (Google Inc., 2019, LiveEachDay, 2018)

The exact address that was found during the process as stated above was redacted, however, the red marker within Figure 1.9 shows the location on the map. Morphing the found address with the search image shows that the location is even within the blue GPS marker of the mobile map, as can be seen in Figure 1.10.

Nevertheless, with the knowledge of the exact address it is possible to use real estate services such as “Zillow” or “Trulia” to gather information about the current price estimation, history of selling and/or listing prices as well as the broker of the house for the seller and the buyer. Figure 1.12 shows a graph of the price history. The prices can be found on the vertical axis whereas the timeline is situated on the horizontal axis.

Moreover, while looking for the address, an entry on a foreclosure website was found. This entry revealed not only the affected persons by the foreclosure but also revealed the parcel number “9941****290” (ForeclosureFreeSearch.com, 2015). With this parcel number it was possible to access a public register of Tulsa City and get information about the current and previous owners, tax information, home improvements and a list of documents and pictures as can be seen in Figure 1.13 - 1.15.

Figure 1.11: Modified and zoomed view of Google Streetview service showing a vage representation of the housenumber. (LiveEachDay, 2018)

Date	Event	Price
06/23/2017	Sold	$295,000
06/05/2017	Posting Removed	$299,900
05/19/2017	Posting Removed	$299,900
04/26/2017	Posting Removed	$299,900
04/05/2017	Price Change	$299,900
03/16/2017	Price Change	$309,900
02/24/2017	Price Change	$319,900
02/06/2017	Price Change	$324,900
01/13/2017	Price Change	$339,900
01/12/2017	Price Change	$339,900
11/06/2016	Price Change	$349,900
10/10/2016	Price Change	$364,900
09/20/2016	Price Change	$379,900
08/19/2016	Price Change	$384,900
07/19/2016	Price Change	$399,900
06/16/2016	Listed For Sale	$409,900
05/30/2012	Posting Removed	$286,900
03/02/2012	Listed For Sale	$286,900
07/13/2011	Posting Removed	$299,900
09/25/2010	Price Change	$299,900
07/11/2009	Price Change	$369,900
07/10/2008	Listed For Sale	$379,000

Table 1.2: List of property price and operation type. (Trulia Group, 2019), (Zillow, LLC., 2019)

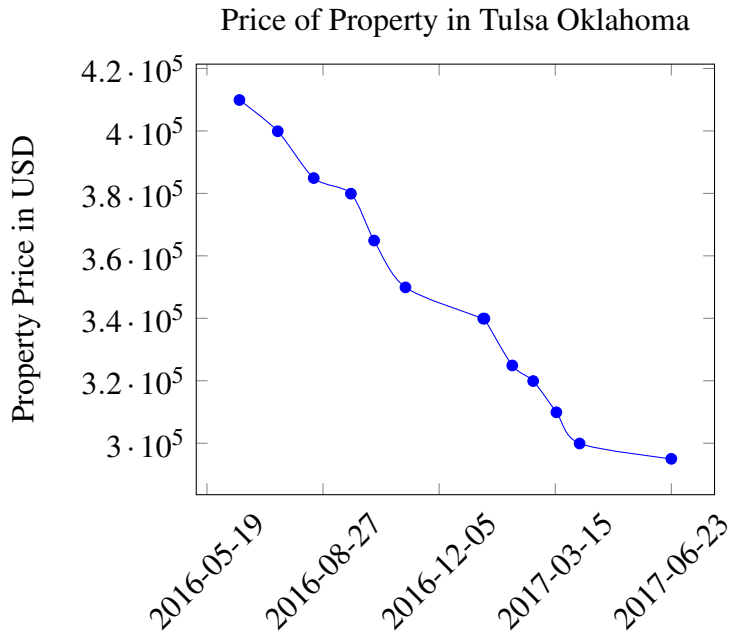


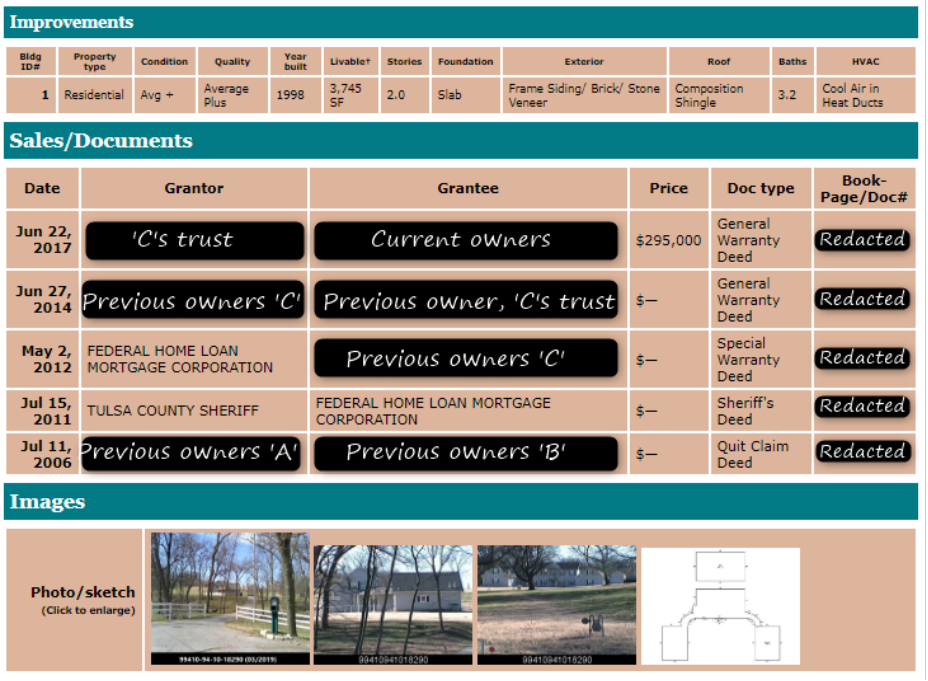
Figure 1.12: Price curve before the owner of the YouTube channel LiveEachDay bought the property. (Trulia Group, 2019) (Zillow, LLC., 2019)

General Information	
Situs address	Redacted
Owner name	Redacted
Owner mailing address	Redacted
Land area†	2.50 acres / 108,900 sq ft
Tax rate	T-1A [TULSA]
Legal description	Subdivision: UNPLATTED Legal: SE NW NW SW SEC 10 19 14 2.50ACS Section: 10 Township: 19 Range: 14
Zoning	RES SINGLE-FAMILY HIGH DENSITY DISTRICT [RS3]

Figure 1.13: Showing general information of the property from the public register. (Wright, 2015)

Tax Information	2017	2018	2019
Fair cash (market) value	$289,900	$295,000	$295,000
Total taxable value (capped)	$289,900	$295,000	$295,000
Assessment ratio	11%	11%	11%
Gross assessed value	$31,889	$32,450	$32,450
Exemptions	$0	$0	$0
Net assessed value	$31,889	$32,450	$32,450
Tax rate	T-1A [TULSA]		
Tax rate mills	137.08	137.34	137.02
Estimated taxes	$4,371	$4,457	$4,446
Most recent NOV	March 6, 2018		

Figure 1.14: Showing tax information of the property from the public register. (Wright, 2015)



Improvements

Bldg ID#	Property type	Condition	Quality	Year built	Livable†	Stories	Foundation	Exterior	Roof	Baths	HVAC
1	Residential	Avg +	Average Plus	1998	3,745 SF	2.0	Slab	Frame Siding/ Brick/ Stone Veneer	Composition Shingle	3.2	Cool Air in Heat Ducts

Sales/Documents

Date	Grantor	Grantee	Price	Doc type	Book-Page/Doc#
Jun 22, 2017	'C's trust	Current owners	$295,000	General Warranty Deed	Redacted
Jun 27, 2014	Previous owners 'C'	Previous owner, 'C's trust	$—	General Warranty Deed	Redacted
May 2, 2012	FEDERAL HOME LOAN MORTGAGE CORPORATION	Previous owners 'C'	$—	Special Warranty Deed	Redacted
Jul 15, 2011	TULSA COUNTY SHERIFF	FEDERAL HOME LOAN MORTGAGE CORPORATION	$—	Sheriff's Deed	Redacted
Jul 11, 2006	Previous owners 'A'	Previous owners 'B'	$—	Quit Claim Deed	Redacted

Images

Photo/sketch (Click to enlarge)

Figure 1.15: Showing document listings on the property from the public register. (Wright, 2015)

1.6.2 Twitter

As shown in Kutschera, 2020, it is possible to gather private information about Mr. Troy Hunt only by using freely public available social media websites. During the process of research, the revisiting of Mr. Troy Hunt's social media was necessary. Surprisingly, Mr. Troy Hunt was teasing an upcoming adventure of his own. He not only announced that he and his family planned a 9.000 km road trip through several states in Australia but also posted a route and updated his Twitter profile with pictures from the current stops, including geotags. (See Figure 1.18 - 1.21)

Figure 1.16: Stating the Twitter profile description of Mr.Troy Hunt. (Hunt, 2021)

It is surprising that Mr. Troy Hunt posts pictures of his ongoing vacation from two points of view. On the one hand Hunt, 2021, states that he is an online security professional and founder of HaveIBeenPwned.com (HIBP) (See Figure 1.16). Thus, a role model for many people. On the other hand, police and crime prevention programs clearly share one conception: Do not post pictures of your belongings at home and certainly do not post pictures of an ongoing vacation, as it indicates that one is not at home, which might be used by criminals to execute a burglary. (Polizei Hessen, PPNH | mkr, 2021), (Polizei Hagen Nordrhein-Westfalen, 2015)

Figure 1.17: A social media post stating, that one should not post pictures of an ongoing vacation as it increases the likelihood of a burglary during the absence. (Polizei Hagen Nordrhein-Westfalen, 2015)

Figure 1.18: Announcement of an upcoming roadtrip through Australia including the route as Google Maps link as shown in Figure 1.19. (Hunt, 2020c)

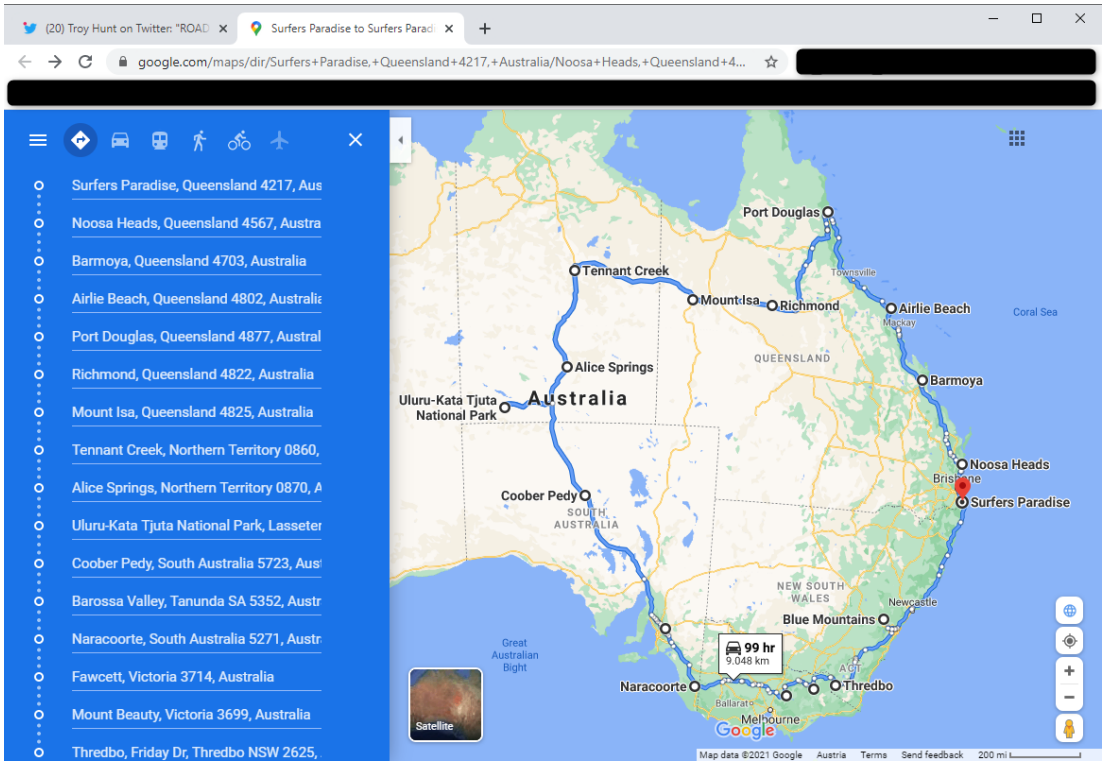


Figure 1.19: Shows the detailed itinerary of the planned road trip through Australia, as shown in Figure 1.18. (Google Maps, 2021b)

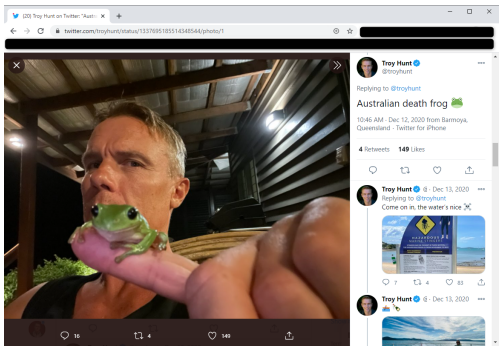


Figure 1.20: A status update of Mr. Troy Hunt of the destination Barmoya, Queensland on his itinerary. (Hunt, 2020a)

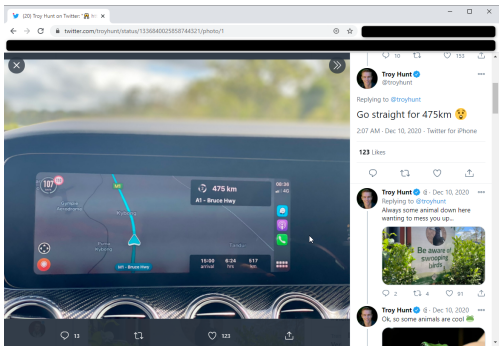


Figure 1.21: Shows the posting of Mr. Troy Hunt announcing his road trip through Southern Territory, AU. (Hunt, 2020b)

Chapter 2

Related Work

2.1 Incidental Data

The term incidental, according to Susan M. Wolf et al., 2008, is used if during an audit or medical examination something non-expected was found, thus *"incidental findings"*. For example, incidental findings in a medical term are when an unexpected mass is detected during a computed tomography (CT) colonography. Hence, a broken rip eventually leads to an x-ray scan where not only the broken bone is visible but also a tumor. This would then be called an incidental finding. Casanovas et al., 2018, use this medical-related term in relation to the area of information security. Hence, it might not be unusual that a wet spot on the wall during an information security audit leads to a closer look behind a server rag, eventually revealing a small fraction of the pipe on the wall. (Susan M Wolf, Paradise, and Caga-anan, 2008, pp. 361–383), (Casanovas et al., 2018). With this in mind, *"incidental data"* is used within this term paper as hidden information, thus an incidental finding behind a social media post[1]. Hence, one intends to film and upload a video of his well-growing tomatoes in his garden but ultimately reveals his residential address and much more.

2.2 Open Source Intelligence - OSINT

Open Source Intelligence (OSINT) describes the production of intelligence from publicly available information through collection or exploitation to distribute to an appropriate audience in order to address specific intelligence requirements. For example, for the Central Intelligence Agency (CIA) this could be broadcast news of a foreign

[1] See Sections 1.6.1, 1.6.2 and 2.2.2 for concrete examples.

country. For an attorney or civil engineer it could mean official government documents which are available to the public. However, OSINT is also about creating reports of the collected information, especially because such information might become unavailable for several reasons. Such a reason could be that a dedicated service stopped his operations or might be automatically deleted after a certain amount of time online. (Bazzell, 2021)

According to Bazzell, 2021, an OSINT investigation follows no repeating recipe but more a selected path out of many options. However, from an abstract point of view, it can be said that some steps have to be fulfilled for every OSINT investigation. Firstly, there is the *Triage* where the expectations and a clear overview for the upcoming mission are defined. Secondly, the *Preparation of Tools* deals with the necessary and needed tools to answer the defined questions from the previous step *Triage*. Thirdly, if applicable, *Closed Source Data Queries* are queried. Such databases can be governmentally provided or require payment in order to access their data. Fourthly, *OSINT: Query All Known Identifiers* is, combined with step five, *Collection*, the heart of every investigation as all necessary and available databases, -sources and techniques are executed. Examples for such data sources can be search engines with the usage of so-called “Google Dorks”, e.g. *site:4chan.org "username"*, searches through real estate websites, social media profiles, (historical-) domain registration databases, archived websites. This step *OSINT: Query All Known Identifiers* generates leads that serve as input for the fifth step, the *Collection*, or as new evidence that can be used for the fourth step *OSINT: Query All Known Identifiers*. In step five, *Collection*, all generated leads are used in order to collect OSINT evidence through dedicated services such as Hunchly[2], scripts or manual queries. Step six, *Analysis*, helps drawing the “bigger picture” as one tries to combine all gathered evidence into a narrative respectively overview of the investigated subject. In the seventh step, all gathered evidence, generated overviews and supportive graphics are used to create a final report used for the specified manner from step one. Last but not least, the notes and the virtual machine are archived. The virtual machine is either reverted to a clean snapshot or newly created in order to have a fresh and unbiased starting point for upcoming investigations. (Bazzell, 2021)

Given the general procedure as described above, the more detailed workflow for specific information can be viewed within Figure 2.1 - Figure 2.4.

[2] https://www.hunch.ly/

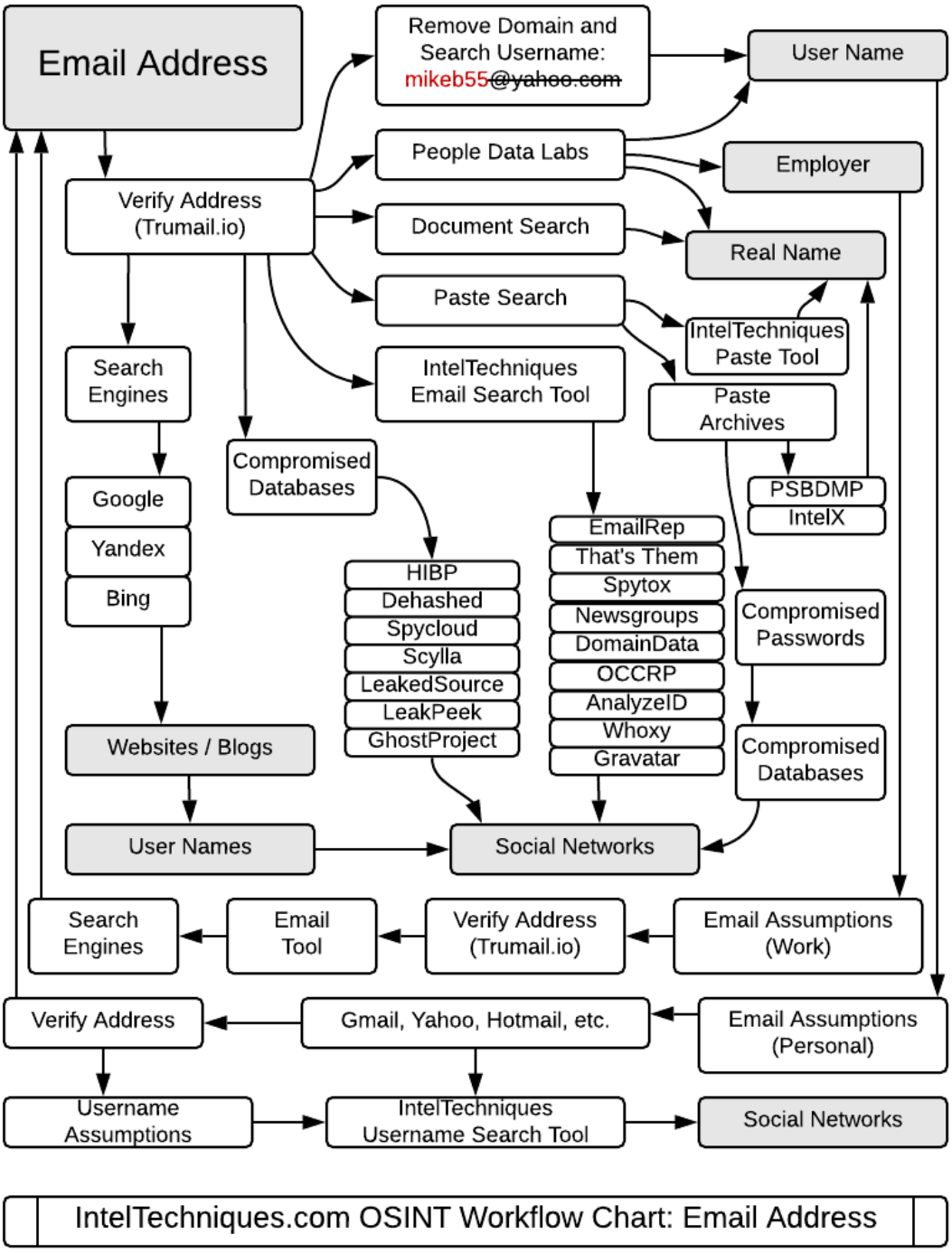


Figure 2.1: Workflow chart showing the methodology on the OSINT process for Email addresses. (Bazzell, 2021)

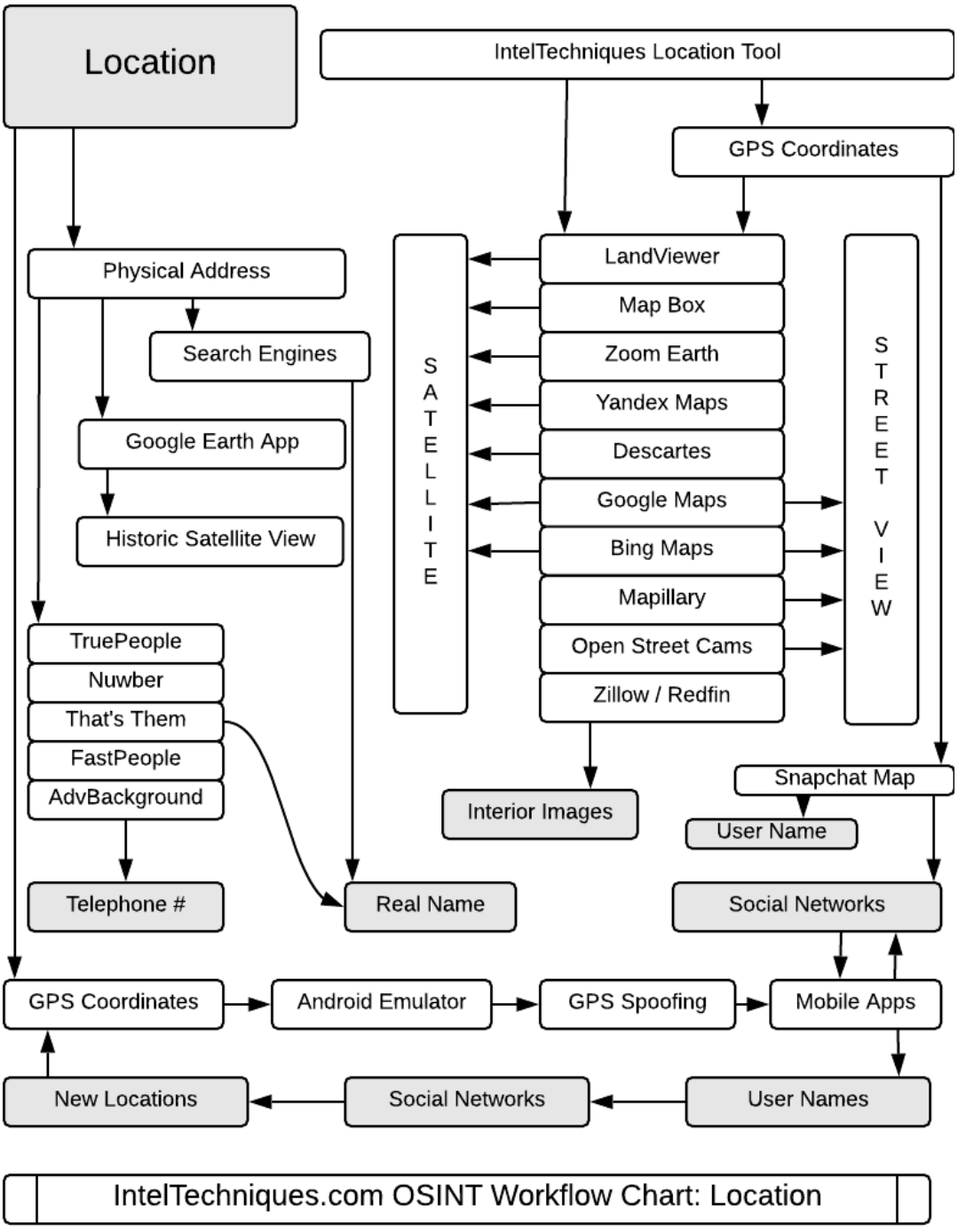


Figure 2.2: Workflow chart showing the methodology on the OSINT process for the Location. (Bazzell, 2021)

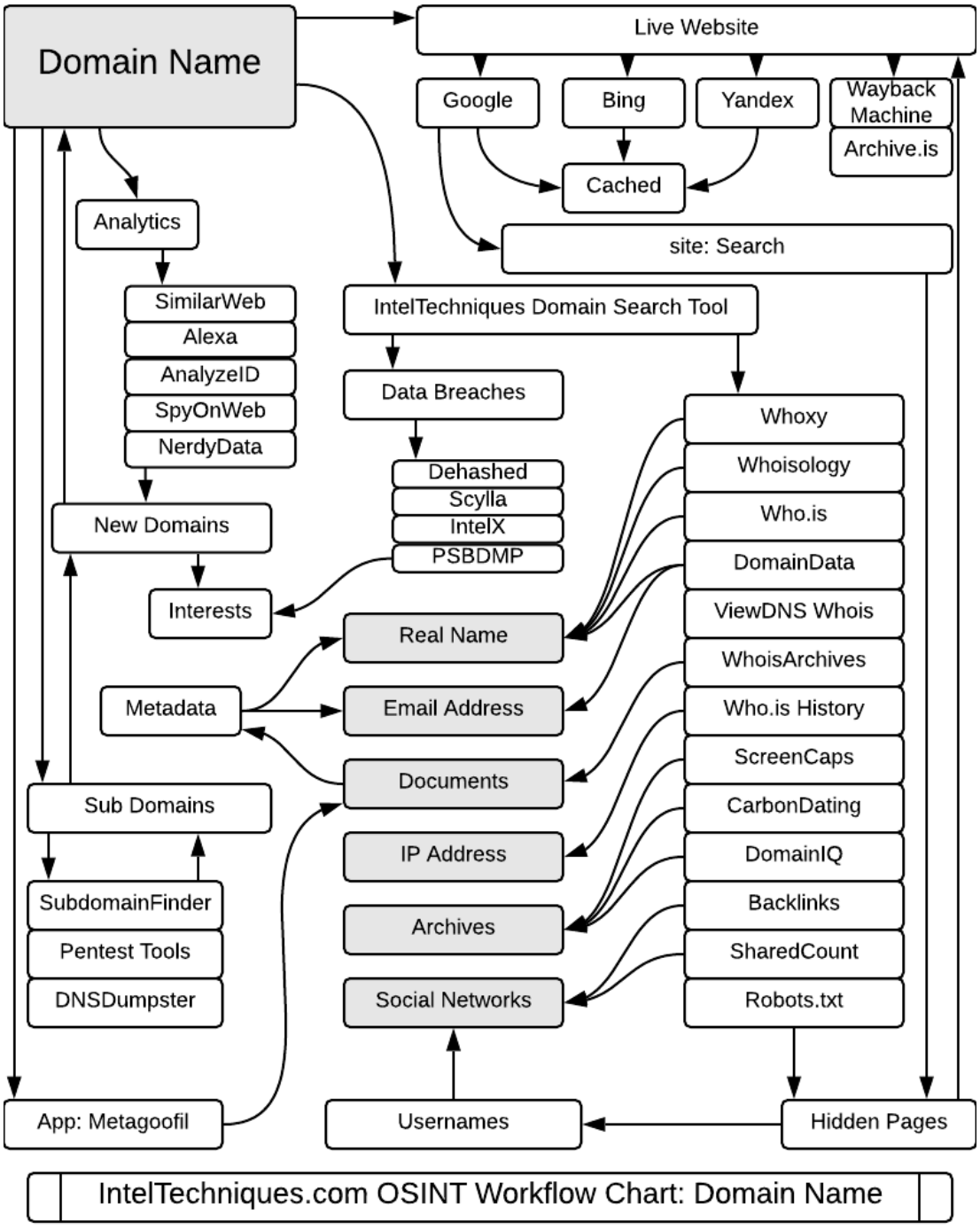


Figure 2.3: Workflow chart showing the methodology on the OSINT process for domains. (Bazzell, 2021)

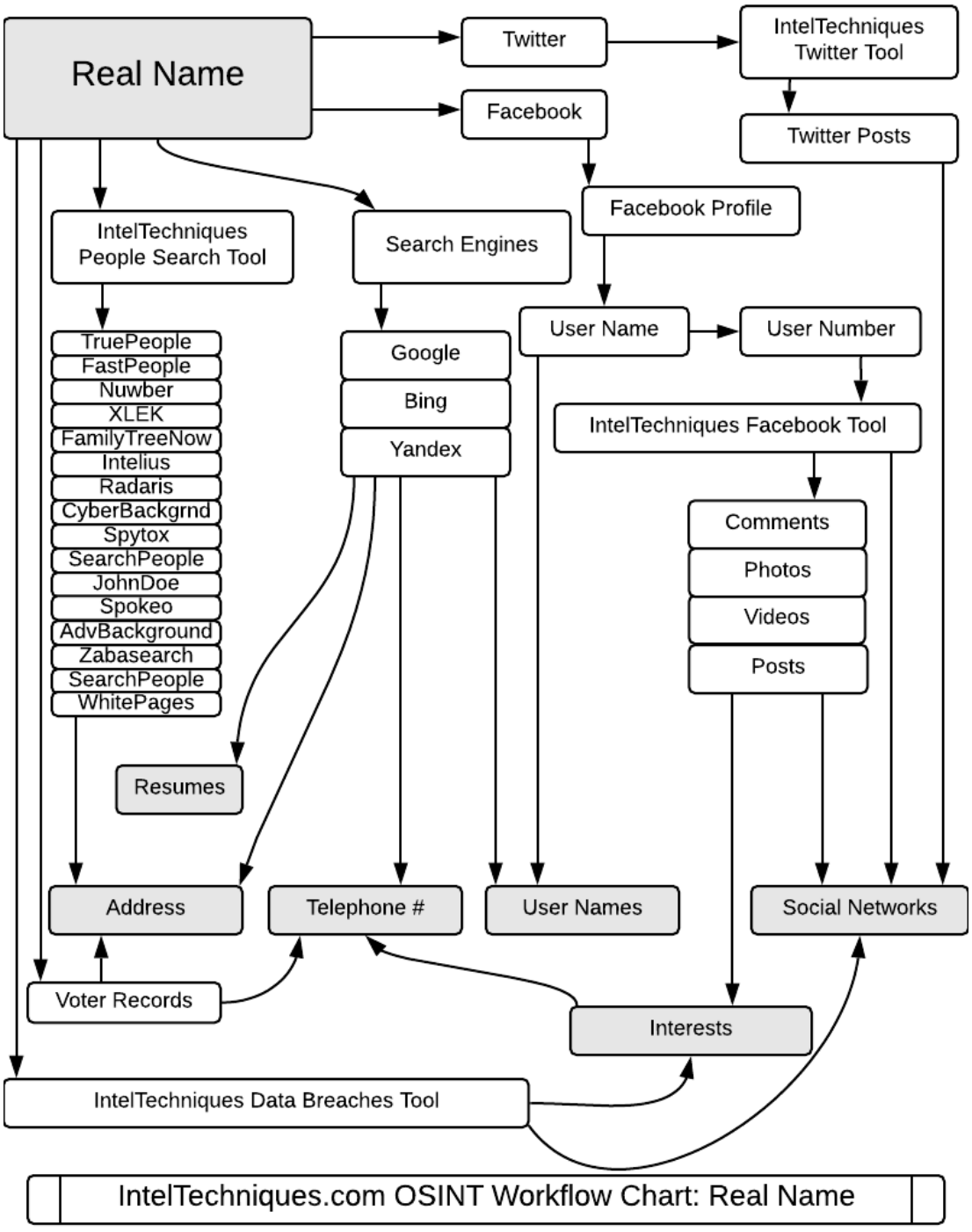


Figure 2.4: Workflow chart showing the methodology on the OSINT process for real names. (Bazzell, 2021)

2.2.1 Origin of Data

The collection starts with incidental data posted on social media platforms such as “Twitter”, “YouTube”, “Vimeo”, “9Gag” and “Instagram”. To give an example, one can post a picture showing their backyard, enjoying their evening and having a good time. Besides giving the audience a great-looking picture of the own backyard, the vicinity might also be visible. This describes two types of data that can be found within posted online data. First is “Primary Data” which is the main reason the data was posted (e.g. having a good time in the evening showing his or her backyard). Secondly, ”Incidental Data” describes data found beside the primary data and is not strictly needed for the primary data. Incidental data can be the size of the backyard, the shape of the swimming pool, a license plate, the sun’s position, surrounding hills, mountains or skyscrapers, or the neighbours house showing a street name or number.

This master’s thesis will use those incidental data and combine them with other services such as “Google Maps”, “Bing Maps”, “Google Street View”, “Zillow”, “Trulia”, “Spokeo”, “True People Search”, Assessor Geo-Information System (GIS) data, and of course, several search engines.

Considering the described collection process above, the following table shows the metadata that might be found of each person.

Overview	
Public channel	The name, or a reference to a social media platform
Full name	The full name of the person connected to the data below
Birthday	Date of birth, full or partial
Address	The main living address of the individual. Several entries are possible e.g. side residential
Relatives	Names and relation to found members of family
Additional Data	All found data that is non-sensitive and not covered above e.g. property tax, marriage information, etc.
Additional Sensitive Data	Same as ’additional data’ but sensitive, e.g. credit card number, social security number, health reports, etc.

2.2.2 Example Data

All data from the manual gathering process, as shown within Table 2.1 and Figure 2.5 is collected within a database from which a rudimentary connector processes it into LaTeXsource files[3]. The following shows an example of the incidental data found for Mr. Troy Hunt. Mr. Troy Hunt is an Australian web security consultant known for public education and outreach on security topics. Further, he is the creator of "Have I Been Pwned". It can be said that he is a trustworthy and recognized member of society within the security scene. Therefore, it shall be assumed that he is aware of what he is posting and what this might imply or reveal about his private life. With this in mind, the as of today unanswered email sent on 5th of April 2020, might imply that the findings of this research were not important to him, or he was already aware of them. Cultural differences could also be a reason for this[4].

Overview	
Public channel	Troy Hunt
Full name	Troy Hunt
Birthday	—
Address	5* A**** D****, 4217, Surfers Paradise, Queensland, AUSTRALIA
Relative	K**** Hunt , Spouse
Additional Information	Property Lot **** on RP****, 721 sqm
Additional Information	Property bought on 23rd March 2018 for **** AUD
Additional Information	Phone (Troy Hunt): +61****76
Additional Information	Phone (K**** Hunt): +61****88

Table 2.1: Shows the redacted information collected from various public free available sources.

[3] LaTeXis a document preparation framework in which plaintext files or so-called source code ".tex"-files are then processed to formatted documents. This master's thesis work is also written with LaTeX.

[4] For instance, during a trip around Tromsø, Norway, I observed that a vast majority of houses did not cover their windows with curtains, not even at night. According to a local guide, people want to let in every bit of light due to the natural phenomena called polar night. Hence, letting in light, even the dim moonlight reflection of the snowy landscape, is worth more than the danger of being visible for cars driving by or an actual Peeping Tom.

Figure 2.5: A collage with 9 out of 30 pictures from the alleged home of Mr. Troy Hunt. (RP Data Pty Ltd, 2020)

2.2.3 K-Index Table

A table with weighted parameters will be created to take several findings and the range of potential exposure into account. As there is no such index available at the time of writing, a formula was created and named *"K-Index"*. Also, the table in Figure 2.6, shows a relative K-Index that is bound to the broadcast range of the social media channel or person themself.

id	Channel Name	Name	Addresses	Birthdate	Relatives	Add. Infos	Sensitive Infos	Broadcast Range in Mio	K-Index	Rel. K-Index
6	[redacted]	0	1	0	1	2	0	3.36	1.00	0.03
1		0	1	0	3	2	1	109.17	7.00	7.64
3		1	1	1	0	1	0	129.77	8.00	10.38
5		1	0	1	0	0	0	100.00	7.00	7.00
4		1	1	1	0	0	0	100.00	8.00	8.00
2		0	2	0	0	0	0	278.36	1.00	2.78

Figure 2.6: K-Index table exported and redacted from the dedicated relational database PostgreSQL.

As for the calculation of the K-Index, several parameters are multiplied by a factor that should weigh the severity as shown in Equation 2.1. Furthermore, the first address should be weighted with 1, for every additional address the value should not exceed the value 2. This sounds quite simple “If addresses is less or equal than 1 then the respective value else 2”. However, the database does not provide such simple if-statements. The solution to this problem is a mathematical function called limit-function, as the solution will not exceed a certain value, see “k.addresses” in Equation 2.1. The function seems quite complicated but given the circumstances, it solved the issue and can be used in the master’s thesis to fine-tune the K-Index table[5].

$$\begin{aligned} k.name &= name * 3 \\ k.birthdate &= birthdate * 4 \\ k.relatives &= \frac{relatives}{2} \\ k.add.info &= add.info * 0 \\ k.sensitive.info &= sensitive.info * 5 \\ k.addresses &\equiv \frac{2 * 1}{1 + e^{-20*(addresses)}} - 1 \pmod 2 \end{aligned} \tag{2.1}$$

$$KIndex = k.name + k.birthdate + k.relatives + k.add.info + k.sensitive.info + k.addresses \tag{2.2}$$

[5] Formular on WolframAlpha https://www.wolframalpha.com/input/?i=Plot%5B2*1%2F%281%2Be%5E%28-20*x-1%29%29%5D+x+from+0+to+20

2.3 Value of Personal Data

It is crucial to raise awareness of incidental data posted on social media platforms as this data may be of worth to others. This ultimately gives an incentive for others to use such data for their own advantage. As Bazzell, 2021, discusses, this might be a lawful entrepreneur who uses the data, but it could also be criminals who are planning their next coup either digitally, or worse, physically. Ablon, 2018, stated the motivation of cybercriminals is to gain a financial benefit by exploiting personal, financial or health data. (Ablon, 2018; Bazzell, 2021)

In addition, the own person can be mistaken for a very similar looking criminal who was hunted by some part of the public as this happened to *David Quintavalle*, which was later proven innocent by the Federal Bureau of Investigation (FBI). (Bazzel, 2021, 15:19min) This section discusses the worth that might be attached to personal incidental data that is manually extracted from several social media postings. As in a discussion on 9th of April 2021 with the Head of the Unit of OSINT & Crime Trends within the Criminal Intelligence Service Austria[6], Heimo Flechl, BA MA, the gathered incidental data is not worth much when sold on the dark web. However, this may change for information on a contractual basis, thus when information about a specific person is requested. Depending on the intentions of the criminal behind the requested data, the information can be worth less than one hundred EUR to several thousand EUR. Such service is called “Crime as a Service”.

However, things change when the focus lies on the damage caused by incidental data. Such data, either used by script kiddies, professional criminals, enemies or governmental agencies, can have a serious impact on one’s life. Depending on the action that follows after the gathering of incidental data, the damage can vary from repair costs after a forceful entry, loss of reputation to the loss of a job.

As an example, a look at Mr. Troy Hunt might help. According to his biography, he is aware of, among many other things, “Online-Security”. With the creation of HaveIBeenPwned.com humanity has a brilliant service that helps the general public. In terms of his private online security, Mr. Troy Hunt may not be the best example as he did not only announce a future road trip of 9.000 km through several states in Australia, providing a detailed itinerary that pinpoints each desired location but also sends on-time updates at the destinations (See Chapter 1.6.2). With such information and the knowledge of the owner’s absence, criminals may try to forcefully enter the building and cause on-site damage that needs to be repaired. Nonetheless, when crim-

[6] German “Leiter des Referats für Open Source Intelligence und Kriminalitätstrends im Bundeskriminalamt”.

inals want to make profit, Weber and Kruisbergen, 2019 showed that cash is still king and preferred over methods such as the use of Cryptocurrencies like Bitcoin or prepaid cards.

2.4 Mock-Up Case Austria-Austria

Considering the gathering and extraction of incidental data from social media platforms, as shown in Chapter 1.6, 2.2.1 and 2.2.2, a fictional build-up case, thus a mock-up, is described within this section.

2.4.1 Facts

The defendant is an Austrian citizen who found and processed incidental data of the plaintiff who also is an Austrian citizen who posted content on social media platforms. The plaintiff has several social media accounts as described in Table 2.2.

Social media platform	Public account name	Media reach	Content
Youtube	MU Account YT	950.000	450 videos
Twitter	MU Account TW	60.000	1.800 tweets
Facebook	MU Account FB	60.000	unknown
Reddit	MU Account RD	unknown	1.000 comments

Table 2.2: List and properties of the owned accounts by the plaintiff.

All social media accounts of the plaintiff that are listed in Table 2.2 are freely accessible without the necessity of owning an account aforementioned platforms. The plaintiff started to upload content as a hobby in 2008. After four years, in 2012, the income of his activities on social media platforms reached a certain threshold that made it indispensable to list it in his tax returns. Eventually, two years later a legal entity was founded. One of the uploaded videos on YouTube called “My beautiful tomatoes are growing so well” has a duration of 15:20 minutes and has 2.584.128 views. The video uploaded in January 2019 shows the plaintiff’s tomatoes in his garden. Also, two sides of the facade of his house are visible, as well as a five-floor building and mountains in the vicinity. However, the plaintiff had, according to a news article, issues with stalkers in the past and ultimately decided to remove his real name from any social media account. Also, the news article only lists his given name.

The defendant has accessed the uploaded video called “My beautiful tomatoes are growing so well” on YouTube in April 2020 and made three screenshots at

1:25, 5:55 and 13:12 min. After not being able to geolocate the position on a first attempt, the defendant got a full name from the autocompletion after typing the channel's name in the Google search engine. With this name the defendant was then able to acquire a business license from the "Gewerbeinformationsystems Austria (GISA)". Within the business license, the full name and date of birth of the entrepreneur are listed as well as the address of the business. The defendant looked the acquired business address up in an online map service called Google Maps. With the taken screenshots showing the garden and the satellite images of the map service, the defendant was certain that he found the main residence of the plaintiff. To get even more clarification, the defendant used the "Geo Informations System Kataster Steiermark (GIS Kataster)" to get old and limited extracts from the land register of the supposed address. The information of the partial extract from the land register listed the same name of the property owner with the same address as looked up. The defendant ultimately assumed that he found the real full name, date of birth, and an owned property of the plaintiff with this information.

2.4.2 Legal Obligations

2.4.2.1 YouTube

The plaintiff posted the content on the social media platform YouTube out of his free will within the limitations of the applicable Terms and Conditions. The Terms and Conditions of YouTube state that YouTube is a hosting provider and the person who uploads content is also responsible for the content. The user of the service provided by the hosting provider YouTube is allowed to view and hear the content but also has limitations. The user is, according to YouTube Inc., 2019, not allowed to access, reproduce, download, distribute, transmit, display, sell, license, modify, adapt, or otherwise use any portion of the service or content except in the manner permitted by the service. The related paragraphs are marked in bold within the quoted Terms and Conditions below. Note that the legal binding version of 22nd of July 2019 is written in German and cited without translation but commented in English.

> *"**Ihre Nutzung des Dienstes***
> ***Inhalte im Dienst***
> *Die Inhalte im Dienst umfassen Video, Audio (z. B. Musik und andere Tonaufnahmen), Grafiken, Fotos, Text (z. B. Kommentare und Skripte), Kennzeichen (einschließlich geschäftlicher Bezeichnungen, Marken oder Logos), interaktive Funktionen, Software, Messwerte und andere Materialien (zusammen "Inhalte"). Nutzer können Inhalte im Rahmen des Di-*

> *enstes einstellen und zugänglich machen. YouTube ist für diese Inhalte ein Anbieter von Hosting-Diensten.* ***Die Inhalte unterliegen der Verantwortung der Person oder Rechtspersönlichkeit, die diese im Rahmen des Dienstes einstellt und zugänglich macht.***
>
> . . .
>
> ***Berechtigungen und Einschränkungen***
>
> *Unter Einhaltung dieser Vereinbarung und der geltenden Gesetze können Sie auf den Dienst in der Ihnen zur Verfügung gestellten Form zugreifen und ihn verwenden.* ***Sie können Inhalte für Ihren persönlichen, nicht kommerziellen Gebrauch ansehen oder anhören.*** *Außerdem können Sie YouTube-Videos über den integrierbaren YouTube-Player zeigen.*
>
> *Die Nutzung des Dienstes unterliegt jedoch bestimmten Einschränkungen.*
>
> ***Folgendes ist nicht zulässig:***
>
> ***Auf jegliche Teile des Dienstes oder der Inhalte zuzugreifen sowie diese zu vervielfältigen, herunterzuladen, zu verbreiten, zu übersenden, zu übertragen, anzuzeigen, zu verkaufen, zu lizenzieren, zu ändern, anzupassen oder anderweitig zu verwenden, ausgenommen (a) in der Art und Weise, wie sie im Dienst genehmigt wurde****; oder (b) nach vorheriger Genehmigung durch YouTube in Textform und, sofern relevant, durch die jeweiligen Rechteinhaber oder (c) soweit durch anwendbares Recht gestattet."* (YouTube Inc., 2019)

Consequently, the defendant was allowed to view[7] the content. The defendant violated the Terms and Conditions of YouTube by making screenshots and therefore reproducing parts of the provided content.

2.4.2.2 Google Search Engine

The autocompletion of the Google search engine revealed the name of the plaintiff for the defendant. Only getting his name through the autocompletion doesn't violate the Terms of Service of Google search engine per se. However, if the defendant would use the search results to violate applicable law, for instance, stalking or harass the plaintiff, a violation of the Terms of Service would be inevitable.

> *"Respect others*
>
> *Many of our services allow you to interact with others. We want to maintain a respectful environment for everyone, which means you must follow*

[7] I'm not sure if I can view something without accessing and display the content? For me it seems like no one is ever allowed to use YouTube?

these basic rules of conduct:
•comply with applicable laws, including export control, sanctions, and human trafficking laws
•respect the rights of others, including privacy and intellectual property rights
•don't abuse or harm others or yourself (or threaten or encourage such abuse or harm) — for example, by misleading, defrauding, defaming, bullying, harassing, or stalking others
•don't abuse, harm, interfere with, or disrupt the services"
(YouTube Inc., 2020)

2.4.2.3 Gewerbeinformationssystem Austria (GISA)

With the gathered name of the plaintiff, the defendant used the service "Gewerbeinformationssystem Austria" (GISA) to look up any now or historical existing businesses registered to the name of the plaintiff. The lookup of the GISA register of Bundesministerium für Digitalisierung und Wirtschaftsstandort and Kooperationsgemeinschaft Bund/Länder/Städte, 2020, is covered by Austrian law § 365e Gewerbeordnung 1994 (Trade Code) ('GewO 1994'), BGBl I 45/2018. Nevertheless, Bundesministerium für Digitalisierung und Wirtschaftsstandort, 2020, states that inquiries to extract information such as place of birth, nationality, main residence or social security number, must provide a legitimate interest in order to be answered. However, many small business owners have their main residence as their business address. Therefore, for a certain amount of small business owners, the main residence is provided by GISA without proof of legitimate interest.

2.4.2.4 Geo Informations System (GIS) Kataster

The outdated but still valuable information of GIS-Kataster have helped the defendant to confirm further that the plaintiff, firstly, owns the property at the alleged address, secondly, that his main residence matches with the business address and the alleged address found within incidental data.

2.4.2.5 GDPR & DSG

As the plaintiff is a citizen of Austria, the General Data Protection Regulation (GDPR) is applicable. This is covered by Art. 3 in Regulation EU 2016/679 General Data Protection Regulation (GDPR) of The European Parliament and the Council of the European Union, 2016. Art. 3 of Regulation EU 2016/679 GDPR states that the territorial

scope of the regulation applies to any processor or controller who is processing personal data, regardless of whether the location of his operation is within the Union or not. Art. 4 of Regulation EU 2016/679 GDPR describes definitions used within the regulation itself. Among the regulated data is *personal data* and *processing*. Personal data describes any information relating to an identified or identifiable natural person. Processing is described as any operation performed on personal data whether or not the operation is done automatically or manually or as a single- or within a set of operations. Such processing operations are defined by Art. 4 Sec. 2 of Regulation EU 2016/679 GDPR, as the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data. Interestingly, a controller is a natural or legal person, public authority, agency, or other body that processes personal data alone or jointly with others.

Furthermore, Art. 15 Sec. 1 Regulation EU 2016/679 GDPR states that the controller has to confirm whether he or she is in possession of personal data concerning the data subject. However, if personal data exists, the controller must give access to the information (The European Parliament and the Council of the European Union, 2016).

In contrast, the material scope in Art. 2 Sec. 2 Lit. c Regulation EU 2016/679 GDPR defines inter alia one exception where the regulation does not apply as *"a natural person in the course of a purely personal or household activity"*. The jurisdiction shows that household activity has a restricted meaning. CJEU C-212/13[8]is a preliminary ruling based on Directive 95/46/EC, thus the predecessor of Regulation EU 2016/679 GDPR. However, current jurisdiction still refers to rulings based on Directive 95/46/EC when it comes to interpreting the exact meaning of Regulation EU 2016/679 GDPR. As a matter of fact, the ruling of Oberster Gerichtshof (Austria) OGH 6 Ob 150/19f, based on regulation EU 2016/679 GDPR also refers in section 5 of the reasoning inter alia the decision CJEU C-212/13where the principle of household activity cannot be claimed if the gathered personal data is also used in order to protect property. In conclusion, there are two facts to point out. Firstly, EuGH decisions and rulings based on the Directive 95/46/EC can still be used to help interpret the successor Regulation EU 2016/679 GDPR. Secondly, natural persons are not excluded from Regulation EU 2016/679 GDPR when their processing of personal data is not based on purely private and household activity, even when the processed data is used to protect their own property.

[8] https://curia.europa.eu/juris/documents.jsf?num=C-212/13

With this in mind, the defendant as a natural person is also the controller, and he or she has to comply with the Regulation EU 2016/679 GDPR to protect personal data and grant certain rights to the data subject.

2.5 Academic Freedom

In many countries of the world so-called academic freedom right exists. For Austria the principle of academic freedom is situated in the Basic Law of 21st December 1867 rights of citizens for the kingdoms and countries represented in the Imperial Council[9], see Art 17 Staatsgrundgesetz 1867 (Basic Law) ('StGG 1867'), RGBl 142/1867.

> *"Art. 17. [1] Knowledge and its teaching are free.*
> *[2] Every national who has furnished in legally acceptable manner proof of his qualification has the right to found establishments for instruction and education.*
> *[4] The Church or religious society concerned shall see to religious instruction in schools.*
> *[5] The right to supreme direction and supervision over the whole instructional and educational system lies with the state.*
> *Art. 17a. Artistic creativity as well as the dissemination of art and its teaching shall be free."*
> (Staatsgrundgesetz 1867 (Basic Law) ('StGG 1867'), RGBl 142/1867)[10]

Whereas the Art. 17 StGG itself reads vague, the decisions and rulings based on it are precise. The ruling of OGH 9Os 49/80 had to decide whether the author of his publication was guilty of the defamatory statement § 111 Abs. 2 Strafgesetzbuch (Criminal Code) ('StGB 1974') and ultimately if the search warrant was lawful or not. However, the reasoning of the decision stated that the publication was written within an academic context and the defendant was executing his rights as of Art. 17 StGG and therefore cannot be held guilty of the accusation.

> *"Auch die Mitarbeiter an der gegenständlichen Publikation seien fast ausschließlich Historiker und als Universitätsprofessoren, Universitätsdozenten und Universitätsassistenten tätig. Nach Art. 17 des Staatsgrundgesetzes vom 21. Dezember 1867 über die allgemeinen Rechte der Staatsbürger sei die Wissenschaft und ihre Lehre frei und eine gerichtliche Verfolgung*

[9] Original text in German: "Rechte der Staatsbürger für die im Reichsrathe vertretenen Königreiche und Länder".
[10] Translated document from Austrian Law Information System (RIS) https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1867_142/ERV_1867_142.pdf

> *wegen der Veröffentlichung von wissenschaftlichen Forschungsergebnissen nicht zulässig. Da es sich bei dem in Rede stehenden Druckwerk um eine wissenschaftliche Arbeit handle, habe der Beschuldigte nur ein Recht ausgeübt (§ 114 Abs. 1 StGB.).“* (OGH 9Os49/80)

Another ruling of OGH 6Ob 182/15f followed the decision and further built upon it. The reasoning of OGH 6Ob 182/15f, Sec 3.2 concludes that it was undisputed that the constitutionally guaranteed freedom of science (research) and its teaching - as long as it was within the framework of human rights - justify interference with the rights of third parties.

2.6 Human Rights Convention

Human rights are the most basic rights a human being can have. Whereas it seems crystal clear that non of any articles within the Human Rights Convention shall be violated, it is often not that simple. Some articles of the European Convention on Human Rights (ECHR) interfere with each other. Even though there is some room for interpretation, decisions show that this room is very small and the borders of each article can clearly be separated. For instance, Art. 8 ECHR the right to respect for private and family life, often comes into conflict with Art. 10 ECHR the freedom of expression. To put it in a simple example, one might express his freedom of expression by writing about a topic and including private information of another human being, as for him this information is crucial to support his writing. The person whose private information is included in the writing complains about a violation of his right to respect for private and family life. Within this section, the interference of Art. 8 ECHR (Right to respect for private and family life) and Art. 10 ECHR (Freedom of expression) are discussed in more detail. Art. 8 ECHR reads as follows:

> *“1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.“* (Article 8 ECHR)

Case law shows that people known to the public can rely on the expectation that his or her private life is protected. In the case of *Alkaya v. Turkey (42811/06 ECHR)*,

a well-known cinema and theatre actress from Turkey, had a home robbery while at home. A journalist of a national newspaper reported not only about the robbery that had happened to the famous actress but also included details of her whereabouts. The details published in the article were the area she lived in, the street name and number, as well as the number of the flat. The domestic court dismissed to remedy her for the damages. The actress filed a complaint of her previous ruling to the ECHR. The ECHR also took into account that the domestic court had not weighted the interest between Art. 10 ECHR (Freedom of expression) of the journalist and Art. 8 ECHR (Right to respect for private and family life) of the actress. The domestic court simply argued that the actress is publicly well known and did not further consider a possible repercussion on the actresses' life.

In the ruling of *Satakunnan Markkinapörssi Oy and Satamedia v. Finland (931/13 ECHR)*, the ECHR stated in the courts' assessment "134. The fact that information is already in the public domain will not necessarily remove the protection of Article 8 of the Convention."

> *"Freedom of expression*
> *1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*
> *2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities,conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."* (Article 10 ECHR)

As for Art. 10 ECHR (Freedom of expression) the ruling of *Cengiz and others v. Turkey* referenced the case of Ahmet Yıldırım where social media platforms are indispensable tools for exercising the right of freedom of expression. However, it was difficult to find a ruling where Art. 10 ECHR was directly violated in regards to publishing addresses. Moreover, the case of *Von Hannover v. Germany* shows that Art. 10 ECHR and Art. 8 ECHR has to be treated with equal respect. In the case of *Von Hannover v. Germany*, several pictures of the plaintiff were taken and published

in a newspaper. The plaintiff filed a complaint that her right for privacy Art. 8 ECHR has been violated. Ultimately, The European Court of Human Rights ruled unanimously that the plaintiff was well known to the public and that there was no violation of Art. 8 ECHR because Art. 10 ECHR (Freedom of expression) has to be treated equally. Furthermore, it was within the publisher's rights as a Public Watchdog to exercise Art. 10 ECHR not only to report about political events but also to report about the common public life on political, economic, cultural, social, sports and other levels.

2.6.1 Public versus Social Watchdogs

Holoubek, 2016, writes about a phenomenon of the digital revolution in his analysis of case law on Art. 10 ECHR (Freedom of expression). Holoubek examines the development of case law on various topics, in essence, the two areas of protection. On the one hand, there is freedom of expression in the classical sense and, on the other, all open communication processes. Holoubek, 2016, makes it clear that although freedom of expression is a right of the general public, certain professional groups enjoy even greater protection or freedom. These professional groups include so-called "Public Watchdogs". Public Watchdogs is journalism in the classic sense, made available to the general public in print or digital broadcasted media. Nonetheless, this freedom of expression also has its limits, as Holoubek, 2016, can substantiate well by different judgments. However, preventive publication bans are very restrictive as such prohibitions inevitably undermine and attack democracy within a country. The few existing restrictive publication bans grant Public Watchdogs more freedom.

As technology advances, the sharing of articles and content is much more accessible to the general public. The case law on Art. 10 ECHR (Freedom of expression) has also adapted accordingly. Thus, there are now so-called "Social Watchdogs" in addition to Public Watchdogs. These Social Watchdogs are citizens without a professional journalistic background. Social Watchdogs must have a similar broadcast range, compared to their shared content and opinion on social media, as Public Watchdogs. Even if current legislation does not yet grant Social Watchdogs the same freedom as Public Watchdogs, it quickly becomes clear that the latter enjoy more freedom. According to Holoubek, 2016, the court rulings also take journalistic diligence into account and include it in the judgment.

It can be concluded that, according to Holoubek, 2016, freedom of expression is an essential cornerstone of democracy which is clearly underlined and supported by the courts. Also, the standard of due diligence for Social Watchdogs, i.e. private individuals, is no higher than for their professional analogy, the Public Watchdogs.

Chapter 3

Implementation

3.1 Off-the-Grid

At first, the term Off-The-Grid may seem confusing; however, in order to lose your current digital identity, one must escape the existing binding to their identity, thus getting off the current surveillance grid. The Internet Service Provider (ISP) is technically capable of identifying who someone is and where he or she is connecting to. Choosing the Tor-Browser or -Network, at first glance, might seem like the right choice. Nonetheless, using the Tor-Network allows one to gain anonymity on the internet and further access the Dark-Net. In reality, most of the Tor-Entry and -Exit points are publicly known and for an ISP it is easy to flag customers who are using such anonymization tools. Certainly, the ISP is not capable of getting knowledge of what one is doing inside the Tor-Network, but simply the fact that someone is using such services may raise suspicion and unwanted attention (Tails, 2019).

The following sections will describe a method that allows gaining total anonymity by vanishing the own identity. In addition, this method should be low-cost and not raise any suspicion by authorities, intelligence-service, or the own ISP. During the direct attempt to reach a potential anonymous network, for example, the Tor-Network, the ISP could also potentially become aware of the intentions that a connection to the anonymization network is desired. To prevent the ISP from knowing each connection, a VPN service would encrypt the whole traffic, and only the VPN connection would be visible for the ISP. After establishing a VPN connection, by either setting up an own server on a distant island or choosing a trustworthy VPN service provider, a second layer of anonymity is now necessary as the VPN service provider might now be capable of analyzing the traffic that is put through his service. This can be circumvented

by using the Tor-network. As the VPN service provider has no direct[1] knowledge of the identity, it is now possible to access the Tor-Network almost unknown. However, using the everyday computer connected to all accounts, browsing history, cookies, undetected malware such as a keylogger or state-trojans, the new identity would eventually be lost and the old identity would be brought back up. For that reason, a clean device shall be used. This can be established by using an operating system specially designed to stay anonymous, namely Tails OS, which was also encouraged by Edward Snowden. Tails OS is best used from a Live-System[2] as it not is holding back tracking cookies and other de-anonymization services but also deletes everything, including the RAM, when shut down.

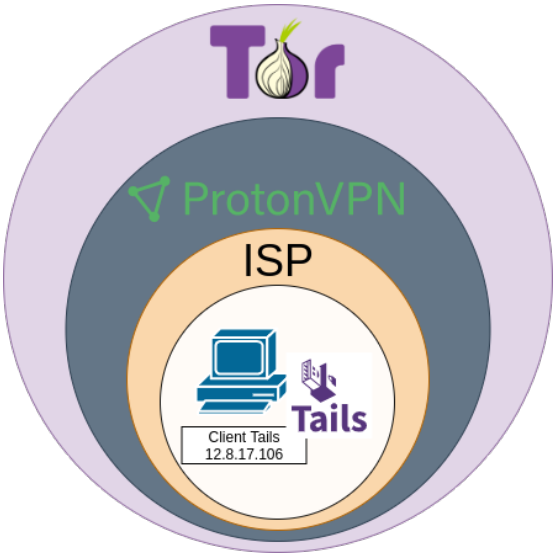


Figure 3.1: A simplification of the Setup used in order to gain anonymity.

The inner core shown within Figure 3.1 represents the client using TailsOS as the operating system through a live stick. The “ISP” layer represents the connection to the ISP, whereas the further next represents the VPN Service provider. Ultimately, the anonymity network is represented through the very last layer within Figure 3.1. Overall, each layer is the next logical connection to a service to gain anonymiously access to the Tor network without allowing authorities, intelligence service, or the own ISP to have a direct connection to the own public IP address. It is important to mention that this methodology still requires trust in all services as complete depersonalization might be jeopardized due to faulty or untrustworthy services. Even though deperson-

[1] Under various circumstances the VPN service provider might know the public IP-Address given from the ISP. Ultimately, by violating his no-log policy, the VPN service provider would be able to connect the ISP-provided public-IP with the usage of the Tor-Network.

[2] A Live-System is a DVD or USB-Stick that is holding an image of the desired operation system and does not need the storage from the attached PC or Laptop.

alization is very unlikely, there is a certain chance.

Further, the “remote-random” functionality of OpenVPN config[3] is used in order to gain a new arbitrary server in an arbitrary country during the boot-up of the router. The Listing 3.1 shows the settings that were used in addition to gain access to a new arbitrary VPN connection from an arbitrary country during the boot-up. Also, using a router flashed with dd-wrt, the option for a scheduled reboot was set to 3:00 AM each day, which results in a daily new arbitrary VPN connection. The settings for a scheduled reboot can be found under “Administration > Keep Alive > Schedule Reboot”.

```
1 remote fi.protonvpn.com
2 remote ee.protonvpn.com
3 remote dk.protonvpn.com
4
5 remote-random
```

Listing 3.1: OpenVPN remote-random settings on dd-wrt router.

However, in order to eradicate the last bit of chance, one must drive away from his home and access the free public internet, e.g. ”Free WiFi”. It would also be important to keep an eye on surveillance cameras as the timestamps combined with the footage could reveal one’s personality in the end or be used as mug shot. Combined with Figure 3.1 the “ISP” layer would be the access to free public internet.

[3] https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/

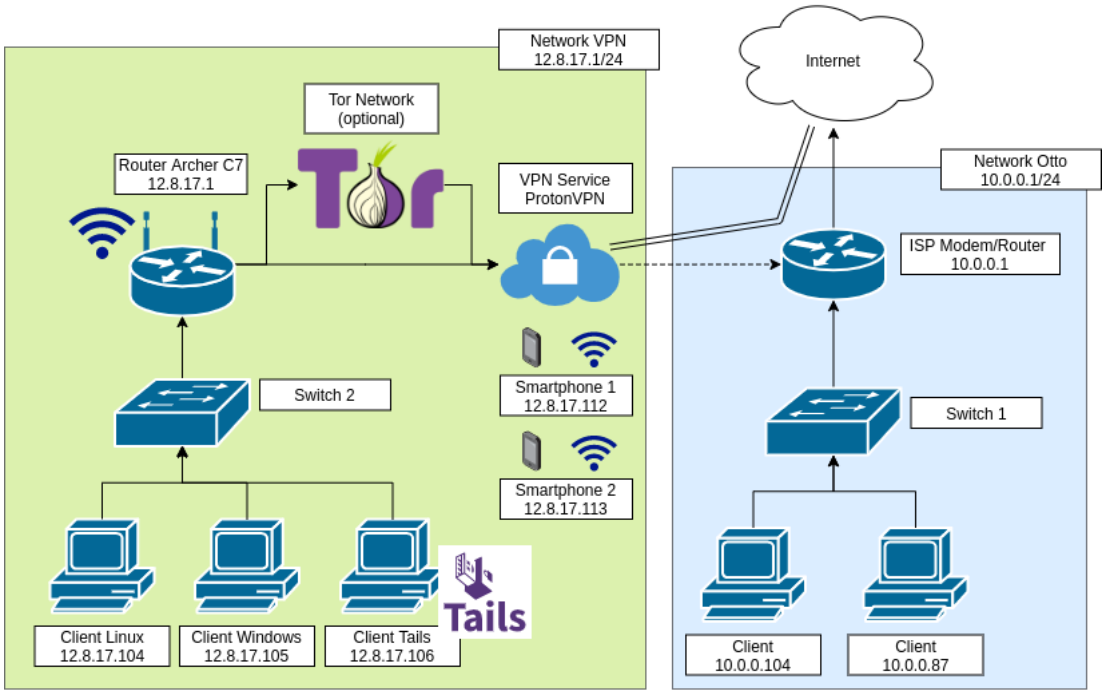


Figure 3.2: Displays the desired network setup including the chosen VPN service provider.

3.2 VPN Service Provider

Choosing the right VPN service provider is a crucial matter. The VPN service provider has to be trusted for general business such as availability, logging policies, and handling of security incidents. However, it is also about one's personal feeling. By personal feeling it is meant that some measures of certain VPN service providers are, no doubt, legal but leave some questions open. At the time of writing, there are many VPN service providers available. Four of them are evaluated in more detail below.

3.2.0.1 NordVPN

NordVPN has, according to NordVPN, 2020, about 5300 servers in 59 countries and allows up to six devices. No log policy and a promise of no DNS leakage is definitely a security, respectively anonymity plus. Unfortunately, it was not possible to get an exact description about the internet speed as it is only advertised as "ultra-fast connection".

Nonetheless, NordVPN is also omnipresent in advertisements on the internet or social media platforms such as YouTube. When visiting the page, a countdown from 9:39:xx hours rushes potential customers to act quickly with no time to have a night to overthink a decision. Surprisingly when accessing the pricing site from an incognito

browser, the countdown resets to 9:39:xx[4]. This advertisement strategy may be legal but deciding a VPN service provider should not be a rushed experience. Rushing customers to buy leaves, in my opinion, a bad feeling.

When it comes to security incidents, NordVPN unfortunately has a history. According to the report of Markuson, 2019, a third-party server located in Finland was compromised at around 5th of March 2018. An unknown attacker had gained access through a misconfigured remote management system and stole TLS and OpenVPN keys. The stolen TLS and OpenVPN keys allowed the attacker to used them to impersonate compromise traffic going through that single server in Finland. NordVPN got knowledge of this incident on 13th of April 2019 and decided not to inform the public until four months later on 21st of October 2019 as "information has recently surfaced". NordVPN claims that the risk for users regarding security anonymity was very low and that the server was shut down immediately. Ultimately it was decided not to inform the public. The handling of information security incidents sometimes leads to the decision not to inform customers and potential attackers due to a greater good and to not further compromise systems. As this is a VPN service provider where the service is based on trust and anonymity, a short notice would have been the better choice.

NordVPN has a high amount of tutorials and a very friendly, clean user interface. The amount of provided apps like Android, Windows, macOS, iOS/iPhone/iPad, AndroidTV, Linux, Chrome and Firefox, is very broad and allows implementation on a router to cover multiple devices.

When it comes to supported protocols, NordVPN stopped supporting PPTP and L2TP/IPSec protocols[5]. When it comes to pricing, NoprdVPN offers one type of plan with discounts on the billing periods. That means, one month with NordVPN costs 10.64 EUR. Choosing a one-year subscription reduces the price by 41 percent to 6.22 EUR per month, two-years to 4.44 EUR (-58%) and three-years to 3.11 EUR per month (-70%). Furthermore, an additional 15% discount for students exists. The company itself is based in Panama City, Republic of Panama.

3.2.0.2 ExpressVPN

ExpressVPN has no known incidents, hence the handling and communication during such events cannot be evaluated at this point. ExpressVPN also provides apps for every major operating system, including smartphones. Further, also for routers as image

[4] After revisiting the NordVPN pricing site a couple of days later, the countdown timer has disappeared; however the discount is still the same.

[5] https://nordvpn.com/de/blog/l2tp-pptp-protocol-update/

or pre-flashed hardware. To help new users, recommendations on some routers are made. The headquarters is situated on the British Virgin Islands. Pricing is 12.95 USD (11.66 EUR[6]) per month, a six-month subscription is 9.99 USD (9.00 EUR) per month. The one-year subscription is advertised trickily with 6.67 USD per month. Billed are actually 99.95 USD each year, the first year includes three extra months for free. 99.95 USD divided by 15 months is 6.67 USD. However, the monthly costs are 99.95/12 after the first year which is 8.33 USD or 7.50 EUR.

3.2.0.3 ProtonVPN

ProtonVPN is incorporated in Switzerland and is connected to the well-known privacy email service ProtonMail. The user interface of the website is clean and at the time of writing, the only discount possible is subscribing for either one or two years. ProtonVPN does not use aggressive marketing or pricing tricks to acquire new customers. According to their privacy policy[7] the latest timestamp of the very last successful login is monitored. According to the policy, the old timestamp is overwritten with a new timestamp. This is used to prevent brute-force password guessing attacks[8]. The website provides well-explained tutorials. In addition, a subreddit[9] is also maintained to connect with the community.

3.2.0.4 CyberGhost

CyberGhost is a VPN service provider based in Romania, a member of the European Union and thereof applicable under GDPR. It offers around 6500 servers in about 90 countries, has a no-log policy. The apps provided by CyberGhost are for Desktop, Mobile, Browser, TV and Routers. For routers the connection can be established with OpenVPN or L2TP/IPSec. However, as of the time writing, a countdown for getting two free months of subscription is running. As this countdown is consistent for incognito browsers as well, it is the same countdown as a few days ago. Nonetheless, pricing is 12.99 EUR per month, a one-year subscription is 5.99 EUR per month, a two-year subscription is 3.69 EUR per month, and a three-year subscription is 2.64 EUR per month.

[6] Pricing in USD was converted with a currency rate of 1 USD is 0.900495 EUR as for the 29th of May 2020.

[7] https://protonvpn.com/privacy-policy

[8] At the time of writing, it is not clear why only successful logins are monitored in order to prevent password guessing.

[9] A “subreddit” is a thread or collection of articles or posts dedicated to a certain topic. Similar to conversations on online forums.

3.2.0.5 VPN Service Provider Conclusion

A very clean and user-friendly webpage can be found throughout NordVPN and ExpressVPN. The CyberGhost might be overwhelming at first glance. However, the user interface is not the main purpose of choosing a VPN service provider but ultimately counts towards happiness during using and troubleshooting.

	Headquarters	Logging	Incident Handling	Free User	Advertisement
NordVPN	Republic of Panama[10,11]	No	Restrictive	No	Aggressive
ExpressVPN	British Virgin Islands[12]	Yes	Unknown	No	Tricky pricing
ProtonVPN	Switzerland[13]	No	Unknown	Yes	Fair
CyberGhost	Romania[14]	No	Unknown	No	Aggressive

Table 3.1: Quick facts on various VPN service providers.

	Pricing			
	No sub	1 year sub	2 year sub	3 year sub
NordVPN	10.64	6.22	4.44	3.11
ExpressVPN	11.66	7.50[15]	—	—
ProtonVPN	10.00	8.00	6.63	—
CyberGhost	12.99	5.99	3.69	2.64

Table 3.2: Pricing table of various VPN service providers. Prices in EUR, 1 USD : 0.900495 EUR as for the 29th of May 2020.

3.3 Attack Vectors using Incidental Data

As shown in Kutschera, 2020, it was possible to gather information on the whereabouts of online security expert Mr. Troy Hunt. Further Chapter 1.6.2 describes a time-critical event on which Mr. Troy Hunt and his family left the residence to pursue a 9.000 km road trip. Moreover, the gathered information on his whereabouts shows the interior of his home. This ultimately allows a burglar to familiarize themself with the environment and prepare tools that they might bring along, thus reducing the weight of the backbag and increasing moving speed, size and silence during walking. Considering his home

[15] ExpressVPN one-year subscription is listed without additional free 3 months.

is worth several million AUD, there is a certain chance that one or the other worthy item lurks around in the home of Mr. Troy Hunt. Also, the burglar must not expect the homeowner is returning home soon as he can calculate how long he might need to come home using the most recent update on his Twitter profile. It can be assumed that more electronic security systems (cameras, motion detectors, etc.) are installed than in an average household due to the personal interests. However, burglars are most afraid of personal confrontation. Also, a butler or maid is easier traceable than the whole household. Furthermore, a more advanced criminal organisation might use the absence of the homeowner, including the family, as he or she only needs to deal with the electronic security systems. Considering the security system sends each alarm silently to the next police station, the security system could be disarmed by cutting off the power or overcharging all electrical devices using an electromagnetic pulse (EMP). (Discovery Channel, 2006) A request for comment in regard of the feasablity of this idea was sent to the US Army station as seen in Discovery Channel, 2006 but left unanswered as of today[16]. The sent request can be found within the Appendix C. Another attack vector is that one can be mistaken for a very similar looking criminal who was hunted by some part of the public as this happened to *David Quintavalle*, which was later proven innocent by the Federal Bureau of Investigation (FBI). (Bazzel, 2021, 15:19min)

3.4 Interviews & Statements

Kutschera, 2020 has shown that it might be more ethical to contact potentially affected persons before conducting a 2-hour manual search on their public social media profiles. For this reason, the approach was to firstly contact the person or organization, get informal consent to analyze the social media presence and secondly, get an interview scheduled. On the contrary, the pre-research phase of this master's thesis was a reason to implement an ethical evaluation. Hence the first few persons or organizations were not asked for consent. Eventually, the expert interviews were either conducted in correlation to the presence on social media or the profession outside of social media platforms. The expert-interview-partners were asked the following five questions in correlation to their presence on social media. Please notice that the interviews were held in either German or English. Each interview has a conclusion that is in style of Mayring, 2010, with consideration on Baur and Blasius, 2019.

[16] June 7, 2021

3.4.1 Question Set 1-5

3.4.1.1 Question 1

[English]*"Is the data found new to you respectively were you aware that I would get to this information?"*
[German] *"Sind die gefundenen Daten neu für dich bzw. war dir bewusst, dass ich zu diesen Informationen gelangen würde?"*

Reason and Background: This should show if the person is aware of the things that could be found during the two hours of the manual gathering process. Hence, if a person is aware of the data, it cannot be declared as incidental data.

3.4.1.2 Question 2

[English]*"If you want to talk about it, how do you feel about it?"*
[German] *"Wenn du darüber reden möchtest, wie fühlst du dich damit?"*

Reason and Background: The intention is to show that the uncovering of incidental data alone can have a (negative) impact on the emotional level of a person.

3.4.1.3 Question 3

[English]*"In your opinion, what danger is connected to it?"*
[German] *"Welche Gefahren siehst du damit verbunden?"*

Reason and Background: Shows whether or not the person sees any possibility of exploiting their incidental data. As this question might uncover unknown attack vectors, all interviewed persons were shortly briefed not to say or mention anything that might bring themselves or their families in danger.

3.4.1.4 Question 4

[English]*"Should data from entrepreneurs without customer-traffic be more secured?"*
[German] *"Findest du, dass Daten von Einzelunternehmen ohne Kundenverkehr besser geschützt werden sollten?"*

Reason and Background: The intention is to get an overview on whether or not the proposed change of law (see Chapter 1.5.2 & Chapter A) might have a positive impact on the privacy of entrepreneurs or if the vast majority would decline such measures.

3.4.1.5 Question 5

[English]*"What would your measures against such dangers be or why do you think the data should be available without any restrictions?"*
[German] *"Was wären deine Maßnahmen oder warum glaubst du, dass diese Informationen ohne Barriere frei zugänglich sein sollen?"*

Reason and Background: This question was asked in order to summarize good examples of preventative security and safety measures.

3.4.2 Interview, Scott Helme

Mr. Scott Helme is a Security Researcher, Entrepreneur and International Speaker. He is the creator of "Report URI" and "Security Headers". In addition, he is also holding trainings on hacking and encryption.

In the case of Mr. Scott Helme, it was possible to gather information on his home address, full birthday, detailed floor plannings and the price and date of the alleged purchased home. The initial lead was a posting on Twitter where Mr. Helme himself posted a picture of his car. In this picture, one could see that the roof of the house had two different colours and a little bit of the vicinity was visible through the reflection of the car's paint. On his public accessible "LinkedIn" profile the city in which he lives is visible. A search through satellite images revealed a relatively small town with three matching houses that have a doubled coloured roof. Unfortunately, none of them matched the picture from Twitter or the reflection from the car's paint. Another attempt for searching his name revealed that Mr. Helme is a business owner. The business address is situated in a residential area. A comparison with the reflections and surroundings on the Twitter image confirms that this may be his residential address. Having the potential address, it was possible to gather additional information. Further, detailed floor plans from the application filings on the completely renewed home were found. These documents date back two years. Another website listed that the building was sold about a year ago, including price and date of purchase. The date of birth could be gathered from a website that lists the business of Mr. Helme alongside his date of birth. However, the listed date of birth contained only month and year but was missing the exact day. The missing day alongside the month but without the year was ultimately revealed by Mr. Helme himself in a Twitter post. Furthermore, with this information at hand it was possible to make an educated guess on the full date of birth. The gathering process of incidental data for Mr. Helme was done within 40 minutes.

Confronted with the found evidence, Mr. Helme confirmed the found results and stated that business owners in the United Kingdom must have their name and address public. In addition, house records also belong to the public, according to Mr. Helme. However, he is also concerned that this information can be used to plan a burglary, impersonate him or make personalized fraud letters sent via mail directly to his home. The amount of effort to hide or remove his data seems unbearable. As a result, he resigned to the system and how it is working.

3.4.2.1 Conclusion Interview Mr. Helme

Within 40 minutes it was possible to gather information on Mr. Scott Helme that would allow a criminal to start an advanced and personalized attack on Mr. Helme. The ruling of "Alkaya v. Turkey" from the European Court of Human Rights has shown that a Public Watchdog, i.e. Journalist, violates the Art. 8 ECHR (Right to respect for private and family life) by publishing the private address of a famous actress when reporting on a robbery at her home. In contrast, there is the ruling of "Von Hannover v. Germany" where Public Watchdogs are allowed to publish information of pictures if it is in the general public's interest. Even though Mr. Helme is a person who is well known to the general public, it is unclear why it is of benefit to the general public to make that much information easily accessible due to the ownership of his business.

3.4.3 Interview, Dr. Ries Bouwman

The interview with Dr. Marinus "Ries" Bouwman, an international entrepreneur and co-founder of Omi's Apfelstrudel, was held on 4th of December 2020, including his view and thoughts on privacy for SME's. Given prior consent that I may search for posted incidental private data, Dr. Bouwman was confronted with the found evidence of his alleged former private address in the Netherlands, including property values and alleged former addresses in Austria, further, details on his shares on companies. Eventually, it turned out that the alleged address in the Netherlands was not valid. For Dr. Bouwman the found data was not new. Moreover, he was aware of the data and comfortable with it. The fact that some data was not his supports that he must not fear any danger from such data. In his opinion, the data is not a threat but more an opportunity for business partners to get in touch with him. For this reason, he also said that such data should be available and the current providing method is completely fine. Further, he needs quick and easy access to track new businesses of untrustworthy former respectively alleged business partners from his own experience.

3.4.3.1 Conclusion, Interview Dr. Bouwman

The data gathering process on Dr. Bouwman took 1:30h. Eventually, not all found data was valid as some of the data found had no direct connection to his person, or the data was simply wrong. Given his own experience, the database of enterprises (GISA) and the easy access did help Dr. Bouwman as he was able to track new business of non-trustworthy businesswoman and businessmen. On the one hand, it can only be assumed that the low barrier to search for such information made him actively search and therefore protected him from untrustworthy businesses. On the other hand, every entrepreneur in Austria must have access to the so-called USP (Unternehmens Service Portal) in which one must identify themselves with the qualified electronic signature based on the Regulation EU 2014/910 electronic identification and trust services for electronic transactions in the internal market (eIDAS) of The European Parliament and the Council of the European Union, 2014. Hence, it may be reasonable that entrepreneurs can search through the GISA database in more detail with an assigned account.

3.4.4 Interview, Dr. Vesna Krnjic

Dr. Vesna Krnjic is a postdoc researcher at the Institute of Software Technology at Graz University of Technology. She dedicated her doctoral thesis in Computer Science at the Institute of Software Technology at Graz University of Technology to Usability within Privacy and Security. The interview was held on 04th of March. A permission to gather personal information was given before the interview, and as for all interviews, the time period shall not exceed two hours. The gathering period took one hour and 50 minutes, and it was possible to find information about her whereabouts and other minor details.

However, the data that was found was not new to Dr. Krnjic. It was more of a surprise to her how the data was gathered and that it would be challenging to find the data. This has the reason that Dr. Krnjic takes a lot of photos in her free time and previously liked to share them on her Google+ account. Therefore, it was surprising to her that only a few of her publicly available photos showed private information or information that could link to her home address. It might be the result of the background knowledge Dr. Krnjic has in privacy and security so that she unconsciously is aware of which information or photos to share, she believes. Regarding the lack of consciousness of the wide mass, it feels a bit frightening to her what kind of information can be revealed by photos posted online, especially when thinking about involving artificial intelligence or unlimited time for analysis. Dr. Krnjic greatly supports the proposed

change of law, as shown in Chapter 1.5.2 and Appendix A, as she sees no need for SMEs without direct contact to customers to publicly disclose the companies address when it matches the personal home address of the owner. In addition, it seems to Dr. Krnjic that the mobile phone signature offers the infrastructure to support an additional layer of security easily. It was fascinating to Dr. Krnjic that it took only one photo that revealed her home address. This motivates her to be even more thoughtful of what to post online, as she would not have thought that this particular photo would reveal such information. In the end, it seems to Dr. Krnjic that everyone might potentially reveal personal information about themselves without being aware of it in today's age.

3.4.4.1 Conclusion, Interview Dr. Krnjic

It was very exciting to have the chance for an interview with a professional within the security area. It was not an easy task as the information gathering for Dr. Krinjic reached almost the threshold of 2 hours as described in Chapter 3.4. That the approach used within this master's thesis was new to Dr. Krnjic emphasizes the importance of a proper set of security measures. Since it was the approach and not the found data that was unexpected for Dr. Krinjic, it shows that it is always important to have a proper set of security measures at hand, and this, for Dr. Krinjic, is, among other things, her knowledge. The support of the idea of stronger privacy for entrepreneurs shows that the master's thesis proposal for a change of law is needed rather sooner than later.

3.4.5 Interview, Austrian SME Entrepreneur

The interview with an Austrian SME Entrepreneur[17] was held on 01st of April 2021. The Austrian SME Entrepreneur owns several homepages and hosts her own podcast. Moreover, she has a lot of international experience, also social media plays a crucial part in her daily business, which is why almost every crucial social media platform is used to get into touch not only with cooperation partners but also to reach out to customers. Her expertise is much appreciated amongst travel enthusiasts but also by professional scuba divers.

Before the interview began, the found data was shown and discussed together. Even though the used approach[18] was new to her, the found data was already known. The obligation in Austria to imprint or disclose is concerning yet helpful at the same time for her. On the one hand, it is a measure to seek for trustworthy businesses. Thus without a proper imprint one is not considered as a serious cooperation

[17] Due to privacy concerns it was decided to redact the interview and the name.
[18] As described within this thesis Chapter 1.6.

partner at first sight. On the other hand, the danger that lurks behind is addresses of business owners, which are easy and free to capture. In her opinion, the privacy measures for SME entrepreneurs need to be reworked to enhance privacy amongst SME entrepreneurs. She personally has many measures against criminals in place. For instance, she never posts pictures of a destination that is currently being reviewed. She also discourages and legally binds her business partners not to release any statements or information revealing her current or future locations. Sometimes she also posts according to a different time zone as she doesn't want to reveal her location, which might be in a completely different time zone as she usually or currently lives. Her efforts already made a trade-off as she has not received any threatening phishing attacks or other dangers as of today.

3.4.5.1 Conclusion Interview, Austrian SME Entrepreneur

In conclusion, it was made clear in the interview with the Austrian SME Entrepreneur with international travel and scuba diving experience that current legislation emerges threats towards SME entrepreneurs, herself included. Her views support the overall idea of this master's thesis as to raise awareness of security and privacy. The measures taken by her are, for instance, to not post on social media that one is currently not at home, to stick to a time zone when posting or to regularly divert and randomize uploads. The proposed change of law, as shown in Chapter 1.5.2 and Appendix A, would also help her as her business address is the same as her private address and therefore is not behind a security wall of legitimate interest.

3.4.6 Interview, Henry from Techlore

The Interview with Henry, the owner Techlore[19], an organization located in the United States which provides content and consultation on Privacy and Security, was held on 5th of April 2021.

Henry mainly was aware of the data that was found since the information is publicly available due to the ownership of his company. The way his information was gathered into a single file had an impact on him because it showed how single data points could paint a broad picture of the individual when put together and how little things you do in your daily life can expose more than what you are usually aware of. When asked what kind of danger could be connected to the publicly available data, Henry mentioned that it would mostly be a physical danger or home invasions for which the well-implemented local security protections compensate. Henry feels a bit

[19] https://techlore.tech

mixed but sees the importance of the current situation in which the company information has to be public since it leads to transparency for business partners and customers as well as in legal actions. Also, there are ways for the owner of the companies to remain private to some degree as long as they are aware and educated on how to do so, for example, with Limited Liability Companies (LLC). The idea of implementing a governmental protection layer by which a person must identify themselves before looking up the addresses of businesses holds mixed views for Henry. On the one hand, he believes that this might be a solution to have finer control of who gets access to the information. On the other hand, Henry sees an opportunity in which companies would find a way to utilize that to protect themselves from people being able to find information and holding companies accountable. Henry would see it as advantageous if there were more programs in place to encourage the owners or the people behind the company to use an address that is not their home address because the key lies in education to be able to make decisions that protect your privacy.

3.4.6.1 Conclusion Interview, Henry from Techlore

The interview with Henry has shown that, even though he, as a professional, was aware of the available information, it had a certain impact to see the data gathered forming a profile about his persona. This makes it clear that such data must be handled carefully. Nonetheless, it is important that there is a necessity for companies to have valid contact data available as it prevents companies from carrying out negative businesses. The effort that Henry and his team put into privacy already made its trade-off as it was not possible to gather much information besides legally compulsory public information. This master's thesis supports most that it would be good to train people to give them the tools to provide good privacy themselves.

3.4.7 Interview, Heimo Flechl

On 9th of April the interview with the Head of the Unit of OSINT & Crime Trends of the Criminal Intelligence Service Austria[20], Heimo Flechl, BA MA, was held.

On the one hand, he deals with the support of investigators in their operational investigations. I.e. an investigator has a case and recognizes based on the data that an OSINT specialist could contribute to the investigation's success. The investigator then contacts the unit of Mr. Flechl which takes care of the OSINT support for the investigation at question. Internally this will be called "operational open-source

[20] German "Leiter des Referats für Open Source Intelligence und Kriminalitätstrends im Bundeskriminalamt".

intelligence". On the other hand, there is "strategic open-source intelligence", which deals with various major topics like the incident in spring of 2020 involving the Greek-Turkish border[21] where the decision-makers in the Ministry of the Interior were very interested in rapid monitoring of information in cases of sudden changes of the situation. Following the translated and edited interview, the full and original transcript can be found within the Appendix D.

Stefan Kutschera: *From your experience, do you believe that data which is collected using OSINT methods has a high value on the black market, specifically for criminals?*

Heimo Flechl: *That is a very complex question. If I think, for example, of the modus operandi of CEO fraud, where, in a nutshell, the perpetrators approach companies or, primarily, the accounting departments of companies and pretend that they are the CEO and urgently need a money transfer to somewhere, disregarding the security regulations that are customary in place, then it is usually the case that these perpetrators have researched all the information they have about the company in advance, and this is essentially OSINT information. Now you could approach it from this side and ask, would this modus operandi be possible at all if the company had no website, for example. And then you could think about adding a value to it. Another thing would be to find out essential information about public figures that might be incriminating or at least extremely embarrassing. We see that in the Ibiza video area, it's not OSINT information, but obviously it should have some black market value. But otherwise, the value is relatively difficult to quantify, to really scale down to a number. From my point of view, it always depends on the individual case in order to evaluate whether this information has any value at all, and if so, which value.*

Stefan Kutschera: *What exactly is Crime as a Service and what does it mean in the digital domain?*

Heimo Flechl: *Crime as a Service is something we have been observing for a good decade. It is essentially, as the economist Adam Smith suggested at the time, a principle of division of labor, and the point is that the IT world has become so complex that one person can no longer do everything. So if you imagine an attack with a netbanking Trojan, for example, there is one person who basically develops the Trojan, because he is good at programming malware. And this person then offers the service, this Trojan,*

[21] https://www.europarl.europa.eu/news/en/headlines/world/20200305STO74150/meps-call-for-de-escalation-of-migration-situation-with-turkey

for sale on the darknet. Then there is another person who thinks it would be a good idea to earn money by defrauding a broad mass of people with such a netbanking Trojan. And then they buy this service, i.e. this Trojan from this one person, and then think, if I have infected the mobile devices or the electronic devices of my victims I can start the money transfer, but then I also need someone to launder the money for me. Because if I transfer the money directly from the victim's account to my own account, the police will knock on my door relatively quickly. Then I further look in the various darknet forums to see if there is someone who offers money laundering for the geographic area of Central Europe and then I add them to the crime. That would be a brief summary of the Crime as a Service situation that we observe in the darknet, using the example of a netbanking infection, which of course has a much wider and larger scale. There are many individual areas where people offer their criminal services on the darknet, but in short, I would say that the world is now so complex that specialists have emerged for individual areas, even in the criminal universe, and they then offer their individual services for sale and there is then just one person who combines these services and then really converts them into an accomplished crime.

Stefan Kutschera: *That would actually mean if someone offers their specialty they could also offer OSINT as a specialty and sell it as a Crime as a Service. How would you assess the value or the harm regarding OSINT as Crime as a Service for the individual concerned?*

Heimo Flechl: *I would like to note that from my point of view it is relatively difficult to call OSINT data or OSINT criminal because essentially an OSINT Analyst, whether on the good side or on the bad side, is not doing anything other than collecting and analyzing public data. Then you have to ask yourself, is that criminal at all? I don't know if an OSINT Analyst makes himself available on the darknet for criminal purposes, it is a good question if that is even conceivable. From personal operational experience, it is usually the case that those who are the implementers of the criminal act in question are also the ones who research it. Of course, they don't do it at that level of which a professional OSINT Analyst could do it, but mostly such that it is sufficient to perform the criminal act. I think at the moment it's more likely that you would sell it as preliminary work on the darknet and say I already have a result and therefore I'm not selling the service but more the data or the result of my analysis. Just as mentioned in a previous question, for example, if I have data that is embarrassing or incriminating about public figures. And I'm not talking about data that I got by infecting their computers or something like that, but really data that was freely available but maybe not directly visible to the average eye but through the application of various OSINT meth-*

ods and analysis methods. So the question is again complex and can't be answered with a number. But I could well imagine that this could become more interesting from year to year, also for this area.

Stefan Kutschera: *What measures would you recommend to better protect yourself online in regards to unintentionally published data?*

Heimo Flechl: *There are also several spheres and I come back to the modus operandi of CEO fraud. In some cases, companies are faced with a decision. On the one hand, if I don't make certain data available online, a customer may not get a clear picture or may be less able to reach the person in question, because that person's contact data is no longer directly available. On the other hand, there is the protection against various criminal activities. So, of course, there is the commercial company dimension and then there is also the private dimension, where I can essentially strongly recommend in the area of social media to take very close look into the various privacy settings. You can avert a great deal by saying that I essentially only give out data that is rather private to people with whom I am friends for example on Facebook. But then you can go one step further and say, well, I shouldn't accept every friend request I get and should think about whether I know this person at all. But the reference to the privacy settings, which are very far-reaching in social media, would be a good one, but of course I'm only really safe if I have no social media profile at all. Of course, that's a decision that everyone has to make for themselves. And basically, if I say I don't like the big data giants anyway, but I do like to have a profile on a social medium in order to be able to stay in touch with my circle of friends, well, then you can research in advance what data is actually collected by the respective social media. Let me remind you of the Facebook data scandal, Cambridge Analytica I think it was called, then I can just choose a social network where something like that hasn't happened yet. That doesn't mean that they don't do it, but at least they claim that they don't do it and it has never been made public. So you're always at a fork in the road there, security and convenience. But the tip for private individuals would be: look at the privacy settings, set them very restrictively and you are only really safe if you do not have a profile.*

Stefan Kutschera: *May I ask if you can also give tips or preventive measures regarding postings of pictures and videos?*

Heimo Flechl: *Yes, we are already one or two steps further now. Let's say the person has a profile and also posts a lot, not only text but also pictures. Of course, you should always have in mind, even if you yourself think, you only post a picture of yourself, for*

example, in your own 4 walls and it anyway only shows what you are doing on this picture - this may be the case for 99% of the population, but when an OSINT Analyst looks at this picture, he sees completely different things on this picture than the average user. He or she might look at the picture and see if there is a security system somewhere in the house, if I can recognize the brand of an alarm system or if I can recognize that there is no alarm system at all or if the picture, or the "Selfie" as it is called in the new German language, is taken in such a way that I might recognize where this person lives, because in the background out of the window another known building is visible or even an address sign. And that also points to the activity of an OSINT Analyst. One very rarely has this one hint which then clarifies everything, you rather move forward piece by piece and with a picture I may have this information, which then fits together with the information from another post or picture and so you slowly build yourself up this chain of evidence until you finally get a hit. So with regard to the posting of pictures one should think about what is actually to be seen on the picture and it is a good idea to post it that way. Globally you have the impression that people tend to think less about that.

3.4.7.1 Conclusion Interview, Heimo Flechl

In conclusion, the interview with Mr. Heimo Flechl has shown that OSINT is not a criminal activity per se but may be used for further criminal activities, like the CEO fraud. Even though the monetary value of personal data collected through OSINT techniques may vary from subject to subject, the impact can be diverse as it may not only impact one's integrity but also one's reputation and can enable damages on a physical or psychological level. Hence it isn't very effective to sell the collected data on the black market but offering one's own expertise as Crime as a Service might be. An example of Crime as a Service is that one creates a Trojan, but another one uses this Trojan to collect banking information/credentials by distributing or infecting individuals and involving another criminal who is able to perform money laundering.

Mr. Heimo Flechl also states that the imprint of companies is one piece of information, but criminals need more information to get the trust of employees in order to perform a successful[22] fraud. Consequently, one must ask themself if the information he or she puts on the company page is necessary to fulfill legal or business requirements and/or to gain customers‘ trust. Also, private individuals who share information on various social media platforms might take a closer look not only on the

[22] successful in the form of executed action performed by the criminal.

primary subject of the posting but also on small visible details such as security measures or the absence of such, street names, house numbers or famous buildings and other landmarks which might reveal unintended information.

This interview emphasized once more that security is a polarizing topic. On the one hand, entrepreneurs use publicly available information on businesses to verify their integrity and to decide whether or not to conduct business with them as also the interviews with Dr. Bouwmann and the Austian SME Entreprenuer[23] has shown (see Chapter 3.4.5 / 3.4.3. On the other hand, the expertise of Mr. Flechl shows that such information can be misused by criminals.

3.4.8 Statement, Amt der steiermärkischen Landesregierung

During the evaluation of the fabricated mock-up case as shown within Chapter 2.4, the "GIS-Kataster" was accessed and gave information of land and property owners upon request without the need of any dedicated account. The mock-up case was created and evaluated around December 2019 and January 2020. It turned out that suddenly without any announcement or change of law the access to the public was withdrawn as shown in Figure 3.3.

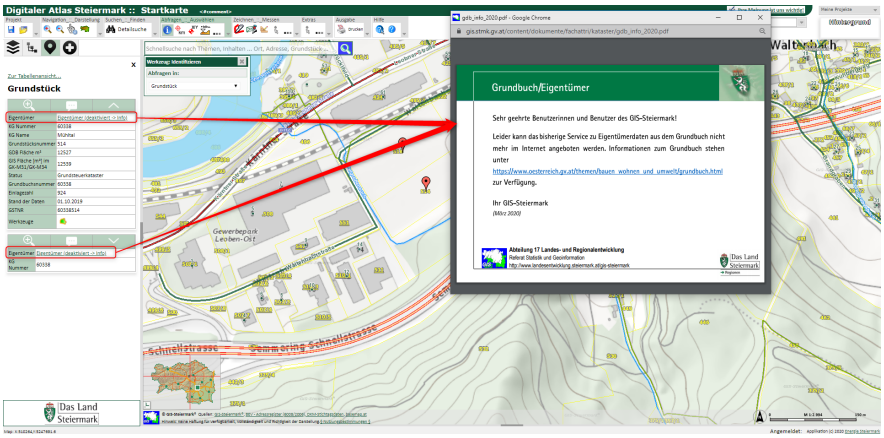


Figure 3.3: Shows a screenshot of the GIS-Kataster with the deactivated ownership information pop-up window.

As mentioned above, during the research progress within this thesis, it became evident that the access of that data was cut off. For that reason a request for comment was sent to Department 17, Office of the Styrian Provincial Government[24] which was answered by Mr. Grießer as stated below:

[23] Name redacted due to privacy reasons.
[24] Abteilung 17, Amt der Steiermärkischen Landesregierung.

"[Translated][25] As you have correctly stated, we were forced to remove the owner query of a predefined property from the web GIS application of the province, although there have been no changes in the land register law. Due to the data protection regulation and increased inquiries, the constitutional service of the province re-evaluated the question of access to land register data via the GIS Styria. The land register access continues to be available to the public on a limited basis via the other known platforms." (Grießer, 2021)

3.5 Problems

Conducting research for a master's thesis is a path that sometimes needs to be freed from stones in order to reach the goal. This master's thesis is no exception to that. The following chapter discusses some of the problems that occurred during the research, and if applicable, the solution to the specific problem. Hence, anyone reading this can learn from those and remove or circumvent the obstacles easier.

3.5.1 VPN on Router

Having put the "—BEGIN OpenVPN Static key V1—" into the wrong section, the VPN could not connect. However, a closer look to the log output led to a "Options error" as shown in Listing 3.2, line 3.

```
1 root@NotMyRouterName:~# cat /tmp/vpn.log
2 Sat May 30 12:00:29 2020 WARNING: Using --management on a TCP port
    ↪ WITHOUT passwords is STRONGLY discouraged and considered
    ↪ insecure
3 Options error: specify only one of --tls-server, --tls-client, or --
    ↪ secret
4 Use --help for more information.
```

Listing 3.2: Logentry with misleading information.

After getting the TLS authentication key into the correct place, the log messages indicated a failed authentication. The password was entered several times using copy and paste. However, somehow a blank space was always in front of the password field and ultimately added to the password. A look into the "/tmp/openvpncl/credentials" as shown in Listing 3.3, had revealed that mistake that was overlooked so often while entering the password.

[25] Translated from German to English, the original version can be found in the Appendix B.

```
root@NotMyRouterName:~# cat /tmp/openvpncl/credentials
SomeBogusOpenVPNUsername
 NotMyOpenVPNPasswordEither
```

Listing 3.3: Credentials as used by the OpenVPN client.

```
root@NotMyRouterName:~# cat /tmp/vpn.log
Thu Jan  1 01:00:35 1970 WARNING: Using --management on a TCP port
    ↪ WITHOUT passwords is STRONGLY discouraged and considered
    ↪ insecure
Thu Jan  1 01:00:35 1970 WARNING: file '/tmp/openvpncl/ta.key' is
    ↪ group or others accessible
Thu Jan  1 01:00:35 1970 WARNING: file '/tmp/openvpncl/credentials'
    ↪ is group or others accessible
Thu Jan  1 01:00:35 1970 OpenVPN *.*.* mips-unknown-linux-gnu [SSL (
    ↪ OpenSSL)] [LZO] [LZ4] [EPOLL] [MH/PKTINFO] [AEAD] built on May
    ↪  27 2020
Thu Jan  1 01:00:35 1970 library versions: OpenSSL *.*.**  21 Apr
    ↪ 2020, LZO *.**
Thu Jan  1 01:00:35 1970 MANAGEMENT: TCP Socket listening on [
    ↪ AF_INET]127.0.0.1:50
Thu Jan  1 01:00:38 1970 NOTE: the current --script-security setting
    ↪  may allow this configuration to call user-defined scripts
Thu Jan  1 01:00:38 1970 Outgoing Control Channel Authentication:
    ↪ Using *** bit message hash '***' for HMAC authentication
Thu Jan  1 01:00:38 1970 Incoming Control Channel Authentication:
    ↪ Using *** bit message hash '***' for HMAC authentication
Sat May 30 12:08:34 2020 RESOLVE: Cannot resolve host address: ca.
    ↪ protonvpn.com:1224 (Try again)
Sat May 30 12:08:37 2020 Socket Buffers: R=[172040->172040] S
    ↪ =[172040->172040]
Sat May 30 12:08:37 2020 UDPv4 link local: (not bound)
Sat May 30 12:08:37 2020 UDPv4 link remote: [AF_INET
    ↪ ]172.254.92.55:1224
Sat May 30 12:08:39 2020 TLS: Initial packet from [AF_INET
    ↪ ]172.254.92.55:1224, sid=1234cc1c b23158db
Sat May 30 12:08:39 2020 WARNING: this configuration may cache
    ↪ passwords in memory -- use the auth-nocache option to prevent
    ↪ this
Sat May 30 12:08:40 2020 VERIFY OK: depth=2, C=CH, O=ProtonVPN AG,
    ↪ CN=ProtonVPN Root CA
Sat May 30 12:08:40 2020 VERIFY OK: depth=1, C=CH, O=ProtonVPN AG,
    ↪ CN=ProtonVPN Intermediate CA 1
Sat May 30 12:08:40 2020 VERIFY KU OK
Sat May 30 12:08:40 2020 NOTE: --mute triggered...
Sat May 30 12:08:40 2020 5 variation(s) on previous 3 message(s)
```

```
    ↪ suppressed by --mute
22 Sat May 30 12:08:40 2020 [ca-02.protonvpn.com] Peer Connection
    ↪ Initiated with [AF_INET]172.254.92.55:1224
23 Sat May 30 12:08:41 2020 SENT CONTROL [ca-02.protonvpn.com]: '
    ↪ PUSH_REQUEST' (status=1)
24 Sat May 30 12:08:46 2020 SENT CONTROL [ca-02.protonvpn.com]: '
    ↪ PUSH_REQUEST' (status=1)
25 Sat May 30 12:08:49 2020 AUTH: Received control message: AUTH_FAILED
26 Sat May 30 12:08:49 2020 SIGTERM[soft,auth-failure] received,
    ↪ process exiting
```

Listing 3.4: Logentry indicating false credentials.

3.5.2 Interview Requests

Table 3.3 shows all sent requests during this master's thesis research as well as during Kutschera, 2020 and Kutschera, 2021. The requests for expert interviews were sent due to the fact that either concrete incidental data was found or strong evidence that such might be of existence. The table contains the name of the person or organisation in column "Contact", the date where the request was sent within "Date", the primary intention of contacting in "Reason", whether the person or organisation was an acquaintance (i.e. a previous contact outside the context of this master's thesis was already established) within column "Acq.", and last but not least if the person or organisation had responded in one way or another to my request within column "Resp.". Multiple sent dates mean that the request was sent again on the days stated because there was no response on the first request, yet a response was categorized as very valuable for this master's thesis. Anyway, the column "Resp." indicated the latest update and response of each request.

Contact	Date	Reason	Acq.	Resp.
"Cody's Lab"[26]	03. Apr 2020 04. Dec 2020	Expert Interview	No	No
EGov/Robert Hammer[27]	03. Apr 2020 15. Jan 2021	Request for Comment	Yes	No
"Live Each Day"[28]	03. Apr 2020	Expert Interview	No	No
Troy Hunt	05. Apr 2020 15. Nov 2020	Expert Interview	No	No
Bundeskanzleramt Ö[29]	30. Apr 2020	Request for Comment	No	Yes
ProtonVPN	01. Jun 2020	Request for Comment	No	Yes
Scott Helme[30]	09. Jun 2020	Expert Interview	No	Yes
"Survival Lilly"[31]	29. Nov 2020	Expert Interview	No	No
"Twitch_Maty"[32]	15. Nov 2020	Expert Interview	No	No
Ries Bouwman	30. Nov 2020	Expert Interview	Yes	Yes
"Backyard Scientist"[33]	04. Dec 2020	Expert Interview	No	No
EGov Stmk[34]	15. Jan 2021	Request for Comment	No	No
Vesna Krnjic	16. Jan 2021	Expert Interview	Yes	Yes
Jonna Jinton[35]	17. Jan 2021	Expert Interview	No	No
"Slow Mo Guys"[36]	17. Jan 2021	Expert Interview	No	No
"Spiel und Zeug"[37]	17. Jan 2021	Expert Interview	No	No
US Army - White Sands[38]	17. Jan 2021	Expert Interview	No	No
"DeLadySigner"[39]	23. Jan 2021	Expert Interview	No	No
Land-Stmk Abteilung 17[40]	04. Feb 2021	Request for Comment	No	Yes
Techlore[41]	17. Feb 2021	Expert Interview	No	Yes
Michael Bazzell[42]	07. Mar 2021	Expert Interview	No	Yes
A-SME Entrepreneur	08. Mar 2021	Expert Interview	Yes	Yes
BK[43]/Heimo Flechl	02. Apr 2021	Expert Interview	No	Yes
Colton Potter[44]	05. May 2021	Expert Interview	No	No
"Tommy Boy"[45]	15. May 2021	Expert Interview	No	No

Table 3.3: Shows all sent requests to a person or organisations with date, contact, response and whether or not the person or organisation was an acquaintance.

[26] https://www.youtube.com/user/theCodyReeder/about
[27] https://web.archive.org/web/20200201034229/https://www.e-government.steiermark.at/cms/ziel/61132671/DE/
[28] https://www.youtube.com/user/DudeLikeHELLA/about
[29] Federal Chancellery of Austria (Bundeskanzleramt Österreich)
[30] https://twitter.com/Scott_Helme
[31] https://www.youtube.com/user/alonewolverine1984/about
[32] https://www.youtube.com/channel/UCp3m6OSfosYlgtaeJEzRzxQ/about
[33] https://www.youtube.com/c/TheBackyardScientist/about
[34] https://www.e-government.steiermark.at/cms/ziel/61132671/DE/
[35] https://www.youtube.com/user/JonnaJinton/about
[36] https://www.youtube.com/user/theslowmoguy/about
[37] https://www.youtube.com/c/spielundzeug/about
[38] https://www.wsmr.army.mil/dbwws/Pages/default.aspx

Acquaintance	# Sent	# Responded	Response Rate
Yes	4	3	75,00%
No	21	7	33,33%
Overall	25	10	40,00%

Table 3.4: Breaks down the response rate of sent requests for acquaintances and non-acquaintances.

Reason	Acquaintance	# Sent	# Responded	Response Rate
Expert Interview	No	17	4	23,53%
Request for Comment	No	4	3	75,00%

Table 3.5: Breaks down the response rate of sent requests for non-acquaintances.

When setting the received responses into perspective of whether the person or organisation was an acquaintance, it can be said that the response rate for non-acquainted persons was 33,33% but for acquaintance persons 75,00% as can be seen in Table 3.4. Comparatively, splitting up the responses of non-acquaintance persons into the reason of the request, it can be said that there was a response of 75,00% for "request for comment", whereas a requested "expert interview" only had a response rate of 23,53%, as can be seen within Table 3.5. Nonetheless, these numbers must be taken with caution as the sent requests did vary for each person and further were not sent on the same day but based on necessity and demand.

3.5.3 No-Log Policy ProtonVPN

In Chapter 3.2 it was discussed which VPN service to use best. Even though the decision fell on ProtonVPN, there are some downsides. To be precise, the No-Log Policy makes false statements, as shown below. On the one hand, the ProtonVPN No-Log Policy states that neither "IP addresses" nor "any location-based information" is logged, as can be seen within Figure 3.4. On the other hand, at the time[46] of conducting the research for Chapter 3.2, the ProtonVPN Privacy-Policy stated that "the timestamp of the last successful login is monitored in order to prevent brute force attacks" as can be seen in Figure 3.5. Besides the fact that through the very nature of brute force attacks, a massive number of unsuccessful login attempts are created, it is technically

[39] https://www.youtube.com/c/DeLadysigner/about
[40] https://www.verwaltung.steiermark.at/cms/ziel/74837988/DE/
[41] https://techlore.tech/contact.html
[42] https://inteltechniques.com/contact.html
[43] Bundeskriminalamt - Criminal Intelligence Service Austria
[44] https://twitter.com/colton_potter
[45] https://9gag.com/u/tomcuttingedge
[46] Around March 2020.

impossible to prevent brute force attacks by looking only at the last successful login. Hence, logging only the last successful login and indicating that only this value is used would make a system blind to the fact that a brute force attack generates numerous amounts of attempts. Furthermore, when the attacker's attempt gets logged because it was a "successful" login, it would imply that the attacker is now in full control over the account. As this made me curious, the ProtonVPN-Support was contacted with a request for comment on this matter because these facts stand in conflict with the Privacy-Policy and the No-Log Policy.

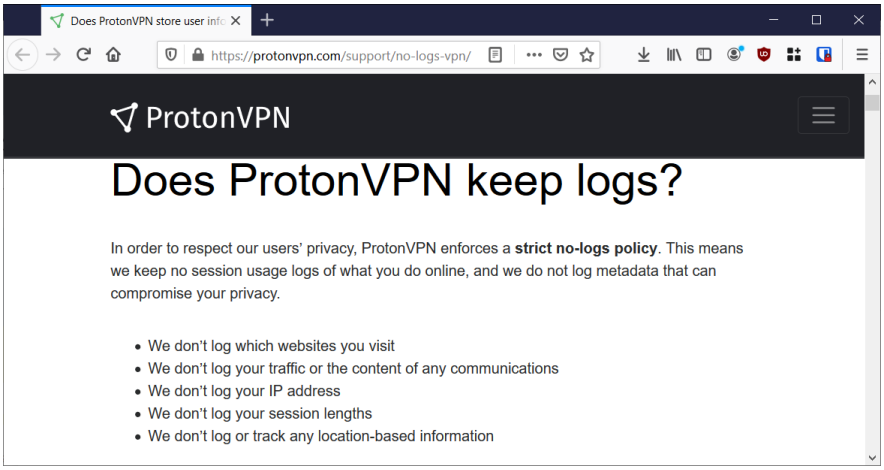


Figure 3.4: Shows the No-Log policy of ProtonVPN. (Proton Technologies AG, 2021)

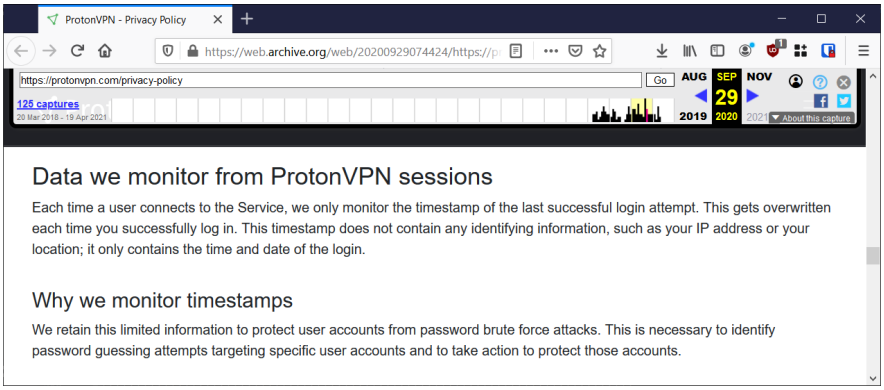


Figure 3.5: Shows the Privacy-Policy of ProtonVPN Version: March 11th, 2020. (Proton Technologies AG, 2021), (Internet Archive, 2021)

Eventually, after some conversation via Email, ProtonVPN made clear that the user may look at their timestamps through their own account. It is unclear whether ProtonVPN has access to those timestamps or not. However, any server-side "brute force prevention" system would need access to those or similar timestamps. Keeping this aside, a closer look at the logfiles mentioned in the statement[47] as seen in

[47] The full correspondence can be found within the Appendix B.

Figure 3.6 is taken. As can be seen within Figure 3.7, the current IP address is *85.206.163.147* and is situated in Šiauliai, Lithuania. It needs to be taken into account that the router was configured as described in Chapter 3.1, in a way to access the VPN network via the OpenVPN software within the router. The router is also set to access a random country server on each reboot and is scheduled to reboot every day at 3:00 AM. Hence, this address shows the current IP. As can be seen within Figure 3.9 this IP address is logged during a login through the webpage. It is also common knowledge that the IP address can be used to locate a system. Given these facts, ProtonVPN does indeed log the IP address and therefore does log a form of location-based information. This stands in direct conflict with two points of the No-Log Policy as shown in Figure 3.4, namely

- We don't log your IP address
- We don't log or track any location-based information

During the master's thesis research, the decision in favour of ProtonVPN was taken early on, 29th of May 2020, and is actively used since then. However, the logs seem not to go further back than approximately two months, as can be seen from the complete log export in Figure 3.8. Interestingly, the logs do not show any of the connections respectively logins conducted via OpenVPN service from the router. In the case of the test setup for this master's thesis, the reboot and further connections to the VPN takes place each day at around 3:00 AM.

In the meantime, ProtonVPN updated their Privacy-Policy and removed the section where brute force prevention[48] is used as reasoning for the collection of timestamps. Those timestamps respectively log entries are viewable by the user themself within the security settings of the user account, as it was clarified by the statement of ProtonVPN (See Figure 3.6). In the end, ProtonVPN still offers a great service and the logs that are kept and used are beneficial for users against malicious attacks. However, the aforementioned facts need to be clarified within the Privacy-Policy and especially within the No-Log Policy, or the authentication logs should be disabled per default (Figure 3.9 shows that this would be possible).

The complications of the logfiles and stored IP addresses clearly exceed the Privacy-Policy. However, in defense of ProtonVPN it cannot be said with certainty what the default settings during the account creation, respectively the upgrade of the same on 29th of May 2020, was. For this reason, a new and plain account was created

[48] See Figure 3.5.

From	To	Date
contact@protonvpn.com	Stefan.Kutschera@edu.fh-joanneum.at	21.Jul.2020 05:26 PM
Re: AW: AW: AW: Fw: Privacy Policy - Monitoring of Timestamps / VPN-Server Documentation		

Hello Stefan,

Thank you for the follow-up and my apology for the delay.

Regarding your questions:

(a) What information is stored for a -failed- login?
-Depends on the user's authentication logging setting. If off, nothing is stored. If basic, the failed login attempt, timestamp, and client. If Advanced, all the previous stuff and the IP used in the attempt. This can be moderated in the ProtonMail account settings > Security > Authentication logs

(b) For how long are those -failed- login attempts logs stored?
-As long as the user has logging enabled. If you turn it off, that deletes the old logs (to prevent someone from turning it off and back on and therefore generate an incomplete log record).

(c) please attach some sample data of failed login attempts for my very own ProtonVPN account ***redacted*** (Please find Documents of Account-Ownership attached to this mail)
-This can be done by your side. You will need to log into the ***redacted*** ProtonMail account > select Settings > Security > Authentication Logs.

We look forward to your reply.

Have a nice day!

Regards,
Robert

The ProtonVPN Team

Figure 3.6: Statement out of the correspondence with ProtonVPN in regards to my request for comment.

on 18th of May 2021 to check the default log settings. A screenshot of the security settings shows that "Basic" was the default log setting. The logs (see Figure 3.10) stand strongly in conflict with the response[49] of ProtonVPN from 08th of June 2020, 11:41AM and 10th of July 2020, 02:01PM (latter response can be seen within Figure 3.11) as the timestamp was not overwritten on the next successful login. As a matter of fact, the successful as well as the, on purpose created, failed login attempts are kept.

[49] For transparency the complete correspondence can be found within the Appendix B.

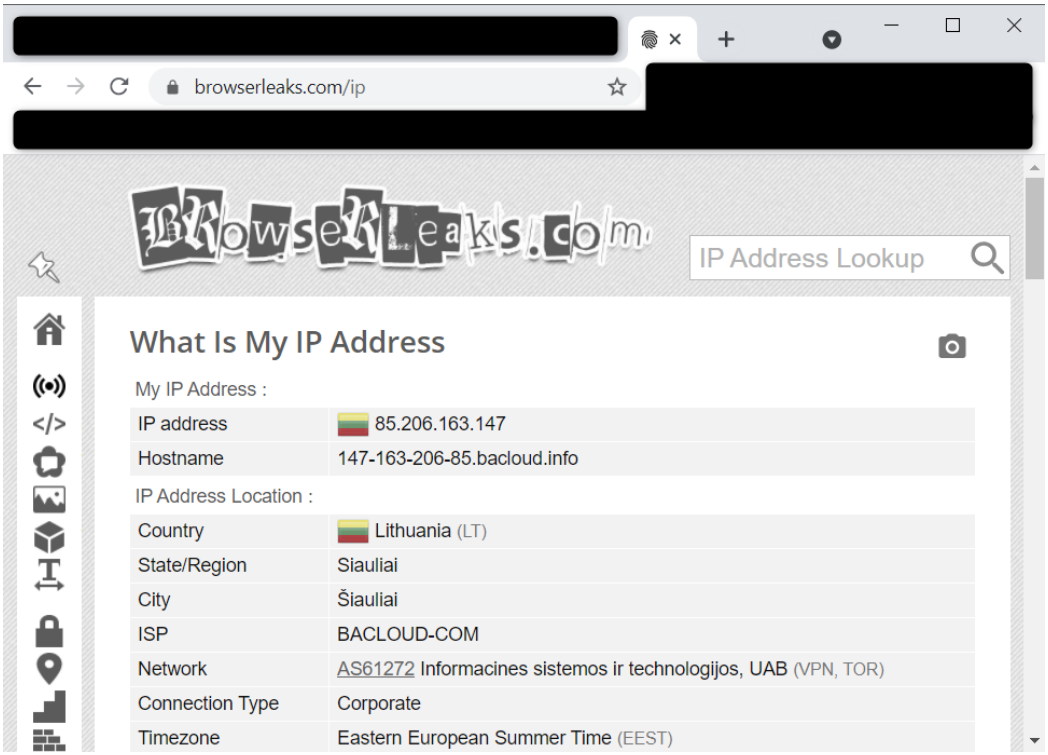


Figure 3.7: Shows the current IP address which is obtained through the router with an active VPN connection.

150	1	Sun Feb 28 2021 14:59:39 GMT+0100	62.112.9.166	28.04.2021	14:59:39
151	4	Sun Feb 28 2021 14:59:31 GMT+0100	62.112.9.166	28.04.2021	14:59:31
152					

Figure 3.8: Last entries from the export of all logs as of 26th of April 2021.

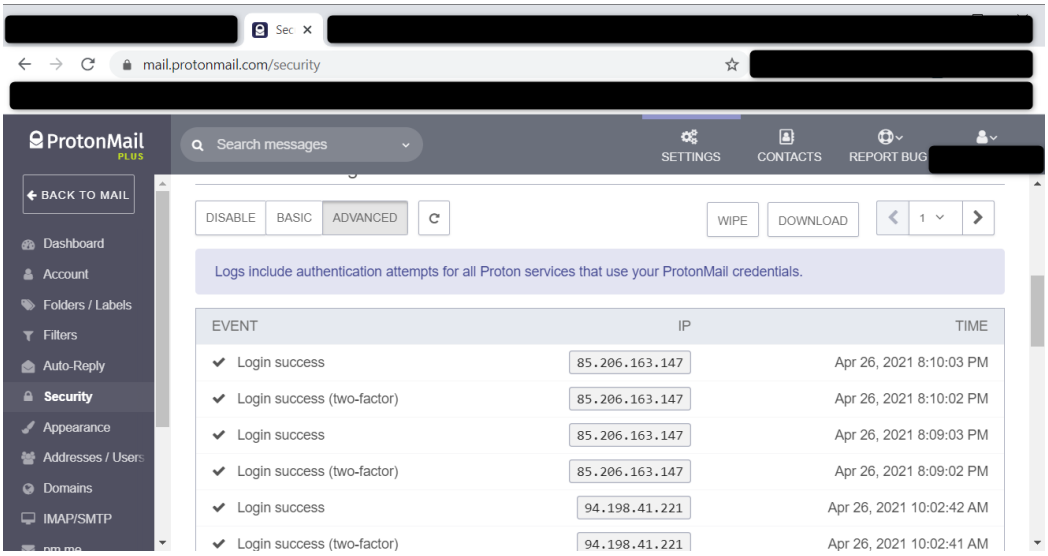


Figure 3.9: Authentication logs as mentioned in the statement of ProtonVPN.

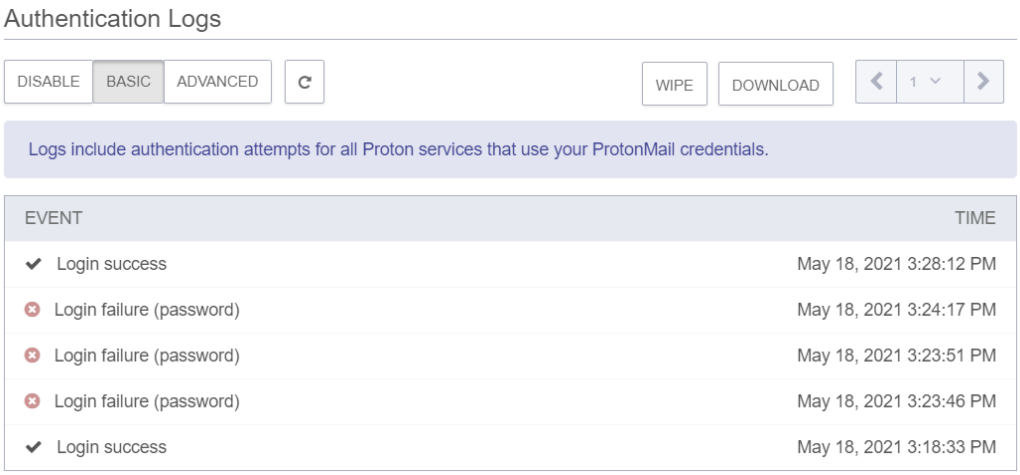


Figure 3.10: Authentication logs of a newly created, thus plain account, with several correct and failed logins, that stand in contradiction with the statement of ProtonVPN as can be seen in Figure 3.11.

From	To	Date
contact@protonvpn.com	Stefan.Kutschera@edu.fh-joanneum.at	10.Jul.2020 02:01 PM
Re: AW: AW: Fw: Privacy Policy - Monitoring of Timestamps / VPN-Server Documentation		

Hello Stefan,

Thanks for replying.

ProtonVPN does not log any of our users' activity, IP addresses, or DNS requests. Our server responsible for authentication retains a timestamp whenever a user connects, which is overwritten with each login.

This timestamp does not contain users' IP address, location any other identifiable information and it is done only as a security measure in order to protect accounts from brute forcing.

I hope this clarifies the situation.

If you have any additional questions, please let us know. We would be happy to help.

Have a nice day.

Kind Regards,
The ProtonVPN Team

Figure 3.11: One response of the correspondence with ProtonVPN stating that logs do not contain a users IP address and that each successful login shall overwrite the previous timestamp.

3.5.3.1 Summary Logging ProtonVPN

To summarize,

a) ProtonVPN was contacted to clarify the Privacy- and No-Log Policy and was asked to hand out stored timestamps respectively log entries. (See Appendix B)

b) The response was to gather the timestamp by one self from "ProtonVPN account > Settings > Security > Authentication Logs". (See Figure 3.6)

c) The evidence showed that ProtonVPN does in fact collect the user's IP addresses alongside the timestamps[50]. (See Figure 3.9)

   (i) The IP address can be seen as localisation data. (See Figure 3.7)

d) Timestamps with log setting "Advanced" and "Basic" contains numerous entries which seem to delete after approximately 2 months[51]. (See Figure 3.8, 3.9 and 3.10)

   (i) According to the response of ProtonVPN only the last successful login is stored. (See Figure 3.11)

   (ii) On the contrary, according to another response of ProtonVPN, the logs are kept as long as the user has it enabled[52]. (See Figure 3.6)

e) Also it is unclear, how the collection of the very last - successful - timestamp can be used to prevent Brute-Force attacks[53]. (See Figure 3.11)

Log-Setting / Collected data	Disable	Basic	Advanced
IP address	No	No	Yes
Timestamp	No	Yes	Yes
Overwritten by last successful login	n.a.	No	No

Table 3.6: Shows which information is stored for a specific ProtonVPN setting.

[50] IP addresses are only collected during "Advanced" logging, it cannot certainly be said whether this was the default setting or not at the time of creation around May 2020. However, as of today, newly created accounts have "Basic" logging as a default setting which does not collect user's IP addresses.

[51] The deletion time was not investigated further, the evidence suggests that after two months the timestamp respectively log-entry is deleted.

[52] Yes, this statement stands in direct conflict with the response from 10th of July 2020 as shown in Figure 3.11.

[53] As stated earlier, by the definition of Brute-Force attacks it is impossible to prevent such events by only collecting successful logins.

Despite the evidence that the ProtonVPN Privacy Policy is not in alignment with current logging processes, ProtonVPN is still favourable. The rather simple request to clarify the timestamps took much back-and-forth; in addition, the responses themselves were conflicting.

***My personal assumption**, which I have no clear evidence for, is that ProtonVPN might have 2 logging mechanisms in place. On one side, the authentication server of ProtonVPN, respectively their systems, stores and processes the - failed - logins in order to prevent brute force attacks. On the other side, authentication logs that solely lie in the user's hand and are stored within the users' account. If my assumption is valid, then I personally think that the responding employee of ProtonVPN did not read all the ongoing conversation within the emails and therefore only responded to my newest response. One was thinking I am talking about the user stored authentication logs, whereas the other responding employee might have thought I wanted to know more about the server-based brute force authentication logs. Another assumption is that we simply had issues understanding each other as English is neither an official language in Austria nor in Switzerland.*

In any case, it seems that ProtonVPN may need to either clarify their logging policy, change the default setting to "Disabled" or remodel the authentication/timestamp service.

Chapter 4

Conclusion and Outlook

This chapter concludes the results of this master's thesis in a comprehensive manner. Further, a guideline on the most relevant security measures for social media posts is created out of this research in Chapter 4.1. The overall awareness about the master's thesis topic and interaction are summarized. Last but not least, the research questions from the beginning of this thesis in Chapter 1.2 are answered within Chapter 4.3.

4.1 Security Measures

This chapter will discuss best practices enhancing one's privacy as it summarizes best practices found during the research of this master's thesis. However, also situations are discussed that might reveal or verify the physical position. On the one hand, the identification of a physical location starts by having no exact address to look for, as it was discussed in Chapter 1.6.1 and Chapter 1.6.2, but posted social media content, including incidental data, might reveal the exact physical location, thus identify the home address. On the other hand, a physical location has already been identified and incidental data is used to verify whether the information of the exact physical location is correct. Both steps can be used separately or, depending on the case, in sequence. Hence, the exact physical location is first extracted from the incidental data and verified in a second step against other incidental data.

4.1.1 Incidental Data Usages

Following two comprehensive examples on address identification and verification based on incidental data in social media posts. Whereas both methods may be used separately, they may also be used to first identify an address and further verify an address.

4.1.1.1 Identification of a physical location

As mentioned above, at the start of this step, no knowledge of the address exists yet. In Chapter 1.6.1, a video in which a person shows a severe storm approaching their home was discussed. To emphasise the storm's severity, a video sequence of the sky and a weather app is shown. The video illustrates that showing the sky and surroundings of one's home can reveal the address. Further, showing the weather app revealed the GPS location marker on the local map present in the app. A collage of the process can be seen in Figure 4.1.

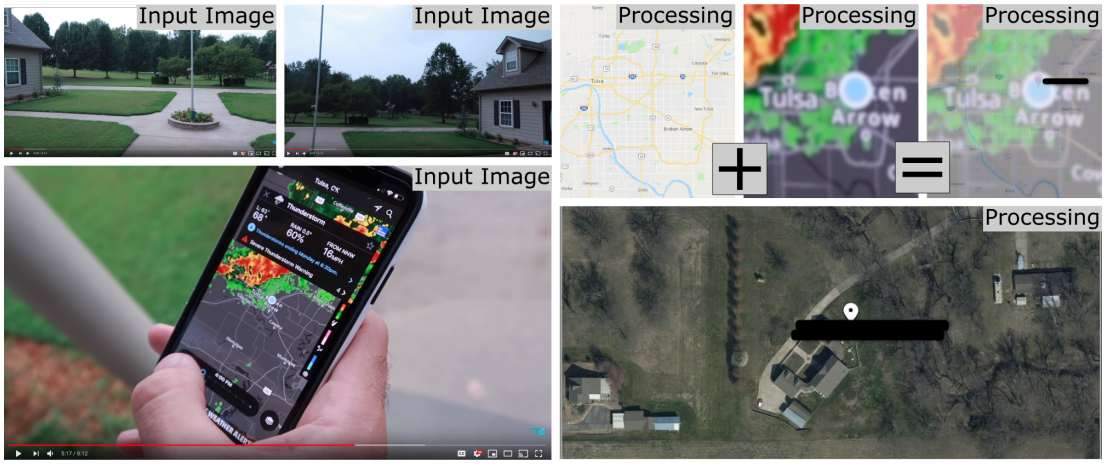


Figure 4.1: Images from a social media post that were used and processed to identify a location. (Google Maps, 2021a) (Youtube, 2021)

4.1.1.2 Verification of a physical location

In contrast to Chapter 4.1.1.1, where one extracts the address solely out of a picture or video sequence, the following shows an example of using a screenshot from a video sequence to verify a physical location. In such cases, one uses satellite images or the Google Street View service on the address to search for further hints and details. For example, Figure 4.2, shows a person using a smartphone. However, visible is also the ceiling and the general structure/colour of the neighbour's roof, the pipe of the rain drainage, and the white post standing horizontally outside. In addition, the hand railing and structure of the railing post, as well as the vegetation make it possible to verify a location with a high amount of certainty.

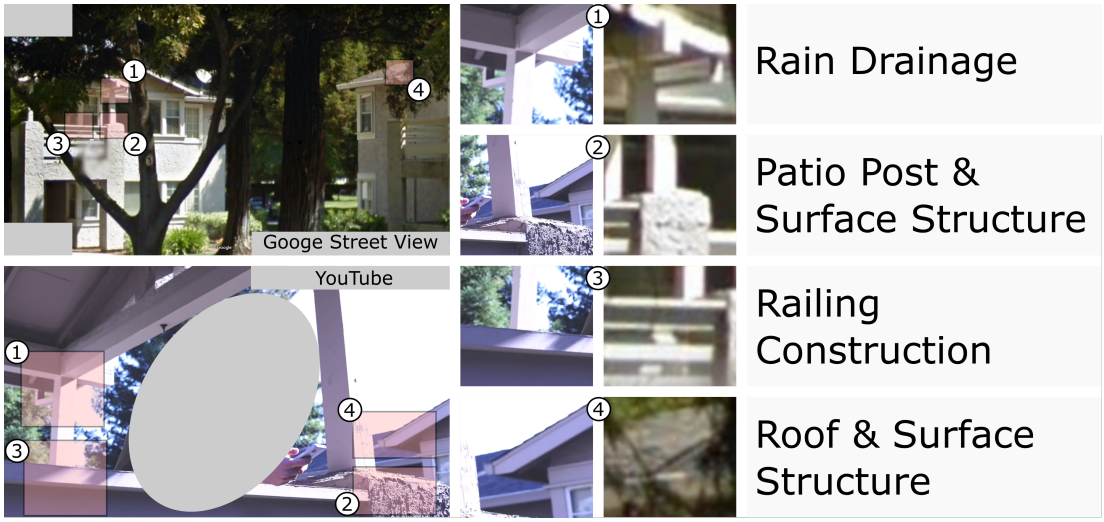


Figure 4.2: Matching features from a social media post compared with Google Street View to verify an address. (Google Maps, 2021a) (Youtube, 2021)

4.1.2 Summarized Security Measures

The following shows a summary of best practice measures to improve ones' online security and privacy behaviour. Even though the implementation of those measures can enhance ones' security and privacy, they might not be applicable for everyone. However, keep in mind that those measures also count when one is at someone else's location.

1. Avoid posting content that includes house numbers and/or street names.
2. Be on the lookout for reflections in mirrors as well as on surfaces such as cars, windows, vitrines, glasses, sunglasses or watches.
3. If any, post content of vacations only afterwards.
4. Avoid repetition of vacation respectively absent times, such as "during new years eve I am - always - on a one week trip".
5. Posts should be in accordance to a single time zone regardless of a currently temporarily diverting one.
6. Avoid posting any information from parcels or letters, such as tracking number, full address, names or QR codes.
7. Don't post ID's such as driver's license, personal ID, credit- or debit card, et cetera.
8. Avoid posting scenes that include location-based map materials, such as navigation maps, weather- or fitness apps, et cetera.

9. Close all curtains or post content where no windows are visible.
10. Try tilting the camera angle as low as possible when showing the own property.
11. Be aware that shadows or the sun's position can also hint additional information about the location.
12. Don't share fitness routes that start and/or end at your home location.
13. Don't share information of your own or surrounding WLAN/WiFi SSID's[1]

4.2 Awareness

During the research conducted in this master's thesis it was possible to show that some people had disclosed their residential address through incidental data posted unintentionally on social media alongside the primarily shared content. It was also possible to show that such self-conducted disclosure of incidental data, which contains a lot of personal data, does affect not only a single person but also television companies and online security experts. An uncomfortable amount of information was found of Mr. Troy Hunt, a well-known member within the online security area and founder of HaveIBeenPwned.com. Sadly, Mr. Troy Hunt was not available for comment. Hence the root and intentions of his postings, see Chapter 1.6.2 will remain unanswered within this master's thesis. In conclusion, this shows that the sharing of unintentional disclosed-, thus incidental-, data can also happen to persons who have either a security background themselves or a security team around them respectively within the production. Surprisingly, Kutschera, 2020, found out that people who publicly complained about being stalked and/or have gotten fake governmental calls in the past have shown a growth in awareness, resulting in further restricting information about their whereabouts. Sadly, despite their previous bad experience with stalkers, it was still possible to geolocate their whereabouts from newly posted content.

As mentioned, the incidental data found related to Schmid, 2019, was revisited and a report of the process alongside a letter was sent to the official email address of the Austrian Federal Chancellery on Tuesday 30th of April 2020. After only three days on 3rd of May 2020, a response was received and a meeting scheduled. The meeting was held on 19th of June 2020 with the Policy Advisor for cybersecurity to the Federal Chancellor Sebastian Kurz, Dr. Bernd Pichlmayer, E.M.B.L.-HSG. The content of the meeting is considered confidential. Nonetheless, I received support in the form of resources and knowledge of experts from the Criminal Intelligence Service

[1] https://wigle.net/

Austria[2], which was very valuable and supported the idea of this master's thesis, see also Chapter 3.4.7. The reaction from the Austrian Federal Chancellery, especially Dr. Bernd Pichlmayer, shows that potential delicate matters are handled quickly and effectively as the detailed report allowed to restrict access to newly found data (Kutschera, 2020). Undoubtedly, the role of Public Watchdogs is significant (see Chapter 2.6.1), but one must also give affected persons or organisations time to react and handle incidental data themselves to prevent more people from gathering the evidence.

4.2.1 Non responses

As described in Chapter 3.5, owners of various social media channels were contacted through their official business email listed on their dedicated about or contact pages. Sadly, as of today[3], a vast majority did not respond to the requests out of this master's thesis in any way (See Chapter 3.5.2). It may be important that none of the sent emails included any found incidental data in order to prevent a breach resulting from this research. The decision to enhance security might have led to the belief that the sent email was a scam or phishing attempt. No one was ever contacted more than two times. In some cases, a response would have been very beneficial and clarifying as for example with Mr. Troy Hunt. Mr. Troy Hunt was contacted through his official email address from his website[4] on 5th of April 2020 and again on 15th of November 2020. Even though the email was in accordance with the provided guideline on his website on "how to get a response", no response was received as of today[5]. As written in Chapter 2.2.2, getting no response at all could mean the found incidental data might not be valuable to him and that he is already aware of it. However, his intentions behind posting pre- and ongoing vacation updates on social media as well as other content that contained incidental data remain unknown.

[2] Criminal Intelligence Service Austria in German language "Bundeskriminalamt Österreich".
[3] June 7, 2021
[4] https://www.troyhunt.com/contact/
[5] June 7, 2021

4.3 Conclusion

The conducted interviews show that incidental data can be of danger and an ominent[6] threat (See Chapter 3.4.2). However, the interview with Dr. Ries Bouwman has shown that it is necessary for entrepreneurs to protect themselves by looking up former untrustworthy business partners' names and using information services like the "Gewerbe Informationssystem Austria" GISA, which has a very low barrier to access. Sadly many interview requests were not answered at all; however, the reason why those requests were not answered is not discussed within this master's thesis. Nonetheless, it was possible to gather incidental data of Mr. Troy Hunt, known for the service HIBP[7] (See Chapter 2.2.2). In my opinion, Mr. Troy Hunt is a role model for many people in terms of online security and should lead by good example. I was quite surprised when I saw him in my Twitter feed announcing an upcoming(!) 9.000 km road trip through Australia, also providing an itinerary. (See Figure 1.18). What surprised me even more were his regular updates that included the geolocation (See Figure 1.20-1.21).

4.3.1 Answering of Economical Related Research Question

All things considered, the economic research question related to this master's thesis can be answered as follows:

- *To which extend is the gathered information valuable to a criminal individual or organization?*

The economic value for a criminal individual or organization is low, as there is no market for such incidental data (See Chapter 2.3). Nonetheless, there is a chance that such information gathering is provided as a service, thus "Crime as a Service". However, the research made evident that incidental data may have a negative impact on a persons' life, such as repair bills after a burglary or, worse, reputation damage or the loss of a job (See Chapter 2.3).

[6] According to Oxford Dictionary "ominent" is not an english word. However, Google Ngram shows that it was used in the past https://books.google.com/ngrams/graph?content=ominent. Moreover, "ominent" is suggested as a new word on Collins Dictionary and described as following: "Adjective - something (such as an event) that is both ominous and imminent", see https://www.collinsdictionary.com/submission/444/ominent.

[7] haveIBeenPwned.com

4.3.2 Answering of Legal Related Research Question

All things considered, the legal research question related to this master's thesis can be answered as follows:

- *What is the legal aspect of unveiling personal information found in videos?*

During examining a fictive case scenario, it turned out that violation of several Terms and Conditions are done. However, considering the *freedom of science*, it will be without consequences for this research. In contrast, even though the person themself posted the information used for geolocation, it would violate Art.8 ECHR (Right to respect for private and family life) and not withstand a balancing between Art.10 ECHR (Freedom of expression) as discussed in Section 2.6. Moreover, the Austrian law § 365e Gewerbeordnung 1994 (Trade Code) has a measure to protect the private details of business owners since interested persons must provide a legitimate interest before receiving information about business owners. However, for small businesses who have the same private address as their business address this measure fails. For this I propose a change of § 365e Gewerbeordnung 1994 (Trade Code), see Chapter A, to implement when the private address matches the business address, the business address - must - be protected by the proof of legitimate interest. The implementation would be as simple as to identify each request using the same mechanics as used for implementing Regulation EU 2014/910 (eIDAS), hence the qualified electronic signature[8]. As a result, the address of SME business owners would be easily available with the comfort of using the digital signature to authenticate. This eliminates fraud yet enhances privacy without making the process complex since the infrastructure already exists.

4.3.3 Answering of Technical Related Research Question

All things considered, the technical research questions related to this master's thesis can be answered as follows:

- *What are the possibilities to extract incidental data that either identifies or verifies a home address within maximal 2 hours using OSINT methods?*

This master's thesis has shown that for several interview partners it was possible to extract their home addresses within a 2-hour search. Further it was possible to uncover more information using the extracted home address and other information like the property number to gain access to information about telephone numbers or family relationships respectively constellations. This was archived by using posted pictures

[8] also known as "Handysigantur'.

from their social media profiles and look for identifying features, such as GPS pointers on a map, house numbers, unique buildings near their home uncommon landscapes. In some cases the gathered incidental data within the used screenshots were reflection of surfaces showing identifying features of the surrounding. The used method of scanning social media profiles is a part of OSINT, were free available data is used to support investigations as described in Chapter 2.2.

- *What are technical options to blur a trace when exploiting and selling the gathered information?*

As shown in Chapter 3.1, it is possible to use a VPN-Service provider in order to connect with the Tor network in order to gain anonymity. Furthermore, the measures taken should also involve an empty device without a harddrive and privacy enhanced operation systems like TailsOS. A further layer of protection is to use publicly free available internet access where there are no camera surveillance is present.

4.4 Outlook

This master's thesis has shown that social media postings containing incidental data, thus information that was not intentionally posted, happens on various platforms among various people with different backgrounds. The danger of incidental data shall not be overseen as it can impact one life financially, physically or psychologically. As next step, the proposed change of law, as discussed in Chapter 1.5.2 and shown in Appendix A shall be implemented. Additionally, informational awareness campaigns shall educate people to give them the possibility to, if desired, enhance their very own privacy. From a technical perspective, it would be interesting to try to extract incidental data by using artificial intelligence. This extraction might also involve feature matching, as shown in Figure 4.2.

Appendix A

Proposed Change of Law

Following a transcription of the submitted proposed change of law as shown on the next page aims to strengthen privacy throughout SME's.
According to Section 365e(1), data of business owners under paragraph 365a(2)(1) to (8) and Section 365b(2)(1) may only be disclosed to information seekers if a legitimate interest can be substantiated. However, if a business owner has such a small business that the location of the business is situated at his residential address, the protection of his residential address is no longer fully given. Information seekers can access this data in vast quantities via the online GISA query without any protective mechanism. In conjunction with satellite image services, it is easy to determine whether the location of the business is also the residential address. It would therefore be advisable to allow the business owner to opt-in this information ("Privacy by Design", Art. 25 GDPR). In other words, by default, a person requesting information must declare a legitimate interest, but the business owner has the option of releasing the authority from this protection of legitimate interest. A one-person company, which works mainly in the field, would therefore not run the risk of encountering stalkers in front of its own house/apartment. The likelihood of family members being harassed by such a stalker is also reduced.

An amendment to the Trade Code 1994, as listed below, would significantly improve the protection of the privacy and family life (Art. 8 ECHR)of business owners and their relatives in Austria without reducing the rights of third parties. No. 1 to 2 does not have to be adopted.

The Trade Code 1994 (Gewerbeordnung 1994 -GewO 1994), Federal Law Gazette No. 194/1994, as last amended by Federal Law Gazette I No. 65/2020, shall be amended as follows:

The following Paragraph 6 shall be added to Section 365e
(6) If the residential address (Section 365a(2)(4)) is the same as the address of the business license (Section 365b(1)(3)), the authority shall treat the address of the business license the same way as its residential address (Section 365a(2)(4)) and shall only provide information of it if the person requesting the information substantiates a justified interest in the information.

1. The business owner has the possibility to inform the authority informally at any time, to provide information on the address of his business license (§365b Paragraph 1 No. 3) to anyone, even without substantiate legitimate interest.
2. The notification of Section 365e Paragraph 6 No. 1 to the authority can be made orally, by telephone, telegraphic, in writing, by telex, by fax, by means of automated data transmission or in any other technically possible manner.

Anregung Ergänzung §365e, GewO 1994

Teilergebnis Masterarbeit Kutschera*

*geplante Veröffentlichung Juli 2021

Anmerkung: Im Einklang mit der GewO 1994 treffen maskuline Bezeichnungen für beide Geschlechter zu.

Gemäß § 365e Abs. 1 sind die Daten § 365a Abs. 2 Z 1 bis 8 und § 365b Abs. 2 Z 1 von Gewerbetreibenden, Auskunftswerbern nur bei Glaubhaftmachung von berechtigtem Interesse zu beauskunften. Hat ein Gewerbetreibender jedoch ein derart kleines Gewerbe, dass sein Standort des Gewerbes an seiner Wohnadresse bewilligt worden ist, ist der Schutz seiner Wohnadresse nicht mehr vollständig gegeben. Es ist Auskunftswerbern über die online GISA Abfrage ohne jeglichen Schutzmechanismus möglich, diese Daten in rauen Mengen abzugreifen. In Verbindung mit Satellitenbilddiensten ist es einfach festzustellen, ob der Standort der Gewerbeberechtigung auch die Wohnadresse ist. Es wäre daher anzudenken, dem Gewerbetreibenden ein Opt-In zu ermöglichen („Privacy by Design“, Art. 25 DSGVO). Sprich, standardmäßig muss ein Auskunftswerber berechtigtes Interesse kundtun, der Gewerbetreibende hat jedoch die Möglichkeit, die Behörde von diesem Schutz des berechtigten Interesses zu entbinden. Ein Ein-Personen Unternehmen, welches hauptsächlich z.B. im Außendienst ist, läuft somit nicht Gefahr Stalkern oÄ. vor dem eigenen Haus/Wohnung anzutreffen oder, dass Familienmitglieder von einem solchen Stalker belästigt werden. Klagszustellungen, Inkassoschreiben oder sonstige berechtigte Interessen Dritter können weiterhin durch ein Auskunftsbegehren mit Glaubhaftmachung von berechtigtem Interesse genüge getan werden.

Eine Ergänzung der Gewerbeordnung, wie nachfolgtend gelistet, würde den Schutz der Privatsphäre und das Familienleben (Art. 8 EMRK) von Gewerbetreibenden und deren Angehörigen in Österreich wesentlich verbessern ohne Rechte Dritter zu kürzen. Die Ziffern 1 bis 2 müssen dabei nicht zwingend übernommen werden.

Die Gewerbeordnung 1994 – GewO 1994, BGBl. Nr. 194/1994, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 65/2020, möge wie folgt geändert werden:

Dem §365e wird folgender Abs.6 angefügt

(6) Ist die Wohnanschrift (§365a Abs. 2 Z 4) dieselbe wie der Standort der Gewerbeberechtigung (§365b Abs. 1 Z 3), hat die Behörde den Standort der Gewerbeberechtigung gleich wie seine Wohnanschrift (§365a Abs. 2 Z4) zu behandeln und nur darüber Auskunft zu erteilen, wenn der Auskunftswerber ein berechtigtes Interesse an der Auskunft glaubhaft macht.

1. Der Gewerbetreibende hat jederzeit die Möglichkeit der Behörde formlos mitzuteilen, den Standort seiner Gewerbeberechtigung (§365b Abs. 1 Z 3) jedermann, auch ohne Glaubhaftmachung von berechtigtem Interesse, zu beauskunften.

2. Die Mitteilung über §365e Abs. 6 Z 1 an die Behörde kann mündlich, telefonisch, telegrafisch, schriftlich, fernschriftlich, mit Telefax, im Wege automationsunterstützter Datenübertragung oder in jeder anderen technisch möglichen Weise erfolgen.

Stefan Kutschera, BSc MSc
stefan.kutschera@edu.fh-joanneum.at

28. Sep. 2020

Appendix B

Statement

Following the statement of the Department 17, Office of the Styrian Provincial Government with respect to a request for comment on why the change in withdrawing of data access was made. In addition, the statement respectively correspondence with ProtonVPN can be found as well. In order to have a better overview of the conversations, they were transferred into a table format. Moreover, the personal information of the user account at question was redacted and marked as such.

AMT DER STEIERMÄRKISCHEN LANDESREGIERUNG

Das Land Steiermark

Abteilung 17

➔ **Landes- und Regionalentwicklung**

Kutschera Stefan

Referat Statistik und Geoinformation

Bearb.: Dipl.Ing.Dr. Rudolf Aschauer
Tel.: +43 (316) 877-4282
Fax: +43 (316) 877-3711
E-Mail: geoinformation@stmk.gv.at

Bei Antwortschreiben bitte Geschäftszeichen (GZ) anführen

GZ: ABT17-25947/2014-401

Graz, am 11.02.2021

Ggst.: Stefan Kutschera, FH Joanneum, GIS Kataster - Anfrage zu Eigentümer deaktivierung - Masterarbeit

Sehr geehrter Hr. Stefan Kutschera, BSc MSc!

Wie Sie richtig festgestellt haben, sahen wir uns gezwungen die Eigentümerabfrage eines vorzugebenden Grundstücks aus der Web-GIS Applikation des Landes zu entfernen, obwohl es beim Grundbuchsrecht zu keinen Änderungen gekommen ist.

Durch die Datenschutzgrundverordnung sowie vermehrte Anfragen wurde durch den Verfassungsdienst des Landes die Frage des Zugangs zu Grundbuchsdaten über das GIS Steiermark neu bewertet.

Der Grundbuchszugang ist weiterhin über die sonstigen bekannten Plattformen eingeschränkt öffentlich zugänglich.

Mit freundlichen Grüßen
Für die Steiermärkische Landesregierung
Der Abteilungsleiter

Dipl.-Ing. Harald Grießer
(elektronisch gefertigt)

EMail Correspondence with ProtonVPN in a Tabularview

From	To	Date
Stefan.Kutschera@edu.fh-joanneum.at	security@protonvpn.com	01.Jun.2020 05:11 PM
Privacy Policy - Monitoring of Timestamps / VPN-Server Documentation		
Dear Sir or Madam, the Privacy Policy of ProtonVPN states that only the timestamp of the last successful login is monitored and stored. Also according to the privacy policy this is done in order to prevent brute force attacks such as password guessing. Therefore, I friendly ask for a more detailed technical description how the monitoring of the last -successful- login is used to prevent brute force attacks? Secondly, is there a technical documentation of the configuration on how the accessed VPN-server is configured and secured? Furthermore, I kindly ask for permission to refer to this email and your response in my masters thesis. I may publish a copy of it in the appendix of my masters thesis (If desired, with redacted names and email-address). best regards Stefan Kutschera, BSc MSc		

From	To	Date
contact@protonvpn.com	Stefan.Kutschera@edu.fh-joanneum.at	08.Jun.2020 11:41 AM
Re: Fw: Privacy Policy - Monitoring of Timestamps / VPN-Server Documentation		
Hello Stefan, Thank you for contacting us and my apology for the delay. ProtonVPN does not log any of our users' activity, IP addresses, or DNS requests. Our server responsible for authentication retains a timestamp whenever a user connects, which is overwritten with each login. This timestamp does not contain users' IP address, location any other identifiable information and it is done only as a security measure in order to protect accounts from brute forcing. We are not allowed to share the security settings and server configuration due to security reasons and this data is considered sensitive. Have a nice day! Regards, Robert The ProtonVPN Team		

EMail Correspondence with ProtonVPN in a Tabularview

From	To	Date
Stefan.Kutschera@edu.fh-joanneum.at	contact@protonvpn.com	10.Jun.2020 11:41 AM
AW: Fw: Privacy Policy - Monitoring of Timestamps / VPN-Server Documentation		
Hello Robert, no worries, thank you for the response. As for the security settings, I was in hope of abstract concept, for instance how the separation of users is done, but I also understand that this is considered sensitive. As for the timestamp, from the Privacy Policy it is clear that ProtonVPN uses the timestamp against brute force attacks. Nonetheless, it is unclear how this is archived, especially by only collecting the last successful timestamp. May I rephrase that question: How is the last successful timestamp used to prevent brute force attacks. mit freundlichen Grüßen / best regards Stefan Kutschera, BSc MSc		
From	To	Date
contact@protonvpn.com	Stefan.Kutschera@edu.fh-joanneum.at	12.Jun.2020 02:44 PM
Re: AW: Fw: Privacy Policy - Monitoring of Timestamps / VPN-Server Documentation		
Hello, Thank you for replying. Regarding your question, we cannot go in depth with the explanation as this information is considered sensitive. For example, if there are too many failed login attempts, the account will be temporarily blocked in order to stop the brute-force attack. If you need any additional assistance/information, feel free to let us know. Have a nice day! Regards, Robert The ProtonVPN Team		

EMail Correspondence with ProtonVPN in a Tabularview

From	To	Date
Stefan.Kutschera@edu.fh-joanneum.at	contact@protonvpn.com	09.Jul.2020 03:39 PM
AW: Re: AW: Fw: Privacy Policy - Monitoring of Timestamps / VPN-Server Documentation		
Hello Robert, thank you for your answer. I'm afraid, I really have a follow-up question. In regards to your answer, I have to assume that in order to prevent brute-force attacks, failed login attempts are logged and saved. With this in mind I have two questions: a) What information is collected and stored for a failed login attempt and b) for how long are those failed login attempt logs kept? Thank you for your support, Stefan mit freundlichen Grüßen / best regards Stefan Kutschera, BSc MSc		
From	To	Date
contact@protonvpn.com	Stefan.Kutschera@edu.fh-joanneum.at	10.Jul.2020 02:01 PM
Re: AW: AW: Fw: Privacy Policy - Monitoring of Timestamps / VPN-Server Documentation		
Hello Stefan, Thanks for replying. ProtonVPN does not log any of our users' activity, IP addresses, or DNS requests. Our server responsible for authentication retains a timestamp whenever a user connects, which is overwritten with each login. This timestamp does not contain users' IP address, location any other identifiable information and it is done only as a security measure in order to protect accounts from brute forcing. I hope this clarifies the situation. If you have any additional questions, please let us know. We would be happy to help. Have a nice day. Kind Regards, The ProtonVPN Team		

EMail Correspondence with ProtonVPN in a Tabularview

From	To	Date
Stefan.Kutschera@edu.fh-joanneum.at	contact@protonvpn.com	15.Jul.2020 02:44 PM

AW: Re: AW: AW: Fw: Privacy Policy - Monitoring of Timestamps / VPN-Server Documentation

Dear ProtonVPN-Team,

thank you for responding.
Frankly, your response did not answer my recent question in any way.

I'm not interested in what is -not- collected. I'm very interested in what -is- collected. I totally understand, and it was already discussed with Robert from ProtonVPN(see conversation down below), that ProtonVPN collects only the last successful login to a user account according to the Privacy Poilicy.
Since my research on my master's thesis also includes VPN Service Providers, which you are, I read a lot of Privacy Policies. What I found very interesting was the Privacy Policy of ProtonVPN as it states the following:

Quote: "Data we monitor from ProtonVPN sessions
Each time a user connects to the Service, we only monitor the timestamp of the last successful login attempt. This gets overwritten each time you successfully log in. This timestamp does not contain any identifying information, such as your IP address or your location; it only contains the time and date of the login.

Why we monitor timestamps
We retain this limited information to protect user accounts from password brute force attacks. This is necessary to identify password guessing attempts targeting specific user accounts and to take action to protect those accounts."
Source : https://protonvpn.com/privacy-policy

Since it is technically not possible to prevent brute force attacks with only the last successful login timestamp I got curious what else, in connection with a ProtonVPN User-Account, is logged/monitored. (I admit that, since this is covered in my studies as well, I have a certain concept/approach in mind on how you may or may not deal with that) Do not get me wrong, it is a good thing that ProtonVPN has a "technique" to prevent brute-force attacks. However, If I'm mistyping my password, I'm suddenly also in these logs. Since "-failed- login attempt logs" are not covered within your Privacy Policy, I'm concerned what happens with that data directly connected to the user account (something has to be stored otherwise you would not be able to prevent brute-force attacks efficiently). As mentioned above, when I'm mistyping my password I'm suddenly as well stored in those -failed- login attempt logs. With that in mind please let me rephrase my questions:

(a) What information is stored for a -failed- login?

(b) For how long are those -failed- login attempts logs stored?

(c) please attach some sample data of failed login attempts for my very own ProtonVPN account ***redacted*** (Please find Documents of Account-Ownership attached to this mail)

I kindly ask you to read the full conversation down below before replying, since you only addressed the successful login timestamps so far.

mit freundlichen Grüßen / best regards
Stefan Kutschera, BSc MSc

EMail Correspondence with ProtonVPN in a Tabularview

From	To	Date
contact@protonvpn.com	Stefan.Kutschera@edu.fh-joanneum.at	21.Jul.2020 05:26 PM
Re: AW: AW: AW: Fw: Privacy Policy - Monitoring of Timestamps / VPN-Server Documentation		

Hello Stefan,

Thank you for the follow-up and my apology for the delay.

Regarding your questions:

(a) What information is stored for a -failed- login?
-Depends on the user's authentication logging setting. If off, nothing is stored. If basic, the failed login attempt, timestamp, and client. If Advanced, all the previous stuff and the IP used in the attempt. This can be moderated in the ProtonMail account settings > Security > Authentication logs

(b) For how long are those -failed- login attempts logs stored?
-As long as the user has logging enabled. If you turn it off, that deletes the old logs (to prevent someone from turning it off and back on and therefore generate an incomplete log record).

(c) please attach some sample data of failed login attempts for my very own ProtonVPN account ***redacted*** (Please find Documents of Account-Ownership attached to this mail)
-This can be done by your side. You will need to log into the ***redacted*** ProtonMail account > select Settings > Security > Authentication Logs.

We look forward to your reply.

Have a nice day!

Regards,
Robert

The ProtonVPN Team

Appendix C

Request for Comment

Following the sent request for comment to the US Army station “White Sands” which was left unanswered as of today[1].

[1] June 7, 2021

Request for literature/info/comments on EMP testing devices for usage in Master Thesis

Kutschera Stefan <Stefan.Kutschera@edu.fh-joanneum.at>

Mi, 27.01.2021 09:09

An: mailusarmy.wsmr.atec.mbx.team-white-sands@mail.mil <mailusarmy.wsmr.atec.mbx.team-white-sands@mail.mil>

Dear Sir or Madam,

I hope this E-Mail finds you well.

During a documentary video on YouTube[1] the impacts of an EMP as byproduct of a nuclear explosion are discussed. The video also states "White Sands Missle Range" as testing location which brought me to your homepage. As the video is 8 years old, technology might have evolved which is a reason why I'm contacting you.

In my Master's Thesis I discuss in a subchapter possible attack vectors and the threats to electronical security systems. Cutting the power would be one way but a more devastating and effective one would be sending an EMP in direction of the security systems eventually overcharge and destroy it. The shown EMP testing device has a range of 15 meters (50ft) but since then time has progressed. Thats why I wanted to ask experts on that matter.

My questions are:

- How difficult is it for "common-burglars" or a criminal organisation to build (or get hands on) an EMP emitting device that can be precharged.
- How advanced are those technologies nowadays (i.e. range, mobility, power, etc).
- Is it possible to precharge an EMP emitting device and release its impulse from a simple vehicle without destroying the electronics of the vehicle?
- Assuming a person is aware on how to build such device, what are the costs to build it?

I would be happy for any literature to refer to or comments I may publish in my upcoming Master's Thesis.

References:

[1] https://www.youtube.com/watch?v=kxi1DJUDxtQ

mit freundlichen Grüßen / best regards
Stefan Kutschera, BSc MSc
Student, IT-Recht & Management 2019
Alumni, IT & Mobile Security 2017
Alumni, Software Design 2014

LinkedIn: https://www.linkedin.com/in/stefan-kutschera/
GitHub: https://github.com/StefanKutschera
Twitter: https://twitter.com/StefanKutschera

Appendix D

Transcript

This chapter does not include all transcripts. All interviews were equally important and relevant, however, it was decided to include the interview[1] with Heimo Flechl, Head of the Unit, Open Source Intelligence and Crime Trends within the Criminal Intelligence Service Austria[2]. The interview was transcripted in the language the interview was held, namely German.

Stefan Kutschera: *So, die Aufzeichnung ist gestartet, ich hoffe die Aufzeichnung ist für Sie in Ordnung.*

Heimo Flechl: *Natürlich!*

Stefan Kutschera: *Super, vielen Dank, dass Sie sich heute Zeit genommen haben, dass wir ein kurzes Interview führen. Ich möchte gleich mit der ersten Frage starten. Möchten Sie kurz Ihre Tätigkeit bzw. die Tätigkeit Ihrer Abteilung im Bundeskriminalamt beschreiben, vor allem im Hinblick auf OSINT?*

Heimo Flechl: *Wie im Vorgespräch bereits erwähnt, leite ich seit 2018 das Referat Open Source Intelligence und Kriminalitätstrends. Im Wesentlichen beschäftigen wir uns mit dem Support von Ermittlerinnen und Ermittlern bei ihren operativen Ermittlungsfällen, das heißt, ein Ermittler hat irgendeinen Fall und erkennt aufgrund der Datenlage, da könnte ein OSINT-Spezialist etwas zum Ermittlungserfolg beitragen und er wendet sich dann an uns und wir kümmern uns dann quasi um den OSINT-seitigen Support für seine Ermittlung. Das ist der eine Part und der andere Part ist,*

[1] See Chapter 3.4.7

[2] German "Leiter des Referats für Open Source Intelligence und Kriminalitätstrends im Bundeskriminalamt"

natürlich gibt's auch immer wieder diverse Großlagen, wenn ich da kurz erinnern darf an die Griechisch-Türkische Grenze voriges Jahr im Frühjahr, da sind natürlich die Entscheidungsträger im Innenministerium auch sehr interessiert an raschen Monitoring-Informationen, sollte sich an der Lage etwas ändern, das ist der zweite Part. Also wir intern nennen den einen Part eben operatives Open Source Intelligence und das andere strategisches Open Source Intelligence. Das ist im Wesentlichen unsere Tätigkeit in a nutshell.

Stefan Kutschera: *Vielen Dank! Glauben Sie aus Ihrer Erfahrung heraus dass mittels OSINT-Methoden gesammelte Daten einen hohen Wert auf dem Schwarzmarkt haben, also speziell für Kriminelle?*

Heimo Flechl: *Ja, das ist eine sehr komplexe Frage. Wenn ich da beispielsweise an den Modus Operandi CEO Fraud denke, wo kurz zusammengefasst die Täter sich an Firmen wenden oder in erster Linie an die Buchhaltung von Firmen und vorgeben dass sie der jeweilige CEO sind und dringend eine Überweisung irgendwo hin benötigen unter Missachtung der Sicherheitsvorschriften die an und für sich üblich sind, dann ist es meistens so, dass diese Täter eben alle ihre Informationen die sie über das Unternehmen haben, vorab recherchiert haben und das sind im Wesentlichen OSINT Informationen. Da könnte man jetzt sagen, man könnte von dieser Seite herangehen und sagen, wäre dieser Modus Operandi überhaupt möglich wenn das Unternehmen zum Beispiel keine Website hätte. Und dann könnte man sich darüber Gedanken machen das irgendwie mit einem Wert zu unterlegen. Eine andere Sache wäre auch wenn ich sage: ich finde wesentliche Informationen über Personen des öffentlichen Lebens raus die eventuell inkriminierend sind oder zumindest extrem peinlich. Das sehen wir auch im Bereich Ibiza-Video, da handelt es sich zwar nicht um OSINT Informationen, aber offensichtlich dürfte das ja doch einen gewissen Schwarzmarkt-Wert aufweisen. Aber ansonsten ist der Wert relativ schwer zu beziffern, also wirklich auf eine Zahl runterzuskalieren. Es kommt immer aus meiner Sicht auf den jeweiligen Einzelfall an um zu bewerten, hat diese Information überhaupt einen Wert und wenn ja, welchen.*

Stefan Kutschera: *Dazu könnte man dann eigentlich Crime as a Service sagen*[3]*, was mich genau in die nächste Frage bringt: Was genau ist Crime as a Service und was kann man sich darunter im digitalen Bereich vorstellen?*

Heimo Flechl: *Crime as a Service ist etwas das wir seit einem guten Jahrzehnt*

[3] corrected, original spoken text was not understandable: *"Das würde eigentlich dann zu sagen, man könnte das dann als Crime as a Service"[sic]*

beobachten. Es ist im Wesentlichen, wie schon der Wirtschaftswissenschaftler Adam Smith damals vorgeschlagen hat, Prinzip der Arbeitsteilung und da geht's darum, dass die IT-Welt schon so komplex geworden ist, dass nicht eine Person mehr alles machen kann. Also wenn man sich zum Beispiel einen Angriff mit einem Netbanking-Trojaner vorstellt, dann gibt es eben eine Person, die entwickelt einmal grundsätzlich den Trojaner, weil die ist eben gut im Programmieren von Schadsoftware. Und die Person bietet dann das Service, diesen Trojaner, zum Kaufen im Darknet an. Dann eine weitere Person, die der Meinung ist, es wäre eine gute Idee Geld zu verdienen, mit so einem Netbanking-Trojaner eine breite Masse an Menschen zu betrügen. Und die kauft dann diesen Service, also diesen Trojaner von dieser einen Person und überlegt sich dann, wenn ich dann die mobilen Endgeräte oder die elektronischen Endgeräte meines Opfers infiziert habe, dann kann ich zwar souverän die Überweisung starten, aber ich brauche dann ja auch noch jemanden der mir das Geld wäscht. Weil wenn ich das direkt vom Opferkonto auf mein Konto überweise, dann wird relativ zügig die Polizei bei mir anklopfen. Das heißt, ich schaue dann weiter in den diversen Darknet-Foren und schaue, gibt es jemanden, der für den geographischen Raum Mitteleuropa Geldwäsche anbietet und dann nehme ich mir den noch dazu. Das wäre so kurz zusammengefasst die Crime as a Service Lage die wir im Darknet beobachten, am Beispiel eben so einer Netbanking-Infektion, das hat aber natürlich eine ganz viel weitere und größere Skala. Es gibt viele viele Einzelbereiche wo Personen eben ihre kriminellen Leistungen im Darknet anbieten, aber kurz zusammengefasst ist es so, dass ich sage die Welt ist mittlerweile so komplex, dass sich Spezialisten für einzelne Bereiche herauskristallisiert haben, auch eben im kriminellen Universum, und die bieten dann ihre Einzelleistungen zum Verkauf an und es gibt dann halt eine Person die diese Leistungen zusammenfasst und dann wirklich in ein vollendetes Verbrechen umsetzt.

Stefan Kutschera: *Vielen Dank! Das würde eigentlich sagen, wenn jemand seine Spezialität anbietet könnte er auch OSINT als Spezialität anbieten und die als Crime as a Service verkaufen. Wie würden Sie den Wert bzw. den Schaden bezüglich OSINT als Crime as a Service für den einzelnen Betroffenen bewerten.*

Heimo Flechl: *Da möchte ich anmerken, dass es aus meiner Sicht relativ schwierig ist, basierend auf OSINT Daten oder OSINT als kriminell zu bezeichnen, weil im Wesentlichen tut ein OSINT-Analyst, sei es auf der guten oder auf der bösen Seite, ja nichts anderes als sowieso öffentliche Daten zu sammeln und zu analysieren. Dann muss man sich die Frage stellen, ist das überhaupt kriminell. Das heißt, ich weiß nicht ob sich ein OSINT-Analyst im Darknet zur Verfügung stellt für kriminelle Zwecke, ist eine gute Frage, ob das überhaupt denkbar ist. Aus der persönlichen operativen*

Erfahrung ist es meistens so, dass die, die die Umsetzer der jeweiligen kriminellen Handlung sind auch die sind, die das recherchieren. Natürlich dann nicht auf diesem Niveau, auf die es ein professioneller OSINT-Analyst durchführen könnte, aber meistens so, dass es ausreicht um die kriminelle Handlung durchzuführen. Ich denke im Moment ist es eher so, dass man es so verkaufen würde im Darknet, dass ich sage, ich biete im Wesentlichen nicht die Leistung an sondern ich bin schon in Vorleistung gegangen und ich habe schon ein Ergebnis und jetzt verkaufe ich weniger die Leistung sondern mehr die Daten oder das Ergebnis meiner Analyse. Eben so wie bei einer vorigen Frage schon erwähnt, wenn ich zum Beispiel Daten habe die peinlich oder inkriminierend sind über Personen des öffentlichen Lebens. Und da rede ich jetzt nicht von Daten an die ich gekommen bin indem ich deren Rechner infiziert habe oder so, sondern wirklich Daten die frei verfügbar waren aber vielleicht nicht direkt für das durchschnittliche Auge sichtbar sondern über Anwendung diverser OSINT Methoden und Analyse Methoden die sich dann herauskristallisiert haben. Also die Frage ist auch wieder komplex, kann man nicht mit einer Zahl beantworten. Ich könnte mir aber gut vorstellen dass das von Jahr zu Jahr interessanter werden könnte, auch für diesen Bereich.

Stefan Kutschera: *Das bringt mich zur nächsten und abschließenden Frage: welche Maßnahmen würden Sie empfehlen um sich online hinsichtlich ungewollt veröffentlichter Daten besser zu schützen?*

Heimo Flechl: *Da gibt es auch mehrere Sphären, da kann ich einerseits reden eben wieder zurückkommend auf den Modus Operandi CEO Fraud. Da stehen die Unternehmen teilweise vor einer Entscheidung. Einerseits wenn ich gewisse Daten nicht online zur Verfügung stelle kann sich ein Kunde vielleicht ein weniger gutes Bild machen oder erreicht die jeweilige Person weniger gut, weil halt die Kontaktdaten dieser Person nicht mehr direkt verfügbar sind. Auf der anderen Seite steht dann der Schutz eben vor diversen kriminellen Aktivitäten. Also es hat natürlich die kommerzielle Firmendimension und dann gibt es auch noch die private Dimension, da kann ich im Wesentlichen nur empfehlen im Bereich der sozialen Medien sich sehr intensiv die Privatsphäreeinstellung vorzunehmen, durchzuarbeiten der jeweiligen sozialen Medien. Da kann man sehr sehr viel damit abwenden, dass ich sage im Wesentlichen gebe ich Daten, die doch eher privat sind, vielleicht nur an Personen raus mit denen ich in einer Freundschaftsbeziehung, beispielsweise auf Facebook, stehe. Dann kann man aber wieder einen Schritt weiter gehen und sagen, naja gut aber dann darf ich halt auch nicht jede Freundschaftsanfrage annehmen die ich so bekomme, sondern sollte ich mir überlegen, kenne ich diese Person überhaupt. Aber der Hinweis auf die Privat-*

sphäreeinstellung, die doch sehr weitführend sind in sozialen Medien, wäre grundsätzlich ein guter, aber natürlich wirklich sicher bin ich nur wenn ich überhaupt gar kein Profil habe. Das ist natürlich eine Entscheidung, die jeder für sich selbst treffen muss. Und grundsätzlich, wenn ich sage, die großen Datenkraken mag ich eh nicht aber ich mag schon ein Profil auf einem sozialen Medium haben um eben auch mit meinem Freundeskreis in Kontakt bleiben zu können, naja dann kann man ja vorab recherchieren, welche Daten werden vom jeweiligen sozialen Medium eigentlich gesammelt? Ich darf da an diesen Datenskandal eben von Facebook erinnern, Cambridge Analytica glaube ich hat der geheißen, dann wähle ich halt ein soziales Netzwerk, wo so etwas noch nicht vorgekommen ist. Das heißt jetzt nicht, dass die das nicht machen, aber zumindest behaupten sie, dass sie das nicht machen und es wäre auch noch nie an die Öffentlichkeit getreten. Also man bewegt sich da immer an einer Weggabelung, Sicherheit und Bequemlichkeit. Aber der Tipp für Privatpersonen grundsätzlich wäre: schauen Sie sich die Privatsphäreeinstellungen an, stellen Sie diese sehr restriktiv ein und wirklich sicher sind Sie nur wenn Sie kein Profil haben.

Stefan Kutschera: *Darf ich noch fragen nach Tipps bezüglich Postings zu Bildern und Videos, ob Sie da auch Tipps geben können für präventive Maßnahmen?*

Heimo Flechl: *Ja, da sind wir dann schon ein, zwei Stufen weiter. Da sagen wir die Personen hat ein Profil und die Person postet auch sehr viel und zwar nicht nur schriftlich sondern auch Bilder. Man sollte natürlich immer im Hinterkopf haben, auch wenn man selbst der Meinung ist, man postet jetzt ein Bild von sich selbst beispielsweise in seinen eigenen 4 Wänden und es kommt eh nur darauf an was man da gerade auf diesem Bild tut. Das mag so sein für 99% der Bevölkerung aber wenn sich ein OSINT-Analyst dieses Bild anschaut dann sieht er ganz andere Dinge auf diesem Bild als der durchschnittliche Nutzer. Der schaut sich dann eventuell an, gibt es vielleicht Hinweise auf ein Sicherheitssystem das irgendwo im Haus ist, kann ich vielleicht die Marke einer Alarmanlage erkennen oder erkenne ich dass vielleicht überhaupt keine Alarmanlage da ist oder wird das Foto, oder das Selfie wie es neudeutsch heißt, so geschossen, dass ich eventuell erkenne, wo diese Person wohnt, aufgrund dessen dass halt im Hintergrund aus dem Fenster raus ein anderes bekanntes Gebäude erkennbar ist oder sogar ein Adressschild. Und das verweist auch auf die Tätigkeit eines OSINT-Analysten. Man hat sehr sehr selten diesen einen Hinweis, der dann alles klärt sondern man handelt sich stückerlweise nach vorne und bei einem Bild habe ich vielleicht diese Information, die passt dann mit der Information aus einem anderem Posting oder Bild zusammen und so baut man sich dann langsam seine Indizienkette auf bis man schlussendlich zu einem Treffer kommt. Also auch hinsichtlich dem Posten von Bildern*

würde ich schon darauf verweisen, man sollte sich schon Gedanken machen was ist eigentlich sonst noch auf dem Bild zu sehen und es ist es eine gute Idee, das immer so zu posten. Natürlich hat man global den Eindruck, dass sich die Menschen darüber eher weniger Gedanken machen.

Stefan Kutschera: *Ich verstehe. Vielen Dank! Das bringt mich zum Ende. Ich bedanke mich für Ihre Zeit, es hat mich sehr gefreut.*

Heimo Flechl: *Gerne!*

Stefan Kutschera: *Ich werde die Aufzeichnung jetzt beenden.*

Appendix E

Ethics Self Assessment Test

This appendix exists almost entirely out of the questionnaire from the Ethics Self Assessment Test[1], which is often needed in order to get EU funding for scientific projects. As some questions of the questionnaire can be interpreted in one way or the other, there exists a step-by-step guideline from European Research Council Executive Agency, 2018. Even though some questions have absolutely no connection to the ethics within this master's thesis and on incidental data, like usage of human stem cells, the decision was made to include all the questions for the following reasons. Firstly, to get a complete overview of the questionnaire. Secondly, for anyone who might use this master's thesis, some questions might be valid for her or him. Thirdly, and most importantly, the overall aim of the self-assessment test is to review and answer all questions to cover blind spots that otherwise might have been skipped. Conclusively, it may seem unnecessary at a first look to transcribe and include all question in this master's thesis but on a second look the biggest mistake would be to skip an important question.

However, the questionnaire will be answered with respect to this master's thesis but will only scratch the surface. Conditional sub-questions that does not need to be answered will be filled with '- - -'

[1] https://erc.europa.eu/sites/default/files/document/file/EthicsSelfAssessmentStepByStep.pdf

E.1 Human Embryos

E.1.1 Does your research involve Human Embryonic Stem Cells(hESCs)?

No.

E.1.1.1 If YES: Will they be directly derived from embryos within this project?

- - -

E.1.1.2 If YES: Are they previously established cells lines? Origin and line of cells.

- - -

E.1.2 Does your research involve the use of human embryos? Origin of embryos.

No.

E.1.3 Does your research involve the use of human foetal tissues /cells?

No.

E.2 Humans

E.2.1 Does your research involve human participants? Please provide information in one of the subcategories below:

Yes. However, not in a physical matter, humans are involuntary involved by publishing publicly content onto social media accounts.

E.2.1.1 If YES: Are they volunteers for social or human sciences research?

No, not voluntary. If their public available content matches creteria its included in the research.

E.2.1.2 If YES: Are they persons unable to give informed consent?

Yes, they have no possibility to give consent.

E.2.1.3 If YES: Are they vulnerable individuals or groups? Details on the type of vulnerability.

Yes, there is a possibility that people of all ages, disabilities or special needs mentally as well as physically are included.

E.2.1.4 If YES: Are they children/minors?

Yes, there is a possibility that children or minors are within the research.

E.2.1.5 If YES: Are they patients? Details on the nature of disease/condition/disability.

No.

E.2.1.6 If YES: Are they healthy volunteers for medical studies?

No.

E.2.2 Does your research involve physical interventions on the study participants?

No.

E.2.2.1 If YES: Does it involve invasive techniques? Risk assessment for each technique and overall. Copies of relevant Ethics Approvals.

- - -

E.2.2.2 If YES: Does it involve collection of biological samples? Details on the type of samples to be collected. Copies of relevant Ethics Approvals.

- - -

E.3 Human Cells / Tissues

E.3.1 Does your research involve human cells or tissues? (Other than from 'Human Embryos/Foetuses' i.e. section 1)

No.

E.3.1.1 If YES: Are they available commercially? Details on cell types and provider (company or other). Copies of import licences (if relevant)

- - -

E.3.1.2 If YES: Are they obtained within this project? Details on cell types including the source of the material, the amount to be collected and the procedure for collection.

- - -

E.3.1.3 If YES: Are they obtained within another project? Details on cell types.

- - -

E.3.1.4 If YES: Are they deposited in a biobank? Details on cell types.

- - -

E.4 Protection of Personal Data

E.4.1 Does your research involve personal data collection and/or processing?

Yes, absolutely.

E.4.1.1 If YES: Does it involve the collection or processing of special categories of data (data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation)

Yes. However, the data was publicly provided by the person

E.4.1.2 If YES: Does it involve tracking or observation or profiling of participants? (profiling)

No.

E.4.2 If YES: Does your research involve further processing of previously collected personal data ('secondary use') (including use of pre-existing data sets or sources, merging existing data sets, sharing data with non-EU member states)?

Yes. This is one main techniques of the research to merge data from social media with Open Source Inteligence (OSINT) usabel platforms.

E.5 Animals

E.5.1 Does your research involve animals? Confirmation of compliance with relevant EU and national legislation.

No. Most likely not.

E.5.1.1 If YES: Are they vertebrates? Information as above. Documents as above.

- - -

E.5.1.2 If YES: Are they non-human primates? Information above plus:

- - -

E.5.1.3 If YES: Are they genetically modified?iv Confirmation of compliance with relevant EU and national legislation.

- - -

E.5.1.4 If YES: Are they cloned farm animals? Information as above Copies of all appropriate authorisations for the supply of animals and the project experiments.

- - -

E.5.1.5 If YES: Are they endangered species?

- - -

E.6 Third Countries

E.6.1 In case non-EU countries are involved, do the research related activities undertaken in these countries raise potential ethics issues?

Yes. Some social media accounts are non-EU as well as their provider service.

E.6.1.1 If YES: Specify the countries involved

Possibly all countries on earth. However, more frequent countries are: United States of America, Australia, Great Britain and Canada.

E.6.2 Do you plan to use local resources (e.g. animal and/or human tissue samples, genetic material, live animals, human remains, materials of historical value, endangered fauna or flora samples, etc.)?

No.

E.6.2.1 If YES: Specify material and countries involved

- - -

E.6.3 Do you plan to export any material, including personal data, from the EU to non-EU countries?

No.

E.6.3.1 If YES: Specify material and countries involved

- - -

E.6.4 If your research involves low and/or lower middle income countries, are benefit-sharing measures planned?

No.

E.6.5 Could the situation in the country put the individuals taking part in the research at risk?

Yes. As my research uncovers incidental data about their main residence, telephone number, relatives and other private details.

E.7 Environment & Health and Safety

E.7.1 Does your research involve the use of elements that may cause harm to the environment, to animals or plants?

Yes, as fired search queries cause a lot of calculation power the production of the power used may come from coal or nuclear power plants

E.7.2 Does your research deal with endangered fauna and/or flora and/or protected areas?

No.

E.7.3 Does your research involve the use of elements that may cause harm to humans, including research staff?

Yes. However, this is only be true for the misuse and uncovering of their private information.

E.8 Dual Use

E.8.1 Does your research have the potential for military applications?

Yes.

E.9 Misuse

E.9.1 Does your research have the potential for malevolent/criminal/terrorist abuse?

Yes.

E.10 Other Ethical Issues

E.10.1 Are there any other ethics issues that should be taken into consideration?

No, none that I'm aware of.

Acronyms

AUD	Australian Dollar
AU	Australia
BGBl	Bundesgesetzblatt
BKA	Bundeskanzleramt
BK	Bundeskriminalamt
CEO	Chief Executive Officer
CIA	Central Intelligence Agency
CJEU	Court of Justice of the European Union
CT	Computed Tomography
DSG	Datenschutzgesetz
DVD	Digital Video Disc
ECHR	European Convention on Human Rights
eg	exempli gratia
EuGH	Europäischer Gerichtshof
EUR	Euro
FBI	Federal Bureau of Investigation
GDPR	General Data Protection Regulation
GISA	Gewerbeinformationsystems
GIS	Geo Informations System
GPS	Global Positioning Syste
HIBP	Have I Been Pwned
ie	id est
IPSec	Internet Protocol Security

IP Internet Protocol address

ISP Internet Service Provider

L2TP Layer 2 Tunneling Protocol

LLC Limited Liability Companies

OGH Oberster Gerichtshof

OSINT Open Source Intelligence

OS Operating System

PPTP Point-to-Point Tunneling Protocol

RAM Random Access Memory

RGBl Reichsgesetzblatt

RIS Rechts Informations System

SME Small and Medium sized Enterprises

StGG Staatsgrundgesetz

Tor The Onion Router

U.S. United States of America

USB Universal Serial Bus

USD United States dollar

VPN Virtual Private Network

Bibliography

Ablon, Lillian (Jan. 2018). *Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data*. DOI: 10.7249/CT490.

Baur, Nina and Jörg Blasius (2019). *Handbuch Methoden der empirischen Sozialforschung*. ger.

Bazzel, Michael (Apr. 16, 2021). *The Privacy, Security, & OSINT Show, 214-OffenseDefense: The Capitol Siege*. Available from: https://soundcloud.com/user-98066669/214-offensedefense-the-capitol-siege [May 3, 2021].

Bazzell, Michael (Jan. 2021). *Open Source Intelligence Techniques - Resources for Searching and Analyzing Online Information*. Independently published. ISBN: 979-8578577086.

Bundesministerium für Digitalisierung und Wirtschaftsstandort (2020). *GISA - Abfragen*. Bundesministerium für Digitalisierung und Wirtschaftsstandort. Available from: https://www.bmdw.gv.at/Themen/Unternehmen/GISA_Gewerbeinformationssystem/GISA_Abfragen.html [Apr. 29, 2020].

Bundesministerium für Digitalisierung und Wirtschaftsstandort and Kooperationsgemeinschaft Bund/Länder/Städte (2020). *GISA Gewerbeinformationssystem Austria*. Bundesministerium für Digitalisierung und Wirtschaftsstandort. Available from: https://www.gisa.gv.at/abfrage [Apr. 29, 2020].

Casanovas, Pompeu, Nicholas Morris, Jorge González-Conejero, Emma Teodoro, and Rick Adderley (2018). „Minimisation of Incidental Findings, and Residual Risks for Security Compliance: the SPIRIT Project“. In: *CEUR Workshop Proceedings*, pp. 97–110. Available from: http://ceur-ws.org/Vol-2309/09.pdf.

Discovery Channel (May 16, 2006). *Future Weapons Season 1 Episode 4 - Future Shock*. Available from: https://www.discovery.com/shows/future-weapons/episodes/1a1a [Jan. 20, 2021].

EUROPEAN COMMISSION Directorate-General for Research & Innovation (Feb. 2019). *Horizon 2020 Programme Guidance How to complete your ethics self-assessment*. O'Reilly. Available from: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf [Mar. 30, 2020].

European Research Council Executive Agency (June 2018). *Ethics Self-Assessment step by step Horizon 2020 European Union Funding for Research & Innovation*. European Research Council. Available from: https://erc.europa.eu/sites/default/files/document/file/EthicsSelfAssessmentStepByStep.pdf [May 18, 2020].

ForeclosureFreeSearch.com (July 27, 2015). *Foreclosure.com | Foreclosures | Foreclosure Listings*. Available from: https://www.foreclosure.com [Dec. 15, 2019].

Google Inc. (Sept. 29, 2019). *Map of Tulsa, Oklahoma*. Available from: https://www.google.at/maps/place/Tulsa,+Oklahoma,+USA/@36.152105,-96.438444,9z/data=!3m1!4b1!4m5!3m4!1s0x87b692b8ddd12e8f:0xe76910c81bd96af7!8m2!3d36.1539816!4d-95.992775 [Sept. 29, 2019].

Google Maps (May 2, 2021a). *Google Maps - Street View*. Available from: https://www.google.com/streetview/ [May 2, 2021].

– (Jan. 16, 2021b). *Surfers Paradise to Surfers Paradise*. Available from: https://www.google.com/maps/dir/Surfers+Paradise,+Queensland+4217/Noosa+Heads,+Queensland+4567/Barmoya+QLD+4703/Airlie+Beach+QLD+4802/Port+Douglas,+Queensland+4877/Richmond,+Queensland+4822/Mount+Isa,+Queensland+4825/Tennant+Creek+NT/Alice+Springs,+Northern+Territory+0870/Uluru/Coober+Pedy,+South+Australia+5723/Barossa+Valley/Naracoorte,+South+Australia+5271/Fawcett,+Victoria+3714/Mount+Beauty,+Victoria+3699/Thredbo+NSW/Blue+Mountains,+New+South+Wales/Surfers+Paradise+QLD/ [Jan. 16, 2021].

Holoubek, Michael (Jan. 2016). *„Social watchdogs": nicht professionell organisierte Medienmacher im Lichte der Medienfreiheit*. in Berka/Holoubek/Leitl-Staudinger (Hrsg), REM 14: BürgerInnen im Web.

Hunt, Troy (Dec. 12, 2020a). *Australian death frog*. Available from: https://twitter.com/troyhunt/status/1337695185514348544/photo/1 [Jan. 16, 2021].

– (Dec. 10, 2020b). *Go straight for 475km, Astonished face*. Available from: https://twitter.com/troyhunt/status/1336840025858744321/photo/1 [Jan. 16, 2021].
– (Dec. 8, 2020c). *ROAD TRIP!!! Dolphin Spider Shark Crocodile Kangaroo Snake Koala*. Available from: https://twitter.com/troyhunt/status/1336432552177856513/photo/1 [Jan. 16, 2021].
– (Jan. 16, 2021). *Twitter Profile: Troy Hunt*. Available from: https://twitter.com/troyhunt [Jan. 16, 2021].

Internet Archive (2021). *Wayback Machine Internet Archive*. Available from: https://web.archive.org/web/20200929074424/https://protonvpn.com/privacy-policy [May 20, 2021].

Kutschera, Stefan (June 2020). *Detect and Process Personal Information from a Video Platform Supported by Artificial Intelligence, Legal term paper 1*. Not Published, FH JOANNEUM.
– (Feb. 2021). *Detect and Process Personal Information from a Video Platform Supported by Artificial Intelligence, Economy term paper 2*. Not Published, FH JOANNEUM.

LiveEachDay (July 2018). *Wild Oklahoma Weather*. YouTube. Available from: https://youtu.be/fRdfxtZDXwE?t=317.

Markuson, Daniel (Oct. 2019). *NordVPN safe after third party incident|NordVPN*. NordVPN. Available from: https://nordvpn.com/blog/official-response-datacenter-breach/ [May 28, 2020].

Mayring, Philipp (2010). *Qualitative Inhaltsanalyse : Grundlagen und Techniken*. ger. 11., aktualisierte und überarb. Aufl.. Pädagogik. Weinheim, Basel, Beltz. ISBN: 9783407255334.

Microsoft (Oct. 2, 2019). *Microsoft Bing Maps*. Available from: https://www.bing.com/maps [Oct. 2, 2019].

NordVPN (June 2020). *Advantages & Benefits of VPN|NordVPN*. NordVPN. Available from: https://nordvpn.com/features/popular/?utm_expid=.AcZA0VY5R52L6Sv7anwsmA.1&utm_referrer=https%3A%2F%2Fnordvpn.com%2Fhome-nordvpn%2F [May 28, 2020].

Polizei Hagen Nordrhein-Westfalen (June 25, 2015). *Facebook*. Available from: https://www.facebook.com/Polizei.NRW.HA/photos/pb.208563659315946.-2207520000.1436266044./439893356182974/?type=3&theater [Jan. 29, 2021].

Polizei Hessen, PPNH | mkr (2021). *Polizei Hessen - Urlaub und soziale Netzwerke - Auch Einbrecher nutzen Facebook*. Available from: https://www.polizei.h

essen.de/praevention/sicher-in-den-urlaub/vor-dem-urlaub/einbruch-und-diebstahlschutz/broker.jsp?uMen=2a370ae5-c345-7e41-d6d6-b0f60ef798e7&uCon=0b960058-53c8-ae41-8569-08820ef798e7&uTem=bff71055-bb1d-50f1-2860-72700266cb59 [Jan. 29, 2021].

Proton Technologies AG (2021). *Proton Technologies AG*. Available from: https://protonmail.com [May 20, 2021].

RP Data Pty Ltd (2020). *Onthehouse.com.au: Your Home for Property Search*. onthehouse.com.au. Available from: https://www.onthehouse.com.au [Apr. 10, 2020].

Schmid, Fabian (Jan. 31, 2019). *Sicherheitspanne: ARD-Doku verrät Adresse von Kanzler Kurz*. Available from: https://www.derstandard.at/story/2000097259454/sicherheitspanne-ard-doku-verraet-adresse-von-kanzler-kurz [Mar. 27, 2021].

Tails (Oct. 2019). *Tor bridge mode*. Tails. Available from: https://vpnpro.com/blog/nordvpn-security-breach-between-fact-and-fiction/ [June 1, 2020].

The European Parliament and the Council of the European Union (2014). *Regulation EU 2014/910 electronic identification and trust services for electronic transactions in the internal market (eIDAS)*. Official Journal of the European Union.

– (2016). *Regulation (EU) 2016/679 General Data Protection Regulation (GDPR)*. Official Journal of the European Union.

Trulia Group (Sept. 29, 2019). *Trulia: Real Estate Listings, Homes For Sale, Housing Data*. Available from: https://www.trulia.com/ [Sept. 29, 2019].

Weber, Julia and Edwin W. Kruisbergen (Sept. 2019). „Criminal markets: the dark web, money laundering and counterstrategies - An overview of the 10th Research Conference on Organized Crime“. In: *Trends in Organized Crime* 22.3, pp. 346–356. ISSN: 1936-4830. DOI: 10.1007/s12117-019-09365-8. Available from: https://doi.org/10.1007/s12117-019-09365-8.

Wolf, Susan M, Jordan Paradise, and Charlisse Caga-anan (2008). „The Law of Incidental Duties“. In: *Incidental Findings in Human Subjects Research* May, pp. 361–383. ISSN: 1073-1105.

Wolf, Susan M., Frances P. Lawrenz, Charles A. Nelson, Jeffrey P. Kahn, Mildred K. Cho, Ellen Wright Clayton, Joel G. Fletcher, Michael K. Georgieff, Dale Hammerschmidt, Kathy Hudson, Judy Illes, Vivek Kapur, Moira A. Keane, Barbara A. Koenig, Bonnie S. LeRoy, Elizabeth G. McFarland, Jordan Paradise, Lisa S. Parker, Sharon F. Terry, Brian Van Ness, and Benjamin S. Wilfond (Jan. 2008). „Managing

Incidental Findings in Human Subjects Research: Analysis and Recommendations“. In: *Journal of Law, Medicine & Ethics* 36.2, pp. 219–248. ISSN: 1073-1105. DOI: 10.1111/j.1748-720X.2008.00266.x. Available from: https://www.cambridge.org/core/product/identifier/S1073110500011074/type/journal_article.

Wright, John A. (July 27, 2015). *Tulsa County Assessor*. Available from: https://www.assessor.tulsacounty.org/assessor-property-search.php [Dec. 15, 2019].

Youtube (May 2, 2021). *YouTube*. Available from: https://www.youtube.com [May 2, 2021].

YouTube Inc. (2019). *Nutzungsbedingungen, Datum 22. Juli 2019*. YouTube Inc. Available from: https://www.youtube.com/t/terms#d676f2b451 [Apr. 28, 2020].

– (2020). *Google Terms of Service*. Google Inc. Available from: https://policies.google.com/terms?fg=1#toc-what-we-expect [Apr. 28, 2020].

Zillow, LLC. (Sept. 29, 2019). *Zillow: Real Estate, Apartments, Mortgages & Home Values*. Available from: https://www.zillow.com [Sept. 29, 2019].