*Maruška NARDONI, Franc MALI**

PLATFORMISATION AND HUMAN RIGHTS: DOES USE OF THE SLOVENIAN #OSTANIZDRAV APP BYPASS PRIVACY RIGHTS?

Abstract. *The article aims to explore the public's fear of data being misused when using European Covid-19 contact-tracing applications. The point of departure lies in considering the research question of whether the Covid-19 pandemic has influenced the platformisation of traditional institutions, i.e., whether the design of Europe's proximity-tracing applications mimic the data-intensive web services of commercial platforms, namely commercial APIs and their data policies, in order to bypass the right to privacy. We accordingly argue that is vital to address the public's fears of governmental and corporate dataveillance as well as data misuse while using such apps. The investigation entails of a critical analysis of the Exposure Notification System framework designed by Apple and Google (or GAEN) and the #OstaniZdrav application. The article rejects the justification of the public's fear of governmental dataveillance, while recognising the possibility of corporate data misuse.*

Keywords: *Covid-19 contact-tracing application, right to privacy, GDPR, API, protocol, metadata, dataveillance*

Introduction

Across the world, the Covid-19 pandemic has been responsible for bans on large gatherings, non-essential businesses, schools and university closures, along with working from home, which have led to people spending more time online, consciously uploading swathes of content and data whilst unknowingly leaving even more digital traces on various parts of the World Wide Web. This shift means popular platforms (Google, Amazon, Facebook etc.) have started to receive substantially growing communication

* *Maruška Nardoni, MSc., Junior Researcher, Faculty of Social Sciences, University of Ljubljana, Slovenia; Franc Mali, PhD, Professor, Faculty of Social Sciences, University of Ljubljana, Slovenia..*

DOI: 10.51936/tip.58.specialissue.536-554

flows, although the patterns of traditional infrastructures undergoing platformisation (Plantin et al., 2016; Casilli and Posada, 2019) accompanied by online platforms experiencing infrastructuralization already existed before (Jørgensen, 2019b: 166; Van Dijck, 2020). The article wishes to consider this pattern's possible presence in European Covid-19 contact-tracing applications. More precisely, the article intends to answer the research question concerning whether these apps have begun mimicking online platforms, which, due to certain ambiguities and technological opacity, sometimes attempt to bypass the right to privacy by gathering non-personal or demographic data without imposing clear limits on its potential for reuse in governmental predictive analytics. Such analysis must therefore clarify issues to do with the application's data authority, data sharing and potential for data re-use. Platform companies can rely on their legal regimes containing privacy statements to avoid the GDPR's requirements on personal data handling with a protocol framework and APIs (application programming interfaces) that are ambiguous and non-transparent when it comes to collecting data.

The implementation of digital tracing applications across Europe has raised concerns. In our digitalized societies, a pressing challenge is who will control all the personal data that is collected and processed. Constantly faced with such challenges, citizens have grown more sceptical of governments' management of the global pandemic using such tools. In times of such global health crises, use of such technology must be protected from all types of governmental or corporate misuse. Hence, the article does not limit itself to merely investigating the potential for governmental dataveillance: our basic thesis takes account of the public's fears of governmental dataveillance, and negative public stances on corporate data misuse together what the causes these fears, while eventually also debunking the ground for this distrust.

A quick glance at history reveals that the state as a political figure was largely missing during the first decades of Internet's development (Callamard, 2017; Lessig, 2006). However, with the appearance of a crisis as overwhelming as the Covid-19 pandemic, the situation has changed. Building a quality and up-to-date digital framework for tracing Covid-19 infections in a short period saw states rely on mobile network operators and relevant technology companies (e.g. Google, Apple) because governments did not possess the in-house expertise to build these apps (Guinchard, 2020). Meanwhile, in later stages of the pandemic, states,

> *will be in need of 'standing' mixed teams; up-to-date technology, basic agreements and legal prescriptions; and data access, procedures, and protocols, predefined also for 'appropriate anonymization and aggregation protocols'.* (Oliver et al., 2020: 5–6)

The search for appropriate ways of detecting virus spreaders and halting the spread currently has the world under pressure. The pandemic crisis reveals that the public health cannot be regulated by laissez-faire economic principles, since "despite the civic-minded narratives used to describe their services, the companies ultimately answer to shareholders rather than the public interest" (Jørgensen, 2019a: xviii).

The contribution is divided into four sections. The first section explains the conceptual framework of the essential software components (protocols, APIs and data). The second section presents commercial trends in datafication concerning the right to privacy prior to the Covid-19 pandemic. In section three, analysis is given of the software basis for European proximity tracing applications that claim to comply with the GDPR and a general comparative overview of such client applications, e.g. their intellectual property status (free, open, proprietary), and of their joint controllership with utilized protocols in selected EU states. Critical analysis of the proximity tracing applications' software continues in the fourth section, where the Slovenian #OstaniZdrav's application interface and its Privacy Statements are scrutinised. However, in order to delve into the app's data authority, data-sharing and potential for data re-use, the fourth section also considers certain GAEN API back-end connections. The concluding remarks give an answer to the research question and interpret European Covid-19 contact-tracing applications and their software in the context of wider datafication trends and the right to privacy.

Platform software components: preliminary clarifications and definitions

Prior to examining the Slovenian #OstaniZdrav mobile app and answering questions regarding authority over its data, data sharing, and the potential for data reuse, we must first explain the following basic terms: (1) web protocol, (2) application programming interface (API), and (3) metadata, to make the examination understandable and clear. Subsequent chapters in this article will regard these entities as socio-material objects.

Computing services like cloud computing, smartphone applications, or various platforms will not be discussed individually. Taking any cloud computing system as an example, we can see it is actually a disorderly knot of material infrastructure (namely server rooms, satellites, phone and optic cables), sensory interfaces, corporate aspirations, and Internet protocols, which for conceptual convenience are all then lumped together in the metaphorical "cloud". By deconstructing them, we can aim to reduce the technological opacity that often surrounds the mentioned computing services. We must consider that, while interacting with web objects and services, "code is

law" (Lessig, 2006: 323) – it dictates what can and cannot happen, what will be seen and what will be recommended. The processes being executed at the back end of our electronic devices are not visible and, to the vast majority of people, not amenable for investigation or critique. This gives designers of software services considerable power, especially if their computational infrastructures are then licensed in an exclusive proprietary form.

The standardization of internet protocols is an ongoing process which began in the early 80s – such early web protocols are in no way obsolete given that even most of the modern world wide web relies heavily on the early standardizations (of TCP/IP or HTTP for instance). Yet, today's commercial platforms (Amazon, Facebook, Google etc.) have generally benefited from the obfuscation of the standardized protocols through privatisation and licensing. Before the rise of platforms, using the World Wide Web was a more time-consuming activity since the average user had to be aware that entering different servers meant dealing with different protocols and their internal rules (Masnick, 2019). The web's landscapes were chaotic and its servers decentralized. Under the rule of a certain protocol, it was not possible to upload any kind of data or data format that one pleased—we must recall that the first version of the Internet was developed by researchers, academics and hackers, namely the non-commercial sector (Lessig, 2006: 6). Platforms hid web protocols behind their easy-to-use attractive front-ends and centralized servers. This has reduced the complexity of the Internet experience and made online activities simpler, at least from the end user's perspective. Initiatives to simplify and increase the coherency of the World Wide Web did not come from governmental or state authorities. They were formed when the private sector attempted to comply with user requests (Lessig, 2006: 38), but it rarely did so at the expenses of its own market interests.

Application programming interfaces (or APIs) may be described as a pre-arrangement of data formats and protocols designed to transfer information between different entities. From a practical point of view, APIs add another layer of standardization in contemporary algorithmic architectures because they unify "a set of routines, protocols, and tools for building software applications that make it easy for an outside programmer to write code" (Parker et a., 2016: 143). In the specific case of platforms, each platform produced its own standard API or (most likely) a set of APIs in order to make an application or a service inter-operational within larger platform ecosystems. The platform API framework may be interpreted as the driving force behind the development of networks that depend on data and other software pieces without being physically constrained to the locality of the platform or its hardware (Fuller, 2008: 151). APIs can be a free piece of software with no limitations on its modulations and distributions, although with an official licence. The latter can also be open-source, meaning their source code is

publicly accessible to software developers, researchers and enthusiasts, but with certain limits. The third option is for APIs to be licenced as a closed form of intellectual property that belongs to a certain platform company or business entity – like the case of the Google/Apple Exposure Notification Service API (or GAEN API in short), which will be discussed later.

Even more importantly, APIs offer a use of metadata unparalleled in a world where software is developed to capture, extract, and analyse diverse sets and kinds of data and metadata. The data industry's business interests used to lie in mining transactional data, data about web application users' activity (e.g., *access logs*), or metadata (Kovačič, 2006: 148) – which is still the case today, along with scraping user data or personal data (uploaded pictures, comments on Facebook etc.)[1]. This points to a more sophisticated conception of data that is not thought of as a ready-made informative object like a book or an article. Instead, data is raw, unprocessed, and closer to "potential information, analogous to potential energy: work is required to release it" (Pomerantz, 2015: 21–26). However, this extraction of value from data is only one aspect of datafication: it also demands the adequate capturing of human life into data through the processes of quantification (Meijas and Couldry, 2019: 4).

APIs play a gatekeeping role in this process of extracting information value from data since the way to give algorithms access to the metadata stored by the service is written in an API's own source code (Pomerantz, 2015: 195). Most commercial APIs are data-intensive: as web services make more data available via APIs, even more services can be integrated into the APIs to make use of that data, thereby producing even more data in return. Commercial APIs have ceased to be user experience-oriented, as "some APIs in fact get as much or even more traffic than the associated front end website for the service" (Pomerantz, 2015: 194).

Datafication, privacy, and data protection prior to the Covid-19 pandemic

The beginning of the 21st century is marked by a trajectory towards ubiquitous computing and deep mediatization (Hepp, 2020) as the amount of time most people are spending online is rising on the global level. Coincidentally, the global amount of digital data is reaching new heights. The exponential growth of digital data is not only due to the number of

[1] *Illustrated by a part of the Facebook Data Policy, explicitly stating it is collecting "content, communications and other information that you provide while using our products, including information that you provide when you sign up for an account, create or publish content, and send messages or communicate with others", with an additional explanation: "this may include information about the content you provide (such as metadata)" (Facebook Data Policy, Last Modified: August 2020).*

people connecting to the World Wide Web and buying numerous electronic devices with the option of interconnectivity, but also due to the technological innovation this growth is tied to. This has made the options available for gathering data cheaper, enabled upgraded capacities of computing powers that, in turn, have led to even more sophisticated and diversified methods of metadata production and data assemblage (Kovačič, 2006: 29; Lupton, 2015: 113). This advanced 'algorithmic veillance' means the private sector currently has more tools for analysing personal data at its disposal than state institutions (Kovačič, 2006: 32) as the developed sophisticated algorithms are the *sine qua non* of constituting and exploiting big data sets (Lupton, 2018: 11). Ubiquitous computing not only implies the constant presence of computation on the societal level, but also results in "dataveillance as a form of continuous surveillance through the use of (meta)data" due to technological advances led by corporate interests (Raley and van Dijck, 2014: 198). It is expected that in the future adoption of 'Internet of things' technologies will drive this global trend of intensifying datafication.

The right to privacy has not fundamentally intervened in the platform companies' business practices since dataveillance has been normalized through a silent agreement in which people must choose between not using a web service or product, or granting illusory consent in a pointless click-tick exercise of reading 'Terms of service agreements'. Elvy describes this silent agreement 'data-as-payment' in which personal data is the cultural currency for the provided free services (Elvy, 2017: 1383–1384). Numerous empirical studies suggest public opinion is negative on dataveillance, e.g., people not being comfortable with platform companies collecting, selling, and analysing their personal data (Special Eurobarometer 431, 2015; Presthus and Sørum, 2018). Evidently, such corporate handling of data is totally out of step with the OECD Privacy Guidelines advising the application of clear and transparent notifications of the motive for collecting data, while also prescribing use-limitation principles. However, public scandals such as Edward Snowden exposing the NSA's practices of routine surveillance and the more recent Cambridge Analytica affair have fuelled a widespread negative stance on governmental surveillance and produced scepticism about corporate data handling (Hern, 2019; eMarketer Editors, 2020). Such events contributed to making privacy and data protection issues a more central field.

The firmest step concerning data protection came with the implementation of the European GDPR in 2018 based on the OECD Privacy Guidelines and which forced platform companies to include tools to empower the users' control over their own data. Nonetheless, several problems remain with respect to strengthening the relationship between information privacy and the human right to privacy. First, the right to privacy is not an absolute human right. Second, the formal institutions concerned with defending human rights

govern the individual-state relationship. They were not formed to directly intervene in the realm of the private sector, which is traditionally the object of private law (Jørgensen, 2019a: xviii). In this respect, certain changes have been made, especially in the European Union; the GDPR deals with the misuse of data processing regardless of whether the institution is publicly-owned or a private enterprise (Jørgensen, 2019a: xix). The next obstacle lies in legally defining an operational notion of personal information. Should the notion of personal information signify anything identifiable or merely information that expresses a certain person's individuality – one's social security number, purchase history, race as a proxy etc. (Mal, 2019: 100)—or "any information relating to an identified or identifiable natural person" (Data Protection Working Party in Mal, 2019: 101). Further, the distinction between personal and impersonal information is swept away in the process of extracting information from various types of data, "where lots of seemingly casual and informal information is used in the algorithmic creation of personal data profiles" (Mal, 2019: 101–102). The ambiguity of commercial APIs and the lack of their transparency (when they are marked as a closed software patent), enable companies to "avoid the regulations around personal data and privacy by claiming to use derived, aggregated, or anonymized data", while the use of different APIs allows them to repackage data, thus allowing companies to claim it no longer qualifies as personal data (Kelleher and Tierney, 2018: 210).

European Covid-19 contact-tracing smartphone applications

Analysing people's mobility and other behaviour is at the core of the statistical modelling of epidemics. This means from both a governmental and an epidemiological point of view, "control of the pandemic requires control of people" (Oliver et al., 2020: 5). Since the European Union's digital landscape is a territory ruled by some of the strictest regulatory standards of data protection and civil liberties, researchers instead chose to focus on exploring the ways digital tools might complement non-pharmaceutical measures like physical distancing (Ferreri et al., 2020). Unlike China, India, South Korea, or Israel, whose governments can use personal smartphone app data to track the movement of their citizens, national and legal GDPR regulations in the European Union limit such use (Oliver et al., 2020: 5). In any case, digital tools should not be the primary method of monitoring the pandemic, only a supportive one (WHO, 2020: 4).

In response to EU political communities having started to become more aware of dataveillance and its controversies, many European governments considered implementing a decentralized protocol that is at odds with the current commercial platforms' business model and APIs. To avoid data misuse, several European research centres, universities and private companies

worked together to create the Pan-European Preserving Proximity Tracing (PEPP-PT) protocol in April 2020; a protocol that adheres to the GDPR (Oliver et al., 2020: 3). Following its official release, there was a call for software developers to work on a framework to minimise the risk of dataveillance. Even so, the PEPP-PT project was not fully carried out or adopted as a common EU protocol due to a rival research team developing their own Decentralized Privacy-Proximity Tracing (DP-3T) protocol backed by Google and Apple. This research team criticised the PEPP-PT protocol, voicing privacy concerns. Google and Apple likewise claimed the DP-3T was more interoperable with the Android and iOS operating systems (Clarke, 2020). Privacy concerns over future tracing applications that would be based on the PEPP-PT protocol have since increased in scope; around 300 European experts from the academic and private sectors signed an open letter setting out concerns with the need for such software products in the first place. They also mentioned the risk of contact-tracing apps being susceptible to "repurposing to enable unwarranted discrimination and surveillance" (Joint Statement on Contact Tracing, 19 April 2020). In Germany and Switzerland, this led to backing out of the PEPP-PT standardization, leaving France[2] alone to finish the initial project. Meanwhile, in May 2020 Google and Apple announced they would be partnering with European countries and, on the functional basis of DP-3T, quickly developed a decentralised protocol called Google/Apple Exposure Notification System or GAEN (Apple, 2020). Table 1 provides a comparative overview of selected EU member states and their private-public partnerships, the declared functionality of mobile applications, and the adopted protocols and software licences. The overview shows the majority of EU member states have adopted the GAEN framework, albeit within different private-public partnerships and with different software licences of the developed apps, which vary from free to proprietary. Even though the apps' legal status varies, it should be highlighted the GAEN API "is not open source and the public documentation is limited" (Leith and Farrell, 2020b). Moreover, controversies still linger about the question of whether DP-3T is genuinely safer than PEPP-PT in terms of data protection since debates on the propriety and effectiveness of digital tracing applications are still ongoing. Notwithstanding the relevance of these issues, they lie beyond the scope of this article.

[2] *France has retained the standardization and later in 2020 developed a new protocol on the ground of PEPP-PT, called Robert. Robert's development occurred as a developmental project involving a a strong consortium of private and public research stakeholders of an exquisite national character (INRIA, Cap Gemini, Dassault, Orange, Withings etc.) that joined forces with French government agencies (ANNSI, INSERM). We believe this consortium was the strongest among the public-private partnerships of other EU member states. Most of the other public-private partnership only consisted of two or three subjects (a governmental agency and a private software development company).*

Table 1: A COMPARATIVE OVERVIEW OF SELECTED EUROPEAN PROXIMITY-TRACING APPLICATIONS

Country	App name	Client app controllers	App licence	Protocol framework
Austria	Stopp Corona	Austrian Red Cross	Open software	GAEN
Belgium	Coronalert	Belgian government, Sciensano	Free software	GAEN
Croatia	Enter Croatia	Ministry of Health of Republic of Croatia	Free software	GAEN
Czech Republic	eRouška	Czech Ministry of Health and Hygiene	Open software	GAEN
Denmark	Smittestop	Danish Patient Safety Authority	Proprietary	GAEN
Finland	Koronavikku	Ministry of Social Affairs and Health, THL, Solita, Kela, SoteDigi	Open Software	GAEN
France	TousAntiCovid	Government of France, INRIA, ANNSI, Cap Gemini, Dassault, Orange…	Open Software	Robert
Germany	Corona-Warn-App	Robert Koch Institute	Free software	GAEN
Germany	ITO	Unknown	Free software	TCN
Germany	OHIO Research	The Linux Foundation, IBM, FH Kiel	Free software	Unknown
Hungary	Virus Radar	Ministry of innovation and technology, NextSense	Proprietary	Unknown
Ireland	COVID tracker Ireland	Health service executive, NearForm	Open software	GAEN
Italy	Immuni	Ministry of Health	Proprietary	GAEN
Netherlands	Private Tracer	Milvum, YES!Delft, Idyssey, Hague	Open software	GAEN
Norway	Smittestopp	Simula Research Laboratory, Norwegian Institute of Public Health	Proprietary	GAEN
Poland	ProteGO Safe	Chief Sanitary Inspector	Free software	GAEN
Portugal	STAYAWAY COVID	INESC TEC, ISPUP, Keyruptive, Ubirider	Open software	GAEN
Slovenia	#OstaniZdrav	Ministry of Health, National Institute for Health	Free software	GAEN
Spain	Radar COVID	Ministry of Economic Affairs and Digital Transformations, Indra Sistemas	Open source	GAEN

Source: authors' analysis is based on sources.

Data on people's mobility can be collected using different technologies, with the major ones being cell sites, GPS and Bluetooth. PEPP-PT, DP-3T and GAEN all employ Bluetooth technology as a base for gathering data on individuals' movement and location. The signal strength of Bluetooth proves to be more reliable (than GPS)[3] for determining whether two individuals and their respective smartphones were in sufficient proximity to transmit the virus. As for the issue of privacy and anonymity, Bluetooth technology does not require the capture of all data on an individual's movement since it only records proximity to other users—usually when two individuals and their devices are less than 2 meters apart for a sufficient period of time. These apps rely on short-range Bluetooth; this does not consume great amounts of power and the extracted data are stored on the smartphone itself. For it to function properly, the application still needs some unique identifiers (IP address, establishing the Covid-19 patient file). Without this base of identifiers, the application cannot notify the user should they, in fact, find themselves in the proximity of an infected person. In order for such an app to function and use the collected data, it needs to call or request the services of the operating system through the GAEN API. It must be stressed that the GAEN API determines specifications about the format of Bluetooth LE beacons and their cryptographic protocols (Leith and Farrell, 2020b).

Nevertheless, "digital tools for measuring relative spatial proximity among phone users are, ceteris paribus, less privacy-invasive than personal contact tracing or quarantine enforcement apps" (Gasser et al., 2020). This means that applications which gather data via Bluetooth technology are less data-intensive than other digital tools which use sensor tracking or GPS. This observation is not simply based on the fact that proximity-tracing applications use Bluetooth, but on its integration with the GAEN. This, in turn, creates a network system of servers with no central authority, although it is worth noting that the GAEN still has central servers to which all the ciphered data is copied. This should be highlighted as a key point in the process of storing data on cloud servers: even though, due to the decentralized protocol approach, the data extracted by the app is stored on people's personal devices, copies of identifiers, albeit ciphered, still exist on cloud servers (Holmes, 2019: 113).

[3] *Most mobile GPS devices prove to be accurate outdoors over 10–15 meters, which does not cover the proximity the applications are searching for. Moreover, the GPS accuracy decreases substantially indoors (Gast, 2015: 6). Even so, it must be stressed that the Bluetooth LE accuracy is far from flawless as its received signal strength can vary and change due to multiple conditions like the device's orientation, reflections and absorption of radio signals inside buildings, especially in metal ones etc. (Leith and Farrell, 2020a).*

The #OstaniZdrav application and the question of privacy

Public fears related to the loss of privacy while using contact-tracing applications can be framed within two different conceptions: one covering governmental data misuse and the second dealing with corporate data misuse. The first public fear concerning lost privacy is the fear of unlimited governmental dataveillance (e.g. surveillance through digital tools that are based on data), which may continue even after the pandemic ends (Kharpal, 2020). This particular public fear might be connected to 'the control theory of information', which states that one's ability to control the flow of information about oneself is a prerequisite for enjoying privacy and freedom from surveillance (Mai, 2019: 109). In the case of the Slovenian public, there was a widespread fear that using an app with the word "tracing" in its name would leave one susceptible to governmental control and endanger one's privacy (Dinevski, 2020; Račič, 2020). The second public fear concerning the loss of privacy due to corporate data misuse transcends the question of privacy being linked solely to individuals and their liberal rights (Mai, 2019: 114). It is connected to "the concerns about the new insights that others can generate on the already available data" (Mai, 2016: 199), as happened in the case of the Cambridge Analytica scandal where data from social media were exploited for political purposes and campaign targeting for the Trump election and Brexit referendum. Underlying the fear of others being able to generate new insights from one's data is the act of repurposing data or repurposing certain web services like facial recognition software to meet the needs of police departments (Weise and Singer, 2020; Fung, 2020).

The Slovenian #OstaniZdrav app is based on the German Corona-Warn. The app uses the free Apache 2.0 licence, meaning its code is publicly available on the GitHub repository. Again, it cannot be stressed enough that although the #OstaniZdrav client app uses a free licence, the GAEN is a closed-source component. #OstaniZdrav's interface thus only represents one part of the full contact-tracing ecosystem, as its core (e.g. exposure notification) is mainly implemented at the operating system level. The #OstaniZdrav app collects three types of data: technical access data, contact data, and data on the random daily keys of individuals who have been infected (#OstaniZdrav Privacy Statement). #OstaniZdrav is not a data-intensive application like with the case with most commercial web service products. On the contrary, it collects a very modest amount of data. It collects exposure loggings in the form of the time and date of accessing the app (time stamp), the volume of the data transmitted (or packet length), and successful access notifications—this is all stored under 'technical access data'. Next, contact data means #OstaniZdrav stores the time and date of the contact, the duration of the contact, the Bluetooth signal strength of the

contact and the encrypted metadata—this type of data is generated, processed and stored on the individual's smartphone device, but only on the condition that the user gives the #OstaniZdrav app permission to execute back-end exposure log activities (#OstaniZdrav Privacy Statement). If the user is infected with Covid-19 and has tested positive, they must again give the app permission to send information with the encrypted keys of other possibly infected users to the central server. The central servers for data exchange belong to the Republic of Slovenia and the EU with any shared transmit codes deleted off the servers within 2–3 weeks of transmission. The EU central server[4] was added following the application's upgrade in January 2021, making #OstaniZdrav interoperable with other GAEN proximity-tracing apps in the European Union. #OstaniZdrav's framework and data are handled by the National Institute of Public Health (NIJZ) and the Ministry of Public Administration (MJU). These governmental agencies have provided the legal framework which complies with GDPR: the application is not data-intensive, the unique identifiers (the IP address of the device) and the contact data are pseudo-anonymised, and the application provides clear agreements on its use and purpose with a univocal limit on data retention and usage (2 to 3 weeks). The joint controllers of the app, the NIJZ and the MJU, state that they will not merge #OstaniZdrav's data with "the database of infected persons kept by NIJZ", nor will they share the assessment of risks of infection or the data from central servers that are processed on individual devices with anybody else, including themselves, let alone with Apple, Google, or other third parties (#OstaniZdrav Privacy Statement). Nonetheless, due to the app not requiring registration or the creation of a profile and it collecting pseudo-anonymised data, the NIJZ and the MJU are not obliged to fully respect GDPR guidelines regarding personal data, specifically the publication of information related to the processing on personal data, the right to rectification, the right to deletion, the right to restriction of processing, and the right to object. In this case, such bypassing of Article 11 of the GDPR, which deals with individual rights, is sensible. The fear of government dataveillance and the risk of governmental data misuse do not seem feasible in the case of #OstaniZdrav because its database information value is modest and, from a governmental surveillance perspective, quite useless if it is not combined with other databases, which the Privacy Statement of the application's current version forbids. Other experts also appear to agree with this assessment, claiming "the health authority client apps are generally well behaved from a privacy point of view" (Leith and

[4] *The inter-operability or data exchange between the national servers and EU central servers is secured with the more complex back-end architecture of the European Federation Gateway Service (eHealth Network, 2020).*

Farrell, 2020c) or assessing the #OstaniZdrav app's manifest code as generally well designed by not containing more than one vulnerable component (Kouliaridis et al., 2021: 15–17).

Still, the technical access data is also sent to another server system, belonging neither to the NJZ nor the MJU, and not to the EU central server. Albeit transmission of user data to back-end servers cannot be denoted as an intrusion of privacy *per se*, it may be seen as troublesome that the device's IP address is being sent to Google servers, as "on Android the GAEN API is implemented within Google Play Services[5]" (Leith and Farrell, 2020b: 1). There is no way a user can opt out of Google Play Services, which within the app make contact to Google servers in approximately 20-minute intervals, revealing the device's IP address to Google. Leith and Farrell show that such Google Play Services requests "also contain persistent identifiers that allow requests from the same device to be linked together", and consequently make feasible "fine grained tracking by Google of device location over time"(Leith and Farrell, 2020c: 1–2). These back-end connections hence represent a privacy intrusion as they carry the risk of deanonymisation. As a result of this GAEN implementation, the NIJZ and the MJU must explicitly state that they are not responsible for exposure logging functions (collecting metadata such as the time and date of access, the volume of the transmitted data, and successful access notifications) which are

> *provided to you by Apple (iPhones) or Google (Android smartphones) and are subject to these companies' respective privacy policies"* on the grounds of exposure logging not being *"part of the app, but an integral part of your smartphone's operating system.* (#OstaniZdrav Privacy Statement)

Although the exposure logging metadata is quite limited at first glance and subjected to the app's functional purpose, research has shown "a truly incredible amount of information can be inferred from 'only' metadata" (Pomerantz, 2015: 2), while other researchers have also claimed "the metadata is not the problem, however, where privacy is concerned, but the inferences that can be made from it" (Mayer and Mutchold, 2014). The fact that #OstaniZdrav also serves to inform the user about Covid-19 protective measures and tips, which means certain websites (like https://gov.si/en/ostanizdrav) will be opened in the smartphone's standard browser, is also worth noting. Those pages belong to a different privacy regime, as "the data

[5] *Correspondingly, the Google Play Services is also a closed or proprietary piece of software used in relation with many other Google products. It provides services used by other apps, such as analytics, an app's crash reporting, fused location etc. (Leith and Farrell, 2020b and 2020c).*

processed here depends on the browser used, your browser settings, and the data processing practices of the website you are visiting" (#OstaniZdrav Privacy Statement). If the exposure loggings datasets are combined with data aggregations of other user activity performed using other web services of Google's or Apple's digital empire, these corporations are able to extract some information of value from the #OstaniZdrav metadata. Alas, the risk of corporate data misuse and public fears of privacy loss in the form of inferring new insights from the combined datasets are feasible and can be realised, although in their legal documents the companies state otherwise and make explicit the obligation "to not to use or combine any data obtained through the described permissions"[6] (Google, 2020: 2).

Conclusion

The analysis of the European Union's standardisation of the GAEN framework together with its API clearly draws attention to the strong negotiating position platform giants Google and Apple have while providing a fast response to the designing of the algorithmic architecture needed to develop public contact-tracing applications. As seen in Table 1, most European countries have adopted the GAEN, although the initially conceptualised PEPP-PT was intended to help achieve the European Union's digital autonomy in relation to the aforementioned platform giants; this effort proved unsuccessful due to expert privacy concerns surrounding PEPP-PT and because both Apple and Google were advocating a decentralized version of the DP-3T protocols, which then served as a conceptual basis for the GAEN, thereby strengthening Apple and Google's monopolistic position in the domain of European smartphone software. Here an unsettled question arises concerning whether Google and Apple's ultimate authority on the functioning of public health apps is truly desirable in the first place.

Although traditional infrastructures (in this case, public health authorities) may have undergone platformisation in employing a supplementary web service to mitigate the pandemic' effects, it is certain they are not mimicking the data-intensive web services of commercial platforms or their data policy regarding the question of privacy. This entails the short answer guiding this article. The GAEN framework (altogether with the Bluetooth LE proximity tracing and with the decentralized system of server authority) and its adequate client app interface offer public health authorities and

[6] *More specifically, Google prohibits "all other uses (including selling or licensing such data, using it to serve or target ads, or providing it to government agencies for purposes other than Covid-19 response)" to software companies which will implement the API, allowing them to use only "third-pay services, such as analytics services, in compliance with these Terms", but without any Android Advertising ID or without associating any Advertising ID API service (Google, 2020: 2).*

other officials an alternative to more data-intensive models of digital tools that involve collecting personal data as well as a rich collection of metadata on the user's activity. Whether this alternative will provide a standard framework for future trends of datafication beyond the Covid-19 pandemic remains unclear. It is worth pointing out that the proximity-tracing applications may have set the standard for any future European platformisation of traditional infrastructures that may outlast the Covid-19 pandemic. The trend of modest datafication and reduced dataveillance might be realised with the broadening of public-private partnerships to include the non-governmental sector.

In the case of #OstaniZdrav, analysis of access to its server system and its privacy statements refutes the public's fear of governmental dataveillance, which is unjustified from a techno-legal point of view. The client app's privacy is, by design, in line with GDPR standards, which have been explained through a detailed overview of the agents responsible for #OstaniZdrav's data and its potential for data sharing. Legally, authority over the app's framework and data is exercised by the joint controllership of the NIJZ and the MJU; however, since #OstaniZdrav's last upgrade in January 2021, its transmit codes are also being sent to the EU central server. The analysis of the collected data, its modest volume, and the app's joint controllership statement claiming that its data will not be shared with any other third party exclude the risk of governmental data misuse. Unfortunately, the GAEN framework is far from flawless in terms of privacy risks. The chance of corporate data misuse is feasible due to the GAEN API's back-end connections with Google Play Services, along the lines with exposure logging data sets being subjected to Apple and Google's commercial privacy. From a privacy aspect, these connections are not transparent and carry a risk of de-anonymisation and even allow fine-grained tracking, whereas a user has no opt-out of the Google Play Services. This allows possible inferences of a user's personal information when combined with data aggregations from other Android or iOS user activities, as these depend on user settings on other Google or Apple web services. The regulation of such GAEN API ambiguities and its lack of documentation both call for a shift from individual empowerment or having control over one's personal information towards to the regulating what can be made from datasets as it would more fully implement the right to privacy in an online context.

BIBLIOGRAPHY

Callamard, Agnes (2017): Are Courts Re-Inventing Internet Governance? International Review of Law, Computers and Technology. March 2017: 1–17.

Casilli, Antonio A. and Julian Posada (2019): The Platformization of Labor and Society. In Mark Graham and William H. Dutton (ed.), Society and the Internet: how networks of information and communication are changing our lives, 293–303. Oxford: Oxford University Press.

Elvy, Stacy-Ann (2017): Paying for Privacy and the Personal Data Economy. Columbia Law Review 117 (6): 1369–1459.

Ferretti, Luca, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner, Michael Parker, David Bonsall and Christopher Fraser (2020): Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science 368 (6491).

Fuller, Matthew (2008): Software Studies: A Lexicon. Cambridge, MA: The MIT Press.

Gasser, Urs, Marcello Ienca, James Scheibner, Joanna Sleigh and Effy Vayena (2020): Digital tools against Covid-19: taxonomy, ethical challenges, and navigation. Lancet Digital Health.

Gast, Matthew S. (2015): Building Applications with iBeacon. Proximity and Location Services with Bluetooth Low Energy. Sebastopol, CA: O'Reilly.

Guinchard, Audrey (2020): Our digital footprint under Covid-19: should we fear the UK digital contact tracing app? International Review of Law, Computers and Technology 35 (1): 84–97.

Holmes, Dawn E. (2019): Veliko podatkovje: Zelo kratek uvod. Ljubljana: Založba Krtina.

Jørgensen, Rikke Frank (2019a): Introduction. In Rikke Frank J rgensen (ed.), Human Rights in the Age of Platforms, xvii-xlv. Cambridge, MA: The MIT Press.

Jørgensen, Rikke Frank (2019b): Rights Talk: In the Kingdom of Online Giants. In Rikke Frank Jørgensen (ed.), Human Rights in the Age of Platforms, 163–187. Cambridge, MA: The MIT Press.

Kelleher, John D. and Brendan Tierney (2018): Data Science. Cambridge, MA: The MIT Press.

Kovačič, Matej (2006): Nadzor in zasebnost v informacijski družbi. Ljubljana: FDV.

Leith, Douglas J. and Stephen Farrell (2020a): Coronavirus Contact Tracing: Evaluating The Potential of Using Bluetooth Received Signal Strength for Proximity Detection. SIGCOMM Computer Communication Review 50 (4): 66–74.

Leith, Douglas J. and Stephen Farrel (2020b): GAEN Due Diligence: Verifying the Google/Apple Covid Exposure Notification API. SCSS Tech Report. Accessible at https://www.scss.tcd.ie/Doug.Leith/pubs/gaen_verification.pdf, 3. 5. 2021.

Leith Douglas J. and Stephen Farrell (2020c): Contact Tracing App Privacy: What Data is Shared By Europe's GAEN Contact Tracing Apps. Accessible at https://www.scss.tcd.ie/Doug.Leith/pubs/contact_tracing_app_traffic.pdf, 3. 5. 2021.

Kouliaridis, Vasilejos, Georgios Kambourakis, Efrastatios Chatzoglou, Dimitrios Geneitakis, and Hua Wang (2021): Dissecting contact tracing apps in the Android platform. PLoS ONE 16 (5): 1–28.

Lessig, Lawrence (2006): Code and Other Laws of Cyberspace. New York: Basic Books.
Lupton, Deborah (2015): Digital Sociology. London, New York: Routledge.
Lupton, Deborah (2018): Digital Health: Critical and Cross-Disciplinary Perspectives. London, New York: Routledge.
Mai, Jens-Erik (2019): Situating Personal Information: Privacy in the Algorithmic Age. In Rikke Frank (ed.), Human Rights in the Age of Platforms, 95–116. Cambridge, MA: The MIT Press.
Mejias, Ulises A. and Nick Couldry (2019): Datafication. Internet Policy Review 8 (4).
Oliver, Nuria, Bruno Lepri, Harald Sterly, Renaud Lambiotte, Sébastien Delataille, Marco De Nadai, Emmanuel Letouzé, Albert Ali Salah, Richard Benjamins, Ciro Cattuto, Vittoria Colizza, Nicolas de Cordes, Samuel P. Fraiberger, Till Koebe, Sune Lehmann, Juan Murillo, Alex Pentland, Phuong N.Pham, Frédéric Pivetta, Jari Saramäki, Samuel V.Scarpino, Michele Tizzoni, Stefaan Verhulst and Patrick Vinck (2020): Mobile phone data for informing public health actions across the Covid-19 pandemic life cycle. Science Advances 6 (23).
Palan, Ronen (1999): Global Governance and Social Closure or Who is to Governed in an Era of Global Governance? In Martin Hewson in Thimothy J. Sinclar (ur.), Approaches to Global Governance Theory, 55–72. Albany: State University New York Press.
Parker, Geoffrey G., Marshall W. Van Alystne and Sangeet Paul Choudary (2016): Platform revolution: How networked markets are transforming the economy – and how to make them work for you. New York, London: W. W. Norton & Company.
Plantin, Jean-Cristopher, Carl Lagoze, Paul N. Edwards and Christian Sandvig (2018): Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook. New Media & Society 20 (1): 293–310.
Pomerantz, Jeffrey (2015): Metadata. Cambridge, MA: The MIT Press.
Presthus, Wanda and Hanne Sørum (2018): Are Consumers Concerned About Privacy? An Online Survey Emphasizing the General Data Protection Regulation. Procedia Computer Science 138: 603–611.
Van Dijck, José (2014): Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. Surveillance & Society 12 (2): 197–208.
Van Dijck, José (2020): Seeing in the forest for trees: Visualizing platformization and its governance. New Media & Society: 1–19.

SOURCES

Apple (2020): Apple and Google partner on Covid-19 contact tracing technology. Accessible at https://www.apple.com/si/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/, 4. 2. 2021.
Austrian Red Cross (2020): Stopp Corona. Accessible at https://www.stopp-corona.at/, 20. 8. 2021.
Chief Sanitary Inspector of Poland (2020): ProteGO Safe. Accessible at https://safe-safe.app, 20. 8. 2021.
Council of Europe (2020): Contact Tracing Apps. Accessible at https://www.coe.int/en/web/data-protection/contact-tracing-apps, 10. 2. 2021.

Dannish Patient Safety Authority (2020): Smittestop. Accessible at https://smittestop.dk/, 20. 8. 2021.

Dinevski, Dejan (2020): Mobilna aplikacija #OstaniZdrav: Ne pustimo se nadzirati! Ali pač?. Večer. Accessible at https://www.vecer.com/v-soboto/mobilna-aplikacija-ostanizdrav-ne-pustimo-se-nadzirati-ali-pac-10207977, 6. 2. 2021.

Directorate-General for Communication (2015): Special Eurobarometer 431: Data protection. Accessible at https://data.europa.eu/euodp/en/data/dataset/S2075_83_1_431_ENG, 4. 2. 2021.

Dutch Ministry of Health, Welfare and Sports (2020): CoronaMelder. Accessible at https://coronamelder.nl/en/, 20. 8. 2021.

eHealth Network (2020): European Interoperability Certificate Governance: A Security Architecture for contact tracing and warning apps. Brussels. Accessible at https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interop_certificate_governance_en.pdf, 4. 2. 2021.

eMarketer Editors (2020): Facebook Ranks Last in Digital Trust Among Users. Insider Intelligence. Accessible at https://www.emarketer.com/content/facebook-ranks-last-in-digital-trust-among-users?_ga=2.186938216.1154069519.1621369086-1423097089.1621183295, 21. 4. 2021.

European Commission (2020): National Joint Controllers and Privacy Policy. Accessible at https://ec.europa.eu/health/sites/health/files/ehealth/docs/gateway_jointcontrollers_en.pdf, 4. 2. 2021.

Facebook (2020): Facebook Data Policy. Last Modified: August 21, 2020. Accessible at https://www.facebook.com/about/privacy/update, 21. 4. 2021.

Finnish Institute for Health and Welfare (2021): Koronavikku. Accessible at https://koronavilkku.fi/en/, 20. 8. 2021.

French Government (2020): Tous AntiCovid. Accessible at https://faq.tousanticovid.gouv.fr/kb/fr/donnees-personnelles-26615, 20. 8. 2021.

Fung, Brian (2020): Microsoft says it won't sell facial recognition technology to US police departments. CNN Business. Accessible at https://edition.cnn.com/2020/06/11/tech/microsoft-facial-recognition-police/index.html, 4. 2. 2021.

Google (2020): Exposure Notifications Service Additional Terms. Last Modified: May 4, 2020. Accessible at https://blog.google/documents/72/Exposure_Notifications_Service_Additional_Terms.pdfhttps://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.2.pdf, 21. 4. 2021.

Hern, Alex (2019): Facebook usage falling after privacy scandals, data suggest. The Guardian. Accessible at https://www.theguardian.com/technology/2019/jun/20/facebook-usage-collapsed-since-scandal-data-shows, 21. 4. 2021.

Hsu, Jeremy (2020): Contact Tracing Apps Struggle to Be Both Effective and Private. Accessible at https://spectrum.ieee.org/biomedical/devices/contact-tracing-apps-struggle-to-be-both-effective-and-private, 4. 2. 2021.

Hungarian Minnistry of innovation and technology, NextSense (2021): Virus Radar. Accessible at https://www.nextsense.com/ns-newsarticle-virusradar-a-mobile-contact-tracing-implemented.nspx, 20. 8. 2021.

Irish Department of Health (2020): COVID Trackr Ireland. Accessible at https://www.gov.ie/en/service/da832-download-the-covid-tracker-app/, 20. 8. 2021.

Italian Ministry of Health (2020): Immuni. Accessible at https://www.immuni.italia.it/download.html, 20. 8. 2021.

Joint Statement on Contact Tracing (2020). Accessible at https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view, 4. 4. 2021.

Kharpal, Arjun (2020): Use of surveillance to fight coronavirus raises concerns about government power after pandemic ends. CNBC. Accessible at https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html, 4. 2. 2021.

Masnick, Mike (2019): Protocols, Not Platforms: A Technological Approach to Free Speech. Accessible at https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech, 4. 2. 2021.

Mayer, Jonathan and Patrick Mutchler (2014): MetaPhone: The sensitivity of telephone metadata. Web Policy. Accessible at http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/, 4. 2. 2021.

Ministry of Public Administration (2020): Privacy notice of #OstaniZdrav. Accessible at https://www.gov.si/assets/vlada/Koronavirus-zbirno-infografike-vlada/APP-OstaniZdrav/Privacy-notice.pdf, 20. 2. 2021.

Ministry of Health of the Czech Republic (2021): eRouška. Accessible at https://erouska.cz/en, 20. 8. 2021.

Norwegian Institute of Public Health (2020): Smittestopp. Accessible at https://www.helsenorge.no/en/smittestopp/, 20. 8. 2021.

#OstaniZdrav (2020): si-covid-19/ostanizdrav-android. Github. Accessible at https://github.com/si-covid-19/ostanizdrav-android, 20. 2. 2021.

Račič, Maja (2020): 'Ne gre za nikakršno sledenje, saj aplikacija nima dostopa do teh podatkov'. 24 ur. Accessible at https://www.24ur.com/novice/korona/ne-gre-za-nikakrsno-sledenje-saj-aplikacija-nima-dostopa-do-lokacijskih-podatkov.html, 4. 2. 2021.

Republic of Croatia (2020): Enter Croatia. Accessible at https://entercroatia.mup.hr/, 20. 8. 2021.

Robert Koch Institute (2020): Corona-Warn-App. Accessible at https://www.corona-warn.app/en/, 20. 8. 2021.

Sciensano (2020): Coronalert. Accessible at https://coronalert.be/en/, 20. 8. 2021.

Slovenian Ministry of Public Administration (2020): #OstaniZdrav. Accessible at https://www.gov.si/teme/koronavirus-sars-cov-2/mobilna-aplikacija-ostanizdrav/ 20. 8. 2021.

Spanish Ministry of Economic Affairs and Digital Transformation (2020): Radar COVID. Accessible at https://radarcovid.gob.es/en/terms-and-conditions-use, 20. 8. 2021.

Weise, Karen and Natasha Singer (2020): Amazon pauses police use of its facial recognition software. The New York Times. Accessible at https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html, 4. 2. 2021.

World Health Organization (2020): Public Health Surveillance for Covid-19. Accessible at https://www.who.int/publications/i/item/who-2019-nCoV-surveillanceguidance-2020.8, 4. 2. 2021.