

## Google and Apple Exposure Notifications System:

### Exposure Notifications or Notified Exposures?

Tatiana Duarte

Email address: [tatiana.duarte.nicolau@vub.be](mailto:tatiana.duarte.nicolau@vub.be)

Twitter @TatDuarte

#### Abstract

This paper proposes a legal and architectural inquiry to Google and Apple's Exposure Notifications system, from a data protection point of view, with the purpose to respond to two main questions. (1) Is the Exposure Notifications framework legal by design? (2) Does it afford legal protection by design? The raw material to answer these questions involves (i) a legal assessment of the contractual framework established between Google and Apple (Gapple) and governments; (ii) a review of relevant aspects of the system architecture; and (iii) the identification of some of the system security vulnerabilities. The contractual assessment reveals the underlying power relations between governments and Gapple regarding the use of the API and the design of national proximity tracking apps. The analysis of the system architecture and of the tools to develop national apps expose contradictions between the available public information on data protection and the functioning of the system. The identified security vulnerabilities show that tracking and profiling are possible if simple attacks are deployed. Our analysis indicates that Gapple's framework may be an example of legal by design which remains blind to legal protection by design.

**Key words:** Data Protection; Exposure Notifications; Legal by design; Legal Protection by design; Proximity tracking; The Rule of Law

## I. THE EXPOSURE NOTIFICATION SYSTEM

### *The Exposure Notifications System within the Strategy of Tackling COVID-19*

Societies worldwide are facing a global pandemic whose proportions are still to be fully identified. Our mode of living together was reshaped and is constantly being adapted to new circumstances, according to the current figures of testing, cases, and deaths. COVID-19 potential for rapid and exponential growth urges national health systems to break the chains of transmission. Therefore, health authorities are adopting a comprehensive strategy that includes case identification,<sup>1</sup> isolation, testing, care, contact tracing and quarantine. To fully understand the significance of Google and Apple (Gapple) Exposure Notifications system, we need to consider the concept of *contact tracing* as part of the overall strategy to contain the spreading of COVID-19.

Contact tracing is the *process of identifying, assessing, and managing people who have been exposed to a disease to prevent onward transmission*.<sup>2</sup> In the context of COVID-19, it involves identification and daily follow up for 14 days – counted from the last point of exposure –, as well as case-assessment and guidance to prevent onward transmission. Contact tracing involves contacting each person by phone or in person

---

<sup>1</sup> World Health Organization, 'COVID-19 Case definition' (7 August 2020) <[www.who.int/publications/i/item/WHO-2019-nCoV-Surveillance\\_Case\\_Definition-2020.1](http://www.who.int/publications/i/item/WHO-2019-nCoV-Surveillance_Case_Definition-2020.1)> accessed 5 October 2020, identifies three kinds of case definitions: suspected, probable and confirmed Covid-19 case.

<sup>2</sup> World Health Organization, 'Contact tracing in the context of COVID-19, Interim guidance' (10 May 2020) <[www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19](http://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19)> accessed 5 October 2020.

to determine whether they meet the contact definition<sup>3</sup> and, if so, monitoring them. When contacted by health authorities, each individual shall be provided guidance, namely on the contact tracing rationale, on symptoms to look out for, and on what to do when feeling unwell. It is worth mentioning that the World Health Organization (WHO) specifically states that information regarding data protection should also be provided, namely how individual's personal information will be used, processed and stored.<sup>4</sup>

Digital technologies may be used to support rapid case reporting, data management and analysis. In this context, distinct design proposals promise to get the most of technological progress without compromising fundamental rights. One of these proposals results from a partnership between Google and Apple (Gapple).

When Gapple launched this joint-effort, they announced that it would be two-phased.<sup>5</sup> In the first phase, an Application Programming Interface (API) would be deployed to enable governments (or developers on their behalf) to develop applications (apps) within the so-called "Exposure Notifications" (EN) framework. In the second phase, the technology would be introduced in the operating system, so that

---

<sup>3</sup> Ibid. According to the World Health Organization, a contact is a person who has experienced any of the following exposures during the 2 days before and the 14 days after the onset of symptoms of a probable or confirmed case: (1) face-to-face contact with a probable or confirmed case within 1 metre and for at least 15 minutes; (2) direct physical contact with a probable or confirmed case; (3) direct care for a patient with probable or confirmed COVID-19 disease without using recommended personal protective equipment; or (4) other situations as indicated by local risk assessments.

<sup>4</sup> Ibid.

<sup>5</sup> Google, 'Exposure Notification, Frequently Asked Questions, Preliminary — Subject to Modification and Extension, v1.0' (April 2020) <[https://blog.google/documents/63/Exposure\\_Notification\\_-\\_FAQ\\_v1.0.pdf](https://blog.google/documents/63/Exposure_Notification_-_FAQ_v1.0.pdf)> accessed 23 June 2020.

an app would not be required for it to work. At the moment of the present writing, the *app-less* system, called “Exposure Notifications Express” (EN Express), has already been deployed within iOS 13.7 update for iPhone.

It should be noted that the second phase does not replace the first phase, which means that national apps will still be operating even when the system affords to work without an app. Health authorities may now choose between three different options: (i) keep using only their app within the EN framework; (ii) use the *app-less* system, by supporting the EN Express without developing a dedicated app; or (iii) offer their app and support the *app-less* system simultaneously. In case a public health authority develops a national app, it will be available for download in the respective app stores. When health authorities engage with the EN system without a dedicated app, the device will receive a notification when such system becomes available for the region. If health authorities decide to offer a national app and, at the same time, the EN Express (which won’t require an app), the system will operate as follows: when an individual enables the EN system and an app is installed, the system will operate with it; when an app is not installed, the system will fall back to EN Express. In any case, the individual is required to consent to the terms and conditions before EN become active.<sup>6</sup>

---

<sup>6</sup> Google, ‘Exposure Notifications Frequently Asked Questions Preliminary — Subject to Modification and Extension v. 1.2’ (September 2020) <<https://static.googleusercontent.com/media/www.google.com/en//covid19/exposurenotifications/pdfs/Exposure-Notification-FAQ-v1.2.pdf>> accessed 3 November 2020.

The Exposure Notifications framework uses Bluetooth Low Energy (BLE) technology to measure proximity between two devices through the strength of Bluetooth signal, detecting if they were close enough to *infer* that their users are *presumably* at risk. To explain it briefly, individuals who (voluntarily) enable EN framework, allow their devices to broadcast Bluetooth pseudorandom identifiers, called Rolling<sup>7</sup> or Rotating<sup>8</sup> Proximity Identifiers (RPI), to be captured and recorded by devices in the nearby. In both designations, RPI means a random ID derived from a device *Temporary Exposure Key* – a key that is randomly generated once every 24 hours, which remains on the device for up to 14 days.<sup>9</sup> A RPI is generated every 10-20 minutes to avoid identification and tracking.<sup>10</sup> When an individual tests positive and decides to report their diagnosis to the devices participating in the system, their keys are uploaded to a server. Regularly, the participating devices check that server. If a match is found between the uploaded keys of a positive diagnosed person and the

---

<sup>7</sup> Google, 'Exposure Notification Cryptography Specification Preliminary' (April 2020) <[https://blog.google/documents/69/Exposure\\_Notification\\_-\\_Cryptography\\_Specification\\_v1.2.1.pdf](https://blog.google/documents/69/Exposure_Notification_-_Cryptography_Specification_v1.2.1.pdf)> accessed 3 November 2020 refers to *Rolling Proximity Identifiers* and states they are derived from a Rolling Proximity Identifier Key, which is in turn derived from a Temporary Exposure Key and a discretized representation of time.

<sup>8</sup> Google, 'Exposure Notifications API' (22 October 2020) <<https://developers.google.com/android/exposure-notifications/exposure-notifications-api>> accessed 3 November 2020 refers to *Rotating Proximity Identifiers*.

<sup>9</sup> Ibid. In the event of a positive diagnosis of COVID-19, and upon individual's permission, Temporary Exposure Keys are provided to the app or to the server.

<sup>10</sup> 'Exposure Notifications API' (22 October 2020) <<https://developers.google.com/android/exposure-notifications/exposure-notifications-api>> accessed 3 November 2020; Google, 'Exposure Notifications Frequently Asked Questions Preliminary — Subject to Modification and Extension v1.2' (September 2020), <<https://static.googleusercontent.com/media/www.google.com/en//covid19/exposurenotifications/pdfs/Exposure-Notification-FAQ-v1.2.pdf>>, accessed 3 November 2020.

keys recorded on device, the device user will be informed that they were exposed to COVID-19.

The Exposure Notifications (EN) system is designed to prevent identification. Therefore, it does not qualify as a system that allows for contact tracing. Gapple's infrastructure performs notifications to immediate contacts of a positive diagnosed individual, which means that it affords proximity tracking. In other words, the system allows individuals to be informed whether they – or, more precisely, their devices – have been close to a device belonging to a person positively diagnosed with COVID-19.

Proximity tracking may be a helpful technique for aiding contact tracing, but it does not qualify as part of such a public health practice. This distinction might have been the reason why the protocol proposed by Gapple was renamed “Exposure Notifications”, in late April 2020, replacing its previous designation, which was “Privacy Preserving Contact Tracing Protocol”.<sup>11</sup>

This article will cover to the two-phases of the Exposures Notifications project. However, some of its sections will exclusively refer to the first phase (API and national apps), as some of the available information refers only to that phase.

---

<sup>11</sup> Google, ‘Privacy Preserving Contact Tracing Protocol’ <<https://covid19.apple.com/contacttracing>> accessed 5 October 2020; Bunnie, ‘On Contact Tracing and Hardware Tokens’ (Bunnie studios May 2020) <[www.bunniestudios.com/blog/?p=5820](http://www.bunniestudios.com/blog/?p=5820)> accessed 5 October 2020.

### *First Phase: the API Functioning*

As the system has already been briefly described, in this section we will suppose that (i) two individuals have voluntarily engaged with a national proximity tacking app; (ii) their devices have exchanged pseudorandom identifiers for a relevant period of time and (iii) one of them has been diagnosed with COVID-19.

When testing positive, it is up to the individual to decide whether their diagnosis shall be reported to the app. If they so decide, a key is attributed to them by the national health authority (diagnosis key)<sup>12</sup>. That key is uploaded to a server, which is regularly checked by all participating devices. In case a match is found between the keys recorded on device and the keys voluntarily uploaded by COVID-19 diagnosed patients, the device receives an exposure notification. Therefore, individuals are required to consent in order to participate in the system by enabling EN on their devices; and, in case of being diagnosed with COVID 19, must consent the report of their diagnosis to the system, by uploading their device's keys to the server as part of the positive diagnosis list.<sup>13</sup> This means that granting authorisation for the EN to operate does not bind individuals to report themselves to the system in case they test positive for COVID 19.

---

<sup>12</sup> Google, 'Exposure Notifications API' (22 October 2020) <<https://developers.google.com/android/exposure-notifications/exposure-notifications-api>> accessed 3 November 2020 defines it as the *Temporary Exposure Key provided by the server that have been confirmed to have a positive diagnosis of COVID-19* and used by the app to check for exposure.

<sup>13</sup> Google, 'Exposure Notifications Frequently Asked Questions Preliminary — Subject to Modification and Extension v1.2' (September 2020), <<https://static.googleusercontent.com/media/www.google.com/en//covid19/exposurenotifications/pdfs/Exposure-Notification-FAQ-v1.2.pdf>>, accessed 3 November 2020.

### *Second Phase: App-less System Functioning (iOS 13.7)*

The iOS 13.7 update for iPhone allows the EN framework to operate without a dedicated app. This functionality is called Exposure Notifications Express (EN Express) and affords the key server's ability to verify diagnosis certifications from health authorities. It will only be available if a public health authority supports it, by deploying two different types of servers: (i) a test verification server, to validate positive diagnosis during the key upload; (ii) a key server to handle key uploads and downloads, which operates both EN apps and EN Express.

The system's ability to verify diagnosis certifications from health authorities afforded by iOS 13.7 (or later) iPhone update will now be briefly described.<sup>14</sup> We will assume that the individual who uses an iPhone 13.7 (or later) has enabled the EN system on their device. In case they test positive for COVID 19, the test centre will report such result to the public health authority, which will in turn generate a verification code, using the test verification server. That verification code (PIN code) is sent to the individual, either by email, read over the phone, or provided as a clickable deep link in a text message. To inform their iPhone of their positive diagnosis, the individual inserts the verification code or clicks on the provided link,

---

<sup>14</sup> Apple, 'Supporting Exposure Notifications Express' <[https://developer.apple.com/documentation/exposurenotification/supporting\\_exposure\\_notification\\_s\\_express](https://developer.apple.com/documentation/exposurenotification/supporting_exposure_notification_s_express)> accessed 2 November 2020; Google, 'Public Health Authority Diagnosis Verification Protocol' (*Github*, last update 27 October 2020) <[https://github.com/google/exposure-notifications-server/blob/main/docs/design/verification\\_protocol.md](https://github.com/google/exposure-notifications-server/blob/main/docs/design/verification_protocol.md)> accessed 2 November 2020.



after which the iPhone checks the test verification server to validate the code. If the code is valid, it will be exchanged for a long-term authentication token from the test verification server, which is sent to the iPhone and stored. At this stage, the individual might be prompted to give additional health-related information (i.e. symptom onset date). Then, the iPhone creates a hashed message authentication code (HMAC) consisting of the temporary exposure keys, along with calculated transmission risk value, rolling period start and rolling period count values (exposure key data and metadata), after which the HMAC and the authentication token are sent to the test verification server. In return, the iPhone receives a certificate and additional per-key metadata, which it validates and stores. After this proceeding, the individual is asked whether they consent to submit their keys to the key server. If they grant such permission, the iPhone will upload their temporary exposure keys to the key server along with the authentication token, certificate, and metadata received from the test verification server. The test verification server confirms whether the certificate is valid and signed by a trusted health authority. If it is, the uploaded information will be imported to the test verification server database and a revision token, which can be used to upload a diagnosis change for the uploaded keys, is returned. At this point, the validated and uploaded keys are available for download by other devices to be used for on-device exposure detection.

## II. LEGAL FRAMEWORK: $2 + 2 = 5$

Many meanings may be attributed to " $2 + 2 = 5$ ". Here, we are deliberately evoking a dialogue from George Orwell famous novel "Nineteen eighty-four", where, during an interrogation, character O'Brien (the interrogator) asks Winston:

*'Do you remember,' he went on, 'writing in your diary, "Freedom is the freedom to say that two plus two make four"?''*

*'Yes,' said Winston.*

*O'Brien held up his left hand, its back towards Winston, with the thumb hidden and the four fingers extended.*

*'How many fingers am I holding up, Winston?'*

*'Four.'*

*'And if the party says that it is not four but five -- then how many?'*

*'Four.'*

Winston was contradicting a dogmatic statement, because his perception of reality – of logic – was different than the one that the interrogator was hypothesising as one he must accept if the Party says so. In a similar way, we will challenge the juridical qualification claimed by the *letter* of the EN contractual terms, which seems to be contradicted by the factual reality involved in data processing within the system functioning, but also by the *spirit* of such contracts. However, contrary to what

happens in Orwell's novel, it is not a totalitarian state that is imposing a dogmatic reality to an individual citizen, but rather Big-Tech companies that are imposing one to States – and, therefore their citizens.

As a previous point, it is important to state that we consider that EN infrastructure processes *personal data*; not *anonymous data*. Otherwise, (part) of data protection regulative *corpus* would not be applicable and some parts of our analysis would be meaningless.<sup>15</sup> It is true that there has been some discussion on whether pseudorandom identifiers are qualifiable as anonymous<sup>16</sup> or pseudonymous information.<sup>17</sup> However, it is not clear whether the different participants on this debate always mean the same thing when referring to *anonymisation*, as they may have not always adopted the meaning provided for in the GDPR,<sup>18</sup> but, instead, refer to the immediate, or effortless possibility of identification. Since the possibilities of re-

---

<sup>15</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1, Recital (26).

<sup>16</sup> COVID watch, <[www.covidwatch.org/](http://www.covidwatch.org/)> accessed 31 October 2020; National Health Service, 'Guidance NHS COVID-19 app: anonymisation, definitions and user data journeys' (1 October 2020) <<https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/anonymisation-definitions-and-user-data-journeys>> accessed 31 October 2020,

<sup>17</sup> Laura Bradford, Mateo Aboy and Kathleen Liddell, 'COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes' (2020) Vol 7 1 Journal of Law and the Biosciences, 1.; EDPB, 'Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak' (21 April 2020) paras. 41, 43, 46; ICO, 'COVID-19 contact tracing: data protection expectations on app development' (4 May 2020) paras 5, 15. EDPB and ICO descriptions seems to fit the Exposures Notification system developed by Gapple; thus, we may infer that both entities also qualify pseudorandom identifiers as pseudonymous information.

<sup>18</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1, Recital (26).

identification are far from being indisputable, we prefer to qualify pseudo-random identifiers as pseudonymous information.<sup>19</sup>

It is fundamental to check what role do Gapple play in processing activities within the EN framework,<sup>20</sup> that is, whether they are processors – which they claim to be –, or controllers. Therefrom, it will be possible to identify whether Gapple shall be ascribed controller's obligations – for instance, those presupposed by data protection by design and by default –, or processor's obligations – such as, assisting health authorities in their obligations as controllers and complying with their instructions regarding data processing.

Google and Apple published separate contractual terms regulating the use of the API and the development of national apps within it, respectively titled as Google COVID-19 Exposure Notifications Service Additional Terms (GEN) and Apple Exposure Notification APIs Addendum to the Apple Developer Program License

---

<sup>19</sup> DP-3T, 'Clarified anonymous communication question' (*Github*, 7 April 2020) <<https://github.com/DP-3T/documents/commit/f9c5ba50726652f914869dab8ebf07877aa4a81d>>, accessed 31 October 2020. Interestingly enough, DP-3T clarified that the protocol does not rely on anonymous communication systems to provide its privacy properties. DP-3T declared that the use of anonymous systems would conceal the IP address of users submitting reports with respect to the backend. According to the information available, DP-3T have considered using an anonymous communication system to efficiently query the server, but have decided against it, based on three arguments: (i) it would increase the complexity of the system; (ii) anonymity requires a trade with latency and bandwidth overhead, not being clear what the best choice in this scheme; (iii) security properties of the anonymous communication system would need to be considered (and some options were required).

<sup>20</sup> In the context of automation, besides the GDPR, it is important to consider other applicable legal instruments regarding data protection, namely Consolidated Version of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector [2009] OJ 2009 L337/11; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS 108.

Agreement (AEN).<sup>21</sup> Despite some differences in their terms, the contractual drawing seems to portray a delegation of government's digital sovereignty<sup>22</sup> to Gapple, handing them powers that shall solely be exercised by the former when pursuing its public interest mission.

Both Google and Apple API contractual terms determine that only governmental entities are allowed to use the EN API and limit the number of proximity tracking apps to one per country, unless governments have a regional approach or if Google or Apple agree otherwise.<sup>23</sup> Gapple are thereby bound to engage exclusively with governmental entities in providing the use of the API for the purposes of building proximity tracking apps. Nevertheless, it is clear that Gapple have a *de iure* and a *de facto*<sup>24</sup> power to choose which States may build their apps within API and to define the number of proximity tracking apps per country, by making it

---

<sup>21</sup> Respectively, available at [https://blog.google/documents/72/Exposure\\_Notifications\\_Service\\_Additional\\_Terms.pdf](https://blog.google/documents/72/Exposure_Notifications_Service_Additional_Terms.pdf); [https://developer.apple.com/contact/request/download/Exposure\\_Notification\\_Addendum.pdf](https://developer.apple.com/contact/request/download/Exposure_Notification_Addendum.pdf), accessed 3 November 2020. Both contracts were last revised 4 May 2020.

<sup>22</sup> The term *Digital sovereignty* is used by several sources, with different meanings. In this context, the concept is used to refer to the exercise of sovereignty by the States on the digital domain. The notion of sovereignty will be necessarily simplified, meaning the existence of an institutional infrastructure to the exercise of the powers of State, equipped with a system of checks and balances that prevents one power of overruling the other. This includes the existence of an independent judicial power and procedures to guaranty that citizens' right to present claims and contest public and private actions or decisions that affect their rights in a court of law. This understanding of sovereignty builds on Mireille Hildebrandt, 'Origins of the Criminal Law: Punitive Interventions before Sovereignty', ch 11, in Markus D. Dubber (ed.), *Foundational Texts in Modern Criminal Law* (OUP 2014); 'Radbruch's Rechtsstaat and Schmitt's Legal order: Legalism, Legality and the Institution of Law' (2015) Vol 2 No 1 New Historical Jurisprudence & Historical Analysis of Law 42, 57.

<sup>23</sup> Points 1. a GEN; 2.1. AEN.

<sup>24</sup> EDPB, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (Version 1.0, 2 September 2020), paras. 12, 20, 23-28, 49; Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (WP 169, 16 February 2010), at 8-9, 11.

depend on their agreement. AEN even states that Apple, at its own discretion, at any moment in time, may decide to cease distributing the national app without that implying any kind of liability<sup>25</sup> and also to decide whether governments are allowed to use or to remain using the EN API or its Entitlement Profile,<sup>26</sup> irrespective of their app's compliance with AEN and Developer Agreement terms.<sup>27</sup>

Besides the power to choose which States may benefit from the EN system, Gapple's hegemony also stems from data processing terms.<sup>28</sup> AEN and GEN determine national apps means of processing, such as the type of data to be processed and who shall have access to them.<sup>29</sup> As BLE technology does not require geolocation data to operate, national proximity tracking apps may not collect it.<sup>30</sup> However, it is noteworthy that in versions previous to Android 11, the use of the EN system requires the device location to be turned on for all apps. Google claims that in the current versions of Android, even when device location setting is turned on, the phone continues to prohibit access to location by apps that do not have the required permission to use it (including Google apps).<sup>31</sup> Device location may nevertheless be

---

<sup>25</sup> AEN, at 2.2.

<sup>26</sup> Entitlement Profile enables the use of the Exposure Notification API (points 2.2. and 2.3. AEN).

<sup>27</sup> AEN, at 4.

<sup>28</sup> Point 3 of GEN and Section 3 of AEN.

<sup>29</sup> EDPB, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (Version 1.0, 2 September 2020), para. 38, distinguishes between *essential* and *non-essential* means of processing.

<sup>30</sup> Point 3. c. i. GEN and point 3.3. AEN.

<sup>31</sup> Dave Burke, 'An update on Exposure Notifications' (*Company News*, 31 July 2020) <<https://blog.google/inside-google/company-announcements/update-exposure-notifications>> accessed 29 September 2020 announced that Android 11 update will allow individuals to use Exposure Notification apps without turning on the device location setting. However, such an update addresses to Exposure Notifications only, as all other apps and services will still be prohibited from performing Bluetooth scanning unless the device location setting is on.

inferred through the IP address, as will be discussed below. Besides these aspects, Gapple's contract models establish processing legal basis (consent)<sup>32</sup> and require governments to comply with data minimisation and purpose limitation principles.<sup>33</sup> Decisions regarding processing are, by definition, under controller's power.

AEN moreover forbids the use of location-based APIs, the collection of location data from devices and the access to identifiable information, such as photos and contacts, using frameworks or APIs in the Apple Software. The clause contains an important exception, though, which is: *unless otherwise agreed by Apple*.<sup>34</sup> If the decision of collecting further data is dependent on processor's agreement, either they are not a processor, but they are, instead, a controller; or, if they are a processor, such decisions may not depend on their will, and the clause is void.

Likewise, it is particularly curious to observe how GEN terms are contradictory in this respect, as, on the one hand, they establish that *In providing the Service, Google has no role in determining the purposes for which, or manner in which, any personal data are processed by the App*;<sup>35</sup> and, on the other hand, they (i) oblige governments to comply with Google's requirements regarding consent; (ii) impose governments to commit exclusively to one processing purpose; (iii) prohibit collection or other forms of

---

<sup>32</sup> Points 2. a. GEN; 3.1. AEN. Point 3.1. AEN determines that consent is also the legal basis that ground the collection of registration data, as well as data use or disclose, whether from the Exposure Notification APIs, or any other data entered by a user in a Proximity tracking App.

<sup>33</sup> Points 3. b. i. of GEN; 3.1. AEN determine that a proximity tracking app may only collect the minimum amount of user data necessary for COVID-19 response efforts and may only be used for that purpose.

<sup>34</sup> Point 3.3. AEN.

<sup>35</sup> Point 3. a. iii. GEN.

processing, such as cross-platform association; (iv) define precise data retention periods and (v) establish conditions for sharing data with third parties.<sup>36</sup> Similar provisions may be found in AEN.<sup>37</sup>

In spite of Gapple's claim that governments determine the purpose of processing, AEN and GEN establish that the former may not process or disclose data using the EN API (or any other data entered by a user in a proximity tracking app) for any purpose not related to COVID-19 response efforts, such as law enforcement, including individual quarantine.<sup>38</sup> Such specific form of consecrating purpose limitation principle within the EN framework demonstrates that Gapple (co-) determine not only the means, but also the purpose of processing. This is furthermore confirmed by AEN terms, according to which moving from an existing COVID-19 app to a contact tracing app (by means of associating data collected through the use of both Apple Software and proximity tracking apps) is conditioned to Apple and user's

---

<sup>36</sup> Points 3. b., i-vi GEN.

<sup>37</sup> AEN contemplates several similar dispositions, such as the data to be collected, transmitted, or accessed (3.2., 3.3., 3.4.); the use of third-party analytics; retention period (3.4.); purpose (3.1.), the legal basis of processing; and disclosing rules (3.1.). It furthermore prohibits processing location data; any form of data association or correlation and the access to personally identifiable information, unless otherwise agreed by Apple (3.2.; 3.3).

<sup>38</sup> Points 3.1. AEN; 1. d GEN. EDPB; 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR', (Version 1.0, 2 September 2020), paras. 57-58 EDPB suggests that *joint determined purposes* do not necessarily mean that joint controllers pursue the same purposes; it may cover situations where different purposes are closely linked or complementary. In case each of the entities involved participates in the determination of the purposes and means of the relevant processing operation, an indicator that purposes are jointly determined may be the existence of a mutual benefit arising from the same processing operation. About mutual benefit, C-40/17 *Fashion ID* [2019] (ECLI:EU:C:2019:629), at para. 80, which involved processing operations performed in the economic interests economic of the parties involved. In the case discussed in the present article, the economic interest is solely from Gapple's, as Governments' interest concerns public interest.



consent.<sup>39</sup> Governments seem to be the sole entity abided by the purpose limitation principle, as no reference to such principle regards the EN infrastructure.

Gapple present themselves as processors who genuinely want to support governments' efforts to control COVID-19 pandemic, by providing a data protection-friendly system where they may develop national proximity tracking apps and verify diagnosis certifications from health authorities. Under the claim that Gapple do not access any data – as it is processed exclusively on device –, the buck of controllership is passed to governments. However, this is a misleading argument, as the concept of joint-controllership (which would apply if Gapple were deemed to be data controllers) does not necessarily require that each of the parties responsible for the same processing have access to the personal data concerned.<sup>40</sup> What is relevant for controllership is the factual (and decisive) influence in data processing, namely by determining its purpose and its essential means – which seem to qualify Gapple as a data controller.<sup>41</sup>

Gapple's statute of processor is also invoked under the argument that the purposes of processing are determined by governments, and that Gapple's role consists *only* in providing the technical resources that afford it. Yet, it must be

---

<sup>39</sup> Point 3.5. from AEN.

<sup>40</sup> C-25/17 *Jehovan todistajat* [2018] (ECLI:EU:C:2018:551), at para. 75; C-210/16 *Wirtschaftsakademie* [2018] (ECLI:EU:C:2018:388), at para. 38; EDPB, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR', (Version 1.0, 2 September 2020), paras. 42, 54.

<sup>41</sup> EDPB, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR', (Version 1.0, 2 September 2020), para. 49.

considered that the use of an existing platform, with standardised tools developed by one of the parties, does not necessarily rule out (joint-) controllership.<sup>42</sup>

GEN and AEN terms allow to infer the joint participation of governments and Gapple in data processing,<sup>43</sup> making quite problematic the tenet according to which the latter are qualified as processors. Interestingly enough, the norms concerning the right to data protection refer only to the design of proximity tracking apps that use the EN system, not to EN system itself. Therefore, it seems clear that GEN and AEN impose on Governments a specific kind of standardized design to their national apps, which they must abide by if they want to engage with (or keep using) their framework.

To sum up, Gapple qualify themselves as data processors (which by definition act exclusively under controller's instructions), but at the same time (i) impose a specific design on national proximity tracking apps; (ii) define the means of data processing; (iii) establish processing legal basis; and (iv) frame processing activities, either by permitting or prohibiting them.

The fact that two private companies determine the above-mentioned aspects of processing personal data in the context of a global pandemic must not be ignored, as

---

<sup>42</sup> C-40/17 *Fashion ID* [2019] (ECLI:EU:C:2019:629), paras. 78, 79, 84; EDPB, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR', (Version 1.0, 2 September 2020) paras. 63, 65.

<sup>43</sup> Ibid. EDPB, paras. 51, 53. EDBP clarifies that joint participation may result either from a common intention regarding processing, or from converging decisions by two or more entities concerning the purposes and means of processing. Decisions may be considered as converging on purposes and means *if they complement each other and are necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing*, at para. 53. An important criterion to identify converging decisions is whether the processing would not be possible without both parties participation in the sense that the processing by each party is inseparable.

its exceptional nature require governments and public health authorities to make decisions that may impact their citizen's fundamental rights and freedoms. This intervention must be exclusively framed by means of democratic participation, free from interferences from outside the system of countervailing powers shaped by the Rule of Law.

We may freely say that  $2 + 2 = 4$  (determination of purpose + determination of means = controllership).

### III. INCURSION TO THE EN AND NATIONAL APP'S ARCHITECTURE

#### *Google's Exposure Notifications Architecture (API)*

The EN design has already been summed up in the first section of this article. We will now specify some of the aspects of the API architecture within Google framework.

The API system is distributed through several subsystems, specifically: (i) Google Play services; (ii) mobile app; (iii) authenticated medical provider validation mechanism; and (iv) Internet-accessible server.<sup>44</sup> Google Play services<sup>45</sup> plays a fundamental role in the architecture of the EN system, as it is within it that Bluetooth functionality operates, which, in its turn, includes all broadcasts and scans for BLE

---

<sup>44</sup> Google, 'Exposure Notifications API' (22 October 2020) <<https://developers.google.com/android/exposure-notifications/exposure-notifications-api>> accessed 3 November 2020.

<sup>45</sup> Google Play services is proprietary app, which makes it impossible to audit.

beacons, along with local database storage.<sup>46</sup> Google Play services connects to Google servers roughly every 20-minute period, sharing the IP address with Google through those connections. The requests generated by these connections disclose the IP to Google, containing persistent identifiers that allow requests from the same device to be linked together.<sup>47</sup> According to Google Privacy Policy, the IP serves as a proxy for device location.<sup>48</sup>

Besides the IP, when Google Play Services is enabled, the “Usage & diagnostics” option is activated by default, and telemetry data is collected even when all other Google services and settings are disabled.<sup>49</sup> Google’s official documents clarify that *turning off usage and diagnostics won’t affect info that apps might collect*.<sup>50</sup> Such collection

---

<sup>46</sup> Google, ‘Exposure Notifications API’ (22 October 2020) <<https://developers.google.com/android/exposure-notifications/exposure-notifications-api>> accessed 3 November 2020.

<sup>47</sup> Douglas Leith and Stephen Farrell, ‘Contact Tracing App Privacy: What Data Is Shared By Europe’s GAEN Contact Tracing Apps, (School of Computer Science & Statistics, Trinity College Dublin, Ireland 18 July 2020) <[www.scss.tcd.ie/Doug.Leith/pubs/contact\\_tracing\\_app\\_traffic.pdf](http://www.scss.tcd.ie/Doug.Leith/pubs/contact_tracing_app_traffic.pdf)> accessed 29 September 2020.

<sup>48</sup> Google Privacy Policy (30 September 2020), <<https://policies.google.com/privacy?hl=en-US>> accessed 3 November 2020 states that device location may be determined with varying degrees by GPS, IP address, sensor data from device, and also information about things near the device, such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices.

<sup>49</sup> Douglas Leith and Stephen Farrell, ‘Contact Tracing App Privacy: What Data Is Shared By Europe’s GAEN Contact Tracing Apps, (School of Computer Science & Statistics, Trinity College Dublin, Ireland 18 July 2020) <[www.scss.tcd.ie/Doug.Leith/pubs/contact\\_tracing\\_app\\_traffic.pdf](http://www.scss.tcd.ie/Doug.Leith/pubs/contact_tracing_app_traffic.pdf)> accessed 29 September 2020. The Authors claim that Google Play Services sends to Google, amongst other things, the phone IMEI, the handset hardware serial number, the SIM serial number, the handset phone number, the WiFi MAC address and the user email address. They confronted Google with the collection of telemetry data and Google responded that their telemetry is “an industry practice” and that it provides information on ways to turn off usage and diagnostics.

<sup>50</sup> Google, ‘Share usage & diagnostics information with Google’ <<https://support.google.com/accounts/answer/6078260?hl=en>> accessed 30 September 2020. Google, ‘Exposure Notifications telemetry design’ <<https://developers.google.com/android/exposure-notifications/telemetry-design>> accessed 30 September 2020 provides further information on telemetry design.

cannot be opted out, therefrom allowing fine-grained tracking of device location over time by Google.<sup>51</sup>

The iteration between Google Play services and Google servers involves substantial data collection – or, more accurately, data processing –, largely transcending what is necessary for COVID-19 response efforts. Such processing transcends the functioning purpose of national proximity tracking apps and is outside any instruction from health authorities. Therefore, Google must be deemed to be data controller with respect to data processing afforded by the above-mentioned iteration.<sup>52</sup> The qualification as controller binds it to comply with several obligations laid down in data protection regulation *corpus* such as Article 25 GDPR, or Article 5 (3) E-Privacy Directive.

It is not clear what legal basis – if any – may ground such an extensive data processing. Consent seems ruled out by the impossibility of opting-out of such data processing - and, in any case, opting-out would not be a valid form of consent in this context.<sup>53</sup> For this specific collection, there seems to be no contract between the individual that uses the device and Google, nor the latter is complying with a legal

---

<sup>51</sup> Douglas Leith and Stephen Farrell, 'Contact Tracing App Privacy: What Data Is Shared By Europe's GAEN Contact Tracing Apps, (School of Computer Science & Statistics, Trinity College Dublin, Ireland 18 July 2020) <[www.scss.tcd.ie/Doug.Leith/pubs/contact\\_tracing\\_app\\_traffic.pdf](http://www.scss.tcd.ie/Doug.Leith/pubs/contact_tracing_app_traffic.pdf)> accessed 29 September 2020. According to the information included on footnote 3 of the referred article, Google was specifically contacted by the Authors regarding the possibility of opting out, and confirmed it was not possible.

<sup>52</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1, Article 28 (10).

<sup>53</sup> We are analogically evoking C-673/17 *Planet 49* [2019] (ECLI:EU:C:2019:801), paras. 56, 57, 70, 71.

obligation, or protecting any vital interest, or carrying out a public interest mission that requires performing such processing. Thus, the only thinkable legal basis that could justify this massive data collection would be legitimate interest. However, to validly invoke any interest as presumably legitimate, the data controller must assess whether fundamental rights of data subjects override such interest, namely considering if they may *reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place*.<sup>54</sup> In case data subjects' fundamental rights override data controller's interest, processing must not take place. The public documents released by Google and Apple about the EN framework claim that data processing happens exclusively on device, thereby declaring that they do not have access to personal data. If such documents are to be trusted, it is untenable to consider that people who voluntarily engage with an app built within Gapple's framework may expect such an extensive data processing. In this case, it seems very hard to sustain that individuals' fundamental rights do not override Google's interest – or, even admitting that hypothesis, the extension of data collection would hardly be strictly necessary to fulfil it.

Moreover, depriving data subjects from opting-out – and, we suppose, from objecting – such a massive *by default* data collection, favours the hypothesis that data subjects' fundamental rights override Google's interest in such collection. We are

---

<sup>54</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1, Recital (47).

aware that the right to protection of personal data is not an absolute right and that in some cases it must be restricted by a legislative measure in favour of other principles, values, or rights, when that restriction respects the essence of the fundamental rights and is a necessary and proportionate measure in a democratic society.<sup>55</sup> But this seems not to be the case – and even if it was, relevant information about processing is not provided.

### *National Apps Design Using Firebase*

Some national apps<sup>56</sup> may use Firebase, a tool developed by Google to build a range of services, that allows developers to be dismissed of the burden of developing those services by themselves into the national apps.<sup>57</sup> According to Firebase documentation, *analytics automatically generates and assigns an app-instance ID to each instance of your app* to compute user metrics.<sup>58</sup> By default, developers will not need to write additional code to collect a significant number of personal information, namely

---

<sup>55</sup> Ibid Article 23.

<sup>56</sup> STOP COVID - ProteGO Safe project, 'STOP COVID - ProteGO Safe Android app' (*Github*, last update 30 October 2020) <<https://github.com/ProteGO-Safe/android>> accessed 3 November 2020; Centre for Disease Prevention and Control (CDPC) of Latvia, 'SPKC Apturi Covid Android Application' (*Github*, last update 20 October 2020) <<https://github.com/ApturiCOVID/apturicovid-android>>, accessed 3 November 2020.

<sup>57</sup> Doug Stevenson, 'What is Firebase? The complete story, abridged' (25 September 2018) <<https://medium.com/firebase-developers/what-is-firebase-the-complete-story-abridged-bcc730c5f2c0>> accessed 29 September 2020; Pieter de Busschere, 'All you need to know about firebase' (29 October 2019) <<https://www.the-reference.com/en/blog/pieter-de-busschere/firebase>> accessed 29 September 2020.

<sup>58</sup> Google, 'Predefined user dimensions' <<https://support.google.com/analytics/answer/6317486?hl=en>> accessed 1 October 2020.

age category, country, gender (in male/female binary form), interests, device language setting, OS version and also data about the app, the device, and the interaction between the individual and the app.<sup>59</sup>

Firestore analytics derives demographic and interest information from users' app activity, through two sources: (i) Android Advertising ID, which, if not shared, analytics will not be able to derive the above-mentioned data; and (ii) iOS Identifier for Advertisers (IDFA). Device location is derived from IP address.<sup>60</sup>

Even if the information transmitted to Google – whether through Google Play Services or Firestore – was metadata, that would not obliterate concerns involving human rights. As Article 29 Working Party underlined, it is not correct to assume that metadata collection is less serious than collecting content, as it involves *all data about a communication taking place, except for the content*.<sup>61</sup> Both Court of Justice of European Union (CJEU) and European Court of Human Rights (ECHR) acknowledged metadata's potential to interfere with private life,<sup>62</sup> to expose individuals to profiling

---

<sup>59</sup> Ibid. Data collected about the App: App Store from which the app was downloaded and installed and App Version (Android) or the Bundle version (iOS). Data collected about device: device brand, category of the mobile device (e.g., mobile or tablet); device model name. Data about the interaction between the individual and the app: the time (in milliseconds, UTC) at which the user first opened the app, rounded up to the next hour; and whether the app was first opened within the last 7 days (classified as 'New') or more than 7 days ago (classified as 'Established').

<sup>60</sup> Ibid.

<sup>61</sup> Article 29 Working Party, 'Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes' (WP 215, 10 April 2014), at 4.

<sup>62</sup> *Malone v UK* (1984) 7 EHRR 14 para. 84; *Ben Faiza v France*, App no 31446/12 (ECtHR 8 February 2018) para. 66; C-203/15 *TeleSverige* [2016] (ECLI:EU:C:2016:970), paras. 100-101; Joined Cases C-293/12 and C-594/12 *Digital rights Ireland* [2014] (ECLI:EU:C:2014:238, 2014/04/08) paras. 26-27; C-673/17 *Planet 49* [2019] (ECLI:EU:C:2019:801), para. 70. Also underlying collection of metadata as an interference in private life, C-311/18 *Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems* [2019] (ECLI:EU:C:2019:1145), Opinion of AG Saugmandsgaard Øe, paras. 257, 259.



risks<sup>63</sup> and to impact the use of means of communication that allow such processing (by interfering with freedom of expression,<sup>64</sup> or by generating a feeling of constant surveillance).<sup>65</sup> Following Recital 24 of E-Privacy Directive – which applies to EN framework, as it concerns processing of personal data in the electronic communications sector –, CJEU case-law has already confirmed that protection of private life regards *any information* stored on the terminal equipment of users of electronic communications networks – not only personal data.<sup>66</sup>

Health authorities, or developers on their behalf, should consider such an extensive data collection before deciding to outsource the development of national apps to Firebase, as it compromises their compliance with data protection principles (data minimisation, lawfulness, fairness and transparency).

In this section we investigated the architecture within Google’s API framework. Contrary to Gapple’s claims that data is only processed on device, Google’s underlying system affords an extensive and surreptitious data collection, which infringes data protection principles<sup>67</sup> and, more broadly, human rights. Outsourcing development tools to Firebase allows governments and Google to access demographic

---

<sup>63</sup> C-203/15 *TeleSverige* [2016] (ECLI:EU:C:2016:970), paras. 98, 99. Specifically mentioning profiling through sophisticated computer tools, Article 29 Working Party, ‘Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes’ (WP 215, 10 April 2014), at 5.

<sup>64</sup> Joined Cases C-293/12 and C-594/12 *Digital rights Ireland* [2014] (ECLI:EU:C:2014:238, 2014/04/08) paras. 26, 28.

<sup>65</sup> C-203/15 *TeleSverige* [2016] (ECLI:EU:C:2016:970), paras. 100, 101.

<sup>66</sup> C-673/17 *Planet 49* [2019] (ECLI:EU:C:2019:801), para. 70.

<sup>67</sup> Especially, data minimisation, purpose limitation, lawfulness, transparency, fairness and storage limitation.

and individual-interests data, transcending by large what is necessary for COVID-19 response efforts and for the EN framework to operate. Such a massive data collection undermines one of the major advantages attributed to decentralised systems, which, unlike centralised options, are *apparently* not (so) prone for repurposing and surveillance by the State or by the entity in charge of managing the server.

#### IV. SECURITY VULNERABILITIES

In this section, we will describe different kinds of attacks to the EN infrastructure. We are aware that many other design-related security vulnerabilities have already been pointed out, such as trolling, location-collection by third-parties through their apps (or by a central server), or re-identification of pseudonymised data.<sup>68</sup> It is not the object of the present article to exhaustively list all possible security weaknesses within Gapple's proposal. Thus, we will report three kinds of successful attacks.

One of the attacks was conducted to verify the risk of profiling and tracking people who reportedly tested positive for COVID-19.<sup>69</sup> The attack involved the deployment of BLE sniffers to capture RPI in six targeted sensitive places downtown the city of Darmstadt, Germany. The captured RPIs were matched with the RPIs of

---

<sup>68</sup> Julia Angwin, 'Will Google's and Apple's COVID Tracking Plan Protect Privacy?' (*Markup*, 14 April 2020) <<https://themarkup.org/ask-the-markup/2020/04/14/will-googles-and-apples-covid-tracking-plan-protect-privacy>> accessed 6 October 2020.

<sup>69</sup> Lars Baumgärtner and others, 'Mind the GAP: Security & Privacy Risks of Contact Tracing Apps' (Law arXiv, 9 June 2020), at 6-9 <<https://arxiv.org/abs/2006.05914>> accessed 18 June 2020.

infected individuals, allowing to track the movements of each of the participants in the experiment. Individuals who did not upload their diagnosis keys to the system were not traceable. However, the Authors argue that tracking infected user's movements for 14 days – as the uploaded keys cover a 14-day period – may reveal travel patterns across different days, therefore allowing profiling and potential identification, by combining them with information available in social networks.<sup>70</sup>

The same experiment (based on DP-3T prestandard SampleApp) conducted a relay-based wormhole attack<sup>71</sup> by combining two or more physical locations into one logical location. At least two BLE enabled wormhole devices were placed in different physical locations, and recorded BLE messages broadcasted by mobile devices in the vicinity. Then, messages were transferred between the wormhole devices and broadcasted to all mobile devices in both locations. As a result, the messages seemed to come from only one location. We may imagine a tunnel, where information enters through one end and is broadcasted in the other end while this process occurs both ways. The message generated at one end, will then be sniffed by devices at the other end, as if it was generated there. Thus, the same BLE message is detected by devices in both ends of the tunnel, as if was generated in two different locations. The attack succeeded in establishing logical contact between devices that were 40 kilometres

---

<sup>70</sup> Ibid.

<sup>71</sup> Yih-Chun Hu; Adrian Perrig; David B. Johnson, 'Wormhole Attacks in Wireless Networks' (2006), in IEEE Journal on Selected Areas in Communications, Volume: 24, Issue: 2.

apart in two cities, without real-world contact.<sup>72</sup> This security-level vulnerability may impact the efficiency of the whole Gapple framework, (predictably) increasing the demand for testing, thus pressing the healthcare system based on false information.

Another attack was steered to smartphones supported *inter alia* by SwissCovid app, based on MAC (media access control address)<sup>73</sup> and RPI rotation scheme. MAC and RPI are programmed to rotate simultaneously every 15 minutes in order to prevent remote tracking. The attack premise was based on the following question: what if MAC and RPI do not rotate at the same time?<sup>74</sup> Google acknowledges this possibility, declaring that *Android doesn't have a callback to notify an application that the Bluetooth MAC address is changing (or has changed)*.<sup>75</sup> Such problem is handled by *explicitly stopping and restarting advertising whenever a new RPI is generated*.<sup>76</sup> However, the attack showed that a passive eavesdropper may be able to correlate RPIs broadcasted by BLE messages, when MAC address is changed before the RPI. This is easily understandable by the example below:

- Message 1 broadcasts MAC 1 and RPI 1;

---

<sup>72</sup> Lars Baumgärtner and others, 'Mind the GAP: Security & Privacy Risks of Contact Tracing Apps' (Law arXiv, 9 June 2020), at 11 <<https://arxiv.org/abs/2006.05914>> accessed 18 June 2020.

<sup>73</sup> A device is attributed a MAC by the manufacturer in order to uniquely identify it within the network.

<sup>74</sup> Serge Vaudenay and Martin Vuagnoux, 'Little Thumb Attack on SwissCovid' (3 September 2020) <<https://vimeo.com/453948863>> accessed 23 September 2020 (this reference is a video explaining the attack, released by its Authors). The video refers to 'Bluetooth Device Address', as an address that is inside every Bluetooth messages, similarly to MAC address on network devices.

<sup>75</sup> Google, 'Exposure Notifications API' (Github, last update 21 July) <<https://github.com/google/exposure-notifications-internals/blob/main/README.md#ble-mac-and-rpi-rotation>>, accessed 15 October 2020.

<sup>76</sup> Ibid. This repository refers to 'Bluetooth Low Energy MAC', whereas the video referenced on the previous note refers to 'Bluetooth Device Address'.

- Message 2 broadcasts MAC 2 and RPI 1; and
- Message 3 broadcasts MAC 2 and RPI 2

It is, therefore, possible to correlate new MAC with previous RPI, thanks to Message 2. The trace left by this asynchronism was nicknamed by the attackers as a ‘Pebble’.<sup>77</sup> Within the 15 smartphones that were tested, 8 were supported by SwissCovid app (Samsung, Huawei, Wiko and Motorola). Five of these 8 devices were vulnerable to the attack. If MAC address and RPI do not necessarily change simultaneously, a device may be tracked for more than a 15-minute period. As a result, Bluetooth messages were eavesdropped within a 50 meters radius, using a *cheap, basic antenna*,<sup>78</sup> which suggests that the attack was easy to deploy. Google qualifies the risk of such an attack as *minimal*, under the argument that the association between MAC addresses and RPI’s could not be done for more than a ~10 minutes (a single RPI period), because once the RPI rotates, MAC address rotates again, making it difficult to track the association of either the MAC address or RPI to a common device.<sup>79</sup>

Besides, SwissCovid app, other proximity tracking apps that use Gapple’s framework were tested, namely: Immuni (Italy); Corona-Warn (Germany) and StoppCorona (Austria). All of them were found to be vulnerable to the attack.

---

<sup>77</sup> The name comes from Charles Perrault fairy tale “Little Thumb”, in which a little boy uses white pebbles to mark the trail back home.

<sup>78</sup> Vaudenay and Vuagnoux, (n 67).

<sup>79</sup> Google, ‘Exposure Notifications API’ (*Github*, last update 21 July) <<https://github.com/google/exposure-notifications-internals/blob/main/README.md#ble-mac-and-rpi-rotation>>, accessed 15 October 2020. According to Google, ‘Exposure Notifications API’ (22 October 2020) <<https://developers.google.com/android/exposure-notifications/exposure-notifications-api>> accessed 3 November 2020, a RPI is generated every 10-20 minutes.

In their official documents, Gapple disseminate the idea that the EN system affords individual controllership, non-traceability, and exclusive access by health authorities. The advantages of the system are advertised and easily accessible, as a commercial approach would advise, whereas information on security vulnerabilities is disseminated through different Google and Apple webpages, and needs to be specifically searched to be found, not being provided in a comprehensive way to the general public. Security vulnerabilities could be addressed by a DPIA in a transparent and comprehensive way. As shown below, a DPIA is mandatory, considering BLE technology and its purpose, therefore being the place *par excellence* where security vulnerabilities could be assessed and the measures to mitigate them be listed. The relevance of transparency in this case is particularly salient, for the context where this technology operates is not commercial for its participants; rather, the EN system is partaking in a public health interest mission. And even if Gapple were not in such a significant position, they would still be subjected to data protection norms and a DPIA would still be mandatory.

If Gapple created a *protective* system, it means that they know *what* they want to avoid, that is, the *quid* of such protection. Therefore, the risks have most certainly been assessed and attributed different degrees of likelihood. Although such information concerns all the potential participants on the system, Gapple are keeping it to themselves. More than security, transparency seems to be the EN major vulnerability.

## V. LEGAL BY DESIGN

### *Concept*

It is important to recall what we mean by *legal by design*. We are building on Mireille Hildebrandt's work, who conceives *legal by design* as a subset of techno-regulation, which aims at ensuring compliance with legal obligations by way of technological enforcement.<sup>80</sup> This way of *brute (en)forcing or nudging* compliance with legal rules is afforded by deliberate design choices, which convey a single interpretation of one or more legal norms, thereby eliminating the possibility of non-compliance with that specific interpretation of a rule or nudging people into compliance as it were behind their backs.<sup>81</sup>

Law as we know it constrains human behaviour in a way that does not take out the individual possibility to disobey it; it speaks a language of *oughts*, being purposely illiterate in the vocabulary of "is".<sup>82</sup> Such language of *oughts* is informed by the inherent elusiveness of natural language, making Law an interpretative game, which is neither random, nor mathematical. The *game* is rule-based (thereby, being technical),

---

<sup>80</sup> Paul Lippe, Daniel Martin Katz and Dan Jackson, 'Legal by Design: A New Paradigm for Handling Complexity in Banking Regulation and Elsewhere in Law', (2015) Vol 93 No 4, *Oregon Law review*, 833. The Authors suggest that the complexity of legal relations requires human and technology ensembles to improve efficiency and accuracy in risk analysis and decision-making. The concept of *legal by design* is connoted, in a different sense, with technological solutions that systematise information for an efficient management of legal information complexity, allowing informed decision-making.

<sup>81</sup> Mireille Hildebrandt, *Law for Computer Scientists and Other Folk*, OUP (2020).

<sup>82</sup> Roger Brownsword, 'Technological management and the Rule of Law' (2016) Vol 8 No 1 *Law, Innovation and Technology*, 100.

but the systemic *moves* of such rules are debatable.<sup>83</sup> *Legal by design* forgets the ductile nature of the game, by embedding a single indisputable interpretation (out of many possible), compiled into programming language and implemented in a hard or software solution, with the purpose to enforce or nudge into compliance with legal norms.

#### *A Specific Interpretation for (im)Proper Compliance?*

As a possible example of *legal by design*, EN incites questioning of *whose* behaviour might be regulated through technology. It seems that it is not the individual citizen who might be forced to comply with legal rules through technological means, as the system is not allowed to be used for purposes of forced quarantine. As we saw, individual engagement with (as quitting using) the EN system is voluntary. Thus, compliance with legal rules might rather be imposed on governments and their health authorities.

Either within the API, or in an *app-less* system, it appears to be very difficult for the health authorities not to comply with the normative logic embedded in the system. This seems to be especially relevant in the EN express architecture, since national authorities do not have a *de facto* power of building an app, thus being (even more) dependent on of the system for proximity tracking purposes. In the case of national

---

<sup>83</sup> Mireille Hildebrandt, 'Legal and technological normativity: more (and less) than twin sisters' (2008) Vol 12 3 *Techné: Research in Philosophy and Technology*, 169.



apps, it is not entirely clear how Gapple will enforce some of the contractual prohibitions,<sup>84</sup> for instance whether they will technically block the access or the use of other platforms that would allow health authorities (as data controllers) to collect more data.

But which specific interpretation do Gapple impose through its system?

If we consider the official documents, the design choices focus on unlikability and de-identification. This means that Gapple's interpretation of data protection principles of minimisation, confidentiality and storage limitation incorporates Privacy Enhancing Technologies' (PETs) approach.<sup>85</sup> The design of the framework does not seem to allow health authorities, as controllers, to collect more information than the one allowed by the system's infrastructure – regardless if it is necessary to the purpose for which the it was designed in the first place.

To be efficient in tackling COVID-19, health authorities might require identification and further information about recent contacts of an infected person. A COVID-19 carrier with mild or no symptoms may spread the disease through their

---

<sup>84</sup> Namely, regarding (i) the use of the advertising identifier (3.2. AEN; 3. b. iv. GEN), or other personal data (3.3. AEN), (ii) keys (3.4. AEN; 3. b. iv. GEN, except for diagnosis keys, under user consent), (iii) cross-platform data collection and profiling (3.5. AEN), (iv) association of Diagnosis Keys from different end users or devices or linking together specific individuals through the use of service (3. b. iii.; 3. b. v GEN).

<sup>85</sup> On privacy as confidentiality and privacy as control, Seda Gürses, 'Can You Engineer Privacy?' (2014) Vol 57 No 8 *Communications of the ACM*, 20. It is important to note that other ensembles of design strategies (structural organisation for software) have been already identified based on data protection law in Jaap-Henk Hoepman, 'Privacy Design Strategies (Extended Abstract)' (6th Annual Privacy Law Scholars conference, Berkeley, June 2013). The Author claims that design strategies do not necessarily impose a specific structure on the system; they, rather, limit its possible structural realisations.

contacts and receive a notification that they have been exposed to the virus, because one of their contacts got tested first, thereby generating misleading information to those affected and to health authorities.<sup>86</sup> Data minimisation does not mean data exiguity, let alone data scarcity; it means that personal data may be processed in the required measure to fulfil the purpose that determined its collection. We are not saying that personal data should be collected *by default just in case* health authorities might need it, but, rather, that they should be able to determine what types of data are required in a case-by-case basis. Moreover, health professionals are bound by statutory obligations of confidentiality, which makes them a trusted party to which health information may be revealed in order to assure an efficient response from the health system. Ultimately, embracing PETs typical interpretation of data protection principles may undermine the efficiency of the strategy to tackle COVID-19.

In case the EN system does not allow – as all seems to indicate – further data collection where necessary for COVID-19 efforts, it means that health authorities will be *forced* to comply with a potentially inadequate interpretation of data protection principles.

A word shall be said about the mismatch between public documentation released by Gapple and the actual system functioning. Gapple claim that no data processed by the system is accessed by Google or Apple and that the system was built

---

<sup>86</sup> Bunnie, 'On Contact Tracing and Hardware Tokens' (Bunnie studios May 2020) <[www.bunniestudios.com/blog/?p=5820](http://www.bunniestudios.com/blog/?p=5820)> accessed 5 October 2020.

to hinder identification and linkability, thus complying with data minimisation, confidentiality and storage limitation principles. These principles are imposed to the States that engage with the Exposures Notifications framework, either in the development of their national proximity tracking apps, or by the architecture that allows them to inform individuals about potential exposures to COVID-19 without a dedicated app. However, the iteration between Google Play services and Google shows a different – indeed, an opposite – narrative, where purpose limitation, minimisation, confidentiality and storage limitation are transfigured into repurposing, data maximisation, disclosure and undetermined storage.

Only governments and health authorities are forced by the system to comply with a specific interpretation of data protection rules; whereas, Google is allowed by its architecture to surreptitiously collect massive amounts of personal information, therefrom continuing the business model by which it became a highly profitable company.<sup>87</sup> In the EN framework, *Legal by design* seems to be one-sided.

## VI. LEGAL PROTECTION BY DESIGN

### *Concept*

---

<sup>87</sup> Shoshana Zuboff, 'It's not that we've failed to rein in Facebook and Google. We've not even tried', *The Guardian*, (London, 2 July 2019) <<https://www.theguardian.com/commentisfree/2019/jul/02/facebook-google-data-change-our-behaviour-democracy>> accessed 25 April 2020.

The concept of *legal protection by design* is also taken from Mireille Hildebrandt's work. *Legal protection by design* acknowledges that technologies have a constraining impact on human behaviour that can be even more significant than the one legal norms have. Thus, automation must be subjected to the same legitimation requirements than those legal norms are before being valid (acceptable) and enforced in the legal order, that is, being subjected to the system of countervailing powers that shapes the Rule of Law in a democratic system.

Legislative, administrative and adjudicative powers must be circumscribed in such a way that each of them exerts sovereignty only within their sphere of competence, thus being limited, but also limiting potential interference of the other powers.<sup>88</sup> In a democratic system, representative powers are personified in the figure of the *legislature*, which makes laws through proper legal procedures that ensure democratic participation, or at least some form of public scrutiny. Administration and adjudication decision making must be subject to procedures that allow proper instances of contestation before crystallising in the legal order.<sup>89</sup> This presupposes that *contestants* understand the logic involved in such decisions and are equipped with adequate means to challenge them. Therefore, the term *legal protection* calls for the intervention of the democratic legislator and underlines the possibility of contesting

---

<sup>88</sup> Mireille Hildebrandt, 'Radbruch's Rechtsstaat and Schmitt's Legal order: Legalism, Legality and the Institution of Law' (2015) Vol 2 No 1 New Historical Jurisprudence & Historical Analysis of Law, 42.

<sup>89</sup> On the relevance of procedures to the Rule of Law, Jeremy Waldron, 'The Rule of Law and the Importance of procedure' (2011) Vol 50, 3, *Nomos*, 3.

the juridical act that impacts individual legal sphere;<sup>90</sup> *by design* emphasizes that the relational nature of the interplay between human and machine is to be considered, rather than merely embedding legal rules into technology by ingenious engineering.<sup>91</sup> In other words, *legal protection by design* is about preserving the Rule of Law within democratic systems, where automation must be subjected to democratic participation before being implemented and its outcome challengeable by those affected by it.

AEN and GEN contractual terms impose a specific form of processing to governments that opt to build their national proximity tracking apps within Gapple's framework. Some could say that a contract presumes that the parties are in balanced positions and that governments *chose* freely to engage with the EN system proposed by Gapple. We do not know to what extent governments could have avoided engaging with tech-giants. However, we know that Gapple have built their proximity tracking system based on a proposal by the international consortium DP-3T,<sup>92</sup> with whom governments maybe could have engaged with, that way preventing the intervention of private companies in public decision-making. That said, it results from the clauses

---

<sup>90</sup> Mireille Hildebrandt, *Smart Technologies and the End(s) of Law*, Edward Elgar Publishing USA (2015); 'Law as computation in the era of artificial legal intelligence: Speaking to the power of statistics' (2018) Vol 68 Supplement 1, *University of Toronto Law Journal*, 12; *Law for Computer Scientists and Other Folk*, OUP (2020).

<sup>91</sup> Mireille Hildebrandt, 'Legal Protection by Design. Objections and Refutations' (2011) Vol 5, 2 *Legisprudence*, 223. In a different approach, but also underlining the importance of individual interaction with the design, Jaap-Henk Hoepman, 'Privacy Design Strategies (Extended Abstract)' (6th Annual Privacy Law Scholars conference, Berkeley, June 2013).

<sup>92</sup> DP-3T, 'DP3T – Decentralized Privacy-Preserving Proximity Tracing' (*Github*, last update 30 September) <<https://github.com/DP-3T/documents>> accessed 30 October 2020. The Decentralised Privacy-Preserving Proximity Tracing (DP-3T) project is an open protocol for COVID-19 proximity tracing using Bluetooth Low Energy functionality on mobile devices. The protocol was developed and implemented in an open-sourced app and server.

detailed in Section II of this paper that AEN and GEN are subscription contracts, whose terms are not open for discussion, let alone to alteration. By entering Gapple's framework, governments void democratic participation upstream, as their power as a publicly accountable legislator is handed over to private companies that dominate digital infrastructure, which are not constrained by the substantial, formal and procedural norms that shape the Rule of Law.<sup>93</sup>

As stated above, governments that get involved with EN framework commit to a single interpretation of data protection rules, that is, PETs approach embedded in Gapple's architecture. EN system is about avoiding identification, whereas an efficient health system able to be functioning on a case-by-case basis requires identification. These different conceptual insights collide in cases where the unlikability between *data* and *individual* runs counter the efficiency of the whole health system and the exercise of rights by data subjects, once both presuppose identification.<sup>94</sup>

Gapple contractual terms bind governments to act in ways that may impact fundamental rights – namely the right to data protection, as provided for in Article 8 of Charter of Fundamental Rights of the European Union. It is, therefore, important to take a look into the means by which *legal protection* may be ensured *by design*.

---

<sup>93</sup> Laurence Diver, 'Digisprudence: the design of legitimate code' (2020) 13, 2 Law, Innovation & Technology (forthcoming).

<sup>94</sup> Michael Veale, Reuben Binns and Jef Ausloos, 'When data protection by design and data subject rights clash' (2018) Vol 8 No 2 *IDPL*, 105.

## *DPIA and Data Protection by Design and by Default*

The use of a new technology to process personal data that is likely to result in *a high risk to the rights and freedoms of natural persons* requires Google and Apple, as data controllers, to conduct a Data Protection Impact Assessment (DPIA), according to Article (35) 3 (b) GDPR. Recital (75) GDPR provides interpretative hints for understanding what the European legislator meant by *risk to the rights and freedoms of natural persons*. One of the aspects that may imply a high risk to fundamental rights is processing health data – which unequivocally happens in the case of diagnosis keys. That circumstance alone would dictate the legal obligation of Gapple to conduct a DPIA. Moreover, such processing occurs on a large scale.<sup>95</sup> But if we look behind what is visible in our scenario, as shown in sections III and IV, Google’s API architecture conveys invisible risks of profiling, through the collection of demographics, personal preferences, and location data on a large scale. Here we see that different risks emerge when looking at the information provided by Google, and when perceiving what happens *de facto* within Google’s API infrastructure.

A DPIA must identify and assess risks to rights and interests of natural persons and mitigate them through the implementation of security mechanisms that ensure compliance with the GDPR. Such security measures call for *data protection by design*

---

<sup>95</sup> Ibid, Recital (91); Article 29 Working Party, ‘Guidelines on Data Protection Officers (‘DPOs’)' (WP 243, 13 December 2016), 7-8 indicates *inter alia* as relevant factors to determine whether the processing is carried out on a large scale: a specific number or as a proportion of the relevant population; or the geographical extent of the processing activity. Both criteria apply to Gapple’s system.

*and by default*, stated in Article 25 GDPR, which is about a thorough balance between the circumstances and risks of processing and individual's rights and interests, and the mitigation *by default* of potential negative consequences that may derive from it. The obligation to conduct a DPIA and the requirements presupposed by data protection by design and by default are mechanisms to implement and enforce data protection principles, stated in Article 5 GDPR, by providing legal protection to natural persons *ex ante*, *by design* and *by default*. Therefore, Articles 25 and 35 GDPR are legal mechanisms that aim to *legal protection by design* within technological systems;<sup>96</sup> they are not about *brute (en)forcing* a one-eyed interpretation of a rule; rather, they presuppose and acknowledge the complexity and delicacy of the equilibrium required for compliance and its practical effect must be to empower natural persons to contest the product of automation.

It is true that if a DPIA transparently addressed the risks involved in the EN infrastructure (especially via Google Play Services), it would reveal an unlawful processing. In any case, a DPIA would allow informed decisions<sup>97</sup> both by the democratic legislator (before opting into the EN system) and citizens (before

---

<sup>96</sup> Mireille Hildebrandt, *Law for Computer Scientists and Other Folk*, OUP (2020).

<sup>97</sup> World Health Organization, 'Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing (Interim guidance)' (28 May 2020) <[https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics\\_Contact\\_tracing\\_apps-2020.1](https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1)> accessed 13 October 2020, where transparency and explainability are explicitly included in the WHO principles that should guide the ethical and appropriate use of digital proximity tracking technologies to address COVID-19.



downloading a national app functioning within API framework or before enabling BLE on their devices).

Until the date of the present writing (November 2020), no DPIA was published. Gapple's lack of transparency seems to be quite transparent.

### *The Right to Obtain Human Intervention*

The access to healthcare has been already identified by Article 29 Working party as an effect of processing *worthy of attention* when covered by Article 22 GDPR.<sup>98</sup> Bearing in mind that participating in the EN system, either by downloading the national proximity tracing app, or by enabling BLE on device, requires consent, Article 22 (3) GDPR consecrates the data subjects' right *to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision*. This right implies that specific information is provided to data subject, either *ex ante*, about the logic involved in decision-making process,<sup>99</sup> and *ex post* by a human being, who will necessarily intervene in the controller's decision (eventually considering data subject's point of view).<sup>100</sup> The interpretation of Article 22, combined with Recital (71) GDPR, seems to aim at providing data subjects the means to react *ex ante* and *ex post* to an

---

<sup>98</sup> Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP 251, 6 February 2018), 22.

<sup>99</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1, Articles 13 (2) (f); 14 (2) (g); 15 (1) (h).

<sup>100</sup> This seems to result from Ibid, Recital (71).

automated outcome and to challenge a decision after automation, even when it had human involvement.

In the case of Gapple EN, Article 22 GDPR would apply to risk scoring afforded by the system. The EN design allows health authorities to get an exposure risk scoring, by matching the collected beacons and computing exposure data in the form of ExposureWindow object.<sup>101</sup> The risk score associated with the exposure window may be obtained, either by getting precalculated risk scores, or by manually calculating risk score.<sup>102</sup> To get precalculated risk scores, the app must retrieve the diagnosis keys from the server and then provide them to the EN system. The precalculated risk score is obtained by calculating each exposure window, aggregated into DailySummary<sup>103</sup> objects for the last 14 days of exposure data. In the case of manual calculation,<sup>104</sup> the

---

<sup>101</sup> Google, 'Define meaningful exposures' (22 October 2020) <<https://developers.google.com/android/exposure-notifications/meaningful-exposures>>, accessed 3 November 2020. Each ExposureWindow instance represents up to 30 minutes of exposure information. As a result, long exposures to a particular key might be split into multiple 30-minute blocks.

<sup>102</sup> By calling the risk scoring *manual*, we are adopting Google's terminology. Such terminology does not seem to be literal, as risk score calculation may remain an automated process. We suppose that risk scoring is qualified as 'manual' to the extent that health authorities have (more) control over risk scoring method.

<sup>103</sup> Ibid. Each DailySummary contains the ExposureSummaryData for a particular day. The ExposureSummaryData takes into account the highest risk score, looking at all ExposureWindows aggregated into the summary; a sum of the risk scores and a sum of the weighted durations for all ExposureWindows.

<sup>104</sup> Ibid provides an example of how to manually compute the risk score, considering three factors: (i) weighted minutes-at-attenuation; (ii) infectiousness weight (available only for v1.6 and later); (iii) report type weight. The method exemplified by Google calculates the risk score based on how many seconds the user has been within close distance of a user that reported a case for each ExposureWindow, which is added to the corresponding day score. The method iterates over the different ScanInstance objects (corresponding to a few seconds during which a beacon with the diagnosis key causing this exposure was observed) and calculates the score based on the duration of the scan and the multiplier values associated with attenuation, report type, and infectiousness. The result is a map of dates with user exposures, measured in seconds. The code uses a filter to remove days with less than 15 minutes of relevant exposure. Such method computes the risk score similarly to how the Exposure Notifications system computes daily summaries.

Exposurewindow provides the exposures matching the diagnosis keys, from which the risk score is calculated. The risk may be calculated in different ways, according to what each health authority considers relevant to estimate an exposure risk, therefore allowing them to control the way by which exposure data is combined and to determine whether to send an exposure notification to a device.

The calculation method may be attributed to the EN system (if precalculated) or to the national authority (if manually calculated), which may make a difference regarding the entity obliged to provide information about the logic involved in such calculation, and to respond to data subjects' requests who want to exercise their rights.

The obligation to conduct a DPIA, the requirements of Data Protection by Design and by default, and the right not to be subject to a decision based solely on automated processing are instances of *Legal Protection by design* in the GDPR.<sup>105</sup> None of them seems to be (fully) guaranteed within Gapple's proposal.

## VII. CONCLUSION

The present article proposed to answer two questions: is Gapple's infrastructure *legal by design*? Does Gapple's EN framework provide *legal protection by design*? These questions led us to explore the contractual models that regulate the relations between governments and Gapple, but also the system architecture and its

---

<sup>105</sup> Mireille Hildebrandt, *Law for Computer Scientists and Other Folk*, OUP (2020).

security vulnerabilities. The iteration between our questions and the answers provided by our research sources opened alleys to reflect on the power relations between States and the companies who control the communications infrastructure, as well as about democratic participation on the process of deploying new technologies and the means to contest their outcome. In other words, Gapple's EN deployment incited us to muse around its significance to the Rule of Law.

Our analysis has shown that Gapple's EN might be an example of legal by design, once it embraces a specific interpretation of data protection norms (based on PETs approach) and is likely to eliminate the possibilities of non-compliance with that specific interpretation. *Legal by design* is not, however, equivalent to what we could call *legality*<sup>106</sup> *by design*, which seems to be connected to Mireille Hildebrandt's concept *legal protection by design*.

Gapple's contractual models reveal how imbalanced are the powers of governments, as citizens representatives, before tech-companies who control the communications infrastructure. In the case of the EN infrastructure, we have shown that a specific design and a static form of processing information are imposed on governments either when developing their national apps, or when working with an *app-less* system. The underlying architecture demonstrates how can these companies

---

<sup>106</sup> By using the term *legality*, we are invoking the meaning stated in Mireille Hildebrandt, 'Radbruch's Rechtsstaat and Schmitt's Legal order: Legalism, Legality and the Institution of Law' (2015) Vol 2 No 1 New Historical Jurisprudence & Historical Analysis of Law 42, 56-57. In this work, the Author connotes *legality* with justice (proportionality), legal certainty (a legal ground as safeguards provided for in positive law) and expediency (the requirement of effective legal remedies).

(Google) undertake a massive collection of personal data, untameably pursuing their own economic interests by taking advantage of an exceptional pandemic context. At the same time, Gapple present themselves as processors which are *just* providing the tools to support COVID-19 combating efforts – therefrom passing all the responsibility about personal data processing to governments. Such an approach aims at getting the most profit out of a global pandemic and simultaneously refusing their accountability as controllers. In other words, the perfect design of a monopoly, still untamed by the Rule of Law.

Companies' decision-making is not supported by procedures that aim to treat people with *equal concern and respect*<sup>107</sup>, *making room for* contestability, nor by institutions who are bound to decide according to standards of proportionality, legal certainty and purposiveness. In Big-Tech world, there seems to be no Rule of Law, nor rule by law, as this *web-suzerainty*<sup>108</sup> is maintained due to lack of specific legislation and law enforcement.

To state that Gapple's proposal does not provide *legal protection by design* is not just a theoretical exercise of conceptual fitness. It is something that affects the heart of our political systems and the concept of law itself. To be (dis)continued.

---

<sup>107</sup> Ronald Dworkin, *Taking Rights Seriously* (Cambridge: Harvard University Press, 1977).

<sup>108</sup> The epithet *suzerain*, used as metaphor in this context, intends to stress the lack of institutional framework and is infused by an idea of personal power (in the case, concentration of power in certain categories of private entities). I took inspiration from Mireille Hildebrandt, 'Origins of the Criminal Law: Punitive Interventions before Sovereignty', ch 11, in Markus D. Dubber (ed.), *Foundational Texts in Modern Criminal Law* (OUP 2014).