INTERNATIONAL JOURNAL OF DIGITAL AND DATA LAW

REVUE INTERNATIONALE DE DROIT DES DONNÉES ET DU NUMÉRIQUE

ISSN 2553-6893

IMODEV
LES ÉDITIONS

Vol. 9 - 2023

International Journal of Digital and Data Law
Revue internationale de droit des données et du numérique

Direction :
Irène Bouhadana & William Gilles

ISSN : 2553-6893

IMODEV
49 rue Brancion 75015 Paris – France
www.imodev.org
ojs.imodev.org

Les propos publiés dans cet article n'engagent que leur auteur.

The statements published in this article are the sole responsibility of the author.

À PROPOS DE NOUS

La **Revue Internationale de droit des données et du numérique (RIDDN)/ the International Journal of Digital and Data Law** est une revue universitaire créée et dirigée par Irène Bouhadana et William Gilles au sein de l'IMODEV, l'Institut du Monde et du Développement pour la Bonne Gouvernance publique.

Irène Bouhadana, docteur en droit, est maître de conférences en droit du numérique et droit des gouvernements ouverts à l'Université Paris 1 Panthéon-Sorbonne où elle dirige le master Droit des données, des administrations numériques et des gouvernements ouverts au sein de l'École de droit de la Sorbonne. Elle est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Elle est aussi fondatrice et Secrétaire générale de l'IMODEV. Enfin, associée de BeRecht Avocats, elle est avocate au barreau de Paris et médiateure professionnelle agréée par le CNMA.

William Gilles, docteur en droit, est maître de conférences (HDR) en droit du numérique et en droit des gouvernements ouverts, habilité à diriger les recherches, à l'Université Paris 1 Panthéon-Sorbonne où il dirige le master Droit des données, des administrations numériques et des gouvernements ouverts. Il est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Il est aussi fondateur et Président de l'IMODEV. Fondateur et associé de BeRecht Avocats, il est avocat au barreau de Paris et médiateur professionnel agréé par le CNMA.

IMODEV est une organisation scientifique internationale, indépendante et à but non lucratif créée en 2009 qui agit pour la promotion de la bonne gouvernance publique dans le cadre de la société de l'information et du numérique. Ce réseau rassemble des experts et des chercheurs du monde entier qui par leurs travaux et leurs actions contribuent à une meilleure connaissance et appréhension de la société numérique au niveau local, national ou international en en analysant d'une part, les actions des pouvoirs publics dans le cadre de la régulation de la société des données et de l'économie numérique et d'autre part, les modalités de mise en œuvre des politiques publiques numériques au sein des administrations publiques et des gouvernements ouverts.

IMODEV organise régulièrement des colloques sur ces thématiques, et notamment chaque année en novembre les *Journées universitaires sur les enjeux des gouvernements ouverts et du numérique / Academic days on open government and digital issues*, dont les sessions sont publiées en ligne [ISSN : 2553-6931].

IMODEV publie deux revues disponibles en open source (ojs.imodev.org) afin de promouvoir une science ouverte sous licence Creative commons CC-BY-NC-ND :

1) la *Revue Internationale des Gouvernements ouverts (RIGO)/ International Journal of Open Governments* [ISSN 2553-6869] ;

2) la *Revue internationale de droit des données et du numérique (RIDDN)/International Journal of Digital and Data Law* [ISSN 2553-6893].

ABOUT US

The **International Journal of Digital and Data Law / Revue Internationale de droit des données et du numérique (RIDDN)** is an academic journal created and edited by Irène Bouhadana and William Gilles at IMODEV, the Institut du monde et du développement pour la bonne gouvernance publique.

Irène Bouhadana, PhD in Law, is an Associate professor in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where she is the director of the master's degree in data law, digital administrations, and open governments at the Sorbonne Law School. She is a member of the Institut de recherche juridique de la Sorbonne (IRJS). She is also the founder and Secretary General of IMODEV. Partner at BeRecht Avocats, she is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

William Gilles, PhD in Law, is an Associate professor (HDR) in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where he is the director of the master's degree in data law, digital administration and open government. He is a member of the Institut de recherche juridique de la Sorbonne (IRJS). He is also founder and President of IMODEV. Founder and partner at BeRecht Avocats, he is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

IMODEV is an international, independent, non-profit scientific organization created in 2009 that promotes good public governance in the context of the information and digital society. This network brings together experts and researchers from around the world who, through their work and actions, contribute to a better knowledge and understanding of the digital society at the local, national or international level by analyzing, on the one hand, the actions of public authorities in the context of the regulation of the data society and the digital economy and, on the other hand, the ways in which digital public policies are implemented within public administrations and open governments.

IMODEV regularly organizes conferences and symposiums on these topics, and in particular every year in November the Academic days on open government and digital issues, whose sessions are published online [ISSN: 2553-6931].

IMODEV publishes two academic journals available in open source at ojs.imodev.org to promote open science under the Creative commons license CC-BY-NC-ND:

1) the *International Journal of Open Governments*/ la *Revue Internationale des Gouvernements ouverts (RIGO)* [ISSN 2553-6869] ;

2) the *International Journal of Digital and Data Law* / la *Revue internationale de droit des données et du numérique* (RIDDN) [ISSN 2553-6893].

SCANNING SMARTPHONE & PRIVACY ISSUES

by **Arthur CHAMPÉROUX**, PhD Candidate in data protection based in both Université Paris Saclay (France) and Université de Laval (Québec), member of Youth Privacy Protection in Online Gaming (YPPOG), a group of research and works at the Chaire de recherche en Blockchain in Université de Laval.

After cellphones' introduction in 1973, Steve Jobs' first iPhone launch speech in January 2007 is usually taken for smartphones' historic kick start, representing 6.648 billion smartphone users in 2022**.** A smartphone is a cellphone with advanced features feeding itself on data collected during usage. These mobile devices are designed to always follow the user, always on, allowing private companies to access to an unprecedented amount of information about their users. Consequently, smartphones are one of the cornerstones of the data collection within the context of the Big Data revolution. In short, this multifunctional tool connects most humans in most accessible places, while processing an exponentially growing amount of data every day. From the constructors to the app platforms, including the app developers, device manufacturers and third parties, these actors are gathering information about our daily habits every second through our personal and professional smartphones. These large-scale data collection and processing are sometimes justified for legal obligations (such as the Know Your Customer regulation or Anti Money Laundering laws[1]), or to execute contract of services, to improve service, for marketing profile, etc. A relatively recent global movement of privacy regulation has emerged to propose a legal frame[2] to these practices. Such norms are meant to protect fundamental individual rights and require professionals to respect multiple principles articulated around data protection and privacy[3]. In this regard, this analysis will not delve into the topic of information security, in order to set the reflection on privacy issues.

[1] Directive 2005/60/EC of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, The Money Laundering Regulations 2017 in the United Kingdom, Act on identification of customers by financial institutions 2003 in Japan, Title III of the Patriot Act and Currency and Foreign Transactions Reporting Act (Bank Secrecy Act) in 1970 in the USA

[2] Regulation 2016/679 (EU), Canadian Federal Law C-25, Chinese Personal Information Protection Law (PIPL), Brasilian Lei Geral de Proteção de Dados (LGPD), Indian Personal Data Protection Bill, etc.

[3] The terminology of privacy requires a careful examination in itself, as it intricates different meanings depending on cultural approaches. Other similar concepts have been developed in other languages such as "la vie privée" (French), "die Privatsphäre" (German), "privatlivets fred" (Danish/Norwegian), although these have known significant evolution over the last decades. For more information about these concepts, see G. MESSADIE, *La fin de la vie privée*, Calmann-Levy, Paris 1974 ; the 1970 proposal by the (West) German Interparliamentary Working Committee for a "Gesetz zum Schutz

Simply put, this research will try to summarize smartphone eco-system, focusing on data collection on a technical level of the hardware, censing the different captors as well as the key role of software with apps and OS. To be perfectly clear, data collection is one form of data processing, oftentimes considered as the first one in the lifecycle of data. Nonetheless, this article shall focus on data collection as the point of this demonstration is that smartphones have a unique ability to absorb personal data. This part is meant to give an overview of which data are being processed and the different possibilities offered by automated algorithms[4]. On a side note, this research will not encompass reflection about data processing as much, as it would require a larger scope of work beyond the goal of catching the essence of how personal data is being captured by smartphone. Nonetheless, reflection revolving around informational privacy widely assumes that automated algorithms are absolutely key to understand data protection laws and their struggle to build effective protection[5] in that sense because of the complexity of these tools[6].

Then, the analysis will focus on assessing various risks regarding privacy when it comes to data collection through smartphones, giving insights about the way smartphones are absorbing personal data, based on emblematic examples. These different examples tend to erode the public confidence in technologies[7] and could become a major factor hindering technologic progress.

---

der Privatsphäre gegen Missbrauch von Datenbankinformationen": described in H. P. Bull, *Datenschutz oder Die Angst vor dem Computer*, Piper, Munich 1984, p. 85; Denmark, Register Committee (Registerudvalget), *Delbetænkning om private registre*, Report no. 687, Statens trykningskontor, Copenhagen 1973.

At best, "the concept of privacy figures prominently in discourse about the social and political threats posed by modern information and communications technology (I.C.T.)", L.A BYGRAVE, "Privacy protection in a global context–a comparative overview", *Scandinavian Studies in Law,* 47.2004, 2004, p. 320.

Given the multiplicity of conceptions of privacy and its evolution the debate, we shall prefer a broader and neutral definition provided by the International Association of Privacy Professionals (IAPP), proposing that "privacy is the right to be let alone, or freedom from interference or intrusion. Information privacy is the right to have some control over how your personal information is collected and used", IAPP, [https://iapp.org/about/what-is-privacy/]

[4] F. PASQUALE, *The black box society: The secret algorithms that control money and information*, Harvard University Press, 2015

[5] P.-L. DÉZIEL, « Les limites du droit à la vie privée à l'ère de l'intelligence artificielle : groupes algorithmiques, contrôle individuel et cycle de traitement de l'information », *Les cahiers de propriété intellectuelle, Yvon Blais*, 30, 2019 ; L. D. GODEFROY, « Pour un droit du traitement des données par les algorithmes prédictifs dans le commerce électronique », Recueil Dalloz, n°8 / 7677, 2016

[6] J.M. DELTORN et (DIR. E. NETTER), « Le droit des données personnelles face à l'opacité des algorithmes prédictifs: les limites du principes de transparence », *Regard sur le nouveau droit des données personnelles*, CEPRISCA., 2019 ; F. GONÇALES, "Privacy, Data Protection and the Age of Algorithms", *Revue Internationale de droit des données et du numérique*, n°7, 2021

[7] This paper will not go into details about the sociologic impact of technology and the privacy concerns, but here are some studies focusing on these aspects: E. CHIN, A. PORTER FELT, V. SEKAR & D. WAGNER, "Measuring user confidence in smartphone security and privacy", in *Proceedings of the eighth symposium on usable privacy and security*, 2012; J. LAU, B. ZIMMERMAN & F. SCHAUB. "Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers", *Proceedings of the ACM on Human-Computer Interaction*, n°2, CSCW, 2018; Interestingly, the

The article argues that smartphone spread overwhelmingly in society to the point that its presence became a natural component of modern reality. On the other hand, smartphones evolved fundamentally and turned into pocket-sized hyper sophisticated sensors surveilling user's every move. The smartphone shall be understood as a gateway concentrating personal data constituting a powerful and democratized tool for surveillance capitalism[8]. The observation of the dark patterns[9] and nudges[10] at work in the smartphone ecosystem will not appear in this work as it goes beyond data collection, despite the interest of the addictive dimension of smartphone apps and cognitive bias utilized by designers to trick users, notably in sharing their data. On another level, the article connects the lack of defiance from users for smartphone invasive nature to the lack of awareness regarding this personal data feeding item. The democratization of smartphone provided a false sense of privacy for users as the digital technology became increasingly harmful for privacy. In essence, the article argues that the exponential intensity of data collection concentrated in smartphone transformed the digital device into the most invasive tool for privacy. Consequently, this new kind of data collection intensity can fundamentally change the very nature of personal data, in the sense that what used to be considered as regular personal data can become sensitive personal data. This category shift towards more sensitive types of data compels the law to apply more protective measures for personal data that formerly did not require such protection. This article will therefore present two case studies with location and vocal data showing how this intensity shift operates and presents new legal challenges. These challenges are namely the public awareness for data collection, the adaptation of data protection law to propose adequate scope of responsibility for data processors and the rethinking of personal data categories in light of the specific smartphone data collection ecosystem.

Privacy regulations will only be effective as the public is informed about their rights and gains awareness of personal data processing purposes. Therefore, the paper will try to underline how smartphones are particularly threatening users' privacy in the

recommendations made by the researchers to improve users' confidence in technology surrounding smartphones are very similar to the ones this paper will make, especially on the educational segment to improve awareness, which should be the cornerstone of public policies.

[8] S. ZUBOFF, B. FORMENTELLI & A.-S. HOMASSEL, *L'âge du capitalisme de surveillance : le combat pour un avenir humain face aux nouvelles frontières du pouvoir*, Paris, Zulma, 2020

[9] REED STEINER, « Dark Patterns: A New Scientific Look At UX Deception », *Fyresite*, 2020; Future of Privacy Forum, « Helping you find healthy mobile games », 2021; M. NIUWENS, I. LICCARDI, M. VEALE, D. KARGER & L. KAGAL, « Dark patterns after the GDPR, Scraping consent pop-ups demonstrating their influence", *Human-Computer interaction*, Corneil University, 8 janvier 2020; F. RADET, Deceived by Design – How Tech Companies use dak patterns to discourage us from exercising our rights to privacy, [https://fil.forbrukerradet.no/wp-content/uploads/2018/ 06/2018-06-27-deceived-by-design-final.pdf]

[10] R.H. THALER et C.R. SUNSTEIN, *Nudge: improving decisions about health, wealth, and happiness*, Rev. and Expanded ed., New York, Penguin Books, 2009

current state of data protection, notwithstanding the benefits of this resourceful technology. The terms "data subject" and "user" are used interchangeably. Plus, there will be some explanation about status and regime technicities between "data controller", that are traditionally "app providers, whereas "data processor" are mostly "app developer"[11]. These last four terms can be regrouped as Internet service providers throughout this paper. In terms of methodology, the analysis will combine both an earth-to-earth empirical assessment of how a smartphone is technically constituted and how it massively collects data, as well as a more in-depth legal analysis of the privacy threats and the legal challenge modern societies are facing.

Data protection law is advocating to find a compromise between imposing a sufficient level of privacy protection for consumers and enhancing economy development through the digital shift taking place. Finding the right balance to regulate actors' behavior in the smartphone data ecosystem implies setting clear and actionable responsibility, obligating the said actors to be accountable. Such legal requirement would logically undertake the path towards the necessity of awareness for the public, supported by pivotal legal principles like transparency, intelligibility, accessibility of information. In the same vein, the legal mechanism of communicating the purpose of data collection before it begins[12], would benefit to be apprehended with a clear taxonomy of acceptable purposes correlated with adapted data protections.

Finally, data collection in the context of smartphone usage is a specific topic that led this article to consider the opportunity of the adaptation of personal data categories, as it challenges traditional typology of personal data under the impact of the intensity of data collection.

These different aspects shall introduce the global context and surrounding challenges for smartphones, shaped by various basic mechanisms and functionalities (1§) constituting the concrete technological implications in modern societies. Consecutively, this presentation should shed the light on privacy threats and legal challenges (2§) for users, app developers and third parties.

---

[11] This paper will reuse the Working Party 29 definition of app developers in the way that the term "is not limited to the programmers or technical developers of apps, but includes the app owners, that is, companies and organizations that commission the development of apps and determine their purposes", Article 29 Data Protection Working Party, *Opinion 02/2013 on apps on Smart Devices*, 00461/13/EN WP 202, 2013, p. 9, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf];
These concerns are shared by the Federal Trade Commission of the "While staff encountered a diverse pool of apps for kids created by hundreds of different developers, staff found little, if any, information in the app marketplaces about the data collection and sharing practices of these apps", US FTC staff report, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing*, 2012, [http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf]

[12] See M. R. Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 Notre Dame L. Rev. 1027, 2013

§ 1 – SMARTPHONE DATA COLLECTION BASIC MECHANISMS AND FUNCTIONALITIES

A) Smartphone Data Ecosystem and Collection Mechanism

Schematically, smartphone's ecosystem is composed of both hardware and software components, from the informatic components to the infrastructural aspect of OS (operating system), apps and apps market. Apps are coded by app developers proposing different services or functionalities to customers[13] *via* app stores, working as apps library. In more technical terms:

> "Smartphones are multi-purpose devices equipped with sensing and recording capabilities such as camera, microphone, fingerprint recognition, proximity sensors, gyroscope, accelerometer, and more. These are embedded into the hardware made available to apps and the OS. Mobile OSs already embedded mechanisms to control and limit the amount of personal information accessed by users' installed apps"[14].

Data of consumers is first collected by a myriad of captors. Here is a non-exhaustive list[15]:

Accelerometer (Acceleration)	Gyroscope (Rotational motion)	Magnetometer/Compass (Magnetic fields)
GPS receiver (Location)[16]	Microphone (Sound)	Camera (Light, Color, Barcode reader)
Photometer/Ambient Light Sensor (Light)	Stopwatch (Time)	Touchscreen (Conductivity or Pressure)
Barometer (Pressure)	Thermometer (Temperature – internal or ambient)	Humidity Sensor (Amount of water in the air)
Fingerprint sensor (Conductivity)	Proximity Sensor (Infrared Light)	Pedometer (Acceleration)
Facial recognition (Light)	Heart Rate Monitor (Heartbeats)	Geiger Counter (Harmful Radiation)
Gravity Sensor (Gravitation)		

[13] App developers are compelled to propose the most accessible, efficient, and accurate services to customers in the first. Then, most business models for apps are based on free access to content and services and advertising to make money. One way to increase incomes for app developers is to proceed to users profiling in order to propose specific content fitting the user, or to simply sell data collected through regular usage of the app. Data circulates in a form of data market organized by the buys and sells from data brokers. Other economy models also exist with premium access, crowd funding, subscriptions, however, the data market is the most fruitful. To understand app developers business models and motivations, see S. HYRYNSALMI, A. SUOMINEN, T. MAKIL, A. JARVI, & T. KNUUTILA, "Revenue models of application developers in android market ecosystem", in *Software Business,* Springer, 2012

[14] M. HATAMIAN, « Engineering privacy in smartphone apps: A technical guideline catalog for app developers », *IEEE Access*, 2020

[15] This list was directly inspired by the census made on: [https://www.societyforscience.org/research-at-home/using-smartphone-for-data-collection]

[16] GPS would be the colloquial expression used by the public, whereas experts are talking about GNSS technology since it replaced GPS in most smartphones since the 2010's. See T. COOKE (eds. M. FILIMOWICZ), "APIs & GNSS (Not GPS) Location Data", *Privacy, Algorithms and Society*, Routledge Focus, 2022

Some captors are more self-explanatory than others. The concrete implications and potential usage will be detailed later on.

Then, user's data is transferred to app developers and OS constructors in order to provide specific services, improve performances, measuring statistics, profiling, etc. depending on the final purpose announced when installing such apps. As a matter of illustration, In early 2022, the number of available apps in the Google Play Store reached 3.3 millions and 2.11 millions in the Apple App Store[17]. These two platforms represent the largest app stores by far. In 2021, around 230 billion apps were downloaded worldwide[18], for a global developer population of 26.8 millions at the end of 2021[19].

Apps are able to collect large quantities of data from the device (e.g. data stored on the device by the user and data from different sensors, including location) and process these in order to provide new and innovative services to the end user. However, these same data sources can be further processed, typically to provide a revenue stream, in a manner which may be unknown or unwanted by the end user[20].

To follow through, it is necessary to ask the general question of the kind of data that is being processed by smartphones to anchor this reflection on material ground. The amount of data collected through our phone daily is simply much more than most would imagine. Besides the traditional phone calls, phone records, text messages, smartphones are collecting navigation data as we use web browsers, location services, then it can collect the content of any text messages without end-to-end encryption, each action of our social networks, as well as sensitive data such as health data, on an everyday basis. This is only a sample of the main categories of data collected[21], although there are many more data acquired by the mobile devices, such as meta-data of our every action.

---

[17] L. CECI, *App stores - Statistics & Facts*, Statista, 2022: [https://www.statista.com/topics/1729/app-stores/#topicHeader__wrapper]

[18] Statista, 2022, [http://bitly.ws/show/yjxo]

[19] Report emitted by DeveloperNation, [https://www.developernation.net/developer-reports/dn21]; This population is expected to reach 28.7 million people by 2024 according to Statista: https://www.statista.com/statistics/627312/worldwide-developer-population/.

[20] Article 29 Data Protection Working Party, *op.cit.*, 2013, p2

[21] The Article 29 Data Protection Working Party, proposed examples of personal data that can have a significant impact on the private lives of the users and other individuals:
– Location
– Contacts
– Unique device and customer identifiers (such as International Mobile Equipment Identity, International Mobile Subscriber Identity, Unique Device Identifier, and mobile phone number)
– Identity of the data subject
– Identity of the phone (i.e. name of the phone)
– Credit card and payment data
– Phone call logs, SMS or instant messaging
– Browsing history
– Email
– Information society service authentication credentials (especially services with social features)
– Pictures and videos

Interestingly, the smartphone does not require any action to continuously transfer data to apps. One recent study found that "Google and Apple smartphones upload data every four and a half minutes, including the device's hardware serial number, phone number, IMEI, Wi-Fi MAC address, and whether or not a SIM card has been inserted, among other details"[22]. The previous statement is referring to a scientifical study led by Prof Doug Leith at Trinity's Connect Centre, which assessed precisely that 1MB of data is being sent from idle Google Pixel handsets every 12 hours, compared with 52KB sent from the iPhone.

The data flow is massive, permanent[23] and raises several privacy issues because of its intensity changing our perception of data. Indeed, "due to the highly personal nature of smartphones, any data collected from them may be classified as personal data as stated in Recital 24 of the Directive on privacy and electronic communications 2002/58/EC"[24]. The extensive habits developed around smartphone usage become problematic for privacy as it indexes and concentrates most of our lives, through a single point of control[25]. The benefits of using a smartphone ritually for our every move, became slowly essential to most people to the point that this technologic item is now the receptacle of modern privacy. As stated by the E-privacy Directive: "Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of users" therefore it requires "protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms"[26]. This statement opens the protection to most data, from the pictures of our phones to "messages but also device's identifiers, location or even metadata"[27].

Followingly comes the question of what a Smartphone can do. Concretely, data is being processed to perform various actions. In order to give a proper overview of the ever-growing amplitude of possible applications performed by apps, there goes a non-exhaustive list of what apps can measure, identify, record:

– Biometrics (e.g. facial recognition and fingerprint templates).
Article 29 Data Protection Working Party, *op.cit.*, 2013, p. 2.

[22] C. ZIBREG, *IPhones and Android Handsets Collect Our Data Even When Idle*, 2021, [https://www.makeuseof.com/iphone-android-data-collection-study/]

[23] See the work of D.C. SCHMIDT, *Google Data Collection*, Digital Content Next, 2018, [https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf]

[24] M. HATAMIAN, *op. cit.*, *IEEE Access*, 2020, p. 35431

[25] J. ZITTRAIN, « Internet points of control », *The Emergent Global Information Policy Regime*, Springer, 2004

[26] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), Official Journal of the European Communities, 2002

[27] M. HATAMIAN, *op. cit.*, *IEEE Access*, 2020, p. 35431

Types of plants and animals	Health conditions such as anemia[28], Parkinson[29]	Earthquakes,
Radiation	Biometric information (Facial recognition & fingerprint)	Temperature & wether forecast[30]
Sounds	Image and video	Bird songs
Distance traveled or height of an object	Brightness of the sky	Etc.

Infinite possibilities of applications are happening *via* our smartphones, despite most people ignores how it precisely functions. The lack of understanding of this common but high-level technology might be one of the central causes of incomprehension of how mobile devices can harm our privacy. The gap between how natural it is to use smartphone and the way it functions is very similar to the lack of awareness regarding connected technology. Considering the level of penetration of digital technology in most parts of humanity, such as the advent of the internet of things, the 5G, the metaverse and so on, the threats menacing privacy are greater than ever.

B) Smartphone Techniques to Undermine Individuals' Privacy

Nowadays apps designs are data driven in ways that enhance user experience, to provide personalized content, propose relevant merchandising to consumers, develop habit and solicitate the most interaction possible with users. Apps are the center of attention for users and the neuralgic access point for data collection. The user's behavior is then analyzed depending on the purpose determined by the data controller as well as the data processors. This is what demonstrate Story, Zimmeck & Sadeh, "oftentimes, the collected data is not only leveraged for the apps' main functionalities but also for other purposes, most notably, to serve advertisements and for analytics"[31]. In short, apps are requiring access to hardware and other apps to proceed to the data collection through smartphones.
Thus, privacy threats can arise if the user is not aware of the data processing, or if the data processing is unlawfully achieved. In

[28] V. Krishna, *Haem: Deep Learning to Detect Anaemia Using Smartphones*, 2020, [https://rb.gy/znacsz]
[29] K. JOLLY, *The iSpy Platform: A Multi-Faceted Suite of Affordable Smartphone Imaging and Sensor-Based Utilities for the Non-Invasive Detection of Parkinsonian Tremor and Skin Cancer via Machine Learning*, 2020, [https://rb.gy/ue3kxt]; N. Ayyagari, *Cepha: An End-to-End Self-Diagnostic Platform for Parkinson's Disease Utilizing Smartphone Sensor Data and Ensemble Machine Learning Methods*, 2020, [https://rb.gy/r0mxuk]
[30] J. Lin, An Atmospheric Visibility Measurement System Using Smartphone, 2020, [https://rb.gy/eym1co]
[31] P. STORY, S. ZIMMECK, N. SADEH "Which apps have privacy policies? An analysis of over one million Google Play Store Apps", *Privacy Technologies and Policy 6th Annual Privacy Forum*, (Eds M. MEDINA, A. MITRAKAS, K. RANNENBERG, E. SCHWEIGHOFER, N. TSOUROULAS), Springer, APF 2018, p3

spite of the significant efforts made by app developers, there are some widespread latent issues concerning data processing at the moment, perpetuated by unaware or malicious app developers. This is what highlights Temming, in her very evocative article[32], presenting the examples of twenty apps on the Playstore, abusing sensor access, which were then removed from the app market[33], "because the apps could — without the user's knowledge — record with the microphone, monitor a phone's location, take photos, and then extract the data"[34]. This illustrates the potential abuses enabled through apps when these are created by malicious app developers. Temming gathered different studies showing very serious threats for smartphones, as access to a myriad of sensors that could directly "reveal what users are typing or disclose their whereabouts"[35]. Moreover, some sensors are not even protected by authorization procedures[36]. For example, apps do not require to ask permission to access gyroscope or accelerometer, as data collected are usually understood as non-personal data. However, these data can reveal personal habits of transportation or else.

These aforementioned examples represent potential malicious types of actions[37], nonetheless they do not represent most data protection violation. Indeed, there are more reasons to think that most dangers are coming from regular apps that are just not considering data protection as seriously as it should be. Followingly, two emblematic examples will demonstrate how

---

[32] M. TEMMING, « Your phone is like a spy in your pocket », *SCIENCENEWS.ORG*, 2018

[33] M. Ruthven, K. Bodzak, N. Mehta, *From Chrysaor to Lipizzan: Blocking a new targeted spyware family*, Google, 2017 [https://security.googleblog.com/2017/07/from-chrysaor-to-lipizzan-blocking-new.html]

[34] M. TEMMING, *op.cit., SCIENCENEWS.ORG,* 2018

[35] "Barometer readings that subtly shift with increased altitude could give away which floor of a building you're standing on", "For instance, touching different regions of a screen makes the phone tilt and shift just a tiny bit, but in ways that the phone's motion sensors pick up", "A pair of researchers built TouchLogger, an app that collects orientation sensor data and uses the data to deduce taps on smartphones' number keyboards. In a test on HTC phones, reported in 2011 in San Francisco at the USENIX Workshop on Hot Topics in Security, TouchLogger discerned more than 70 percent of key taps correctly", *Ibidem*; For the scientific experimentation, see M. MEHRNEZHAD, E. TOREINI, S. F. SHAHANDASHTI, & F. HAO, "Stealing PINs via mobile sensors: actual risk versus user perception." *International Journal of Information Security* 17, n°3, 2018, [http://bitly.ws/show/yjvw]; L. CAI & H. CHEN. "{TouchLogger}: Inferring Keystrokes on Touch Screen from Smartphone Motion." In *6th USENIX Workshop on Hot Topics in Security (HotSec 11)*, 2011; D. BEREND, S. BHASIN, & B. JUNGK, "There goes your PIN: exploiting smartphone sensor fusion under single and cross user setting." *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 2018. All these research showed average results of successful cracking keystrokes from 70 to 99.5% depending on the methods and sensors used

[36] "Motion detectors within smartphones, like the accelerometer and the rotation-sensing gyroscope, could be prime tools for surreptitious data collection. They're not permission protected — the phone's user doesn't have to give a newly installed app permission to access those sensors", M. TEMMING, *op.cit*, *SCIENCENEWS.ORG,* 2018.

[37] "Electronic mail and use of secondary devices are the major sources for the transmission of malicious objects in computer network these days"; "Malicious object is a code that infects computer systems", B. KUMAR MISHRA & H. SAINI, *Cyber Attack Classification using Game Theoretic Weighted Metrics Approach*, World Applied Sciences Journal, n°7 (Special Issue of Computer & IT), 2009, p1

privacy can be undermined by a regular usage of common apps, by treating of two types of data concentrating a lot of attention recently: the location and the voice.

1) Location Data Within the Smartphone Context

As a matter of fact, location is a very good example of personal data that can become rapidly sensitive because of the intensity rendered possible by the smartphone location services, as "smartphones are ideally suited for location-aware services"[38]. Location data recently evolved and spread massively in common usage of smartphones, "the popularity of location aware smartphones has led to the prevalence of apps that access users' location in order to provide personalized/customized services"[39]. This development of location analysis grew to the point that it created unprecedented threats, potentially allowing adversary to locate individuals physically, as well as to profiling and identifying a person based on the places that person goes. Data location used to be a mildly invasive kind of data until recently.
Since the generalized smartphone use, the increased precision performance of location and the vast possibilities of crossing this intel with other data, location data became more and more sensitive[40]. Indeed, location data might be considered as part of the sensitive data category, with special protection, as this data can reveal a large portion of intimate and personal aspects of our lives, such as potential health condition, political beliefs, sexual orientation, and the list goes on, based on the places individuals visit. The degree of precision of location data crossed with other sensors allows to locate a person in a building, at a certain floor, which can be utilized to know which doctor you are seeing, which shop you are visiting, or which political demonstration you were attending, based on your data, other users' data and public data. The main aspect to put in perspective is that location data is not fundamentally a sensitive type of data, but it might become sensitive in case the data processing purpose is more invasive[41].

---

38 E. CHIN, A. PORTER FELT, V. SEKAR & D. WAGNER, "Measuring user confidence in smartphone security and privacy", in *Proceedings of the eighth symposium on usable privacy and security*, 2012, p. 2.

39 K. FAWAZ, & G. S. KANG "Location privacy protection for smartphone users", *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014, p239, [http://bitly.ws/yjvj]

40 "It has never been easier to track consumer movements and daily routines because they are almost always equipped with what are effectively personal tracking devices. Information about where consumers live, work, spend free time, and what businesses they frequent is extremely valuable to advertisers, especially when movements can be tracked in real time. […]. This real time collection of geolocation data allows marketers to predict consumer habits and preferences and provide location-based advertising using geofencing and beacon technology", S.J. BLODGETT-FORD & M. SUPPONEN (dir. W. BARFIELD, M.J. BLITZ), "Data privacy legal issues in virtual and augmented reality advertising", *Research handbook on the law of virtual and augmented reality*, Edward Elgar Publishing, 2018, p. 497.

41 "Suppose you are a woman aged 18–24 and you visit a clinic that offers abortion care. Maybe you use Google maps to find it. And while you are waiting for your appointment, you might scroll through Facebook, Instagram, Twitter, or the news. An

This issue of increased sensitivity is also globally treated in the last part of the paper; thus, a longer reflection will be elaborated later.

2) Voice Data Within the Smartphone Context

The voice is also an interesting kind of data as it gradually became a personal data with the phone, with the sound recording technology. As of today, the voice is almost systematically a personal data[42], considering the state of the art of biometric data science wich makes it possible to identify individuals via one's voice. As Article 4(1) GDPR states that recording is personal data if it is possible to identify the author(s). Now, the specific case of smartphone will, by default, connect a recording, like" leaving a message on a voicemail, even without stating your identity" and therefore constitutes personal data since the call is (or could be) associated with your telephone number"[43]. On top of this, voice is resourceful in information as it is possible to deduce "the speaker's gender, location or mood that can be used to single out an individual"[44]. Voice can also become a potential biometric data, when used to identify a natural person[45] which is considered as a sensitive type of data in the Article 9 of the GDPR. On the other hand, Kröger & al. report that "[b]eyond their legitimate processing purposes, organizations may use personal information extracted from voice recordings for malicious ends or pass it on to other parties"[46]

The increasing interest of the voice recording brings one simple question: are smartphones listening to us? "For years, countless reports have been circulating on the Internet from people who claim that things they talked about within earshot of their phone later appeared in targeted online advertisements, leading many to believe that their private conversations must have been secretly recorded and analyzed"[47] stated researchers, relating the tensed atmosphere between technology and users. A large number of users from around the world reported their concerns of being

---

ad pops up on your phone. It could be for anything—clothing, college courses, a competition. Even if you scroll past it, marketers can capture your ID. If you have location services enabled for that app, marketers can capture your location as well. Anti-choice activists have paid for information about people who fit this profile . . . Once they have your advertising ID, they can send you anti-choice messages like ads for these crisis pregnancy centers", Rewire Multimedia, *How Geo-Fencing Works . . . and How It Can Be Abused*, 2017, [https://rewirenewsgroup.com/2016/05/25/geofencing-works-can-abused/]

[42] C. JASSERAND, *What is Speech/Voice from a data privacy perspective? Insights from the GDPR*, STeP, 2020

[43] J. PAWERYCK et S. VAN DER SMITH, *When is voice (a special category of) personal data under GDPR?*, 2021

[44] *Ibidem*

[45] *Ibidem*

[46] J.L. KRÖGER, L. GELLRICH, S. PAPE, S.R. BRAUSE et S. ULLRICH, « Personal information inference from voice recordings: User awareness and privacy concerns », *Proceedings on Privacy Enhancing Technologies*, 2022

[47] J.L. KRÖGER & P. RASCHKE, "Is my phone listening in? On the feasibility and detectability of mobile eavesdropping", in *IFIP Annual Conference on Data and Applications Security and Privacy*, Springer, Cham, 2019, p102.

spied on, as a Forbes article stated[48] about US workers, as well as surveys in Australia in which one in five Australians believe to be listened by smartphones[49]. In a similar fashion, further active investigations recently began on the initiative of the US House Committee on Energy and Commerce by directly requesting Google and Apple about the ways iOS and Android devices record private conversations. Alleged privacy threats are serious, in the sense that it could represent a major breach of people's intimacy:

> "The security threats of a malicious application gaining access to an unsuspecting victim's voice or conversation are particularly devastating. Sensitive information can be leaked in surreptitious manner if the malicious application is able to reconstruct speech from motion sensor readings. For example, sensitive verbal communications would be exposed, including information such as credit card numbers and social security numbers as the victim speaks into or near the phone such as over a phone call. In addition, various aspects of the eavesdropped speech signals can be utilized for speaker and gender identification. This threat violates the privacy of the victim(s) by revealing the identity and gender information that may otherwise be considered personal and should not be revealed unless proper permission has been granted by the involved parties"[50].

Scientists also started to investigate the technical possibilities for smartphones to record and share conversation secretly, "however, a consensus has not yet been reached, not even regarding the fundamental technical feasibility of the alleged eavesdropping attacks"[51]. Notwithstanding the fact that most of the aforementioned scenarios were not technically adapted to technology in 2018[52], last research showed new forms of natural language transcriptions and recording potentially threatening privacy. On a side note, the introduction of AI based vocal assistant is a game-changer on this topic and normalizes the fact

[48] The US-based market research company Forrester reports that at least 20 employees in its own workforce have experienced the phenomenon for themselves, F. KHATIBLOO, *Is Facebook Listening (And So What If They Are)?,* 2017, [https://www.forbes.com/sites/forrester/2017/03/17/is-facebook-listening-and-so-what-if-they-are/ 41]

[49] B. HASSAN, *1 in 5 Aussies convinced their smartphone is spying on them,* Finder, 2018, [https://www.finder.com.au/press-release-july-2018-1-in-5-aussies-convinced-their-smartphone-isspying-on-them]

[50] S. A. ANAND, N. SAXENA, "Speechless: Analyzing the Threat to Speech Privacy from Smartphone Motion Sensors", *IEEE, Symposium on Security and Privacy*, 2018, p1000

[51] J.L. KRÖGER & P. RASCHKE, *op. cit.*, *IFIP Annual Conference on Data and Applications Security and Privacy*, 2019, p102

[52] Both articles agreed on this point at the time, S. A. Anand, N. Saxena, *op.cit.*, *IEEE, Symposium on Security and Privacy, 2018,* p1000; Z. KLEINMAN, *Is your smartphone listening to you?,* 2016, [https://www.bbc.com/news/ technology-35639549]

that users are permanently recorded[53]. Such vocal assistants are present on most smartphones nowadays. Additionally, Temming alerted about privacy and information security impacts through extensive data collection through smartphone based on the hijacking of the microphone: "Criminals can hack into your device to find your address, your bank account login credentials, or other sensitive information that could be used to harm you or your finances. Companies can tailor their marketing to your habits"[54].

These two examples of location and voice are emblematic of the deeper personalization of data as a more global movement, enabled by more precise sensors illustrated by the evolution of smartphone. This digital shift is surfing on the rise of the intensity, permanence and accuracy of data collection which is seriously raising new legal challenges.

§ 2 – Smartphone Data Collection and Privacy Legal Challenges

In order to encompass the challenge to build data protection for individuals around the common usage of smartphones, this section will describe three main points of attention, namely the awareness about data protection rights and data processing, the fundamental prism of responsibility of data collection[55] for data controller within the context of app store and app developers and finally, the evolution of personal data categories considering the smartphone eco-system. This section does not try to give an exhaustive list of all the legal challenges about smartphone, privacy, and data protection, although it should be a solid basis for improvement as these challenges are emblematic of the current issues.

A) Challenging Awareness for Data Protection Rights

Awareness is the starting point for all the issues around data privacy in a sense. Recent surveys gave indicators about awareness of data protection key features about smartphones:

> "In 2018, 75% of people aged 16-74 in the European Union (EU) used a smartphone for private purposes. Yet,

[53] M. Vimalkumar, S.K. Sharma, J.B. Singh et Y.K. Dwivedi, « 'Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants », *Computers in Human Behavior*, 120, 2021; J. Lau, B. Zimmerman & F. Schaub, *op.cit.*, in *Proceedings of the ACM on Human-Computer Interaction 2*, CSCW, 2018

[54] M. Temming, *op. cit.*, *SCIENCENEWS.ORG*, 2018

[55] "The term information security is generally based on information being considered as an asset which has a value requiring appropriate protection, for example, against the loss of availability, confidentiality and integrity. […] Information security is achieved through the implementation of an applicable set of controls, selected through the chosen risk management process and managed using an ISMS, including policies, processes, procedures, organizational structures, software and hardware to protect the identified information assets.", *ISO/IEC 27000:2018(E) Information technology — Security techniques — Information security management systems — Overview and vocabulary*, 2018, p9-12

> 28% responded that when using or installing an app on the smartphone they never restricted or refused its access to personal data. 7% of smartphone users in the EU did not know it is possible to restrict or refuse access to their personal data when using or installing an app on the smartphone"[56].

If users are aware of the privacy threats, they can adopt a more conservative approach, like choosing service providers that appear safer, and develop obfuscation techniques[57]. To come back to the voice example, in Kröger & al.'s survey, "many participants have rarely (28.4%) or never (42.5%) even thought about the possibility of personal information being inferred from speech data"[58]. Down to an earth-to-earth approach, "apps have to get user permission upon first installation or first use to access certain sensors like the mic and camera. But people can be cavalier about granting those blanket authorizations"[59]. Awareness in technology and rights is at the foundation of trust for users and enhances digital progress. Besides, awareness should also involve professionals, such as app developers, so they could naturally propose privacy friendly applications. Logically, developing awareness amongst both users and Internet service providers participate to the enforcement of social normative behaviors and the law, as it encourages to use privacy respectful apps and spread legal awareness of what is legal or not, including individual rights and data controller and processors responsibilities.

In this case, the awareness of the individual rights starts with an emphasis on the right to be informed. This right to be informed for users is broad and constitutes the core center of the regulation as it allows users to know their rights and what data are involved[60]. The challenge of informing consumers is even greater as smartphones collect extensive amount of data for various uses. There comes into play the fundamental principle of transparency[61]. This principle is one of the cornerstones of data protection[62] and is linked to fairness of data processing and requires the data controller to provide clear information about which data is collected and the way it is treated. Consecutively, the data controller should provide accessible and clear

---

[56] Eurostat, *Trust, security and privacy – smartphones*, Last update: 30-03-2022, [http://bitly.ws/yjtu].

[57] F. BRUNTON et H. NISSENBAUM, *Obfuscation: A user's guide for privacy and protest*, MIT Press, 2015.

[58] J.L. KRÖGER, L. GELLRICH, S. PAPE, S.R. BRAUSE et S. ULLRICH, *op. cit.*, *Proceedings on Privacy Enhancing Technologies*, 2022, p. 6.

[59] M. TEMMING, *op. cit.*, *SCIENCENEWS.ORG*, 2018.

[60] "App developers are constrained by the features made available by Operating System manufacturers and app stores to ensure comprehensive information is made available, at a relevant time, to the end user", Article 29 Data Protection Working Party, *op.cit.*, 2013, p. 6.

[61] M. HATAMIAN, *op. cit.*, *IEEE Access*, 2020, p. 35437.

[62] The Working Group 29 stated that "key data protection risk is the lack of transparency", Article 29 Data Protection Working Party, *op.cit.*, 2013.

information about the purpose and the legal basis invoked for the data processing, the time of data conservation, if their personal data will be automatically processed, if there are transfers to third parties and if the data is being transferred abroad[63]. As Hatamian outlined, "the significance of this [transparency] aspect is even greater for smartphone apps since third-party components (that might collect data as well) are often integrated into an app's development phase"[64]. As a matter of fact, some regulations included a dedicated mention stating that the recipients or categories of recipients of personal data must be revealed to users[65]. Beyond the right to receive and access information, the lack of privacy indicators in smartphone ecosystems prevents users from being able to compare apps in terms of privacy and to perform informed privacy decision-making when selecting apps[66]. Data protection laws require app developers and data processors to be transparent on many levels, including the specification of the legal basis attached to the purpose of data processing. In most data protection legal systems, the choice of the legal basis is pivotal as it will determinate the specific legal regime of application and will ground the data collection juridically. The choice of the legal basis is not entirely up to the data controller and answers both some requirements of proportionality and adequacy between the private person's interest and other parties involved. For example, "monetizing purposes, i.e., advertising, are not classified as necessary and therefore need to be based on another legal ground. Similarly, the processing of data to develop new features and services is not specific enough to comply" [67]. The European legal system distinguishes six legal bases as follows: the law (mandatory legal basis), the contract, the consent, the legitimate interest, the vital interest, and the public interest.

[63] If processing personal data the relevant data controller must inform potential users at the minimum about:
– who they are (identity and contact detail),
– the precise categories of personal data the app developer will collect and process,
– why (for what precise purposes),
– whether data will be disclosed to third parties,
– how users may exercise their rights, in terms of withdrawal of consent and deletion of data).
Article 29 Data Protection Working Party, 2013, *op.cit.*, p. 22.

[64] M. HATAMIAN, *op. cit.*, *IEEE Access*, 2020, p. 35437; Such context comes with a cost for privacy and affects information security at multiple levels. These issues will be discussed later on, but here is a piece of advice emanating from the ENISA, "App developers should choose third party components carefully because their behavior may pose privacy and security risks to users, e.g. by collecting user data on their own without a legal ground and transparency for the users", C. CASTELLUCCIA, S. GUERSES, M. HANSEN, J. H. HOEPMAN, J. VAN HOBOKEN, AND B. VIEIRA, *Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR*, ENISA 2017, p57, [https://edps.europa.eu/sites/edp/files/publication/16–11-07_guidelines_mobile_apps_en.pdf].

[65] For example : Article 13 (1) of the Regulation 2016/679 (UE), of the European Parliament and of the Council.

[66] M. HATAMIAN, J. SERNA & K. RANNENBERG, "Revealing the unrevealed: Mining smartphone users privacy perception on app markets", *Computers & Security*, 83, 332-353, 2019.

[67] M. HATAMIAN, *op. cit.*, *IEEE Access*, 2020, p. 35437.

This information has to be accessible for users, in an understandable manner, with a special attention to children[68] that are often protected by additional legal measures.
Before the data processing begins[69], users must receive clear and comprehensive information in appropriate language in order to be able to consent[70]. It is a common statement that users do not have access to clear information, thus their consent to share personal data is biased and might not be juridically acceptable, leading to unlawful data processing. Consequently, there are some cases where consent will not be valid, such as when information was not accessible, unclear, deceitful as well as if data processing is not proportionate or does not match the purpose set in advance. A final word on consent shall underline that this legal basis should not be abused[71], in the sense that there shall be granular options proposed to users in case the consent is asked, like a form of granularity allowing to customize the data processing by the data subject. Smartphone users shall have options to withdraw their consent easily, especially for children's consent that has additional protection in different legislations[72].

---

[68] Services targeted at children must provide information in clear and plain language that children can understand easily and respect age limits for consent. The Article 29 Data Protection Working Party identified specific dangers for children as they "are avid users of apps, either on their own devices or on shared devices (e.g. those of their parents, siblings or in an education setting) and there is clearly a large and diverse market for apps targeted at children. But at the same time children have little or no understanding of and knowledge about the extent and sensitivity of the data to which apps may gain access, or the extent of data sharing with third parties or advertising purposes", Article 29 Data Protection Working Party, *op.cit.*, 2013, p. 26.

[69] "Providing such information only after the app has started to process personal data (which often starts during installation) is not deemed sufficient and is legally invalid", *Ibidem*, p. 22.

[70] "Availability of this information on personal data processing is critical in order to obtain consent from the user for the data processing. Consent can only be valid if the person has first been informed about the key elements of the data processing", *Ibidem.*

[71] To summarize Corgas' analysis, the blurring of the lines would allow the mechanism of positive consent to be circumvented, tending towards a legal basis oriented towards a multiplication of the legal bases invoked, such as the contractual basis for Facebook, followed by consent in a substitute position, accompanied by legitimate interest. Consent would only be used in the processing of sensitive data. Such maneuvers blur the lines and require much more effort to understand for the user. Therefore, the processing of data can only be refused through a proactive approach of the user, who must use his right to object explained in annexed documents, which should be researched and the appropriate intellectual gymnastics to resort to the aforementioned social networks. It should be noted that the use of the legitimate interest solution is relatively common in the TOS of Anglo-Saxon companies, without really clearing the practices of companies in the EU. C. CORGAS (dir. A. BENSAMOUN, M. BOIZARD & S. TURGIS), « L'articulation avec le contrat. Conditions générales d'utilisation des réseaux sociaux et profilage », *Le profilage en ligne : entre libéralisme et régulation*, Mare Martin, Libre Droit, 2020. This is a long-standing practice, as also denounced by E. Netter. Netter "Data controllers and subcontractors [...] could not always justify a precise basis of lawfulness, or relied on a consent that was grossly extorted from the persons whose data were processed, or abused the particular basis of legitimate interest", in E. NETTER, "Le modèle européen de protection des données personnelles à l'heure de la gloire et des périls", *Regards sur le nouveau droit des données personnelle*s, CEPRISCA, collection colloques, 2019, p. 7.

[72] With COPPA in the US, GDPR and DSA in the EU and the recent Children's code (or the Age appropriate design code) of the British ICO. "Protective measures are also laid on the processing of children's data. Many app stores offer a large assortment of apps targeted at children. However, children are considered to have little or no

In the same vein, data controllers of digital services relying on smartphone usage should inform users about their right to withdraw consent, to access to their own data, their right to proceed to portability, their right of erasing their personal data or to modify incorrect data. Similarly, the transparency principle applies for automatic data processing and profiling[73]. Data subjects commonly shall have access to the general functioning of the automatic processing, in order to understand how their profile is treated and to be able to contest in case of unlawful treatment. In spite of such measures, it can be hard to access to this information as they can be directly connected to industrial secrecy, as algorithms are protected by law of intellectual property for example. Besides, explaining the way automatic decisions are taken can be tough when considering that most of them are artificial intelligence based, with machine learning process involved[74]. Consequently, it becomes difficult to offer adequate information to users as they might not be familiar with these concepts. Moreover, some machine learning techniques are barely explainable by data scientists[75], especially the ones using deep learning.

These are constitutive norms that shall not be forgotten, or the data protection right would be severely undermined. Information has to be fundamentally acknowledged as axiomatically connected to the awareness aforementioned, which has been hammered several times throughout this paper. The awareness of the data protection norms is obviously a strategic issue amongst app developers, as outlined the Working Group 29: "app developers

knowledge of the risks associated with the usage of smartphones", therefore the processing of children's data is only lawful if the child is over certain age depending on regions, M. HATAMIAN, *op. cit.*, *IEEE Access*, 2020, p. 35432.

[73] "Profiling techniques can be divided into two main groups, depending on whether they use a state or not. On the one hand, there are "stateful techniques [that] store the information necessary to track a user locally on his or her device; this information is then retrieved during subsequent visits to recognize the user. Cookies are the most commonly used technique on the web today," while stateless techniques "allow trackers to recognize a user, and thus track and profile them, without having to store any information on their device. Among these techniques, 'device fingerprinting' consists of collecting information about the user's web browser, its configuration, and the operating system he uses, in order to be able to re-identify him with a very high probability in a unique way", B. BAUDRY, D. BROMBERG, D FREY, A. GOMEZ-BOIX, P. LAPERDRIX, F. TAÏANI (dir. A. BENSAMOUN, M. BOIZARD ET S. TURGIS) « Profilage de navigateurs : état de l'art et contremesures », *Le profilage en ligne : entre libéralisme et régulation*, Mare Martin, Collection Libre Droit, 2020, pp. 185-186.
CEPD, « Guidelines on automated individual decision-making and Profiling for the purposes of Regulation 2016/679", final revision adopted on 6 February 2018; CNIL, *Profilage et décision entièrement automatisée*, *2018,* [https://www.cnil.fr/fr/profilage-et-decision-entierement-automatisee]*;* A. BENSAMOUN, (dir. A. BENSAMOUN, MARYLINE BOIZARD ET SANDRINE TURGIS) « Profil, Profilage et prophétie », *Le profilage en ligne : entre libéralisme et régulation*, Mare Martin, Collection Libre Droit, 2020, p. 11.

[74] G. LOISEAU, (Dir. A. BENSAMOUN, G. LOISEAU), « Intelligence artificielle et droit des personnes », *Droit de l'intelligence Artificielle*, LGDJ Lextenso, Les intégrales, 2019, p. 36; A. DEBET (Dir. A. BENSAMOUN, G. LOISEAU), « Intelligence artificielle et données à caractère personnel », *Droit de l'intelligence Artificielle*, LGDJ Lextenso, collection Les intégrales, 2019, p270; J.M. DELTORN (Dir. E. NETTER), *op. cit.*, *Regard sur le nouveau droit des données personnelles*, 2019.

[75] *Ibidem.*

unaware of the data protection requirements may create significant risks to the private life and reputation of users of smart devices"[76]. On a side note, researchers investigated how app developers make decisions about privacy and security, about what data to collect from end-users, and how that data is effectively used[77].

Indeed, this is one of the main challenges for privacy policies, as awareness should be spread to develop a culture of privacy friendly processing. App developers shall develop a responsible approach of data protection, which is logically easier if there are accustomed to data protection legal matters. However, the complexity of data protection legal structures can be quite overwhelming for app developers and represent a form of insurmountable obstacle. As soon as app develop start to deal with handful of personal data or sensitive data, they need to comply with the law. Rapidly, app developers would require receiving legal counsel from experts, which comes with a cost that might not be bearable by a newly starting app developers working alone. To sum up, app developers, in most legal systems including data protection norms, have the obligation to present a clear and understandable privacy policy, sometimes also introduced as a confidentiality section that should be directly accessible from both the application store and the app itself. This imperative has distinctively not been followed by app developers as most empirical studies have shown so far[78]. These elements represent some of the ongoing and pressing issues undermining data protection norms as new mobile apps, more often than not, do not have the proper infrastructural ground nor the human resources to comply with the law.

[76] Article 29 Data Protection Working Party, *op. cit.*, 2013, p. 2.

[77] The groundwork was basically a series of interviews with 13 app developers for qualitative information about privacy and security decision-making, followed by an online survey of 228 app developers to quantify behaviors and test our hypotheses about privacy and security behaviors related to company characteristics. This research indicated that smaller companies are less likely to demonstrate positive privacy and security behaviors. Additionally, although third-party tools for ads and analytics are pervasive, developers aren't aware of the data collected by these tools, R. BALEBAKO, A. MARSH, J. LIN, J. HONG, L. FAITH CRANOR, *The Privacy and Security Behaviors of Smartphone App Developers*, Carnegie Mellon University, 2014.

[78] "The Google Play Store gives app developers the option to include links to their privacy policies on their Play Store pages. However, in three separate crawls of apps we found that only 41,7% (August 28 through September 2, 2012), 45,2% (November 29 through December 2, 2017), and 51,8% (May 11 through May 15, 2018) have such links. While there appears to be an upward trend, these percents are relatively low, especially, as they include links for apps that are legally required to disclose their pratices in privacy policies", P. STORY, S. ZIMMECK, N. SADEH "Which apps have privacy policies? An analysis of over one million Google Play Store Apps", *Privacy Technologies and Policy 6th Annual Privacy Forum*, (M. Medina, A. Mitrakas, K. Rannenberg, E. Schweighofer, N. Tsouroulas), Springer, APF 2018, p. 4.

B) A Fundamental Prism of Responsibility of Data Collection for Data Controller and Processor Within the Context of App Store and App Developers

Amongst the persistent difficulties to raise responsible behaviors, it seems important to outline a special aspect of responsibility in which smartphone is emblematic. Most data protection regulation is settling the share of responsibilities between data controller and data processors as data controller is choosing the technical means and setting the purpose of the data processing. Some sectorial regulations are complicated to apply when it comes to dispatch responsibility between data controller and processors. Regarding smartphone apps, app market providers are usually considered data controllers and app developers would logically be processors[79]. However, such distribution of roles is sometimes blurring the lines of responsibility as it seems difficult to come back to the criterions based on organizational prerogative and setting purpose. Private companies and experts have both alerted about this constant issue[80]. Furthermore, this distinction makes it more complicated for consumers to have their right observed. Other situations can bring multiple data controllers at the same time when purpose and/or means are determined jointly by them. For example, "if data-driven functionalities such as advertisement networks are integrated into an app, several data controllers might be at place. There might as well exist several data processors, for instance, if cloud services are used"[81]. Within the smartphone eco-system, apps are the software that people use to access most services. One app is created by an app developer, however, this one will usually require some assistance of other apps to make it accessible and fully optimized. Although these app developers are accessory, they also participate to data processing in various ways. Consecutively, these secondary app developers also bear a part of responsibility regarding data protection norms, which creates an endless chain[82] of processors and/ or several joint data controllers. This is what stressed the European Data Protection Working Party since 2013[83]. The increasing number of app

[79] "Typically, the data controller is thus the app provider, whereas the app developer is typically a data processor. In cases where the app provider is the same person as the app developer, she is regarded as the data controller. In legal terms, the data controller is the most important entity, since she must guarantee compliance with legislation", M. HATAMIAN, *op. cit.*, *IEEE Access*, 2020, p. 35432.

[80] P.-L. DÉZIEL, *op. cit.*, *Les cahiers de propriété intellectuelle, Yvon Blais*, 2018.

[81] M. HATAMIAN, *op. cit.*, *IEEE Access*, 2020, p. 35432.

[82] "This is particularly important with regard to security, where the chain of multiple actors is only as strong as its weakest link", therefore the multiplication of actors is huge risk factor as mentioned by the Article 29 Data Protection Working Party, *op.cit.*, 2013, p. 2.

[83] "A high risk to data protection also stems from the degree of fragmentation between the many players in the app development landscape. They include app developers; app owners; app stores; Operating System and device manufacturers (OS and device manufacturers); and other third parties that may be involved in the collection and processing of personal data from smart devices, such as analytics and advertising providers", *Ibidem.*

developers involved in data processing is obviously complicating the distribution of responsibility.

Data processing is one of the most central concept of data protection law, and responsibility is mostly held by data controllers and can be attributed to data processors in some cases. Therefore, the data protection norms raised protective principles to limit data processing to preserve privacy, namely limitation purpose and data minimization. Article 29 Data Protection Working Party delimited the limitation purpose principle as it "enables users to make a deliberate choice to trust a party with their personal data as they will learn how their data are being used and will be able to rely on the limitative purpose description to understand for what purposes their data will be used"[84]. Along the same lines, the minimization principle is explained in the ENISA study of 2017 and understood as "the minimum amount of data for specific processing should be processed by app providers/developers. For instance, they should not store the exact location point when a generic location area is sufficient for their app functionalities"[85]. This cardinal and protective principle has for a global purpose to avoid excessive processing.

These principles are structuring data processing performed by app developers, internet operators and OS constructors. These actors can be identified as points of controls[86], as Zittrain explained, thus legislator could apply specific pressure on professionals that handle smartphone data. In order to respect these principles, app developers should consider that even though smartphones contain a considerable amount of sensitive personal data, they "must only collect and process the data that is strictly necessary (data minimization) for the purposes for which it has been collected (purpose limitation)"[87]. Data controllers should set in advance the type and precision level of data they will collect. Additionally, they shall stick to what is truly necessary for the data processing. In the context of smartphone, data collection and processing are too often disproportionate for their initial purpose, thus, the level of precision can sometimes undermine privacy because the accuracy level of information collected is too high (e.g. location privacy issues). Data protection laws entail complete restriction for further purposes than the one announced initially, as they are incompatible with the purpose limitation principle. App developers must only process data when the app has a specific lawful purpose for doing so. As limitation purpose and data minimization are both two sides of the same coin, the second principle is also actively working on balancing the data processing, especially considering the context of "big data

[84] *Ibidem*, p17

[85] C. CASTELLUCCIA, S. GUERSES, M. HANSEN, J. H. HOEPMAN, J. VAN HOBOKEN, & B. VIEIRA, *op.cit.*, ENISA 2017, p22

[86] J. ZITTRAIN, *op. cit.*, *The Emergent Global Information Policy Regime,* 2004

[87] M. HATAMIAN, *op. cit.*, *IEEE Access*, 2020, p. 35437

applications where huge amounts of personal data are collected to analyze customers"[88]. Only necessary data, with a restrictive approach of precision level, should be collected by data controllers and processors.

One of the mechanics of smartphones is the fact that "mobile apps are constantly sharing data (including sensitive ones) to different parties ranging from remote servers to other apps"[89]. On top of that, smartphones also constitute the very center of data collection as they gather most connected objects[90]. Followingly, data sharing with third parties is undermining privacy by essence, thus it should be restricted as much as possible. Data transfer[91] to private actors is a major issue that needs to be observed and regulated. As much as it became a new dynamic enhancing data brokers economy[92], personal data flow is causing privacy breach on a daily basis[93], and undermines data transfer safety leading to cybersecurity issues[94] as *"there is the chance that data transmission will be compromised or accidentally shared"*[95]. *As Hatamian stated, "t*he transmission of personal data to third parties must be avoided, unless such transfer is necessary for the purpose" as much as "developers need to appropriately limit the amount of personal data being shared with other apps"[96].

These transfers, which are commonly operated although not explicitly mentioned, represent both additional information security issues and privacy invasion that weaken data protection. The Group 29 insisted on the actors' responsibility embracing a holistic vision, "in order to comply with their respective security obligations as data controllers, app developers, app stores, OS

---

[88] *Ibidem.*, p. 35433.

[89] *Ibidem,* p. 35434.

[90] S. LEE, *The Ethics of Data Collection: Smart Phones and Wearable Technology*, 2017

[91] Android Smartphones are transmitting 50 times more data to Google than Iphones to Apple, see D. C. SCHMIDT, *Google Data Collection*, Digital Content Next, 2018, [https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf]

[92] S. MELENDEZ & A. PASTERNACK, "Here are the data brokers quietly buying and selling your personal information", *Fast Company*, 2019: [https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information]

[93] Speaking to Forbes in early 2020, security researchers Gabriel Cirlig and Andrew Tierney claimed that Xiaomi's web browsers collect an excessive amount of data even in incognito mode. This allegedly included all URLs and search queries made in the stock MIUI browser, Mi Browser Pro, and Mint Browser. Combined, these browsers have more than 15 million downloads on the Google Play Store; S. DALUL, *Is selling your privacy for a cheaper phone really a good idea? Xiaomi has addressed its recent privacy controversies — here's what's changed*, Android Authority, 2021: [https://www.androidauthority.com/xiaomi-privacy-cheap-phone-1118444/]; B. MANN Are Smartphone Apps Stealing Your Personal Data?, 2020: [https://blokt.com/guides/are-smartphone-apps-mining-your-personal-data].

[94] Examples of apps breaching privacy: J. BALL, *Angry birds and 'leaky' phone apps targeted by NSA and GCHQ for user data*, 2014: [http://www.theguardian.com /world/2014/jan/27/nsa-gchq-smartphone-app-angry-birdspersonal-data]; M. C. GRACE, W. ZHOU, X. JIANG, & A.-R. SADEGHI, "Unsafe exposure analysis of mobile in-app advertisements", in *Proceedings of WISEC '12*, 2012

[95] M. TEMMING, *op. cit.*, *SCIENCENEWS.ORG*, 2018

[96] M. HATAMIAN, *op. cit.*, *IEEE Access*, 2020, p. 35435

and device manufacturers and third parties have to take the principles of privacy by design and by default into account"[97]. This privacy by design[98] concept shall be the ground from which app developers should build their confidentiality policy and apps. The privacy by design approach brings pragmatic and technical answers to legal issues in that case[99]. Naturally, "privacy by design is connected to the 'Principle of Least Privilege' […]" which literally means that app developers "must give apps the minimum number of permissions necessary for providing a certain functionality/service"[100]. To conclude on the benefit of privacy by design, this paradigm should be seen as a methodology for data controllers and processors to implement privacy friendly measure in the lifecycle of personal data, hence its relevance and impact on data processing. This type of data management is evidently fundamental for users' rights and shall be systematically implemented on the way to create a good practice-based approach. Such inspiration goes beyond the legal obligation of data controllers and processors; however, they are the current main roads to improvements[101].

A small word on information security is required as it is one obligation stated in some data protection regulation and is necessary to build trust between users and data controllers. As it was above-mentioned in the last paragraph, responsibility for data controllers and processors also naturally lies in the obligation to ensure technical and organizational security measures to protect

---

97 Article 29 Data Protection Working Party, *op.cit.*, 2013, p. 18.

98 A. CAVOUKIAN, *Privacy by design : the 7 foundational principles*, 2009; The GDPR introduces privacy by design and by default in Article 25(1) Regulation 2016/679 (EU); See E. NETTER, Numérique et grandes notions de droit privé, la personne, la propriété, le contrat, Mémoire pour HDR, CEPRISCA, Essais, 2017; See also P.O PIEALET, « La privacy by design à l'épreuve des dark patterns », in *Revue du Droit des Technologies de l'Information*, Larcier n°80, 2021.

99 "The main advantage of this approach is that it clearly separates the legal requirements from the more concrete engineering goals. This removes the current unreasonable expectation that engineers need to think like lawyers or social scientists", C. CASTELLUCCIA, S. GUERSES, M. HANSEN, J. H. HOEPMAN, J. VAN HOBOKEN, AND B. VIEIRA, *op.cit.*, ENISA 2017, p. 55.

100 "For instance, a flashlight app simply needs to access the device's sensor to properly deliver its desired functionality. Hence, such an app does not need to access sensitive information, such as contact list, location, phone number, etc.", M. HATAMIAN, *op. cit.*, *IEEE Access*, 2020, p. 35433.

101 This argument will not be discussed, although these are pivotal aspects of data management including new tools for data protection such as "data protection impact assessment" concept (DPIA) or more globally the initiative of private actors to sign "Code of conduct" or "Charter of good practices". These elements truly represent the extension of the law translated into the corporate world as we know it today. This legal trend is exponentially booming and will impact corporate culture massively. This has mostly a sectorial approach at the moment, though it is gaining a clear momentum, see S. GUIDA, "The first GDPR EU-wide code of conduct approved by Data Protection Authorities", *European Journal of Privacy Law & Technologies*, 2021; B. M. KNOPPERS, J. R. HARRIS, A. M. TASSÉ,I. BUDIN-LJØSNE, J. KAYE, M. DESCHÊNES, M.N.H ZAWATI, "Towards a data sharing Code of Conduct for international genomic research", in *Genome Medicine*, *3*(7), 2011; For more about DPIA, see F. BIEKER, M. FRIEDEWALD, M. HANSEN, H. OBERSTELLER, M. ROST, "A process for data protection impact assessment under the european general data protection regulation", *Annual Privacy Forum*, Springer, Cham, 2016; R. BINNS, "Data protection impact assessments: a meta-regulatory approach", *International Data Privacy Law* 7, no. 1, 2017.

access to personal data. Accordingly, app developers shall choose data processors considering their ability to protect personal data equally. This dimension of information security englobes the ability to provide confidentiality, integrity, availability and resilience of processing systems and services. These key-concepts are the main standards for data protection, which always has to be considered on the verge of the state of the art and analyzed in proportionality to the cybersecurity context, the sensitive nature of data and the means at disposition of the data controllers and processors. Technical and organizational measures have to prevent data breach, with procedures such as organizing backups, controlled access to personal data, data encryption and end-to-end secure channel such as TLS. For example, by trying to proceed to pseudonymization, the app developer is showing good faith in trying to preserve consumers' privacy, although anonymization would be the best way to eradicate security issues. As the Working group 29 stated, "poor security measures may lead to unauthorized processing of (sensitive) personal data, for example if an app developer suffers a personal data breach or if the app itself leaks personal data"[102]. Therefore, a series of procedures should be elaborated in advance to show resilience in cyber systems. In case of cyber incidents, the app developer should inform users of the data violation as well as the relevant authorities. Additionally, the app developer should do anything it takes to make the data violation cease and try to retrieve data loss. This is of particular importance in smartphone ecosystems since they are typically linked to a huge amount of data transfers.
Furthermore, personal data security shall serve two important purposes that are strategic for private companies: "It will empower users to more stringently control their data and enhance the level of trust in the entities that actually handle users' data"[103]. Such changes would contribute to a long-term and sustainable cultural adaptation of consumers, keener to adopt new technology and protect cyber infrastructures.

C) Evolution of Personal Data Categories Considering the Smartphone Ecosystem

A last word on the legal challenges awaiting data protection regulation lies in the very nature of data that is being influenced by the intensity of data collection. The specific smartphone eco-system entails new privacy challenges and tends to question the classic conception of personal data categorization. First of all, "the omnipresence of smartphones in every sphere of society leads to the situation that everyone's privacy is affected, as one does not have to own a smartphone to be recorded by users of smart devices"[104] alerts Temming. This goes further, if there are

[102] Article 29 Data Protection Working Party *op.cit.*, 2013, p. 6.
[103] *Ibidem,* p. 18.
[104] M. TEMMING, *op. cit.*, *SCIENCENEWS.ORG*, 2018.

laws protecting privacy within the realm of the private home or certain public spheres, balancing with the secrecy principle mitigated by the public interest to access information, "the general rule of thumb is that anything happening in a public area may be recorded"[105].

Secondly, the permanent character of data collection processed through smartphone along with an unprecedented level of precision of data is changing the nature of data on at least two points. Indeed, the technologic improvement are leading to two major shifts: the movement of personalization of any type of data and the increased sensitivity of formerly common data. Succinctly, what was not personal data by nature in the past, could be considered as personal data considering the intensity of data collection through smartphones and the capacity of calculation and storage. The ever-growing data collection comes to a point that most data emanating from an individual can be used to identify the latter when crossed with other sets of data. As a result, non-personal data might effectively become identifiable, *"every day, your smartphone is tracking where you are, how long you were there, who you've contacted, and what you've searched for"*[106].

Then again, the intensity and precision of the data collected can affect privacy in threatening manners. This can raise serious question when personal data are shifting to sensitive personal data. For example, the precision and permanent collection of location data can reveal where and when individuals are going for medical appointments, which religious building, syndicate and so on and so forth. Even though location data was primarily not a sensitive data such as health data, biometric data, or data related to religious beliefs, syndicate association, etc., such data can become sensitive depending on the intent of data controllers. Such shift from regular personal data to sensitive ones derives directly from the choice data controllers are making about data processing. This simply means that if the purpose of data processing has an invasive nature, therefore, it will affect privacy greatly and changes the legal regime of collected data. Finally, it seems that traditional distinction between non-personal data, personal data and sensitive personal data is being shaken by the evolution of smartphone ability to collect data. Data protection law is clearly challenged by the intensity of data collection and needs to adapt.

CONCLUSION:

Overall, the personal nature of data tends to evolve drastically towards a more invasive impact on privacy, by crossing sets of data and increasing data collection precision, intensity and permanence which adds informational value to personal data to

[105] *Ibidem*
[106] *Ibidem*

the point that it shifts to sensitive information. Thus, non-personal data becomes personal data and regular type of data can even turn into sensitive data, as it was demonstrated with location and voice data. The digital shift happening before us needs answer or the data protection laws will become soon obsolete. As of today, the balance between data protection regulation and data controllers and processors interests is challenged constantly by the rapid progress of digital technology to capture personal data.
Some solutions are proposed by diverse entities, rather technical, following privacy by design and by default principles. As a matter of examples, researchers tried to conceive different tools to enhance apps privacy. There are some experimental works that assessed the different cyber threats of certain data, such as the location privacy protection concept[107]. Concrete solutions are brought to aforementioned issues about location and voice[108] for examples[109]. Technical answers could arise as forms of safeguards directly within apps, or through operating system updates. Consequently, such solutions are tested by the scientific community[110], however there seems to be no follow up by private

[107] K. FAWAZ, & G. S. KANG, *op.cit.*, in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014, p. 241.
[108] See for the voice issue, see A. M. REDIGER, "Always-Listening Technologies: Who Is Listening and What Can Be Done About It", in *Loy. Consumer L. Rev.* 29, 2016, p229
[109] To answer to the motion sensor issue and keystroke capture, see the work of A. K.SIKDER, A. KUMAR, H. AKSU, & A. S. ULUAGAC, "{6thSense}: A Context-aware Sensor-based Attack Detector for Smart Devices", in *26th USENIX Security Symposium (USENIX Security 17)*, 2017:
[https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/sikder].
The scientist team proposed "a system called 6thSense, which monitors a phone's sensor activity and alerts its owner to unusual behavior, in Vancouver at the August 2017 USENIX Security Symposium. The user trains this system to recognize the phone's normal sensor behavior during everyday tasks like calling, Web browsing and driving. Then, 6thSense continually checks the phone's sensor activity against these learned behaviors.
If someday the program spots something unusual — like the motion sensors reaping data when a user is just sitting and texting — 6thSense alerts the user. Then the user can check if a recently downloaded app is responsible for this suspicious activity and delete the app from the phone", explains M. Temming
[110] Researchers propose an AI based reviews analysis platform called Mobile App Reviews Summarization (MARS). This tool processes user reviews on the Google Play Store to extract and quantify privacy relevant claims associated with apps. "Based on Machine Learning (ML), Natural Language Processing (NLP) and sentiment analysis techniques, MARS detects privacy relevant reviews and categorizes them into a pre-identified list of privacy threats in the context of mobile apps". MARS is made to spread information about apps' privacy standards, raising awareness for consumers and developers which did not realize this issue. Consequently, this mechanism allows to socially sanction developers missing on privacy concerns but can also help them improve their app privacy structures. On the other hand, assessing privacy levels of apps based on comments from users, which are most of the time amongst the least informed protagonists both in terms of user rights and technical information security, could be a limited solution overall. M. HATAMIAN, J. SERNA & K.RANNENBERG, *op.cit.*, in *Computers & Security*, *83*, 2019; K. FAWAZ, & G. S. KANG, *op.cit.*, in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014; Another team of researchers proposed the app AWare, which would request user permission for an app to access a certain sensor the first time a user provided a certain input, like pressing a camera button. Additionally, the AWare system memorizes the state of the phone when the user grants that initial permission, thus, AWare can tell users if the app later attempts to trick them into granting unintended permissions, G. PETRACCA, A. A.

companies, as underlined Temming: "Just because someone has built and successfully tested a prototype of a new smartphone security system does not mean it will show up in future operating system updates"[111]. Even though we can observe the Android security team at Google trying to mitigate privacy risks posed by app sensor data collection[112], there is a huge gap between the data protection regulation and technical and organizational measures implemented in reality. Setting practical solution to protect users' privacy is necessary but temporary due to the rapid evolution of digital technologies, therefore digital law remains the staple for durable preservation of informational privacy. Long-lived legal principles still have their roles to play in this transition, although our wish is not to fall for the unreasonable proposition of a price for our privacy.

REINEH, Y. SUN, J. GROSSKLAGS, T. JAEGER, "{AWare}: Preventing Abuse of {Privacy-Sensitive} Sensors via Operation Bindings", in *26th USENIX Security Symposium (USENIX Security 17)* 2017, [https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-petracca.pdf]

[111] M. TEMMING, *op. cit.*, *SCIENCENEWS.ORG*, 2018

[112] Apple. Protecting the User's Privacy. Accessed May 2, 2022, [https://developer.apple.com/documentation/uikit/protecting_the_user_s_privacy; Google Developers. Design for Safety: Android is secure by default and private by design. Accessed May 3, 2022. https://developer.android.com/design-for-safety]