Privacy nutrition labels, app store and the GDPR: Unintended consequences?

Miloš Novović
Associate Professor of Law, BI Norwegian Business School, Norway

Miloš Novović is an associate professor of law at BI, specialising in law and technology. He is responsible for several courses on privacy and data protection, as well as legal tech courses covering issues such as digital contracts, copyright, AI and digital platforms. His teaching and research interests also include international commercial contracts and arbitration law. Miloš holds a PhD in law from the University of Oslo, where he wrote about copyright, contract and private international law issues stemming from copyright-related terms of use agreements offered by the largest online companies. He also holds an LL.M. in intellectual property law from George Washington University, as well as an LL.B. from the University of Montenegro. Miloš provided privacy and IT contract-related advice to major Norwegian and international companies over several years and is a chairman of the Norwegian Society for Comparative Law.

BI Norwegian Business School, Nydalsveien 37, 0484 Oslo, Norway
Tel: +47 974 22 223, E-mail: milos.novovic@bi.no

Abstract In an effort to increase the transparency of personal data processing carried out via applications listed on their mobile store, Apple recently announced the launch of privacy nutrition labels (PNLs). Aimed at informing users about an application's use of data, these card-like labels are prominently visible on each application's App Store page.

This paper explores whether such disclosures made via PNLs can help data controllers fulfil their duty of transparency under the EU General Data Protection Legislation (GDPR). It establishes that the PNLs, in their current, highly standardised fashion, cannot convey the mandatory obligations required by the GDPR. Added to this, they cannot adequately supplement existing privacy policies, either — as they neither serve an adequate role as a 'first layer' of a privacy notice, nor help communicate information more efficiently.

However, the paper finds that the PNLs might serve another purpose: enhancing data controllers' internal compliance routines. PNLs, even with their current limitations, can bring tangible improvements to cross-functional communication, third-party sharing awareness, records of processing accuracy, adherence to the data protection principles and adequate resource assignment.

The overall conclusion of the paper, counterintuitive as it might appear, is that PNLs should be viewed as an organisational measure-enhancing mechanism rather than a transparency tool.

KEYWORDS: privacy labels, Apple App Store, transparency, data processing notice, software development, compliance

INTRODUCTION

Transparency is a cornerstone principle of data protection law.[1] Data protection rules serve two fundamental purposes: they allow individuals to exercise decisional autonomy over the use of their data, and they make it possible for society at large to hold those who process personal data accountable.[2, 3]

Without transparency, such objectives cannot be met — and no safeguard of data protection laws would be efficient in its absence.

However, ensuring transparency of processing is no easy task. In the digital realm, and specifically within the context of smartphone end-user applications, two fundamental problems are compounded. On the one hand, data controllers often struggle to provide concise, useful or even correct information to their users. On the other, users notoriously find privacy notices difficult to read and understand, questioning the value of investing their time in parsing the dense, non-negotiable text.

In an attempt to bridge this gap, Apple introduced its newly created privacy nutrition labels (PNLs), the result of asking the developers to provide an overview of their privacy practices in a simple, standardised label.[4] In early 2021, Google followed suit, announcing the new Data Safety section for applications deployed on the Play Store.[5] Both initiatives claim to be aimed at enhancing end-users' privacy, by helping them make informed choices on how their data will be used.

The aim of this paper is to examine whether such privacy labels can be used to satisfy the transparency requirements embodied in the General Data Protection Regulation (GDPR), and the extent to which they can contribute to the overarching principles of accountability and privacy by design. Specifically, can such labels be a useful tool for fulfilling data controllers' transparency obligations — and what kind of effects could they have on data controllers' internal compliance processes?

PNLS ON THE APPLE APP STORE

For many years, Apple, the world's largest technology company, has used privacy as a part of its customer value proposition. In early 2019, Apple strategically placed a building-tall billboard in Las Vegas — the city hosting the Consumer Electronics Show — proclaiming that 'what happens on your iPhone, stays on your iPhone'.[6] The company continued the advertising efforts focusing on privacy well-into 2022, with billboards in major cities boldly stating: 'Privacy. That's iPhone'.[7]

When version 14 of the iOS operating system was introduced in 2020, Apple announced new system-wide privacy requirements. Any developer wishing to create or update applications on the App Store — which is the only way of distributing iOS apps — would have to comply with the new policies.

The first of these policies — app tracking transparency — asked the developers to actively obtain user permission for data used 'in order to track them or access their device's advertising identifier'.[8] Under Apple's definition, 'tracking' is construed broadly, encompassing matching of datasets and sharing of data with 'data brokers'.[9] User tracking permissions would have to be obtained through a standardised system dialogue box, asking the user whether they 'allow the application to track their activity across other companies' apps and websites'.[10]

App tracking transparency has had a profound effect, rippling through the ad ecosystem. Meta's (formerly Facebook) shares have dropped considerably; projected loss caused by Apple's iOS changes is estimated to be between US$10 and 12.8bn.[11] The majority of the public lauded Apple's policy changes, as did academia. Ad tech companies decried the practice, as did a few scholars, who claimed that 'thinly veiled as a privacy-protecting measure, Apple's iOS 14 policy changes harm the entire ad-supported ecosystem — from developers to advertisers to end consumers'.[12]

Given the scope of the app tracking transparency changes, the other iOS 14 privacy change garnered less attention. Under the new policies, developers would be obliged to provide a high-level summary of the way their apps 'collect and use'

data. Such a summary would be called a *privacy nutrition label* (PNL), and developers would be required to fill in the required information prior to submitting their application to the App Store — or updating an existing application. As Apple explained to developers during its Worldwide Developers Conference (WWDC):

> Today, we already require that all apps have a privacy policy. This year, we're going one step further by adding more information to help you easily pick out the most important details.
>
> Starting in fall 2020, when you submit your app to the App Store, you will need to fill out a questionnaire to describe how your app uses user data. The information you provide will be shown to users directly on your store page.
>
> This gives users the ability to see what an app does before they download it. They will be able to see if you collect a little data or a lot of data and if any of that data is used to track them. You should make sure to still provide further details to your users to explain your data usage, such as in your privacy policy or on your website.[13]

This statement caused some confusion among the developers and the public, who were, initially, under the impression that Apple would be verifying their privacy practices. Apple quickly announced that no such verification would be embodied in their review of applications submitted to the App Store, and that each developer is obliged to follow any applicable data protection laws.

Once released, the PNLs presented mobile users with a short summary of the data *categories* divided into three *sets*: 'data used to track you', 'data linked to you', and 'data not linked to you' (Figure 1). Upon clicking on 'See details', users would be presented with a more exhaustive list of the data categories, divided into the same three sets, and categorised by the purposes of data use. At the top of this page, Apple states that

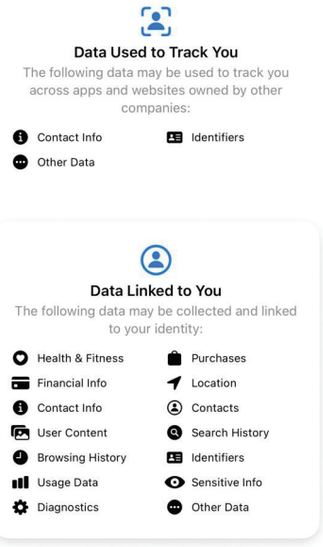

Figure 1: A privacy nutrition label shown on the Apple App Store

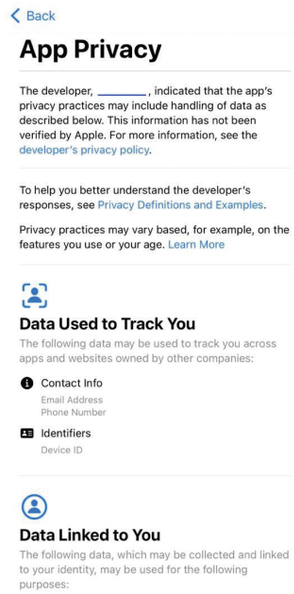

Figure 2: Further details a user can see upon clicking on a 'See more' button on a privacy nutrition label

'the developer has indicated that the app's privacy practices may include handling of data as described below. This information has not been verified by Apple' (Figure 2).

On the developer side, when submitting a new application, there is no option to add

custom categories of data or purposes of processing to such labels. The form is fully standardised, and the developers are limited to choosing between the following purposes and data categories:

When submitting an app to the App Store, developers enter into a contractual obligation to fulfil any data protection obligations they have under the applicable laws, as well as to adhere to Apple's Developer Policies. These policies contractually define the terms pertinent to the PNL creation process.

Importantly for discussions on the relationship between PNLs and the GDPR, developers are only obliged to disclose information on the data 'collected' by the app; collection being defined as 'transmitting data *off the device* in a way that allows *you* and/or your *third-party partners* to *access* it for a period *longer* than what is necessary to *service* the transmitted request in *real time*'.[14] In other words, any data categories processed locally on the device, or externally processed exclusively in real-time (ie, with no retention), would *not* trigger the disclosure requirements.[15] Apple exemplifies the latter by stating that 'if an authentication token or IP address is sent on a server call and not retained, or if data is sent to your servers then immediately discarded after servicing the request, you do not need to disclose this in your answers in App Store Connect'.[16]

Furthermore, developers are obliged to disclose the categories of data collected by 'third-party partners'. This term refers to 'analytics tools, advertising networks, third-party SDKs, or other *external vendors* whose *code you've added to your app*'.[17] In other words, the term is open-ended, referring both to organisations and software tools, fuelling further uncertainty as to the type of disclosure this provision calls for.

Lastly, the term 'tracking', used to separate PNL into sections, is contractually defined as 'an act of linking user or device data collected from your app with user or device data collected from other companies' apps, websites, or offline properties for targeted advertising or advertising measurement purposes. Tracking also refers to sharing user or device data with data brokers'. Under Apple's developer agreement, therefore, the only kind of tracking that triggers disclosure requirements is tracking done for advertising purposes.

Naturally, Apple's contractual definitions do not create any legal effects on their own, and they would have to be construed in light of the applicable national contract laws.[18] They govern the relationship between Apple and developers alone — and the assessment of developers' compliance with these policies is outside the scope of this paper.

Can such contractual arrangements, nonetheless, help data controllers satisfy some of the legal requirements under the GDPR, or can they at least serve a purpose as a compliance enhancement tool? The first question is considered in the next section, while the latter is explored in the section 'PNLs as an Internal Compliance Tool'.

GDPR'S TRANSPARENCY REQUIREMENTS AND PNLS

The fundamental requirements of the GDPR

The principle of transparency is a fundamental principle of data protection law — and is explicitly recognised as its primary component. Article 8 of the European Convention of Human Rights has been interpreted by the European Court of Human Rights as requiring an open disclosure of information gathering, as well as granting data subjects the right of access to their data.[19] Similarly, Charter of Fundamental Rights of the European Union provides, by Article 8, that 'everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified'.[20] Internationally, OECD, an organisation with 38 member countries (including the United States and numerous EU Member States), provides, in its guidelines, that data controllers shall meet

the principle of openness. As stated in the Guidelines:

> There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.[21]

Within the GDPR, transparency is considered to be a part of the core, fundamental data protection principles enshrined in Art. 5. As stated in the Article, personal data shall be 'processed lawfully, fairly and in a *transparent* manner in relation to the data subject'.[22]

GDPR Rec. 39 elaborates on this principle, dedicating to it, tellingly, more space than to any other data protection principle:

> It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. [. . .] Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.[23]

Further specifying data controllers' obligations arising out of the principle of transparency, Art. 12 provides that a data controller must provide the specific information required by GDPR's other articles, 'in a *concise*, *transparent*, *intelligible* and *easily accessible form*, using *clear and plain language*'.[24] Rec. 58 provides that this nature of the disclosure is of particular importance, 'in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising'.[24]

At the core of disclosure duties, Arts. 13 and 14 of the GDPR contain a list of the specific information which must be disclosed — as a minimum — in order to ensure adherence to the transparency principle. The list is long, comprising items such as the identity of the data controller, purposes of processing, lawful basis of processing, any rights which the data subjects have, and other information necessary to understand the scope of controller's processing activities.

Finally, of relevance to for the PNL discussion, GDPR Art. 12 stipulates that information may be provided '*in combination* with *standardised icons* in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing', adding that 'where the icons are presented electronically they shall be machine-readable'.[26]

Adherence of PNLs to GDPR requirements

To what extent are PNLs able to satisfy such strong transparency requirements under the GDPR? If they were the sole source of information offered to end-users, they would undoubtedly fail to satisfy these requirements.

Disclosure of mandatory information

Looking at the wording of GDPR Arts. 13 and 14, it is apparent that PNLs do not provide all the information listed in the articles. There are only a few PNL disclosures that could even remotely provide the mandatory information required by these articles, but their content is only tangentially related to the legal requirements.

To start off, the *identity* of the developer is provided at the top of the 'App Privacy'

section. There are, naturally, no assurances that the *developer* who uploaded the application is in fact the data controller, nor any apparent ways to access information about joint controllership of data. This is especially relevant when reflecting on the fact that, according to empirical research:

> [M]any app owners or developers delegate the app development to app makers, who operate an app builder business to automatically and instantly create apps or landing pages. In such cases, the actual owners of these apps are never in the position to specify privacy labels, while the compliance of the privacy label relies largely on the awareness and the honesty of app makers.[27]

Thus, while the PNLs do disclose the name of the entity that uploaded the application, one should be careful before assuming that this satisfies the requirement for disclosing the identity of the data controller. There is no direct information on how to *contact* a data controller or their data protection officer in PNLs, either.

PNLs do, to an extent, present users with information on the *purposes* of processing. However, such information is severely limited by the fact that the developers cannot manually enter their purposes of processing; rather as noted above, they must pick them from Apple's pre-defined list (Table 1). Such an approach suffers from two fundamental problems: first, it is very likely that most data controllers will have additional purposes to list; and secondly, some of the purposes listed are hardly compatible with the purpose limitation principle. Looking at the list of purposes of processing provided by the PNLs, end-users are unlikely to be able to deduce meaningful information on the actual processing practices.

The same argument can be made about the disclosure of *categories of personal data* being processed, as required by GDPR Art. 14. While the primary focus of a PNL is exactly on offering an overview of the relevant data categories being used, some of the categories predefined by Apple are simply too vague ('app use data' being one example). The limited list of predefined data

Table 1: Choice of purposes of data processing and data categories that Apple offers to developers

Purposes of processing	Categories of information
Third-party advertising	Contact info
Developer's advertising or marketing analytics	Health & fitness
Product personalisation	Financial info
App functionality	Location
Other purposes	Sensitive info
	Contacts
	User content
	Browsing history
	Search history
	Identifiers
	Purchases
	Usage data
	Diagnostics
	Other data

categories which can be entered into the PNL is equally problematic.

Adding to this, one of the mandatory disclosure requirements under the GDPR is whether certain processing is required for the performance of a *contract*, and the consequences that the refusal to provide such data might entail. One of the purposes of processing listed in the PNL is 'app functionality', and users are, as with other purposes, able to see which categories of data will be used for this purpose. However, the PNL neither refers to the existence of any particular contract, nor makes it possible for the user to infer what the consequences of not providing such data might be. This is further compounded by the fact that Apple's examples of 'app functionality' refer to processing required to 'authenticate the user, enable features, prevent fraud, implement security measures, ensure server up-time, minimize app crashes, improve scalability and performance, or perform customer support'.[28] Some of these might be necessary for the application to function as intended — such as data required for user authentication; others, such as diagnostic data, might have no implications for the user experience at all.

PNLs provide no other information connected with the requirements of GDPR Arts. 13 and 14. There is no information on the legal basis of processing, data subject rights, third-party recipients, international transfers of data, storage periods or further processing.

In conclusion, PNLs *do not* provide data subjects with information that could satisfy the disclosure requirements of the GDPR. In other words, they cannot be seen as fully-fledged replacement for the privacy notice a data controller should disclose.

Supplementary disclosure

If the PNLs fail to meet the mandatory disclosure requirements alone, can they at least be used as a *supplementary measure* to help the data controllers meet their broader duty of transparency under the GDPR?

A strong case for such an approach can be made on the surface. Apple *does* require its developers, in addition to using a PNL, to post a public link to their *privacy policy* on the App Store, presumably being more detailed than the PNL itself. The PNLs, if viewed as a supplementary disclosure by the data controller, can be perceived as helpful, given the very favourable approach to *layered notices* taken by the supervisory authorities. Arguably, given their seemingly short and clear nature, the PNLs could help users make informed, better choices — while satisfying the requirements of being *concise*, *transparent*, *intelligible* and in an *easily accessible form*, using *clear and plain language*.[29] Arguably, PNLs could be seen as an early form of the *data protection icons*, mentioned in the GDPR Art. 12. Can such arguments turn PNLs into a meaningful supplementary measure?

PNLs as 'layered notices'

The complexity of presenting users of digital services with the information required by GDPR Arts. 13 and 14 is well acknowledged. Given the very broad scope of the information that has to be disclosed, combined with the commonly acknowledged information fatigue, presenting efficient notices can be challenging. This has led data protection authorities to broadly adopt a preference for 'layered notices'. As described in the WP29 Guidelines on transparency:

> In the digital context, in light of the volume of information which is required to be provided to the data subject, a *layered* approach may be followed by data controllers where they opt to use a combination of methods to ensure transparency. WP29 recommends in particular that *layered privacy statements/notices should be* used to link to the various categories of information which

> must be provided to the data subject, *rather than displaying all such information in a single notice on the screen,* in order to avoid information fatigue. Layered privacy statements/notices can help resolve the tension between completeness and understanding, notably by allowing users to navigate directly to the section of the statement/notice that they wish to read.[30]

This preference for layered notices is firmly fixed in the advice of national data protection authorities as well. However, it is hard to observe the PNLs as a good form of such practice.

First, if seen as a 'first layer' of a GDPR-required notice, a PNL would fail to communicate the key information on processing of personal data that such a layer should contain. As explained in the WP29 Guidelines on Transparency:

> As regards the content of the first modality used by a controller to inform data subjects in a layered approach (in other words the primary way in which the controller first engages with a data subject), or the content of the first layer of a layered privacy statement/notice, WP29 recommends that the first layer/modality should include the details of the purposes of processing, the identity of controller and a description of the data subject's rights. [. . .] The importance of providing this information upfront arises in particular from Recital 39. [. . .] Therefore, the data subject should be able to understand from information contained in the first layer/modality what the consequences of the processing in question will be for the data subject.[31]

As demonstrated above, the way that the PNLs are currently structured does not give data controllers an ability to provide such information in the first layer.

Secondly, a critical part of a layered notice is *consistency* between different layers. In accordance with the principles of transparency, fairness and accountability, different parts of a notice should not contain conflicting information. The WP29 Guidelines underline the same point. However, research indicates that there is often a *discrepancy* between the PNLs and the full privacy notices made available on the developer's website, leading to conflicting disclosures.

Specifically, in a study carried out in 2022, Xiao *et al.* gathered a set of 366,685 applications from the App Store. Mapping their tested functionality to the disclosures made by the developers, a set of apps whose privacy label and privacy policy have inconsistent data practice disclosures was measured as including 164,056 apps. A subset of 5,102 apps was selected for further testing.

Among those 5,102 apps, a total of 3,281 were identified as cases of *neglect disclosure* — a situation in which the app developer collects information without disclosing it.[32] Amongst these, 238 were in the subset where 'the privacy policy is reliable while the privacy label fails to reflect the code behavior'.[33] Furthermore, a set of 1,628 apps was classified as *contrary disclosure*, indicating that the developers disclosed the category of data their app uses but failed to classify it under a relevant purpose. Out of these, 202 had correct disclosure in the privacy policy and incorrect disclosure on a PNL. Lastly, 677 apps were classified as *inadequate disclosure*, which means the developer has already declared one or multiple purposes for a specific data item but failed to disclose all of them.[34] Out of those, 74 did have a correct disclosure in their privacy policies.

While it is easy to blame such discrepancies on the developers and data controllers, they have to be observed in light of the previously explored limitations that Apple places on the PNL disclosures. How can developers provide a consistent notice, if the first layer does not offer them the possibility of customising it to the particularities of their data processing?

Thirdly, in line with the principle of fairness, a layered notice cannot be

used to give data subjects a false sense of trustworthiness. As per their policies, Apple does *not* verify the truthfulness of the PNLs at any stage of their application review process. The users, however, can only find out about this fact when opening the 'See details' page of the PNL (Figure 2). This, naturally, leads to many users assuming that the PNLs are verified for compliance by Apple. As Zhang *et al.* found in their empirical study:

> The majority believed (wrongly) that Apple had reviewed or verified the information in the labels. N7 explained: '[Apple is] allowing that app, that product on their system . . . . So I think Apple, if they're approving that app and they're behind it, then I would think they should be checking [the privacy label]'.[35]

If data subjects are under the impression that the first layer of the privacy notice has been verified and scrutinised by Apple, they will be predisposed to feel more confident in sharing their data. Such practice in notice layering is therefore fundamentally misleading and consequently unfair to the data subjects.

PNLs as a communication enhancement method

Setting their potential for layering the main data protection notice aside, can PNLs help data controllers to establish clear, transparent, intelligible communication with the data subjects — as required by the GDPR?

The existing research indicates a negative answer. In the study by Zhang *et al.*, the division of the PNL into three sets of data (data used to track you, data linked to you, data not linked to you) — coupled with a two-layer access to purposes of processing — left half of the participants confused as to which information the PNLs contained.[36] Specifically, the subjects were confused about how to find the purposes and did not understand why different data categories appeared multiple times.

Participants of the study were also confused about the terms used on the PNLs. In relation to the purposes of processing, some specifically enquired about the meaning of 'App Functionality'.[37] Furthermore, as explored above, 'tracking', as defined by Apple, only pertains to sharing of data for advertising purposes; some participants were clearly confused about this, thinking that the term pertains to location tracking. Many expressed confusion about the terms 'data not linked to you', with one participant stating 'It states it's not linked to you, but obviously it is linked to you because it's your personal information, like your address, your email address, your phone number, and your name.'[38]

Further to this, while some research does indicate that shorter privacy notices can improve comprehension, there are also studies implying the opposite — that shorter notices, such as PNLs, can be a *worse* method of communication with data subjects. In their study with 200 participants, Gluck *et al.* found statistically significant indication of this. Under the heading 'shortest notices led to less awareness', they explain:

> Our results show that removing well-known privacy practices to make short-form notices even shorter actually led to similar or *worse* participant awareness of privacy practices. Our intuition was that further condensing a short-form privacy notice would lead to even better performance, provided that the practices removed were well known. However, this intuition proved false, as our results show no increase in awareness of the practices remaining in the notice when some practices are removed.
> [. . .]
> *Our shortest notices performed significantly worse than our longest notices*, suggesting that there may be a lower bound to the length of an effective privacy notice. In addition, the awareness threshold we selected for

> removing practices from the shortest notice may have been too low.[39]

Lastly, it might be tempting to observe PNLs as an enhanced mode of communication with the data subjects due to the explicit referral to the standardised data protection icons contained in the GDPR Art. 12. However, there is no reason to assume that the PNLs can serve such a purpose in their current form. As noted in WP29 Guidelines, 'the utility of icons to effectively convey information required under Articles 13 and 14 to data subjects is dependent upon the *standardisation* of symbols/images', which, additionally, need to be machine-readable. The labels and images do not currently appear to be standardised across mobile platforms; for standardisation within EU, the Commission and the EDPB are tasked with development of such code of icons. However, the Guidelines rightfully advise caution:

> WP29 recognises that, in line with Recital 166, the development of a code of icons should be centred upon an evidence-based approach and in advance of any such standardisation it will be necessary for extensive research to be conducted in conjunction with industry and the wider public as to the efficacy of icons in this context.[40]

The research previously presented indicates low probability of the PNLs fulfilling this efficacy requirement in their current form.

PNLS AS AN INTERNAL COMPLIANCE TOOL

If the PNLs serve little use for the purposes of transparency towards the data subjects, could they still prove to be useful for data controllers' *internal processes* around compliance efforts? There seem to be strong indications that this could be the case.

To start with, PNLs could prove useful in facilitating proper *communication* between the developers and the data controller's data protection officer (or, if one is not appointed, those in charge of handling the similar tasks). In their presentations aimed at developers — presentations that programmers developing for Apple's operating systems are very likely to watch — Apple quite explicitly recommends consulting with other internal stakeholders prior to developing a PNL:

> Make sure to reach out to the stakeholders working on your app. For example, you can check with your marketing team to understand what data they use and work with legal counsel to ensure you document all data uses described in your app's privacy policy. We also recommend consulting internal documentation in this process.[41]

Another reason why the developers may be likely to involve their data protection officer is because a majority of them find the PNLs to be inherently confusing, rendering it unlikely that they will feel comfortable providing the details on their own. In a recent empirical study of developer attitudes towards PNLs by Li *et al.*, the results strongly indicated that the developers see filling out the PNLs as challenging extra work:

> Many participants perceived accurately filling out privacy labels to be challenging, especially for apps that collected a lot of data. For example, P8 individually developed an app as part of their hobby. With the help of the interviewer, he corrected several errors in the privacy label due to misunderstanding of some key concepts in Apple's def[i]nitions. Later in the interview, he expressed his frustration as follows: 'I'm not like a big company or whatever, so it's a little hard to go through all this information. And as you can see, I didn't get everything totally accurate'.[42]

Just as pertinently, the study indicated that some developers felt that privacy was not a part of their organisational responsibility; as stated by one of the study participants: 'From my experience, the developer will not handle the app privacy. When an organization have teams for privacy, it's not his work to do this. That's my opinion. We are just here to make things.'[43]

This kind of developer attitude often ends up dealing critical blows to data controllers' lawfulness of processing. And yet, Li *et al.* show empirically that PNLs actively encourage developer reflection on data protection issues:

> Some developers viewed this task as beneficial, as it prompted them to reflect on their privacy practices. P6 reflected on his data use: 'I think the positive thing is, it forces the developer to think about all the data that they're capturing. Every time you're adding a new column, every time adding a new table, it's important to think of the information that's being collected, you know, and usually, we think about it in performance terms. but we never think about [it] in the privacy context.'[44]

Taking this a step further, one can observe that PNLs place a very heavy focus on third-party data sharing; as explored above, the very definition of 'tracking' revolves around data sharing for advertising purposes. As this is one of the prime data protection compliance concerns, Apple communicates its importance clearly. As an example of the term 'tracking', Apple offers the following:

> Placing a third-party SDK in your app that combines user data from your app with user data from other developers' apps to target advertising or measure advertising efficiency, even if you don't use the SDK for these purposes. For example, using a login SDK that repurposes the data it collects from your app to enable targeted advertising in other developers' apps.[45]

In *three* separate developer presentations, Apple explains the importance of checking the terms under which any data sharing with third parties takes place, especially through the use of software development kits (SDKs), code libraries offered by third parties. Apple expressly acknowledges the importance of the SDKs for the app ecosystem, while reminding developers of their responsibilities:

> Many of you embed third-party SDKs to avoid reimplementing functionality or to take advantage of helpful third-party services. You need to be aware of what those SDKs are doing. You're responsible for the behavior of your whole app. If an SDK collects data, you need to put that behavior on your Privacy Label. If an SDK is going to track, you need to get people's permission before calling those methods. Many SDKs have documentation related to the Privacy Nutrition Label. You can also reach out to them to ask. We know that advertising is a key part of how our developers thrive, so we've been hard at work building privacy-preserving ad-attribution technologies. If you run ads in your app, pay for ads to grow your customer base, or work directly in the ad ecosystem, here are some of the improvements. [46]

This is not to say that such talks can *immediately* improve developer's understanding of third-party data sharing practices. In fact, one of the most common sources of PNLs non-compliance with the processing operations is the lack of overview of third-party data use. As Li *et al.*'s study finds, developers mainly focus on the SDK's functionality, rather than any incidental data processing.[47] This is strongly confirmed by Xiao *et al.*:

> In our study, non-compliance of 854 is caused by opaque data collection by third-party service providers. Contrary to the previous common understanding

> which attributes privacy non-compliance to opaque third-party disclosure guides, we find that even when the third-party libraries declare the collection and usage of data, such information sometimes cannot be leveraged by app developers to create compliant privacy label[s]. [. . .] The app developers usually integrate those [advertising] SDKs for app monetization, user behavior measurement, scaling marketing campaigns, etc. In our study, we observed 2,086 non-compliant behaviors from those advertising and analytics SDKs in iOS apps. [. . .] In our study, we found that 273 non-compliant apps leak sensitive data to 22 data brokers.[48]

However, the more one works on raising developers' awareness of the importance of due diligence on third-party SDKs, the easier it becomes to encourage developers to seek professional data protection help when implementing third-party features. Apple's messaging on the topic, coupled with a good internal policy, could certainly contribute to reducing this risk — this is consistent with the findings of Li *et al*. above.

Lastly, PNLs can be used to ensure that data protection efforts are adequately prioritised during internal decision-making processes, such as resource and budgetary assignments. The research carried out by Bian *et al*. suggests that the PNL announcement caused a pronounced stock market reaction. Quite significantly, the companies collecting more personal data were losing their stock value at a considerably faster rate than their counterparts:

> Using the CAPM [capital asset pricing model] model, we observe a CAR [capital adequacy ratio] of −4.49% over the six months window following the privacy label release of a given firm's most popular app when compared with firms without any apps. This negative stock market response is significant and robust to alternative models. [. . .] Consistent with the heter[o]genous reaction on the product markets, we also find a more negative effect for firms that collect more data and rely more on mobile users to generate revenue. [. . .] Using the CAPM model, firms that report above-median data collection intensity earn a six-month CAR of −13.30%, while their below-median counterparts earn a CAR of −4.76%. The difference is over 8% and significant, suggesting amplified market reactions to more privacy-intrusive apps.[49]

Such a demonstratable effect of the over-collection of personal data on the market is likely to resonate with the management, in turn helping data protection officers articulate the long term-impacts of poor data protection practices.

Taken together, all these factors show a potential for the PNL-completion process to actively contribute to data controllers' internal compliance efforts — despite not being able to significantly contribute to data controllers' duty of transparency.

CONCLUSION

The importance of the principle of transparency cannot be overstated. Transparency ensures that proper checks upon the lawfulness of their processing are placed — without it, 'all other checks are insignificant'.[50]

Apple's PNLs seemingly offer a way to contribute to the data controller's transparency efforts. And yet, their contribution is questionable. Not only do such labels fail to satisfy the detailed disclosure requirements of Arts. 13 and 14 of the GDPR, but they are surprisingly inadequate as a supplementary disclosure modality. In other words, they contribute very little to data controllers' duty to present information in a clear, transparent and intelligible form.

As flawed as they are, seen in the light of the transparency principle, PNLs can still be quite useful to data controllers. They can help boost their compliance work internally,

bringing tangible improvements to cross-functional communication, third-party sharing awareness, records of processing accuracy, adherence to the data protection principles, and adequate resource assignment.

Seen as such, PNLs are rather valuable — as long as one shifts one's perspective from external transparency to internal awareness.

References

1. Charter of Fundamental Rights of the European Union (OJ C 326, 26.10.2012, p. 391–407); Article 29 Working Party (2018) 'Guidelines on Transparency Under Regulation 2016/679'.
2. Solove, D. J. & Schwartz, P. M. (2020) 'Information Privacy Law', Aspen Publishing, New York.
3. Spinello, R. A. (1998) 'Privacy Rights in the Information Economy', *Business Ethics Quarterly*, Vol. 8, No. 4, p. 723–42.
4. Apple (2021) 'App Privacy Details — App Store, Apple Developer', available at https://developer.apple.com/app-store/app-privacy-details/ (accessed 3rd November, 2022).
5. Google (2020) 'Provide Information for Google Play's Data Safety Section — Play Console Help', available at https://support.google.com/googleplay/android-developer/answer/10787469?hl=en (accessed 3rd November, 2022).
6. The Washington Post (2019) 'Apple Stars at Giant Tech Confab CES — without Actually Being There', available at https://www.washingtonpost.com/technology/2019/01/07/apple-burns-google-giant-billboard-touting-privacy-ces/ (accessed 3rd November, 2022).
7. Apple (2021) 'Designing for Privacy — WWDC19 — Videos. Apple Developer', available at https://developer.apple.com/videos/play/wwdc2019/708 (accessed 3rd November, 2022).
8. Apple (2021) 'User Privacy and Data Use — App Store. Apple Developer', available at https://developer.apple.com/app-store/user-privacy-and-data-use/ (accessed 3rd November, 2022).
9. 'Tracking refers to the act of linking user or device data collected from your app with user or device data collected from other companies' apps, websites, or offline properties for targeted advertising or advertising measurement purposes. Tracking also refers to sharing user or device data with data brokers.' *Ibid*.
10. Apple ref 4 above.
11. Bobrowsky, M (2021) 'Facebook Feels $10 Billion Sting From Apple's Privacy Push', Wall Street Journal, available at https://www.wsj.com/articles/facebook-feels-10-billion-sting-from-apples-privacy-push-11643898139 (accessed 3rd November, 2022).
12. Sokol, D. D. and Zhu, F. (2022), 'Harming Competition and Consumers under the Guise of Protecting Privacy: An Analysis of Apple's iOS 14 Policy Updates', *Cornell Law Review Online*, Vol. 107, No. 3, p. 127.
13. Apple (2021) 'Apple's Privacy Pillars in Focus — WWDC21 — Videos', available at https://developer.apple.com/videos/play/wwdc2021/10085 (accessed 3rd November, 2022).
14. Apple, ref 4 above, emphasis added.
15. *Ibid*.
16. *Ibid*.
17. *Ibid*., emphasis added
18. See eg Cordero-Moss, G. (2014) 'International Commercial Contracts: Applicable Sources and Enforceability', Cambridge University Press, Cambridge.
19. See eg Gaskin *v* the United Kingdom, ECHR (7th July, 1989).
20. Charter of Fundamental Rights of the European Union, ref 1 above.
21. Organisation for Economic Cooperation and Development 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data', available at https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.html (accessed 3rd November, 2022).
22. European Parliament and Council Regulation (EU) No. 2016/679 of 27th April, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation[GDPR]), Art. 5, emphasis added.
23. *Ibid*., Rec. 39.
24. *Ibid*., Art. 12, emphasis added.
25. *Ibid*., Rec. 58.
26. *Ibid*., Art. 12, emphasis added.
27. Xiao, Y., Li, Z., Qin, Y., Bai, X., Guan, J., Liao, X. and Xing, L. (2022) 'Lalaine: Measuring and Characterizing Non-Compliance of Apple Privacy Labels at Scale', *arXiv preprint arXiv:2206.06274*.
28. Apple, ref 4 above.
29. GDPR, ref 22 above Art. 12
30. Charter of Fundamental Rights of the European Union, ref 1 above.
31. *Ibid*.
32. Xiao *et al*., ref 27 above at 10.
33. *Ibid*.
34. *Ibid*. at 11.
35. Zhang, S., Feng, Y., Yao, Y., Cranor, L. F. and Sadeh, N. (2022) 'How Usable Are iOS App Privacy Labels?', *Proc. Priv. Enhancing Technol*., p. 26.
36. *Ibid*. at 214.
37. *Ibid*.
38. *Ibid*. at 215.
39. Gluck, J., Schaub, F., Friedman, A., Habib, H., Sadeh, N., Cranor, L. F. and Agarwal, Y. (2016) 'How Short is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices', SOUPS '16: Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security, p. 21.
40. Charter of Fundamental Rights of the European Union, ref 1 above.

41. Apple, ref 13 above.
42. Li, T., Reiman, K., Agarwal, Y., Cranor, L. F. and Hong, J. I. (2022) 'Understanding Challenges for Developers to Create Accurate Privacy Nutrition Labels', CHI Conference on Human Factors in Computing Systems, ACM, New Orleans, LA, USA, pp. 1–24.
43. *Ibid*.
44. *Ibid*.
45. Apple, ref 4 above.
46. Apple, ref 13 above.
47. Li et al., ref 42 above at 9.
48. Xiao *et al*., ref 27 above at 13.
49. Bian, B., Ma, X. & Tang, H., (2021), 'The Supply and Demand for Data Privacy: Evidence from Mobile Apps', Working Paper, *SSRN Electronic Journal,* available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3987541 (accessed 3rd November 2022).
50. Bentham, J. & Mill, J. S. (1827) 'Rationale of Judicial Evidence, Specially Applied to English Practice: From the Manuscripts of Jeremy Bentham', Hunt and Clarke, London.