

CONTACTLESS MOBILE PAYMENT

LIBERATING SMARTPHONES
AND THEIR USERS

FROM HOUSSEM ASSADI (*DEJAMOBILE*)
LIONEL BARABAN (*FAMOCO*)
NICOLAS BRULEY (*ANTELOP SOLUTIONS*)
JEAN-MICHEL CHANAVAS (*MERCATEL*)
VINCENT DUVAL (*PAYLIB*)
MICHEL GANZIN (*GROUPEMENT DES CARTES BANCAIRES*)
RAPHAËL RICHARD (*PLAYFRANCE.DIGITAL*)

CONTACTLESS MOBILE PAYMENT: LIBERATING SMARTPHONES AND THEIR USERS

FOREWORD	5
INTRODUCTION	7
The sensitivity of banking data	7
Big techs, guarantors of our banking data?	7
Free choice for the consumer!	8
Mobile payment, a necessary solution in times of health crisis	9
CONCLUSION	10
APPENDIX	11
French legislative Proposal on contactless mobile payment (in French only)	11
Proposal for a European Regulation on contactless mobile payment	14

FOREWORD

Today, the dominant digital platforms govern all human activities, whether personal or professional, individual or collective. On the one hand, our work consists of alerting and raising awareness among public and private representatives regarding the digital transformation processes under way, and the sometimes predatory nature of the companies that dominate this ecosystem, and on the other, devising legal, technical or economic solutions to free consumers and businesses from the yoke of platforms. This is the whole point of the Digital New Deal Foundation's activities.

Apple's refusal to allow the French application StopCovid to access bluetooth in the background jeopardizes the capacity of the State to respond to the current health crisis. Indeed, the sovereignty of States is called into question by companies with intangible services – the Big Techs – contesting traditional sovereign control in fields as essential as taxation, security or even monetary creation. The obsolescence of positive law becomes obvious: copyright, intellectual property law, media law, tax law – the list is not exhaustive – suddenly turn out to be unsuitable for the realities of use while new legal concepts must emerge such as, for example, net and terminal neutrality, as well as many others.

We recently contributed to the reflection on the future Digital Services Act directive, which notably highlights the issue of platform liability, in a note entitled *Reflections in the perspective of the European Digital Services Act*¹. In our work and our speeches, we also highlight the one-way balance of power between Big Techs and consumers/user companies, both trapped in closed ecosystems, embodied by proprietary operating systems. Big Techs, playing on powerful network effects, have an undeniable competitive advantage, allowing them to consolidate their monopolistic positions on the one hand, and on the other, to make it difficult – if not impossible – for alternative competing solutions to emerge.

The instant mobile payment market is a good illustration of this, with the presence of *gatekeepers* who, by abusing their dominant position, end up destroying all forms of competition. For example, Samsung reserves convenient and quick access to its own payment application via a swipe. Another example: Apple does not allow third parties to access the NFC antenna that equips its phones (iPhones) and other portable connected objects (iWatches), consumers who have acquired these products cannot make contactless in-store payments via applications or solutions competing with Apple Pay. Apple thus reserves the market for contactless in-store payment solutions, restricting consumers' freedom of choice and competition among payment solutions, and hindering the development of payment by contactless phone, at a time when the current pandemic confirms the need to facilitate this method of payment.

Legislative initiatives are emerging on this subject in Europe. In particular, Germany adopted legislation at the beginning of the year asking Big Techs to allow European payment applications to be able to access the NFC antenna. In France, a bill aimed at guaranteeing free consumer choice in cyberspace, unanimously adopted by the Senate, also seeks to ensure free consumer choice on terminals. These initiatives aim to make the Internet a more open ecosystem, favourable to innovation, where consumers regain their power to act; in other words, their ability to make choices as they can in other regulated markets.

In our opinion, adopting a legislative provision on mobile payment in national law, with the objectives of opening up NFC access to competition, ergonomic fairness and regulation of access costs, is a legal means of corroborating the more global need to specifically regulate Big Techs at the national and European levels.

¹ Report available [here](#) in French and [here](#) in English – March 2020

Contactless mobile payment

This note is an invitation to take a different view of the instant mobile payment market. Some operators operating in this market do not seem to respect the rules of competition. After the presentation of a certain number of observations proving this drift, we shall propose a legislative text for national law, and if the will to act extends to the scale of the continent, an outline of European regulations.

—
Arno Pons, General Delegate of The Digital New Deal Foundation

INTRODUCTION

Is the position of cash bound to be reduced? Will we all have pay for most of our in-shop purchases with our smartphone? Will Facebook succeed in issuing its own Libra cryptocurrency? Will this future, still dystopian a few years ago, become reality? Will Big Techs replace banks? Will they establish themselves as true gatekeepers of the market worlds of our European economies? While structural shifts are being made by Big Techs, whose major interest we perceive in the banking and market sectors, questions are emerging. And even more than questions, doubts.

If we look at recent innovations in the banking sector, it is clear that behind seemingly invisible or incidental innovations – NFC is a good example because it reproduces a gesture that we are now used to, contactless payment – major issues of sovereignty and security are at stake.

Apple, Google and Samsung have respectively launched Apple Pay, Google Pay and Samsung Pay. While the use of Apple Pay has spread, the company with the apple has also worked with Goldman Sachs on the creation of a bank card, the limits² of which have already been highlighted. Google and Samsung are adopting the same³ strategy by announcing that they will also do the same. The intention of these global digital operators to interfere in the banking – or even monetary – sector is a major political issue, an important issue of sovereignty.

In this sense, why is it the ambition of Big Techs to establish themselves in the banking sector, and in particular in the instant mobile payment market, a threat to our sovereignty?

The sensitivity of banking data

The collection, processing and use of personal and non-personal data is at the heart of the Big Tech business model. These operators have an immense quality and quantity of data at their disposal; this data can relate to an individual, come from social networks, from our purchasing habits or from search queries.

These operators considerably enrich their customer knowledge with the relevance of the information contained in banking transaction data. At the heart of the interest of these cross-sector operators in this new data is the ability to weave networks of interactions; for example, to further improve the efficiency of their targeted advertising service, or even to increase the price of available space. Indeed, banking data is not only useful for learning more about an individual; its value is concrete and structuring since it makes it possible to link individuals to each other or to companies.

Investing in the banking and payment market is proving attractive to Big Techs: the commercial exploitation of this new strategic data will constitute a new source of income, make it possible to make users even more captive and threaten the ability of merchants to develop and preserve the value of their business.

Big techs, guarantors of our banking data?

European sensitivity regarding data protection is very strong, as evidenced by the adoption in May 2018 of the General Data Protection Regulation (GDPR). Its objective, which applies to all

² <https://www.theverge.com/2019/11/12/20960409/apple-card-discriminatory-credit-limits-goldman-sachs-brand>

³ <https://www.theverge.com/2020/5/7/21251293/samsung-pay-debit-card-sofi-this-summer>

Contactless mobile payment

organisations processing personal data, is twofold: to protect citizens with regard to the processing of their personal data and to make those involved in this processing more responsible.

Unlike other sectors, the use of personal information is compulsory in the banking sector: financial situation, assets, income, profession, etc. without forgetting information on the state of health with regard to loan insurance. In just a few years, the web and mobile devices have become the main interfaces for connecting with banks, generating so-called sensitive banking data. In this respect, the obligations of the GDPR that companies and banks have had to comply with – collection, storage and analysis – and the rights to which citizens now have access – right of access, portability, right to be forgotten and right of rectification – have made it possible to strengthen the relationship of trust between Internet users and banking institutions.

Recently, the regulation of digital technology, and especially that of these dominant players, the Big Techs, has been troubling the public and private spheres. From the enthusiasm of the beginnings – these companies were the embodiment of progress and innovation – to the repeated excesses of a predatory model – there is no shortage of examples – the need for regulation is gradually becoming apparent. Conversely, it is clear that the banking market is particularly regulated, especially with regard to access to data. Indeed, strong legal constraints, and in particular statistical and professional secrecy, govern and protect access to data⁴.

Banks and instant payment players are thus establishing themselves, in the face of Big Techs, as a true trusted third party when it comes to the use of our banking data. Furthermore, the issue of the processing and storage of payment data by Big Techs deserves to be addressed, particularly on the issue of the location of servers, which is of significant importance since it determines the applicable law. As far as Big Techs are concerned, the outsourcing of data retention to foreign cloud players raises issues of security, data protection and sovereignty.

Free choice for the consumer!

A report⁵ by Mr Franck Montaugé and Ms Sylviane Noël, produced on behalf of the French Senate's Economic Affairs Committee on the bill aimed at guaranteeing the consumer's free choice in cyberspace specifies that *"The iOS operating system offers third party applications very limited access to the NFC chip of Apple terminals, as Apple does not open the application programming interface (or API) giving access to this functionality. However, as such access is necessary for being able to use a mobile terminal to make contactless payment, applications competing with Apple Pay are unable to offer their contactless payment services to users of Apple terminals independently. In order to access this functionality through the Apple Pay application, third-party services must pay a commission to Apple. This lack of access to NFC chips also jeopardises the supply of paperless tickets. This is the case, for example, with the paperless Navigo pass, which cannot be deployed on most terminals for public transport users in the Ile-de-France region."*

This point raises two major problems:

- A matter of protecting the consumer's freedom of choice, insofar as the latter does not have alternative means of mobile payment if he or she uses a terminal equipped with an iOS operating system or if he or she is preferentially referred to Samsung Pay or Google Pay solutions on Android.

⁴ Page 41 – 42 : https://www.cnis.fr/wp-content/uploads/2017/10/RAP_2015_140_acces-aux-donnees-bancaires.pdf

⁵ <http://www.senat.fr/rap/l19-301/l19-3011.pdf>

- And a matter of protecting free competition; in this regard, Margrethe Vestager, Executive Vice-President of the European Commission and Commissioner for Competition, addressed the Apple Pay dossier during a press conference in conjunction with the 2019 Web Summit in Lisbon, saying: *"People see it becomes increasingly difficult to compete in the market for easy payments"*⁶

As a reminder, the competition rules make it possible to create the conditions for fair competition in a market. In particular, in the interests of the consumer, they encourage a significant reduction in prices and an improvement in the quality of goods and services. With regard to the problems of the instant mobile payment market, it is necessary to combat the abusive unilateral practices of operators which, like Apple, but also Samsung, reserve the use of equipment (Apple's NFC antenna) or functionalities facilitating practical and rapid access to an application (Samsung's swipe) for the benefit of their own payment solutions.

These abusive practices reduce and distort competition to the benefit of already global leaders, Big Techs, at the risk of making the European payment industry lose the ability to compete with these leaders and generating a loss of sovereignty for States in the area of payments. It should be recalled that along with the free movement of goods, competition is considered to be a driving and fundamental element in the construction of the European internal market. In these respects, it seems essential that the various operators of payment solutions should be accessible, without distinction, via all existing operating systems.

Mobile payment, a necessary solution in times of health crisis

La crise du Covid-19 a permis d'accélérer le projet de relever le plafond de paiement par carte sans contact. The Covid-19 crisis has enabled accelerating the project to raise the ceiling for contactless card payments; from now on, we can use the contactless technology of our bank card for transactions up to 50 euros. Contactless payment is now seen as a "barrier gesture" for the authorities; it is a way to send a strong signal to consumers – it would also seem that this increase in the ceiling has a positive and dynamic impact on consumption. Michel Ganzin, Chairman of the Management Board of Groupement des Cartes Bancaires, agrees, stating that *"not having to touch the keyboard with your fingers effectively adds extra protection"*⁷ and that *"it has been verified in several studies that contactless payment, through the facilities it provides, boosts business and increases merchants' turnover"*.

This reasoning, which takes into account health considerations, seems to be applicable to the mobile payment market as well. In the context of a health crisis, and particularly in an epidemic situation, wouldn't it be in our interest to widely disseminate the uses of mobile payment? As it stands, with the barriers erected by international operators, whether it be Apple reserving its NFC antenna for its own use or Samsung favouring its mobile payment solution to the detriment of others, this is not possible.

Legislating to open up mobile payment access to competition and thus allow free consumer choice will not only lead to encouraging new uses, but is above all necessary because it is part of the health measures that the government is trying to enforce throughout our territory, the need for which is no longer in doubt.

⁶ <https://www.reuters.com/article/us-eu-antitrust-apple/eus-vestager-says-apple-pay-has-prompted-many-concerns-idUSKBN1XH1YL>

⁷ <https://www.franceinter.fr/economie/vers-moins-de-contact-y-compris-dans-vos-achats>

CONCLUSION

While the GDPR has enabled asserting a certain vision of the digital world, specific to fundamental European values, it appears that this regulation was put in place as a reaction to the hegemony of Big Techs over data. With regard to the issues of abusive practices by certain operators in the mobile payment market, which this note proposes to study, it is necessary to intervene quickly, i.e. before the digital giants have consolidated strong positions or attacked excessively large market shares.

Furthermore, as the Financial Stability Board (FSB) points out, *"it is not the role of the authorities to protect financial institutions from competition, but regulators and supervisors should be particularly vigilant about the impact of such competition on the viability of existing business models and the nature of the response to be provided"*.⁸

Finally, the rapid intervention of France, and certainly of Europe in the long term, appears all the more necessary since, in a context of unprecedented economic crisis, any potential inertia could create a practically irreversible advantage for Big Techs, to the detriment of European consumers and payment providers, and hinder the development of contactless payment, the health benefits of which are nevertheless obvious, especially in the context of Covid-19.

Furthermore, if we are all specialists of contactless mobile payment thanks to the various position we hold in the sector, an issue is of major concern to us as citizens. Apple's refusal to allow the French application StopCovid to access bluetooth in the background is symptomatic of a regrettable shift. Even such exceptional circumstances didn't prevent private operators to take upon themselves an important part of the State's responsibility, health.

— Signatories list:

- Houssein Assadi (*Dejamobile*)
- Lionel Baraban (*Famoco*)
- Nicolas Bruley (*Antelop Solutions*)
- Jean-Michel Chanavas (*Mercatel*)
- Vincent Duval (*Paylib*)
- Michel Ganzin (*Groupe des Cartes Bancaires*)
- Raphaël Richard (*PlayFrance.Digital*)

⁸ <https://www.lesechos.fr/finance-marches/banque-assurances/les-regulateurs-financiers-vigilants-face-a-loffensive-des-gafa-dans-la-banque-1154851>

MESURES VISANT À FACILITER LE PAIEMENT MOBILE SANS CONTACT EN PRÉSERVANT LA LIBERTÉ DE CHOIX DU CONSOMMATEUR ET LA LOYAUTÉ DE LA CONCURRENCE

Article 1

Est qualifiée de fournisseur de système d'exploitation toute personne qui, à titre professionnel, édite ou adapte le système d'exploitation d'un terminal mobile, ou qui est responsable de la première mise à disposition sur le marché de l'Espace Economique Européen d'un terminal mobile, dès lors que ce terminal permet aux consommateurs situés sur le territoire français d'effectuer un paiement mobile sans contact.

Article 2

Est considéré comme un service utile au paiement mobile sans contact tout service, système d'exploitation, logiciel, émulation, matériel, composant, antenne, élément sécurisé, ou autre élément contrôlant ou facilitant l'accès à une fonctionnalité, outil ou raccourci ergonomique d'un terminal mobile, dès lors qu'il permet, améliore ou facilite le paiement sans contact.

Article 3

I. Tout fournisseur de système d'exploitation s'assure que les produits et services qu'il offre permettent à tout consommateur situé sur le territoire français d'exercer librement et sans entrave sa liberté de choix entre tout prestataire de services permettant ou facilitant le paiement mobile sans contact.

II. Tout fournisseur de système d'exploitation garantit des conditions de concurrence équitables entre sa propre activité de services de paiement et les activités concurrentes exercées directement ou indirectement par les établissements de crédit, établissements de monnaie électronique, prestataires de services de paiement, établissements de paiement et agents au sens de la Directive (UE) 2015/2366. Le respect de cette obligation est apprécié au niveau de l'ensemble du groupe du fournisseur de système d'exploitation, en tenant compte de toutes les sociétés directement ou indirectement contrôlantes ou contrôlées au sens de l'article L. 430-1-III du code de commerce.

III. Le respect des obligations prévues à l'article 3 I° et II° du présent texte implique notamment que le fournisseur de système d'exploitation assure un égal accès ergonomique au consommateur, afin qu'il puisse exercer sa liberté de choix des applications liées au paiement, et s'assure que :

(i) tout outil ou raccourci ergonomique que le fournisseur de système d'exploitation propose ou met en place sur le terminal mobile pour faciliter l'utilisation d'une application concernant le paiement sans contact soit librement et gratuitement ouvert au consommateur, quelle que soit l'application de paiement qu'il aura choisie ;

(ii) tout consommateur soit libre d'installer sur son terminal mobile toute application tierce de son choix liée à un service de paiement ou une opération de paiement et de définir cette application comme l'application par défaut ou favorite.

Article 4

Le fournisseur de système d'exploitation est tenu de mettre à disposition de tout prestataire de services de paiement, établissement de crédit, établissement de monnaie électronique, établissement de paiement ou agent au sens de la Directive (UE) 2015/2366 qui lui en fait la demande, tous les services utiles au paiement mobile sans contact dans des conditions équitables, raisonnables et non discriminatoires.

Article 5

L'accès visé à l'article 4 du présent texte est accordé, au choix du fournisseur de système d'exploitation, soit gratuitement, soit moyennant une redevance, dans le respect des conditions cumulatives suivantes :

- 1° la redevance n'excède pas les coûts marginaux, c'est-à-dire les coûts effectivement encourus liés au travail supplémentaire spécifiquement demandé par le tiers demandeur d'accès ;
- 2° il n'existe pas d'autre solution pratique et économiquement viable qui permettrait de traiter la demande d'accès de manière équivalente ou plus efficace à un coût égal ou inférieur ;
- 3° les coûts sont déterminés et ventilés avec précision, afin de permettre une vérification aisée.

Article 6

I. Par dérogation à l'obligation d'accès énoncée à l'article 4 du présent texte :

- 1° un fournisseur de système d'exploitation n'est pas soumis à l'obligation d'accès s'il établit que ce système compte moins de 2 millions d'utilisateurs enregistrés dans le marché intérieur de l'Espace Economique Européen au cours du dernier exercice financier. Ce seuil doit être évalué à la date de la demande d'accès.
- 2° le fournisseur de système d'exploitation peut refuser d'accorder l'accès prévu à l'article 4 s'il démontre que cet accès menace de façon concrète, documentée et substantielle la sécurité des paiements au préjudice des consommateurs.

II. Le fournisseur de système d'exploitation ne peut se prévaloir d'une menace sécuritaire et bénéficier de la dérogation prévue à l'article 6 I 2° du présent texte que s'il démontre avoir fait ses meilleurs efforts pour l'éviter et pour offrir aux tiers demandeurs d'accès des options alternatives sécurisées, pratiques et économiquement viables, afin de préserver une concurrence libre et loyale entre les prestataires de services de paiement et la liberté de choix des consommateurs.

III. Le fournisseur de système d'exploitation ne peut en tout état de cause refuser une demande d'accès conforme à l'article 4 si le requérant ou l'établissement de paiement, de crédit ou de monnaie électronique dont il est l'agent consent à le garantir par écrit par avance contre toute éventuelle réclamation d'un consommateur, en ce qu'elle serait due à cet accès. Une telle garantie ne pourra pas porter préjudice au consommateur et n'exonérera pas le fournisseur du système d'exploitation de son obligation de respecter les dispositions des articles 3 et 6 II° du présent texte.

Article 7

Tout manquement aux obligations prévues par le présent texte peut donner lieu à une action devant la juridiction compétente, y compris devant le juge des référés, et aux sanctions dans les conditions définies à l'article L. 442-4 du Code de commerce, à l'initiative du ministère public, du ministre en charge de la consommation, du président de l'Autorité de régulation des communications électroniques et des Postes, du président de l'Autorité de contrôle prudentiel et de résolution ou du président de l'Autorité de la concurrence ou de toute autre personne justifiant d'un intérêt à agir.

**OBLIGATIONS APPLICABLE TO PROVIDERS OF TECHNOLOGY
INFRASTRUCTURES SERVICES ENSURING A LEVEL PLAYING FIELD
AND CONSUMERS' FREEDOM OF CHOICE AS REGARDS
PAYMENT SERVICES**

Whereas:

1. Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) n°1093/2010, and repealing Directive 2007/64/EC Directive (EU) 2015/2366 (Payment Service Directive 2 — PSD 2) provides the legal foundation for a better integrated internal market for safe electronic payments within the EU. Given that the retail payments market has experienced significant technical innovation and the emergence of electronic and mobile payment, the PSD 2 established a new framework for payment services, with the goal of making international payments within the EU as easy, efficient and secure as payments within a single country. It also seeks to open up payment markets to new entrants to ensure that consumers, merchants and companies enjoy choice and transparency of payment services to benefit fully from the internal market.
2. Payment services are essential for the proper functioning of vital economic and social activities.
3. In recent years, payments with mobile phones, digital tablet or other personal digital devices became increasingly popular in Europe and an increasing number of European citizens make use of a mobile device on a day-to-day basis for their financial services, including payments.
4. Since the adoption of the PSD2, and as recently underlined by the German Parliament and the French Senate, the consumer's liberty of choice in the field of payment transactions appear however to be more and more dependent upon access to technology, hardware, component, know-how or software enabling, facilitating or preventing the use of a third-party application in relation to a payment transaction or a payment service. This may include, for example access to a hardware or secure element, a Near Field Communication antenna, a manual for developing the software under the OS or applications, or a card emulation which displays the card information on the mobile device that is required in order to enable a payment transaction or the use of a payment application or service.
5. New rules should be established to close the regulatory gaps within the Union regarding access to such technology, tool or component while at the same time providing more legal clarity and ensuring consistent application of the legislative framework across the Union. This should generate efficiencies in the payment system as a whole and lead to fair competition, more choice and better prices for consumers and strengthening their trust in a harmonised payments market.
6. New rules shall also prevent distortions of competition to the detriment of consumers. Thus, each provider of technology services that may contribute to the provision of payment services or to e-money activities, including tool facilitating the use of any application relating to payment service, payment transaction or e-money (e.g. ergonomic or fast access tools) shall ensure a level playing field between its own payment services business (at group level), and other payment service providers, payment institutions, credit institutions, payment systems, agents and e-money issuers.

7. These new rules shall be defined and applicable without prejudice to EU competition law rules and to EU regulations or national laws protecting consumers.

8. Member States should lay down rules on the penalties applicable to infringements of this Regulation and should ensure that those penalties are effective, proportionate and dissuasive and that interim measures and compensation are applicable in due time.

Article 1

Definitions

The following definitions shall apply:

(1) 'agent' means a natural or legal person who acts on behalf of any payment institution and/or credit institution.

(2) 'credit institution' means an undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account, as defined in point (1) of Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council, including branches thereof, within the meaning of Article 1(1)(a) of the PSD2 Directive.

(3) 'e-money' means electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC.

(4) 'group' means the undertaking concerned and all other undertakings belonging to the same group, i.e. all other undertakings mentioned in Article 5.4 (b), (c), (d) and (e) of the Regulation (EC) N° 139/2004 of 20 January 2004 on the control of concentrations between undertakings.

(5) 'personal digital device' means mobile phone, laptop, digital tablet personal computer or other mobile personal device enabling a consumer to make a payment transaction.

(6) 'payer' means a natural or legal person who holds a payment account and allows a payment order from that payment account or, where there is no payer's payment account, a natural or legal person who makes a payment order to a payee's payment account.

(7) 'payment institution' means a legal person that has been granted authorisation in accordance with Article 11 of PSD2 Directive⁹ to provide and execute payment services throughout the European Union.

(8) 'payment service' means any business activity set out in Annex I of PSD2 Directive.

(9) 'payment system' means a funds transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions.

(10) 'payment transaction' means any payment transaction act, as defined in Article 4 (5) of PSD2 Directive.

(11) 'PSD2 Directive' shall mean Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

⁹ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015L2366&from=FR>

Proposal for a European Regulation

(12) 'technology infrastructures services' means the operating system (OS) and any other technology on mobile personal digital devices (including any component, tool, function, information, know-how or software) enabling, facilitating or preventing the use of a third-party application in relation to a payment transaction or a payment service, such as, for example a hardware component or secure element, a NFC antenna, a manual for developing the software under the OS or applications, or a card emulation which displays the card information on the personal digital device.

Article 2

Right of access to all technology infrastructure services

2.1. Any provider of technology infrastructures services that may contribute to or hinder the provision of payment services or to e-money activities in the internal market shall be obliged, upon written request from a payment service provider, a payment institution, a credit institution, a payment system, an agent or an e-money issuer, to make all technology infrastructure services available without undue delay under fair, reasonable and non-discriminatory conditions, in a way that the requesting undertaking can provide or operate its payment services or e-money transactions without hindrance.

2.2. The access set forth in Article 2.1 above shall be granted either for a fee complying with the following cumulative conditions:

(a) the fee does not exceed the incremental costs, i.e. the efficiently incurred costs related to the additional work requested by the seeking access third party;

(b) there is no practical and economically viable alternative to the arrangement which would lead to an equally or more efficient handling of the request for access at equal or lower cost;

(c) the costs shall be precisely determined. The breakdown of the amount of the costs, including separate identification of each of its components, shall be part of the arrangement to allow for easy verification and monitoring.

2.3 As exceptions to the access requirement set forth in Article 2 above:

(i) a provider of technology infrastructures services is not subject to the obligation if it has less than 2 million registered users in the European Union during the last fiscal year. This threshold is to be assessed at group level and on the day of the request for access.

(ii) the provider of technology infrastructures services may refuse to grant access only if there are objective reasons to deny that access, such as for example a concrete, documented and substantial threat to the safety and integrity of its technology infrastructure services.

The provider of technology infrastructures services bears the burden of proof of:

(a) the existence of such concrete threat;

(b) that it has complied with the guidelines enacted by the European Banking Authority, if any;

(c) that it has made its best efforts to minimize such threat and to offer access notwithstanding such threat; and

(d) that it has also made its best and prompt efforts to offer third-party access seekers practical and economically viable alternative options preserving competition among payment services providers and consumers' freedom of choice.

2.4 Subject to Article 2.3, no refusal to grant access may be opposed by the provider of technology infrastructures services should the credit institution or the payment institution acting for the payer accept to hold such provider of technology infrastructures services, subject to its full compliance with this regulation, harmless from any third party claim relating to a fully disclosed threat to the safety and integrity of the technology infrastructure services resulting from the access granted in accordance with Article 2.1 above.

Article 3 **Level Playing Field**

3.1 Any provider of technology infrastructures services that may contribute to the provision of payment services or to e-money activities shall ensure a level playing field between its own payment services business (at group level), and other payment service providers, payment institutions, credit institutions, payment systems, agents and e-money issuers. This shall notably imply that the provider of technology infrastructures services opens its operating system in order to grant the access set forth in Article 2 above, but also that it ensures a consistent customer experience for third-party services compared to its own services.

3.2 Any tool, feature or component facilitating the use of any application on a personal digital device relating to payment service, payment transaction or e-money (e.g. ergonomic or fast access tools)¹⁰ shall be open to third-party applications on a free and open-source software licence basis.

3.3 Payers shall be free to install any third-party application relating to payment service, payment transaction or e-money of their choice on mobile phones, laptops, digital tablet personal computer or wearables and to set such application as the default or favourite application.

Article 4 **Payment data**

Any provider of technology infrastructures services shall enable payment service providers, payment institutions, credit institutions, payment systems, agents and e-money issuers to guarantee consumers and end-users that their payment data are not collected, processed, shared or used for any commercial purpose. The general terms and conditions of use of the technology infrastructures may not lead consumers or end-users to waive such guarantee.

Article 5 **Liability**

Without prejudice to the provisions of EU regulations or national laws protecting consumers, the provider of technology infrastructures services shall not reduce or exclude any liability in relation to a payment transaction unless it proves full compliance with all Articles of this regulation.

¹⁰ e.g. Samsung Pay vertical swipe or Apple Pay double-click.

Article 6
Compensation and penalties

6.1 Any provider of technology infrastructures services that does not comply with the obligations mentioned in articles 2, 3, 4 and/or 5 above is bound to compensate competitors and consumers for the harm in full, and the injured party has the right to require full compensation. Such compensation shall be promptly granted, without prejudice to and in addition with fines or remedies that may be applicable under competition law rules and/or Article 6(2) above.

6.2 Member States shall, by [...], lay down rules on interim measures and on the penalties applicable to providers of technology infrastructures services that do not comply with of this [Regulation] and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive. Member States shall notify the Commission of those rules and measures by [...] and shall notify it without delay of any subsequent amendment affecting them.

DIGITAL NEW DEAL

THE NEW DEAL THINK TANK

The aim of the Digital New Deal think tank is to shed as much light as possible on the developments at work within the phenomenon of "digitalisation" (in the widest sense of the word) and to develop concrete courses of action for French and European companies and decision-makers. With the expertise of the various contributors and their insertion in the public debate, the work of the think tank will be able to play a part in the development of a French and European understanding of digital regulation supporting the implementation of a balanced and sustainable framework.

The Board of Directors

The members of the Digital New Deal Board of Directors are all founding members. They come from various backgrounds while having direct contact with the digital transformation of companies and organisations. Given their shared interest in digital issues, they decided to deepen their debate by creating a formal framework for production and publication within which they can dedicate their complementary experience to serve public and political debate. They're personally involved in the life of Digital New Deal.

Arno Pons, executive officer, is responsible for strategic steering with Olivier Sichel, founder and chairman, and supervises a project manager that coordinates all the think tank's daily activities.

CONTACT: contact@thedigitalnewdeal.org | **WEBSITE:** www.thedigitalnewdeal.org



Sébastien Bazin
PDG AccorHotels



Nicolas Dufourcq
DG de Bpifrance



Axelle Lemaire
Ex-Secrétaire d'Etat du Numérique
et de l'Innovation



Alain Minc
Président AM Conseil



Denis Olivennes
DG Libération



Yves Poilane
DG Ionis Education Group



Arno Pons
Délégué général du think tank
Digital New Deal



Judith Rochfeld
Professeur agrégée de Droit,
Panthéon Sorbonne



Olivier Sichel
Président Digital New Deal
DGA Caisse des Dépôts



Robert Zarader
PDG Equancy

OUR PUBLICATIONS

Partage de données personnelles : changer la donne par la gouvernance
Personal data sharing : governance as a game changer

Matthias de Bièvre and Olivier Dion - September 2020

Paiement mobile sans contact - libérer les smartphones et leurs utilisateurs
Contactless mobile payment : liberating smartphones and their users

Various - June 2020

Réflexions dans la perspective du Digital Services Act européen
Reflections in the perspective of the European Digital Services Act

Liza Bellulo - March 2020

Préserver notre souveraineté éducative : soutenir l'EdTech française

Marie-Christine Levet - November 2019

Briser le monopole des Big Tech : réguler pour libérer la multitude
Big Tech Regulation: Empowering the Many by Regulating A Few

Sébastien Soriano - September 2019

Sortir du syndrome de Stockholm numérique

Jean-Romain Lhomme - October 2018

Le Service Public Citoyen

Paul Duan - June 2018

L'âge du web décentralisé

Clément Jeanneau - April 2018

Et si le CAC 40 ubérisait...sa R&D

Paul-François Fournier - November 2017

Fiscalité réelle pour un monde virtuel

Vincent Renoux - September 2017

Réguler le « numérique »

Joëlle Toledano - May 2017

Appel aux candidats à l'élection présidentielle pour un #PacteNumérique

January 2017

La santé face au tsunami des NBIC et aux plateformes

Laurent Alexandre - June 2016

Quelle politique en matière de données personnelles ?

Judith Rochfeld - September 2015

Etat des lieux du numérique en Europe

Olivier Sichel - July 2015

