CONFEDERATION OF FAMILY ORGANISATIONS IN THE EUROPEAN UNION

COFACE Policy Briefing – 2016 Digital Economy Ministerial Meeting in Cancún - CSISAC

21 June 2016

Main Recommendations

COFACE fully supports and subscribes to the Seoul Declaration of 2008. The principles expressed in the declaration acutely reflect the challenges at stake with regards to the future of the Internet and the digitalization process.

The policy debate over the future of the Digital Economy and the Internet cannot happen without the input of **civil society** as their numerous organisations are the only ones which can accurately reflect the **general/public interest** without falling prey to either authoritarian tendencies (governments spying on citizens) or commercial imperatives (private companies putting their profits before people).

COFACE further wishes to shed light on a number of more recent issues related to the digital economy:

- **Moving from "value for money" to "value for data".** Data has imposed itself as a new form of online currency via innovative business models, mostly relying on targeted/behavioural advertising, but also moving towards other forms of monetization of users' data such as insurance or financial products. While raising serious concerns relating to privacy or security, it is the inability for users to assess what their data is worth and whether the service/content offered is worth the data they share. COFACE calls for the necessity to develop **new indicators,** to help users make decisions about the services they use, the content they consume or the apps they download. Such indicators could include, among other things, how much money is generated from the use of their data, an indicator of the ratio of advertising to content, and an assessment of the uses for their data (only used for advertising,

resold to third parties for reasons such as insurance risk calculations, background checks, etc) This is only a first step in order to remove certain roadblocks for better competition and consumer choice. A more general problem is the inability for most consumers to assess whether the "price is right". In the physical world, which is arguably much easier to understand, consumers are aware of "added value" for manufactured products and can roughly estimate whether the price of a good is adequate or clearly a rip-off. In the digital world, consumers are even more at a loss when it comes to estimating value. This is what enabled many start-ups selling digital services/goods to grow at rates never seen before in history, especially since the marginal cost of selling a digital good to an additional consumer is virtually null as opposed to the cost of manufacturing an extra physical good. Further reflection is needed, therefore, on ways in which consumers can be assisted in understanding value in a digital world, especially when they pay with data.

- **Consumer protection laws applicable also in case of paying with "data"**. Users sharing data to access a service should be considered **consumers** with the full protection of consumer law. Too often, online service/content providers can get away with poor service/content arguing that these are provided for "free", whereas clearly, the user has simply "paid" in the form of another currency, namely his or her personal data. A move towards such a provision can be exemplified with by the recent EU Commission proposal for a Directive on the Supply of Digital Content would apply "to any contract where the supplier supplies digital content to the consumer or undertakes to do so and, in exchange, a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal data or any other data."[1] However, further reflection needs to be taken on the forms of compensations users can get if services/content/apps or any other digital good/content does not meet certain quality standards.

- **A Centralized Web 2.0 or a Decentralized Web?** The current flaws and issues surrounding the way the Web works has sparked many initiatives to create alternatives, one of the most important being the idea of a **Decentralized Web,** supported by Tim Berners Lee, which would work by combining current technologies such as Peer-to-Peer networking, blockchain, encryption, mesh networking and open source/interoperable languages such as Javascript[2]. The emergence of a viable alternative to the Web as we know it may provide a real incentive to address many of the issues that the Web has. Failure to make progress in securing that the Web and its Governance works for the public interest will accelerate the likely emergence of a Decentralized Web and civil society needs to be prepared for such a scenario.

- **Putting the user at the centre of the Web.** One of the major criticisms behind the Web is the dominance of big players such as Amazon, Google and Facebook, which rely on virtual monopolistic positions to control parts of the Web. Recent developments such as the General Data Protection Regulation and principles such as data portability and data ownership may be the right impetus for shifting power back to users. At present, user data is hosted directly on the servers of companies providing certain services (social networking, search engine…). An alternative, which

[1] Article 3, Scope http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52015PC0634&from=EN
[2] http://brewster.kahle.org/2015/08/11/locking-the-web-open-a-call-for-a-distributed-web-2

takes inspiration from the idea of the "FreedomBox"[3], is to put users back in control of the data they generate. User data could be stored on a users' personal cloud service and access to parts of that data could be given upon the users' explicit consent, with the right to terminate such access at any moment. This principle could be generalized to any and all data, including data generated from Internet of Things or data generated by user activity online (clicks, browsing history…).

- **Consistently check the impact of any development on discrimination, social exclusion, inequalities and vulnerable groups.** Current technological advances bring with them many potential benefits but also extremely dangerous risks in terms of discrimination of the most vulnerable groups (lower socio-economic groups, migrants, people with disabilities, children, the elderly…). Big Data could transform the financial services industry, with insurance risk premiums and creditworthiness based on **individual risk based pricing,** which will inevitably break the solidarity system based on a mutualisation or socialisation of risk, making the most vulnerable elements of our society pay high premiums or be priced out of the market, which will even further accentuate the wealth gap.

  COFACE has been a strong proponent of a setting up a **governance body** which would decide, through a strict democratic process, to which extent data should be used to assess creditworthiness or health risks. (*See COFACE's paper on Big Data and impact on financial services*[4]). This issue can be generalized to many other aspects of life which are under threat: car insurance based on data generated from connected cars, employers or tenants making decisions based on algorithms which screen through user generated data on their social networks[5]. COFACE insists that Big Data analytics should be used, not to **penalize and punish people for "bad behaviour"** but instead **empower users to make positive lifestyle choices** and **serve as an early detection/prevention tool** (for instance, helping identify financial difficulties early before a family falls into over-indebtedness, detect health problems early to avoid costly healthcare intervention)**.**

- **Closely monitor new developments such as Internet of Things, Virtual and Augmented Reality** which will deeply transform the Digital world as we know it. Most of these technologies are young and consumers/users are only beginning to use them on a larger scale. However, there are a great number of challenges which emerge from these innovations including interoperability, privacy, security, identify theft, cyberbullying, harassment, trauma and many more. Civil society should help identify potential risks, reflect on how to curtail them while at the same time ensuring that the beneficial uses for such technologies greatly outweigh the risks. This is an extension of the "safety by design" or "privacy by design" debates, which will be an integral part of the CSISAC meeting and the OECD conference. (*See COFACE paper on Virtual Reality and Cyberbullying*[6]).

[3] http://freedomboxfoundation.org
[4] http://www.coface-eu.org/en/Policies/Education-ICT/Digitalisation-and-families
[5] https://www.washingtonpost.com/news/the-intersect/wp/2016/06/09/creepy-startup-will-help-landlords-employers-and-online-dates-strip-mine-intimate-data-from-your-facebook-page
[6] http://www.coface-eu.org/en/Policies/Education-ICT/Digitalisation-and-families

- **Manage the digitalization process.** While digitalization will not necessarily lead towards a dystopian world with mass unemployment, conversely, it will certainly not be a smooth transition with jobs being created at the same pace that they are destroyed, and with job seekers being equipped with all the skills necessary to meet the demand. The digitalization process needs to be managed, to ensure that any shocks on the labour market can be absorbed and that education keeps pace with technological developments.

Specific Recommendations and Reflections

The impact of digitalization on families: new skills and jobs

At most of the conferences dedicated to digitalization, the same argument eventually surfaces: the dystopian, mass unemployment scenario due to digitalization is like the story of the "boy who cried wolf". At every technological leap, people have made such projections, and none of them became true. Ironically, the "moral" of this fable, is that once the boy told the truth, no one believed him, and the sheep ended up being eaten by the wolf.

Looking at **job creation and matching skills**, at present, we already see a gap between the demand and offer on the labour market. The EU Commission has launched a "Grand Coalition for Digital Jobs", pointing out that while "millions of Europeans are currently without a job companies have a hard time finding skilled digital technology experts. As a result, there could be up to 825,000 unfilled vacancies for ICT (Information and Communications technology) professionals by 2020."[7]

The "economics" behind the digitalization process also look worrying. Creating jobs means investing in the **human capital**, however, a study published in 2013 by the University Lille1 examined the cost of capital, and basically showed that paying out dividends to shareholders sucked up most of companies' profits, with little left to reinvest in human capital[8]. This, in turn, accentuates inequalities as shareholders are mostly the wealthiest and workers (the human capital) the poorest. Breaking out of this trend and making sure that companies can adopt long term economic development strategies as opposed to short term margin squeezing to please shareholders is an absolute necessity if we are serious about investing in human capital and thereby ensure that the digitalization process does indeed create jobs.

While Europe may seem behind in terms of innovation, this should not always be seen as a "bad" thing. Yes, there are more American "unicorns" then European ones, but the US market basically allows companies to use the market and consumers as guinea pigs to test "new" and innovative products, potentially at the expense of very high externalities and consumer detriment. In Europe, many innovative start-ups are incubated inside European Universities, developed under strong ethical standards with oversight and advice from leading academics and entrepreneurs. At the same time, public education including universities, are suffering from budget cuts. It is time to put our money where our mouth is.

[7] https://ec.europa.eu/digital-single-market/en/grand-coalition-digital-jobs
[8] http://www.cgt.fr/IMG/pdf/Document_-_Cout_du_capital_CLERSE-5.pdf

Some have pointed to the boom of the **sharing economy** as a potential for growth and absorbing unemployment, enabling families to better reconcile their work and family life with flexible working hours and independence. At the same time, many of these platforms directly put in competition workers from third world countries with developed countries, which creates a tremendous pressure on prices. Some independent content creators, be it musicians, designers, coders, are even willing to work *bro bono* just for a chance to get noticed and find a job. While this trend is highly advantageous to companies, since they can tap into a very cheap or even "free" workforce, it is disastrous for workers who see their revenue shrink massively.

Nevertheless, COFACE has identified many benefits of digitalization, especially regarding work life balance and the possibilities for tele-work, flexible hours and reconciling family and work life within the "traditional" full time job contracts.

For more information, see COFACE's European Reconciliation Package here:
http://www.coface-eu.org/en/Publications/European-Reconciliation-Package/

COFACE will be exploring the impact of digitalization on families in November 2016, looking specifically at the skills gap, the labour market and the sharing economy.
http://www.coface-eu.org/en/Policies/Education-ICT/Digitalisation-and-families

Transparency and information about controversial business models ('Freemium')

In the physical world, when you shop for a salad or a carton of milk, you know that paying 300€ for either of these items would be a rip off. On the Internet, however, both the advertising based models and the "freemium" models are misleading to an average user, and even more so to a child.

The model based on advertising makes you pay for content or services via the **information** gathered about you, the **time** you spend looking at content, the **interaction** you may have with advertising and occasionally the **sale of your information to third parties** allowing them to better target you in the future. All of these metrics are not something that users understand. In the physical world, it is possible to compare products and choose the best "value for money", something which is impossible online. There is no way to compare whether Facebook gives you more or less "value for time and information" compared to Google+. Moreover, it's impossible to even assess whether the information that is being gathered about you and the time you spend looking at advertising is fair, considering the service/content that you get in return. Is the service you are getting out of Facebook worth all the data you share and the advertising you are being exposed to?

Finally, this business model has a major shortcoming: the fact that users are **not** considered to be consumers as they did not **"pay"** for the service/content with money, but rather with their data and the time they spent on the service/looking at content. This means that **consumer rights do not apply to them,** even though, according to the latest estimates, Facebook makes about 12$ per user on average and this figure has been growing steadily for the last few years. This clearly provides a hint as to why such a business model is so attractive: companies can steadily increase their revenue by optimizing advertising to their

users or increasing the proportion of advertising inside their content/service; something that is very hard to do with a fixed price subscription based model, where users would not be happy if the price paid increased each year!

Looking specifically at the "freemium" or "free-to-play" model, it is also impossible for users to estimate the costs and compare between different apps or services. To make a comparison with real life, it's as if an action movie advertised the entrance price as being "free" but viewers would need to pay 10 cents for every bullet fired in the movie. Now imagine if that movie were the Matrix, viewers would probably end up paying three digit figures by the end of the movie! And good luck keeping count how many bullets were already fired and therefore, how much you have spent. By the same token, downloading a game with a "freemium" model, you have no idea how much you will end up spending. Of course, app developers or service providers will tell you that purchasing is "optional", but then again, behavioural sciences come to the rescue, and there are many examples where games or services have used addictiveness or other strategies to push users towards purchasing premium features.

Transparency and information are therefore essential to secure, and COFACE has several proposals which could help achieve that. The General Data Protection Regulation (GDPR) includes a provision for more transparency and information to users but it's implementation will determine whether it will make any difference for users or not.

The key recommendation from COFACE's side is the need to develop **standardized indicators** to help users compare services/content providers between each other and get an insight into the business model.

With regards to the business model relying on targeted advertising, it will be important for users to understand **which data is being collected about them and how much advertising there is on the service or content provider.** An indicator such as "advertising to content" ratio should be developed. This can look at the number of posts which are "sponsored" as opposed to "native" posts, the percentage of the screen taken up by advertising, the number of "native advertising" articles on newspaper's websites and so forth. It is important for users to understand how much of the content they are looking at is advertising and also, to monitor its development. For instance, on YouTube and Facebook alike, advertising has steadily increased its prevalence over native content. YouTube included ever longer pre-screening videos, and Facebook introduced newer forms of advertising such as sponsored posts or auto-playing videos. Should this trend continue, users need to have a way to monitor to what extent advertising takes over "native" content and the balance between the two.

The same applies to the "freemium" business model. An indicator which gives the user an estimate of how much he/she is likely to spend if using such a service or playing a game. App developers always beta test their app before publishing it online.

During such a beta test, they can also test the "premium" features and provide an estimate for the premium features of the app. After certain number of users have downloaded the app and used it for a certain amount of time, the app developer would have to display three figures on the app's description page: the median average spent by users, information on the 10% of users who have spent the most and the least using the app.

These are initial proposals of course, but such indicators must be developed in the future. Being able to compare services and apps between each other, how good they fare in terms of privacy protection, advertising ratio to content or estimated spending is essential for competition between "new" business models and older ones like paying a licensing fee for an app or recommending an online platform for your child.

Control over user generated data

COFACE has initiated a reflection on how users can regain control of their data.

At present, user data is scattered across thousands of company owned clouds/databases, aggregated together, which makes it easy for hackers, to steal millions of similar information about users like credit card numbers, usernames and passwords etc.

One alternative would be to make all and any data generated by users hosted on a cloud service owned and controlled by the user directly. For instance, data generated from IoT devices would not connect directly to a company's server, but would store any information generated into an encrypted database hosted on a user's cloud, and the company would only get access to the data generated depending on the user's access policy (one time access only, unlimited access until specified otherwise).

In case of a security breach, all access policies could be blocked and the user would have to take action to generate new access keys. Since access keys would be unique to each company which has manufactured a specific IoT device, even if a users' cloud is hacked, the data could not be stolen directly. With regards to competition, it is worth considering how users could enable access to data generated by an IoT to other IoTs in case they wish to switch devices, or share information between devices manufactured by different companies.

The same applies to other user generated data. For instance, instead of uploading videos to YouTube directly, users would upload a video to their personal cloud and YouTube would have access to it. The video could be processed and hosted in YouTube's native video format on the user's cloud, including any metadata such as title of the video, description etc. This would be beneficial from many different reasons: it would minimize the multiplication of user generated data since a user would not have to upload his/her video for it to be hosted on 10 other on demand video sharing platforms.

Finally, such a system could also apply, in theory, to more complex user generated data such as social networks. The content of a post or anything shared on a social network is in essence, a simple set of key entries in a database, typically SQL, with corresponding content, such as "title", "body", "image" etc. By agreeing on standardized sets of database keys, posts and content generated on social networks could in theory be compatible between social networks, meaning that you could consult all your posts via Google+ or Facebook, concatenating all the content into a single feed using either Facebook's design or Google+'s design. Social networks would therefore stop functioning as monopolies via the "lock in" effect, but rather compete on design choices, ease of use, user experience,

respect of privacy, adequacy of their newsfeed sorting algorithms, and the balance between native content and sponsored content.

Although centralizing user data in a single point may raise security concerns, this also means that security can be focused on a single entry point, continuously using cutting edge security mechanisms such as three or more factor authentication, encryption, blockchain etc.

It may also help achieve the initial intent of regulations such as the GDPR's data portability provision, or ensuring that data generated by European consumers stays inside the borders of Europe.

Internet of Things

The following are a series of reflections building on the report by Consumer International entitled "The Internet of Things and challenges for consumer protection".

- *Who decides what is "good" and "bad" behaviour?* The Internet of Things has much potential in areas such as insurance, but who decides what defines a "good" and a "bad" behaviour is? With regards to responsible driving, there may be some "objective" criteria such as observing speed limits, but for creditworthiness, it is much less clear. Checking whether you have repaid previous credits as a key indicators pushes towards more use of credit as opposed to using savings when purchasing goods, thus encouraging a certain "model" of consumption. And even in the case of more "objective" criteria, will these be decided internally by the industry players? In that case, how can anyone guarantee that they are objective, proportionate to the goals they seek to achieve (minimize risk), transparent, and work in the interest of consumers as opposed to maximizing revenue/profits?

- *New indicators for a new industry:* Big Data can be used not only to make sense of a lot of consumer data, but also to analyze the data that is being exchanged, who it is shared with, for what purpose it is shared. Just like appliances have ratings for energy consumption, so too, IoT devices should receive an adequate labelling which provide consumers information about confidentiality, protection of privacy, security, advertising, data sharing, etc.

- *New methods for identifying liability:* Smart devices should be equipped with accurate diagnostic tools to help identify problems, propose solutions, and clarify liability issues. For instance, testing the internal communication hardware, the local connectivity hardware (router), the ISP, the IoT company's servers etc. All actors can easily monitor the "state" of their service, whether all connections are up and running, by sending "test" communications every so often, helping to identify a problem and determine liability. It would similarly to "push or pull" notifications on smartphones. This information can be stored in log files that a user can consult to identify where a failure came from at any given time.

- *Avoid the trap of pretending that interoperability is more complex than it really is:* Interoperability clearly needs to be addressed, notably to avoid the "lock in"

problems explicated in the Consumer International report. However, it may not be as "complex" as one may think. First, there are only a limited number of hardware options for communicating data to and from IoT: WiFi, Bluetooth, NFC, all of which have standardized communication protocols. Furthermore, on the application level, apps also typically use standardized ways of transmitting data, which are often linked to the operating system. For instance, Android uses its own native methods for transmitting data which work in the same way across all Android apps[9]. Finally, on the receiving end, data is typically stored and analyzed using standardized databases such as SQL, which means that even if two apps use completely different communication protocols, they can "speak" to each other via a common shared SQL database. Besides, most apps use pre-programmed APIs for handling "standard" features such as sending/receiving data, since these types of codes are available open source and often provide little "added value" or benefits to be coded from the ground up. Therefore, a lack of interoperability is mostly the result of lack of political will and especially lack of a business case for doing so, since companies have a vested interest in locking consumers within their ecosystem and making it painfully difficult to switch to another ecosystem (see Apple…).

- *Balance between Internet, LAN and Mesh connectivity:* Most IoT are dependent on an Internet connection to work, with little to no justification for such a dependency. This situation has led to problematic cases such as the NEST debacle where consumers' devices were bricked due to a decision to discontinue the online service. All IoT devices should provide the option to communicate via either the Internet, a LAN or mesh connectivity (which could be either via WiFi, NFC, 5G or Bluetooth). The features of IoTs should require Internet connectivity based on a justifiable need and whenever such a feature can also work in a LAN or a mesh networking setting, it should include such an option.

- *Open standards enabling mesh networking:* So far, it is unclear whether 5G standards will include the possibility for mesh networking, but in COFACE's view, this is absolutely **imperative** as it would create a massive added value for consumers who would not be dependent on 5G coverage by cell phone operators/ISPs to benefit from interconnected IoT devices. Many other advantages can be cited. For instance, connected cars being able to communicate to each other directly in case of an accident in areas with no or problematic 5G coverage such as tunnels or in remote areas.

- *Closely monitor the emergence of new business models:* IoT is a recent phenomenon and new business models emerge constantly. The Consumer International report has already identified the dangers of being "locked in", forced to use the service of the IoT manufacturer. But there are many new controversial business models emerging, such as Tesla's "in app purchase" business model which relies on selling at a discounted price a connected car equipped with all features which are thwarted by software limitations. For instance, while the battery has a capacity of 60 kWh, it is artificially crippled by software, and consumers are required to pay a premium to unlock its full potential. While such a business model might allow consumers to access a costly product and "purchase" additional features along the way, unlocking

[9] https://developer.android.com/training/sharing/receive.html

them "instantly" without the need to buy a new car, it requires close monitoring to ensure that consumers do not lose out[10].

Connected Toys

The following are a few initial reflections on the risks posed by the emergence of connected toys such as the "Hello Barbie" doll or the Lego Dimensions game.

- *Misleading claims and marketing:* As connected toys will become more and more popular, there will be the temptation to use their connectivity and features as a sales pitch, by extrapolating on preliminary studies or funding studies which already have as a goal to support the claim that connected toys are better for children (in terms of brain developments, child development, skills etc…). This should be prevented at all costs to avoid a backlash against the industry when more substantial studies are published and also, to ensure that children do not suffer from unintended harm. Connected toys may have an added value of interactivity but are being criticized already by certain academics for killing creativity, or even killing the development of resilience to frustration (a toy should not necessarily always do exactly what a child wants! For instance, a "self-assembling" puzzle might be very "pleasant" and "enjoyable" to play with, but will completely kill the child's – painful - learning process of putting it together manually).

- *Safety/security:* Connected toys are often running standard open-source OS like Android for cost efficiency (developing a "home grown" software solution is very costly and often less efficient than using existing software), which means that it may have many more functionalities than those needed to run the toy, but since it doesn't have a screen or interface, it's much harder to configure it to prevent hacking or to detect a security breach (something that might get noticed on a device with a UI since there is an interface and you could spot irregular behavior or background processes)… Similarly, it may be tempting to include unnecessary sensors inside a toy which may prove to be a privacy or security threat. If it's not necessary for the purpose of playing with the toy to include a GPS or a camera, than it's best to leave it out. The same can be said about the software running the toy: it should be optimally configured to prevent hacking, possibly tweaked so that unnecessary features are removed. Ideally, the OS should be adapted specifically for connected toys.

- *Privacy:* Data should not be collected by default under the pretext that it is used to optimize a company's services. There are many ways to do it without having to collect data directly from consumers and especially from children. Most of these toys will use algorithms/speech recognition software that is already existent for some time and can rely on other data to evolve besides that of children. Data generated by children should always be encrypted and only data needed to make the toy work should be processed. No matter how secure a system is, hacking is now a common phenomenon and a company can expect to be hacked every other year or so.

[10] https://www.wired.com/2016/06/teslas-plan-rule-auto-industry-app-purchases

All data is extremely sensitive. For instance, it is possible, by analyzing data from connected toys, to predict when a family will be at home or not, which would be perfect to schedule a robbery. Logging and recording features should include an option for LAN based or direct recording and not necessarily require a cloud based solution. This centralization of data poses many security risks again. A connected device can be easily set up on a LAN to record play time with a child without the necessity for the data to transit via a cloud based service. The mere fact of logging and recording is controversial as it crosses a line in terms of children's privacy. Some steps need to be taken about that like including a "notification" light that lights up when the toy is recording/logging a child's play session, and the logging/recording feature being turned off by default.

A child should always have an easy way to know if he is being "watched" or if his play session is recorded or not. Toys will not only be connected to the internet, but connected to each other. This poses even more security threats since they will all provide a potential point of entry into a person's network. There needs to be more reflection done about further securing domestic networks. Analog security is still the best: a physical "override" or "disable connectivity" button is the best solution. Whenever possible, prefer to include the software that is needed to run the toy directly on the toy itself rather than always through the cloud and use the connectivity for updating it. A connected toy which can only work when it's connected and has no "offline" option would not only be a big minus, it also would present a greater security threat than a toy that can work offline. Besides, many online services are now proposing offline options (google maps search, google speech recognition…). Only use connectivity when absolutely necessary.

- *User control:* With Big Data, machine learning and algorithms, it is now possible to analyse a person's behavior and start to react in anticipation of perceived needs/expectations. However, besides the fact that it may be detrimental to the evolution of an individual (especially a child), what control does a person have over the "profile" that is being created about him/her? What if a kid suddenly changes his habits, tastes, what he/she likes… How will this be interpreted by algorithms and reflected in the toy's behaviour? What about the "character" that the toy will develop? Will the software adopt a "yes man" attitude, always listening and immediately responding to a child's expectations? Human interactions are rarely this selfless and frictionless… How will this impact the social skills of children? Their tolerance to frustration or their acceptance that their needs should be balanced with the needs of others? Much of these questions will remain unanswered, but it is best to formulate them early.

- *The endless consumption trap:* Connected toys also carry the risk of creating an obscure business model. Some toys like the LEGO dimensions already ask you to buy 400€ in extra gadgets to have access to all features and quests of the main game. Cost structures need to be as transparent as possible and avoid misleading models such as the "freemium" model or a "subscription based" model where consumers are locked in with a specific service provider, paying an unjustifiably high price.

***

About COFACE – FAMILIES EUROPE

COFACE – FAMILIES EUROPE works towards a family friendly environment, enabling all families and their members to benefit from sufficient financial resources, available quality services and adequate time arrangements in order to live and enjoy their family life in dignity and harmony. More: www.coface-eu.org

COFACE – FAMILIES EUROPE is supported by the EU Programme for Employment and Social Innovation (EaSI). This document is produced with the support of the European Commission but does not necessarily express its views.

COFACE – FAMILIES EUROPE Rue de Londres 17, 1050 Brussels, Belgium
Tel: +322 511 41 79 Email: secretariat@coface-eu.org Website: coface-eu.org
Facebook /COFACE.EU Twitter @COFACE_EU