Effective age verification techniques:

Lessons to be learnt from the online gambling industry

Final Report

December 2012-December 2013

Victoria Nash, Rachel O'Connell, Bendert Zevenbergen, Allison Mishkin

Contents

I Executive Summary

This one-year Oxford Internet Institute research project set out to explore the lessons learnt by the online gambling industry with respect to the successful application of age verification processes. These experiences and lessons were compared with age verification techniques applied in other industries including parts of the online retail and social gaming sectors. Specifically we sought to:

- Understand the rationale for the use or non-use of age verification in three case studies, (online gambling, online sale of age-restricted goods and social gaming)
- Explore lessons learnt from the development and deployment of existing age verification practices in these sectors
- Identify examples of good practice to inform future practice across online industry sectors

Our study investigated these objectives in three overlapping steps: a literature review of academic research, policy documents and publicly available market analysis; 38 in-depth interviews with experts on age verification drawn from across three online industry sectors as well as regulatory bodies, identity and payment providers and children's charities; a workshop with experts in the field to gain feedback on draft findings.

Rationale for the use or non-use of age verification

Legislative requirements with respect to age-restricted products and services – including alcohol, tobacco, knives, fireworks, spray paints, solvents and petrol, gambling, film and gaming content – share the common objective of protecting the health, safety and wellbeing of young people. These requirements are grounded in the context of research evidence and public debate. Both the literature review and interviews confirmed that public concern for risks and harms related to goods such as alcohol, and services such as gambling are an appropriate basis for current use of age verification procedures. In the case of social gaming, the academic evidence is nascent and there is (as yet) no evidence of clear harms resulting from minors' uptake of this new product, although there has been increasing regulatory concern about the manner in which these games are marketed to under-18s. This uncertainty was reflected in our interviews with members of the social gaming industry, with some suggesting that there is no need for age verification measures to be introduced, especially in the light of a recently introduced self-regulatory code of 'Best Practice Principles' which purports to address issues such as privacy, transparency and ethical game design.

In addition to the backdrop of research evidence, representatives from the retail and social gaming sectors highlighted a number of important drivers that underpin a renewed interest in age verification, these include changing business practices and consumer behaviours (including the rise of children as consumers), innovative business models, scope to build both existing and new revenue streams, a persistent concern for protecting minors and anticipated changes to the regulatory environment. The latter includes moves toward harmonisation of identity and age verification techniques across Europe. Together these create a 'perfect storm' of conditions for the development of innovative practices in online age verification. It is too early to predict how and where such practices will evolve most rapidly, but as this report has suggested, one very fruitful area would be the online sale of goods or services currently subject to legal restriction by age.

Lessons learnt from the development and deployment of age verification practices

The interviews conducted provided a nuanced account of the contexts in which different age verification practices are developed. It was clear from these that whilst there is great value to be gained from clearer communication between relevant stakeholders and across sectors, there is unlikely to be a 'one-size fits all' single model of age verification that suits the diversity of all business needs. For example, the level of assurance (reliability) needed will vary across transactions: customer registration for an online gambling account will require both a wider range of information, and a higher level of assurance than would be needed to process the sale of a 15-rated DVD, for example. On the other hand, all business sectors place a value on certain core principles, most importantly proportionality. This means that the costs of age verification measures to be introduced must deliver enough benefit to the customer and the company to counter any additional costs (not just financial, but also in terms of time, convenience etc) imposed.

Examples of good practice

The project exposed a wealth of information about existing good practice and (most encouragingly) a great willingness to discuss this. Our findings indicate that whilst companies in the online gambling sector are rightly to be praised for taking a strong lead, many businesses in the retail sector have also have adopted a responsible approach to complying with legal requirements relating to the advertisement and sale of age-restricted products and services. In doing so, all these businesses apply a range of age verification methods that afford differing levels of assurance and are subject to various levels of enforcement, generating many examples of good practice which should be of interest within and beyond their sectors. Some of the most interesting examples of good practice include:

- Effective and efficient use by the online gambling sector of government-led e-ID schemes in Spain, Italy and Denmark as a reliable means of asserting legal majority age.
- Effective leveraging of online third-party databases by UK online gambling and some retail operators as reliable means of verifying age for the majority of those aged 18+.
- Innovative business practice within the retail sector to 'design out' underage alcohol purchasing by specifying minimum purchase quantities, and to 'design in' individual store responsibility for online sales.
- Responsible practices observed amongst some larger social game developers targeting under-13s, who view age verification coupled with parental consent and the ability for parents to set spending limits as potential business enablers rather than overly burdensome compliance costs. This view was not reflected across the wider social gaming sector.

Wider policy implications

In addition to the very specific lessons learnt about good practice across the three different sectors, several broader conclusions should also be noted:

- Age verification has come a long way since the Internet Safety Technical Taskforce Report of 2008: age verification is no longer just about child protection, it's about good business practice online.

- Recent advances in identity authentication and assurance mean that public authorities bear a renewed interest in the possibility of improving protection for minors through use of technological measures to verify age.

- This is a rapidly developing area: innovations are emerging from both the private and public sector, with developments in both attribute exchange ecosystems, and state-led e-ID schemes. Both online industry sectors and policy-makers should be monitoring innovations, and scoping for new business opportunities not just thinking about compliance.

- There is a clear role for more cooperation between sectors, with even interviewees from the European Commission asking how the online retail sector could more effectively leverage age verification measures.

- If the potential benefits of age verification are to be maximised, it's vital that trust is not destroyed through lapses in data protection or requests for more information than is strictly necessary: the implementation of trust frameworks is foundational.

- Children should not be age-gated at every step: the recommendations here are intended to strengthen existing regulatory frameworks limiting access to age-restricted goods, rather than to create new barriers as there is great value in free exploration of the Internet.

- Insofar as age verification is one possible technical measure which can help prevent illegal access to age-restricted goods or services, it is still not a perfect solution for what is ultimately a social problem, but there have been significant improvements in the past five years, and it may now deliver enough additional benefits to be worth serious consideration across a wide range of online businesses.

II Research Context: Age-restricted goods and services, online and off

In the offline context, we're familiar with the idea that certain types of goods, services or activities are unsuitable or even harmful for minors, and regulatory frameworks exist to control their access with varying degrees of efficacy. The level of regulation or control imposed is usually expected to be proportionate to the perceived level of risk involved, thus for example, a shop may not sell cigarettes or alcohol to a minor even with a parent's consent, but a UK cinema may admit a child of under 12 years to a certificate 12A film so long as they're accompanied by an adult. The challenge of determining a consumer's age arises both offline and online, with many online industries being subject to legal requirements to sell products or services, or display advertisements only to Internet users over a certain age. Online retailers, for example, may not sell age-restricted goods such as alcohol, cigarettes or DVDs to minors below the legal minimum, whilst online games are also restricted to certain age groups, as denoted by the Pan European Game Information rating system (PEGI). In online environments, age-restricted access may thus be equally desirable, but is often presumed to raise its own challenges, not least the lack of easy means of remotely confirming someone's age, and the lack of commonly accepted examples of good practice.

It is the latter assumption that this research project was established to address. As a first jumping-off point, we do not assume that offline age verification is easier or more effective than online age verification. In the offline context, customers seeking to use betting shops, to purchase alcohol or view an 18-rated film at the cinema might be asked to provide physical identification to prove their age. Although this process is often held up as the gold standard for age verification, it's important to note that it's not foolproof – staff require training, and may prove variable in their willingness to confront potentially under-age users, whilst the identification provided may not be genuine, or may not belong to the individual presenting it. At the same time, online age verification procedures should not automatically be seen as problematic: they may enable a company to ensure consistent practice in all transactions with consumers, as well as offering a clear audit trail for regulatory oversight. Further, high levels of assurance may only be needed in high risk transactions, meaning that other less costly, lower assurance options may be more achievable. In this context, it is important to be open-minded about the different challenges and opportunities provided by the move towards online methods of age verification.

It's also vital to note at the outset that there may be important differences between determining whether an individual Internet user is 18 or over, and whether they are 7+, 13+ or 16+. Identity and age verification solutions for adults can draw from numerous public datasets, such as the electoral role, credit history, telephone directory or driving license databases, against which it possible to corroborate the identity and age information asserted by an individual. When the question is simply 'is this individual aged 18 or over?', their presence in one or more of these databases is usually sufficient to answer the question positively. The same does not apply to minors. If an individual does not feature in any of these databases, this does not prove that they are a child, and certainly can't shed any light on whether they are 6, 12 or 15. In the UK, it's estimated that up to 85%[1] of the adult population can be ID validated with good access to data sources, however the availability of such

---

[1] Figures drawn from pre-study meeting with Experian.

datasets can vary significantly from country to country. In relation to those under 18, datasets do exist and are maintained by government and public bodies, but these are often not accessible to the private sector, particularly during the development of first and second-generation e-identity solutions. This is one of the key factors that gave rise to the disparities between the ability for commercial entities to positively age verify the ages of adults and minors.

Although the potential contribution of age verification solutions aimed at the young demographic has long been a central concern of debates around online child protection, over the years various reviews have drawn different conclusions as to their suitability and efficacy as a regulatory solution. The Berkman Center-led review conducted in the US in 2008 concluded at that time that no one technology or set of technologies could effectively protect children online, but this report focused on a wide range of online risks and harms (Internet Safety Technical Task Force 2008). By contrast, a report commissioned from Malcolm Sparrow at the Kennedy School of Government around the same time, concluded that at least in relation to preventing minors from gambling online, age verification techniques were an appropriate regulatory tool. In some ways, the differences between these two policy-focused reports neatly evoke the importance of this research. On the narrowly focused question of whether or not minors should be able to access online gambling websites, there is a large body of pre-existing literature which sets out a convincing evidence base for the potential risks and harms associated with minors' access to gambling services. Such services have (up until relatively recently) been well delimited online, and are delivered by an industry which in many countries, is already heavily regulated. By contrast, the range of online risks and harms (cyber-bullying, sexual predation, problematic content) covered by the Internet Safety Task Force are rather less well-understood, with a much more variable evidence base, and (more problematically) the sources of risk or harm are widely drawn. In this case there is neither a single family of risks to be mitigated against, nor a single target for regulation. Further, the nature of the risks are such that granular age verification of minors at various points below 18 would be required, which is a much tougher proposition than ensuring simply that a person is 18+. Against this backdrop, regulatory responses have tended to favour mechanisms which empower schools or parents to intervene in their children's Internet use, such as parental control technologies or educational campaigns or state-led initiatives which offer or require filtering of Internet content.

However recent advances in identity authentication and assurance mean that public authorities bear a renewed interest in the possibility of improving protection for minors through use of technological measures to verify age[2]. In addition, developments in the range of commercial content and services now available online, in the technological devices and platforms used and the trend towards more private but networked use, even by children (Livingstone et al 2011), means some of the most basic assumptions about the nature and extent of risk may also now be outdated. This is therefore an appropriate moment to revisit questions about the appropriateness and efficacy of age verification measures for protecting minors in their online transactions and experiences.

This timely research project is therefore well-placed to contribute to wide-reaching policy debates about how best to protect consumers, and specifically minors in an online commercial environment. The focus on the commercial environment rather than interpersonal interactions is deliberate, and

---

[2] The European Commission's DG CONNECT has conducted expert workshops on the topic of Age Verification in the Digital Age whilst there are a number of pan-European eID projects which seek to rationalise the enaction of online identification across borders (e.g. STORK, FutureID).

will enable us to make an important contribution to the evidence base informing online child protection policy where much of the literature fails to address this angle. More specifically, our agenda is justified by a need to give more recognition to the benefits of economic socialization for minors engaging in commercial services or transactions online whilst balancing this against the risks of economic exploitation and other harms. To this end, the study will comprise of three case studies, each addressing a different type of online commercial activity, which may entail different risks and opportunities for minors, as well as facing different regulatory and economic pressures. The expectation is that lessons can better be learnt by comparing experience across sectors, particularly as this may serve to identify common concerns which would not normally be discussed across different industries. The comparative approach should also enable us to identify more general policy principles which could be more widely applied in the day-to-day operation of online industries that are regularly used by (but not necessarily targeted at) under-18s.

III Research Design and Methodology

Case Study Selection

This one-year research study seeks to contribute to wide-reaching policy debates about how best to protect consumers, and specifically minors in an online commercial environment. To this end, the study is comprised of three case studies, each addressing different types of online activity which may entail risks for minors. The first case is online gambling, where Know-Your-Customer (KYC) procedures including strict age-verification requirements have been a standard requirement of government licensing for several years. We compare practice in this industry with that of two other cases: one where age verification is required by regulation, but is not subject to the same level of enforcement (sale of age-restricted goods) and another where no age verification is required by regulation, but where age-related risks might be deemed to arise (online social gaming). The choice of online gambling as a case study is particularly appropriate given that its age verification practices have previously been held up as exemplary by child protection charities, for their purported efficacy in restricting access by minors. This case study selection enables comparison of standards and practices across different sectors, and maximizes the opportunity to highlight policy implications with a broad application.

Given that there is currently no single framework for age verification practices in operation across Europe, this project draws on practice across several member states which can serve as exemplars of different regulatory approaches. This is most obvious in the online gambling case study, where licensing requirements differ significantly across member states and we have consequently investigated age verification practice in four different countries on the basis of their different KYC requirements. The countries studied in relation to online gambling are UK, Spain, Italy and Denmark. We also set out to conduct interviews in France, but were unable to gain access to high-level participants in either the online gambling industry or regulatory body despite repeated requests. To that extent, we make reference in our analysis to age verification practises in the French online

gambling industry, but this information is drawn only from desk-based research. In each of these cases, it should be noted that although the details of the licensing requirements vary across each state with associated costs for operators, the underlying ethical principles are the same, namely a determination to protect minors and vulnerable people, a need to ensure a fair gambling experience, and the prevention of fraud and money laundering. Given that in the cases of online retail and social gaming the different regulatory requirements are not so marked or specific across different EU states we did not set out to conduct interviews in particular jurisdictions. Many of the interviewees for these case studies were drawn from the UK, but in several cases had responsibilities extending across other EU countries.

Research Questions

The over-arching aims of this project were:

- To understand the rationale for the use or non-use of age verification in three case studies, (online gambling, online sale of age-restricted goods and social gaming)
- To explore lessons learnt from the development and deployment of existing age verification practices in these sectors
- To identify examples of good practice to inform future practice across online industry sectors

With these aims in mind we set out to answer four more precise research questions:

1. Within Europe, what regulations guide age verification (AV) practices across the three different sectors?

2. What evidence of risk or harm underlies these regulations?

3. How adequate are the regulations and corresponding AV practices in the light of this evidence?

4. What are the policy implications of the findings, and specifically are there any examples of "good practice" that could be adopted across online industry sectors or in other countries.

In order to answer these questions we collected data from three different sources:

- Interview data drawn from industry and regulatory experts across the three sectors, as well as leading academic and NGO experts
- Research findings drawn from academic literature
- Publicly available market information and industry analysis

Interviews

In total we conducted 38 elite interviews, each lasting between 45 and 90 minutes. Given the necessity of reaching individuals in specific roles and areas of expertise we employed a purposive sampling strategy, based on an initial review of literature, company websites and media reports. We used existing personal contacts and direct e-mails to ensure direct negotiated access and then expanded our sample using snowball sampling. In order to ensure the best combination of comparability and flexibility we chose to employ a semi-structured questionnaire. The interview

schedule was drawn up to be broadly applicable to interviewees from across all three sectors, but where questions were clearly irrelevant these were not asked, and similarly, where interviewee expertise justified more detailed questioning we were able to probe more deeply with additional questions. We initially carried out four pilot interviews to test the interview schedule, and as very few revisions were consequently made we have chosen to include the data from those interviews in our analysis. Where possible, interviews were carried out face-to-face. Where this was not possible due to scheduling restrictions or travel cost interviews were carried out via skype or phone. All interviews were recorded, apart from two where the recording device or application failed. In one of those two cases, the interviewer had taken detailed notes so this content is included, but in the second interview, the notes taken were too insubstantial to justify the interview's use. This interview has not been included in the 37 interviews analysed for this report. All interviewees were asked to give their informed consent is sought in advance of the interview in line with the University of Oxford's ethical research guidelines. Copies of both the consent form and interview schedule are attached as appendices to this report.

Literature Review

An initial literature review was undertaken during the first three months of the project. A search of bibliographic databases was undertaken, utilising search terms such as age-restrict* AND Internet, Internet gam* AND children, Social media AND gam*, age verification AND online. Further articles were then identified using processes of citation-chaining (searching for articles that cite known core research) and hand-combing of relevant journals. In addition, new literature was added to an earlier study of the evidence of harms relating to children's Internet use. The initial searches yielded a large number of articles, of which over 100 were deemed to be particularly relevant, and were consequently downloaded for further review. Further literature was added over the course of the project, including a more specific review of the literature relating to social gaming undertaken by an OII MSc student with experience in this field.

The articles returned cover a range of aspects related to this study, with most research found on topics of risk and harm, legal and policy issues relating to online gambling, and rather less specifically focused on practices of age verification online. Despite the range and quantity of literature reviewed no studies were found that offered a consistent and comparative approach to the assessment of age verification techniques online, and there were no studies which used qualitative methods to gain insights from industry and regulatory insiders. These gaps demonstrate the potential contribution of this project to the academic literature, and we will be seeking journal publication accordingly.

Market analysis

In order to gain an understanding of the different business models across the three case studies, we undertook regular searches of online industry news sources and mainstream media reports, set up media alerts for key terms, monitored and attended industry conferences and studied the websites of major players and industry regulators. We also identified the main regulatory frameworks affecting each sector. Whilst it is not within the scope of such a short project to offer a fine-grained analysis of these three large and rapidly developing sectors, the investigation offered considerable insight into the different market and regulatory pressures affecting the three sectors.

IV Literature Review: The Risks and Opportunities of Internet Use

Children's Use of the Internet

Many aspects of children's personal lives are mediated by the Internet. It offers valued platforms for playing with identities, making and talking to friends, playing games and even spending pocket money. It's not so much that these activities are new in themselves, but rather that children and teenagers "…are doing this while the contexts for communication, friendship, play, and self-expression are being reconfigured through their engagement with new media" (Ito et al. 2010: 1). As a recent UNICEF report noted, online and mobile technologies are no longer 'an optional add-on', but permeate every aspect of children's everyday lives (Livingstone and Bulger 2013: 8). Evidence also suggests that Internet use is becoming increasingly common at ever younger ages (Holloway, Green and Livingstone 2013), with a recent UK survey suggesting that a third of 3-4 year olds go online, rising to 87% of 5-7 year olds (OfCom 2012). Unsurprisingly, such shifts in behaviour are associated with both new opportunities and risks, and it's no surprise that so many tabloid headlines are devoted to luridly reporting the terrible things that can result from children's determination to engage online. For many parents and policy makers, the greatest source of anxiety is the extent to which children and teenagers can conduct much of their personal life online, in an environment which is perversely private in the sense that a responsible adult can easily be excluded, but public insofar as it offers opportunities to interact with unknown others or transact in a marketplace designed for adults.

Much existing research into children's Internet use endeavours to provide a sense of what kids do online, and the extent of the risks that may arise. In this context, for example, the EU Kids Online Survey finds that 60 per cent of European 9–16 year olds go online almost daily, with an average duration of just under an hour and a half for all 9–16 year olds, and more than three hours a day for those aged 15–16 (Livingstone et al. 2011). Despite the emphasis placed on Internet use in schools, the most common point of access is still home rather than school and increasingly, such use is becoming more private, with children using a personal device such as a laptop or a mobile or having access within their bedroom rather than a shared family space (Livingstone et al. 2011). Apart from schoolwork, the most common uses of the Internet amongst this group are for entertainment and socializing, such as playing online games, watching videos, and using Instant Messenger (IM), e-mail, or social networks to communicate with friends (Livingstone et al. 2011).

Many of the most popular online activities or services are not specifically designed for use by minors, and some are supposedly age-restricted. As a result of the US Children's Online Privacy Protection Act (COPPA), social media sites such as Facebook, Tumblr or Google+ are currently for use only by those over 13 even in Europe, whilst others, such as the mobile photo-sharing app Snapchat have tried to introduce safer (non-sharing) versions for under-13s. Despite these professed efforts to limit use by under-13s, 59 per cent of European children between 9 and 16 claim to have a social networking profile, with age-specific practices varying from 26 per cent for those aged 9–10 to 82 per cent for those at the top of the age range (Livingstone et al. 2011). In the US, 80 per cent of online teenagers between 12 and 17 use social networks, far more than the 60 per cent of online adults using such services (Lenhart et al. 2011). Whilst the use of SNS for social and expressive

purposes is not necessarily problematic (and may be very beneficial), these figures do raise legitimate policy concerns, implying that large numbers of children are using sites not designed for their age group, and potentially without parental consent or knowledge. Taking this concern even further, (and possibly serving as evidence of the failure of existing age verification measures) it would seem that online deceit is remarkably common, with 39% of online teenagers in the US admitting to lying about their age in order to access age-restricted services according to the latest Pew survey (Madden et al 2013).

There is surprisingly little academic survey data about children's engagement with commercial activity online. Although the EU Kids Online surveys do not ask children specifically about their use of commercial services or sites, it's possible to get a sense of the popularity of such activity by considering that 83% of 9-16 year olds who use the Internet played online games on their own or against a computer, 62% visited a social network profile and 44% played games with other people on the Internet (Livingstone et al 2011: 34). Figures from industry-commissioned research provide more details. A survey of adults and children for the UK premium phone lines regulator found that 89% of 7-15 year-olds play online games, and half of these pay to play, most usually with their parents' help (Phonepayplus 2012). A recent UK survey of children's financial literacy suggested that 84% of 8-15 year olds have bought items online or had someone else buy for them, with 58% having done this before the age of 12 (BBA 2013). In this latter survey, half of these young shoppers reported buying clothes, books and video games, whilst just under half bought music and DVDs. Given that video games and DVDs come with age ratings, this finding suggests that online retailers should already be exercising a duty of care when selling these products to young consumers, or risk breaking the law. The range of payment methods used by children to purchase good online include online credits, debit or credit cards, Paypal, or pre-paid cards (Phonepayplus 2012). Although this survey reports that most payments are made by parents, it's worth noting that many children do have bank cards, and that in the UK, up to one in ten of those with bank accounts even use online banking (BBA 2013). Other methods of online payment, such as in-app purchases, or payment using virtual currencies (previously bought game tokens, for example) are used less frequently, but are a source of possible concern. Other research commissioned by UK premium phone regulator Phonepayplus reports that children who had used virtual currencies (such as Playstation points or Smurfberries) find it difficult to keep track of how much they are spending, whilst online apps purchases may not be transparent about the distinction between free content and in-app purchases (Phonepayplus 2013).

It's important to remember that exposure to commercial activity online is not just about buying goods or services: advertising is now omni-present online, and the availability of 'free' services such as Facebook, Myspace, Spotify[3] or Twitter is premised upon the selling of targeted advertising, based on user profiles. Again, it's hard to gauge exactly what adverts minors are exposed to, and parents may choose deliberately to install ad-blockers, but given that many minors register for social networking sites using a false age (boyd et al 2011; O'Neill 2013), it's no surprise that a third of online teens surveyed in the US have received online advertising 'clearly inappropriate' for their age. A recent small-scale compliance study by the UK advertising Standards Authority found that whilst

---

[3] Services such as Spotify do offer paid 'premium' products without advertising, but as these usually require a regular monthly payment by debit card, it's questionable whether kids will choose to use the free service or bother parents to pay for their music streaming.

advertisers on major social media websites appeared to take account of the *registered* age of users, age-restricted adverts were still seen by under-18s as a result of the use of false age information (ASA 2013).

The determination in this project to focus on children's commercial activity online stems from two observations: a positive recognition of the value of safe online experiences in the economic socialisation of children, and a more protective concern that the current policy focus on filtering and parental controls may do little to safeguard against either the illegal purchase of age-restricted goods or services or limit exposure to age-rated advertising, especially given evidence outlined above of falsification of age credentials.

Whilst we now know more than ever about what children do online and how this shapes their experience of risks and opportunities, there are still some real gaps in our understanding. From a policy perspective, one of the biggest problems is that we know relatively little about the relationship between risks and actual harm, or the way in which different risk factors combine to increase or decrease risks for particular children. Most fundamentally, there are real methodological and ethical challenges involved in measuring harms to children resulting from Internet use. You simply cannot undertake randomly controlled trials whereby children are assigned to groups to compare the effects of watching pornography, or playing violent games, whilst studying those who already have undertaken such activities tells us little about effects on others who did not seek out such experiences. For this reason, many studies of Internet-related harms measure not harm, or even risk, but the "risk of risk" (Livingstone 2010: 4), for example, the likelihood that any one child will access pornography or a gambling site, rather than the likelihood that he/she will be harmed by this experience. Exposure to risk indicates the probability (but not certainty) of harm, and risk may be successfully encountered and overcome by more resilient Internet users. This poses a problem for responsible evidence-based policy-making, meaning that even with the best of intentions, policies are likely to be constructed on the basis of judgments about the *potential* risk of Internet use.

Much of the research into the risks and harms associated with children's Internet use focuses on contact or content risks, rather than conduct risks (i.e. what children actually do online). There is also often a tendency to focus on risks associated with inappropriate, harmful or offensive content and conduct rather than on content or services which it may be illegal to provide to minors (although high-profile media and policy concerns about online gambling may be the exception here). Whilst this may be justifiable to the extent that by definition, laws already exist to protect minors in these circumstances, there is surely value in assessing whether such regulatory frameworks are effective in the online context. If certain goods or services, such as alcohol or violent movies are deemed to be so harmful for minors that it is illegal to sell or provide them to consumers below a certain age, then surely policy resources should be devoted to ensuring that existing legal requirements are adequate and well-enforced before wading into more controversial questions of how to protect against lesser risks.

Given that the main aim of this project is to understand the rationale for the use or non-use of age verification, it makes sense to consider case studies where there is a clear impetus to apply age verification processes. To that end we chose to consider the online gambling sector, where European licenses have imposed strict requirements regarding Know-Your-Client and Anti-Money-

Laundering processes, and also the online retail sector, in which it has long been illegal to sell certain goods or services to those below particular ages. We also selected a third case study where the case for age verification is currently less clear. As will be seen below, debates around the harms associated with video and Internet games have not reached a resolution, and show little sign of doing so. Despite this, recent policy pressures on the emerging social gaming sector suggested that it would serve as a useful contrast as an example of an industry not currently required to apply age-gating, but which might face such calls in the near future. In order to understand the rationale for regulatory requirements or voluntary implementation of age verification procedures, it's worth briefly reviewing the evidence of risk or harm which might inform such decisions. Specifically, two of the cases are supported by rich and longstanding research traditions, albeit with varying levels of consensus, whilst one is relatively nascent and divided.

The rationale for age-restricted retail goods: the example of alcohol

The category of goods whose purchase is subject to age restrictions online is very broad, and varies by jurisdiction. In England, Wales and Northern Ireland, for example this category includes tobacco products, alcohol, fireworks, offensive weapons, aerosol spray paint and petrol[4]. Age restrictions may be set at different ages for different products, depending on the perceived level of risk, thus for example, you have to be 18 to purchase alcohol or adult fireworks, but can buy liqueur chocolates, lottery tickets and low hazard fireworks at 16. For the purposes of this study we chose to focus mainly on the online sale of alcohol, as this is both very widely sold online and also subject to age-based purchase restrictions in many jurisdictions[5]. We also interviewed retailers in the general retail space, as games and DVDs are known to be commonly purchased online by minors but these goods are also subject to age-ratings, and are even subject to legal restriction in the UK (BBA 2013). A brief overview of the risks and harms associated with the purchase of these goods follows below.

Whilst it is beyond the scope of this study to provide a detailed literature review of the research evidence of harms caused by alcohol consumption, even a cursory inspection reveals both the consistency of research findings over a long period of time (Room et al 2005; or see Pearl 1926 as an example of early seminal work), and the broad array of harms associated with such consumption (Bouchery et al 2011). Academic research has shown alcohol consumption to be linked to more than 60 medical conditions (Rehm et al 2003), violent crime (Graham & West 2001), injury and accidents (Waller et al 2003; Smith et al 1999) and a variety of social ills such as risky sexual behaviour, domestic violence and loss of economic productivity[6]. In addition, research suggests that some of these risks or harms may weigh particularly heavily on adolescents who are, as a group also often more subject to peer pressure, unused to the effects of alcohol and prone to risk-taking behaviours. Thus there is evidence that adolescents who start drinking during adolescence may be at greater risk

---

[4] List available from the Trading Standards Institute, available at:
http://www.tradingstandards.gov.uk/advice/advice-business-sfsum1.cfm. Accessed 25 June 2013.
[5] Although there are variations: for example, in France, Spain and the UK, the minimum purchase age is 18, but UK customers may be challenged to provide ID if they look under 21; in Italy and Denmark, minimum purchase age is 16. Private consumption in the home is unregulated in most countries apart from the UK. See the data gathered by the International Center for Alcohol Policies at:
http://www.icap.org/PolicyTools/ICAPPolicyGuides/. Accessed 1 July 2013.
[6] See for example summaries provided at: http://www.cdc.gov/alcohol/fact-sheets/alcohol-use.htm or
http://www.dassa.sa.gov.au/site/page.cfm?u=122 Accessed 25 June 2013

of alcohol dependency in later life (Grant & Dawson 1998), as well as being susceptible to particular health-related harms (Clark et al 2001) and that teenage binge drinkers are more likely to engage in other risky behaviours such as drug-taking or having multiple sexual partners (Grunnbaum et al 2004). Against such a backdrop, it is unsurprising that the purchase of alcohol is age-restricted, and whilst such policies are not sufficient to prevent the array of harms described above, there is some evidence that they do make a measurable difference (see, for example Kypri et al 2006).

Online gambling: for adults only

In reviewing the evidence for risks and harms associated with gambling or online gambling, we are very aware that colleagues at Bwin are necessarily more familiar with this literature than we can become in such a short timescale. What is notable from reading many of the most-cited studies is that the relationship between gambling and the reported personal, social or economic harms is complex, multi-faceted and difficult to study. A report produced by Adelaide University for the Australian Ministerial Council on Gambling notes the challenges of defining and research gambling-related harms as including:

- Absence of any commonly agreed definition of harm;
- Identification of harms often based on individuals' own self-assessment of problems brought on as a result of their gambling behaviours;
- Methodological challenges of separating out various personal and social factors interacting with gambling behaviour and purported harms;
- The difficulty of distinguishing cause and effect (University of Adelaide 2005: 39-44).

In addition, as that same report makes clear, different stakeholders have varied understandings of what constitutes the negative features of gambling, with some for example adopting a moral stance that gambling is (of itself) morally undesirable, whilst others such as regulators or social policy experts being concerned with links between gambling and negative social outcomes, and still others such as clinical psychologists or psychiatrists focusing on problematic or pathological behaviours (University of Adelaide 2005: ii-iv).

Despite the challenges of identifying and measuring the potential negative impacts, the range of different gambling behaviours is frequently divided into problem or pathological and non-pathological categories, although as Blaszczynski et al (2011) point out, both the terminology and categorisation are inconsistently applied. In relation to pathological gambling there is a rich and expanding literature on the demographic, psychological and physiological characteristics, on the behaviour patterns, associated activities and disorders, social, economic and legal implications, although there remain many areas of disagreement and debate (see for example Lesieur and Rosenthal 1991 or Raylu & Oei 2002). One helpful framework for reviewing the literature relating to problem gambling is the new Conceptual Framework of Harmful Gambling produced by a collaboration of researchers for the Ontario Problem Gambling Research Centre (OPGRC) (Abbott et al 2013). The increased vulnerability of adolescents in relation to gambling is also well-studied, with concerns raised about their higher prevalence of gambling-related problems, and the apparent association between adolescent gambling and other risk-taking activities, as well as lower educational outcomes (Delfabbro and Thrupp 2003). To this extent, it is perhaps unsurprising that in

countries where gambling is regulated at all, minimum age restrictions tend to be imposed on gambling activities, with proof of age checks in physical gambling venues.

In the online context, research concerning the implications of Internet gambling is still in its (relative) infancy, but already there have emerged studies suggesting that adolescents and children are a particularly vulnerable demographic given their familiarity with and frequent use of the Internet. Thus studies suggest that the convergence of gambling and new technologies may have made gambling more accessible and attractive to young people (King et al. 2010), whilst others have investigated links between problematic substance use, delinquent behaviour and Internet gambling amongst adolescents, although the developmental sequence involved is not clear (Brunelle et al 2012).

Social gaming: an emerging and uncertain genre

Popular media rhetoric suggests video games may negatively impact child development. While often based on preliminary academic studies, such reports worry politicians and parents and often underpin prevalent concerns about game-based experiences. Academics, lobbyists, trade associations and regulators currently disagree over whether harms exist, how best to protect children from hypothetical harms, and how to structure play around any potential benefits. Despite play's importance, the increasing mediation of a child's game experiences and concerns about game content underscore the need to assess how best to protect children from the genre's impacts (Lange 2011).

Compounding the issue, outdated reports inform much of our current understanding of video game engagement. Tania Byron's 2007-2008 Review underpins the UK's current regulatory efforts and how parents and educators perceive the digital space (Byron 2008). However, recent scholarship suggests that it no longer reflects how children engage with digital games. Byron based her recommendations on console games. Since 2008, casual social games have exploded in popularity and availability. By 2012, 66% of teenagers were playing mobile games and 25% reported using Facebook games (Caoilli 2012) and the number has likely grown since then.

While formally defining "social games" eludes games scholars and designers, all agree that these games share at least one of the following characteristics: 1) embedded in a social network, 2) light-weight play style or a short learning curve, and 3) rely on social ties to influence the gaming experience or a specific game mechanic[7]. Mobile platforms have helped this genre grow by emphasizing an "anytime/anywhere" attitude and also through the emergence of freemium content models whereby games are available, even if only initially, at no cost to users. Interestingly, social gaming has changed the profile of gamers: 5 years ago, when Byron surveyed the online game space, 80% of boys played compared to 50% of girls, and in both cases, games were mostly accessed on game consoles (Byron 2008). However, partly because of the reliance on social media platforms with their attendant social and financial incentives, the gender divide is now nearly gone (Juul 2012). Most critically, industry figures suggest that children and teenagers make up almost 30% of this market (Fidgeon 2012), incentivizing designers to design for this vulnerable population, and making

---

[7] See for example Wallace & Robbins (2006), Kuittinen et al (2007), Lovell (2011).

it all the more important to understand the possible risks and opportunities associated with these games.

New types of game experiences may pose behavioral risks ranging from Internet addiction, aggression, to shaping individual norms or values. There is as yet remarkably little academic research examining the impact of casual social games, even though their players are becoming the majority (Consalvo 2009). What research there is, focuses mainly on behavioral impacts, consumerism in social games, the relationship between social games and gambling and benefits from social game play.

In relation to the first, academics have studied links between video games and aggressive behavior, increased sexuality, and decreased attention span (for an overview see Buckingham et al 2007). In principle, these might seem less likely to apply to social games (Ivory and Kalvanaraman 2007) with social game designers typically expected to target wide audiences through lightweight and family-friendly play experiences. This expectation has so far been backed up by research evidence suggesting that if *casual* games are disaggregated from previous studies of games and sexualized content these display no significant sexualized imagery or negative gender roles (Wohn 2011). However, it remains to be seen whether social games in the broadest sense must necessarily aim for such a wide audience, and as games such as Grand theft Auto and Everquest move to mobile platforms for more social, casual gaming, there is a need to monitor this issue carefully over the next few years.

There is also conflicting evidence surrounding connections between games and attention span, but this debate may be particularly salient to social games. In one recent Pew white paper, scholars theoretically link short experiences and instant gratification with a potential decline in attention span in the "Always On" generation (Anderson & Rainie 2012). Social games share features the authors associate with this attention lag, namely escapist attitude, short-play periods, and increasing mediated experiences through mobiles, SNS, etc. Unfortunately, despite the strong hypothetical links between social games and attention-risk literature, specific examinations of how social games influence attention-span have not been conducted.

Of particular policy relevance are concerns about the possible financial harms of social games, currently the subject of an investigation by the UK Office of fair Trading[8] and also recently the US Fair Trade Commission[9]. In addition to concerns about a lack of transparency about in-game purchases, the virtual-object acquisition mechanics may introduce children to purchasing behaviors that predispose them to later consumption habits. Children are known to be susceptible to in-game brand placement, either through explicit advertisements or interactive "adver-gaming" (Bellman et al 2014). Younger players are more susceptible to such effects, and the more fun the social game, the more susceptible the child may be to make in-game purchases (Van Reijmersdal et al 2010). Since most online worlds geared towards children cannot rely on in-game purchases to make money, child-focused virtual worlds often use in-game social experiences to drive offline purchases (Shontell 2012). The same social pressures that proved effective in Moshi Monsters and Webkinz' successes underlie in-game purchases in social games geared at teenagers or embedded in social networks like

---

[8] http://www.oft.gov.uk/news-and-updates/press/2014/05-14#.UwYKi_l_tig
[9] http://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million

Facebook. Many social games construct a player's identity through virtually purchasing in-game goods, without ever spending in-game currency. The basic design structures social ties around a shared shopping/consumption game mechanic.[10] While this research strand has not examined whether this leads to increased consumerist child values, it highlights the increasing consumption inherent in child definitions of "fun."

Social game companies have also been accused of embedding gambling-like mechanics into their games and therefore introducing impressionable children to the excitement of gambling, potentially predisposing them to gambling addictions (Gainsbury & Derevensky 2013). Some social games may engage users through the same mechanics as casino games – namely small and unpredictable rewards, albeit non-monetary rewards. In doing so, these games may shift children's definitions of fun by normalizing betting and other gambling-mechanics as part of the play experience (Torres and Goggin 2014). However, such a suggestion is not yet supported by empirical evidence and there are few models conceptualizing how exposure to these concepts impacts later performance. While some propose that early access might teach children healthy and realistic responses to gambling experiences, others caution that early exposure might either encourage children to experiment with real gambling or to develop gambling problems.[11]

Social games blur the lines between games and gambling experiences bringing gambling-like experiences closer to minors and vulnerable populations (King, Delfabbro & Griffiths 2010). Particular concerns arise around certain features of simulated gambling games on social platforms, such as the distortion of risk via higher payback percentages, or the expectation that social factors such as group inclusion and participation or enhanced self-esteem may serve as added motivations to try real-money gambling (Parke et al 2013). However, there is as yet little evidence to suggest that these risks are significant. Although correlations have been drawn between free gambling-like games and later behavioral patterns, little research suggests that these play experiences actually cause the observed gambling behaviors (Ipsos Mori 2011; Griffiths & Parke 2010). One recent study found that roughly 30% of 12-17 year olds had played an online gambling game or social game and that those specifically engaged in simulated gambling were more likely to focus on the activity and display a future intent to gamble (King et al 2014). Determining the elements of a social game that either simulate or lead to gambling could inform age-verification approaches, but at present, such attempts to restrict access would be based on tenuous analyses.

Although beyond the scope of this project, it is worth noting that within the burgeoning field of "Game Studies" there is a significant strand that considers the psychological benefits of gaming, such as increasing resilience and risk-taking. For example, Carol Dweck found that children who believe that intelligence grows through sustained practice did not fear failure and performed better both academically and socially (Dweck 2006). Not only do games offer educational benefits, games may encourage pro-social behavior. Longitudinal, experimental, and correlational studies have jointly identified that games whose content promotes sociability produce pro-social behavior in teens and college-aged students (Gentile et al 2012). Recognizing games' power to promote intrinsic motivation and self-directed learning, the educational game market grew enormously in 2009 (Shuler 2012).

---

[10] e Silva, S. D. A. (2012). Buy and Share! Social Network Games and Ludic Shopping.

[11] For example, see King et al (2014) and Griffiths (2013).

In addition to research identifying the nature and scale of various risks and benefits associated with games and social gaming, it's worth noting that not all risks or benefits weigh equally on each child. The extent to which gameplay may influence a child depends on three factors: 1) individual psychology, 2) a child's sociocultural environment, and 3) individual rules and societal regulation. For example, individuals with high self-regulation, or an ability to manage short and long-term desires, show fewer negative repercussions from sustained gameplay (Kopp 1982). This relationship between societal rules and individual traits underscores how sociocultural environment shapes an individual's experience with the game. Rules and regulations also influence the risks from gameplay. Parental impressions of video games influence the mediation strategies they adopt and specific strategies and attitudes have been linked with mitigating or exacerbating gameplay's consequences (Shin & Huh 2011). Those strategies are often shaped by societal norms and regulations such as classification systems (Nikken, Jansz & Schouwstra 2007).

V The regulatory framework for age-restricted goods and services online

Given the evidence of risks and harms noted above, it is unsurprising that there is a substantial and complex framework of regulations designed to restrict or prevent access to certain sorts of goods or services online. As noted above, the sectors chosen are characterised by the absence of harmonised legislative frameworks across Europe. However, whilst the particular laws governing access to online gambling, online retail goods and social games are specific to the various member states, there are some overlapping features which helped to guide the selection of cases for this project. Thus, most western European states which have licensed online gambling require a minimum age of at least 18 to participate (with the exception of online lotteries), and similarly the online purchase of alcohol is usually restricted to those over 18, even in countries where those under this age may legally consume alcohol at home or in the company of parents. In the context of gaming, there has been European convergence on the issue of rating video games, but casual/social games have so far fallen outside of this remit, for reasons discussed below. We now offer a brief overview of the regulatory context across the three case study areas.

Online gambling

The EU does not currently have a harmonised legislative framework for regulating online gambling, with different member states making their own decisions about whether or how to license gambling and specifically, Internet gambling. Despite the challenges this poses for international companies thus required to apply different standards and procedures within different markets, the current European political landscape is considered too hostile towards any gambling activity to attempt a harmonisation effort. A recent opinion of the European Parliament Legal Affairs committee on the matter states that "a single European legislative act, uniformly regulating the entire gambling sector, would not be appropriate owing to subsidiarity concerns but that, in some areas, a coordinated European approach, in addition to national regulation, would clearly provide added value in view of

the cross-border nature of online gambling services."[12] The European political institutions have not been inactive in this policy area, however, creating several non-legislative policy initiatives that may pave the way for some EU level regulation in the future.

The European Council set the wheels in motion in 2010 with its official "Conclusions on the framework for gambling and betting in the EU member states".[13] In 2011, the European Commission held a consultation online gambling, which resulted in the "Green Paper on on-line gambling in the Internal Market".[14] The Green Paper was followed up by the official Communication "Towards a comprehensive European framework on online gambling".[15] Both policy papers were generally welcomed by resolutions from the European Parliament in 2011[16] and in 2013.[17] On a policy level, the European Commission has established thematic workshops regarding online gambling as part of a five-year research project regarding addictions with specific focus on gambling, among a few others topics.[18] The workshops involved Member States' experts from national governments and the establishment of a Group of Experts on online gambling, who report periodically and provide the Commission with advice and expertise in relation to the preparation of policy initiatives.

These steps have led to the announcement in a European Commission Roadmap that new recommendations on the common protection of consumers of gambling services and on responsible gambling advertising are being developed.[19] The Roadmap specifically mentions that the Commission will address the problem of "[i]nsufficient adequate identification and verification checks" and that policy options regarding the "registration and identification controls and procedures of the player" will be explored. However, it should be noted that this recommendation in no way establishes a more holistic approach to online gambling, but simply aims to guide Member States' own regulation on these specific areas.

The Roadmap also includes a Recommendation on responsible gambling advertising, which aims to address the current lack of common principles among Member States with regards to advertising and online gambling, even though self-regulatory initiatives exists.[20] For example, in the UK only licensed operators may advertise their services, in conformity with the established Codes of Practice.[21] French law requires certain warnings on the landing page after the advert is clicked,

---

[12] Paragraph 8 of the opinion, http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2013-0218&language=EN

[13] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/intm/118398.pdf

[14] COM(2011) 128, http://ec.europa.eu/internal_market/gambling/green-paper/index_en.htm

[15] COM(2012) 596, http://ec.europa.eu/internal_market/gambling/communication/index_en.htm

[16] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2011-492

[17] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2013-348

[18] ALICE-RAP (Addiction and lifestyles in contemporary Europe – Reframing Addictions project), http://www.alicerap.eu/

[19] http://ec.europa.eu/governance/impact/planned_ia/docs/2013_markt_022_023_gambling.pdf

[20] See for example the CEN Workshop Agreement (2011), Responsible Remote Gambling Measures, http://www.eesc.europa.eu/self-and-coregulation/documents/codes/private/143%20MARKT%202011%20CEN%20Responsible%20Remote%20Gambling%20Measures_Workshop%20Agreement_final_16259-2011.pdf or http://www.rga.eu.com/data/files/Pressrelease/cen_leaflet_final.pdf

[21] http://www.gamblingcommission.gov.uk/advertising.aspx

whereas Germany disallows advertising for games of chance, like raffles.[22] Pending impact assessments, the final recommendation will provide a set of common principles for responsible gambling and for socially responsible advertising in the EU. There is no further mention of advertising standards with regards to social gaming or other free forms of gambling.

In the absence of such over-arching harmonisation, the regulation of online gambling is therefore fragmented across Europe, with quite significant differences existing across jurisdictions (and even within jurisdictions in (relation to different gambling products)[23]. A number of countries, including UK, Denmark, Spain and Italy, have to varying degrees opened their markets to online gambling operators that compete along with incumbent state-owned gambling operators. Others, for example Germany, are in the process of liberalisation, whilst others such as Portugal are expected to do so soon. Despite this, online gambling operators still serve an estimated market of €1 billion annually in Germany, according to industry reports.[24]

The most common approach to the regulation of the online gambling market is through licences, although the details of these licenses vary by country. By making the legality of a gambling service dependent on a licence, the government has extensive control over the functioning and duties of the operators that serve its population, so long as this is backed up by regular audits or enforcement checks. This allows governments to ensure that a system of oversight with respect to identification and age-verification, KYC and AML operates effectively. Denmark and Italy, for example, have developed a standard interface, which operators must include in the registration process. The personal information that is provided by the prospective gambler is checked against official government databases. Italy uses the "Fiscal Code" identifier, which is used for tax purposes, whereas Denmark uses a new identifier called NemID. A prospective gambler must go to a local Danish government office to apply for a NemID, at which point identification takes place, after which he will be sent the identifier. Similarly, in Spain, customer asserted data is checked against an eID database to which the Spanish regulator affords operators access. France has not yet developed a functioning national method by which prospective gamblers can be identified.

Country	Legislation	Year came into force
Denmark	Lov 202: Bill for a Regulation of Gaming Act	2012
Italy	Finance Act 2007(FA07), "The Abruzzo Decree"	2010
Spain	Ley 13/2011 de Regulación del Juego[25]	2011

---

[22] A good overview is offered by Google's and Twitter's advertising policy websites with regards to online gambling: https://support.google.com/adwordspolicy/answer/176014,
https://support.twitter.com/articles/20170426-gambling-content
[23] See for example the interactive map of Online Gambling Regulation provided by Olswang at:
http://www.olswang.com/industry-sector-insight/gambling-regulations#country=16639 Accessed 17th February 2014.
[24] http://www.goldmedia.com/uploads/media/Press_Release_Goldmedia_study_Betting_Gambling_01.pdf
[25] http://www.olswang.com/pdfs/gambling_jun11a.pdf

United Kingdom	Gambling Act 2005	2007

Age-restricted goods

Across the EU, online sales of age-restricted goods are regulated through a mix of existing offline retail laws and new online directives. However, an overall lack of clarity regarding appropriate verification strategies and the lack of a unified contract policy across the EU limits the growth of the online sales sector and likely facilitates circumvention.

Within the UK, online sales of age-restricted goods are regulated through remarkably vague directives. The Trading Standards Institute, the trade association that translates the Local Better Regulation Office's statutes to commercial traders harmonizes the country's legislation for local sellers. Their official leaflet calls for "effective systems" of age-verification and states that stores are expected to take "reasonable" precautions to limit underage sales.[26] However, this official advice also notes:

> "There is no definitive answer as to what constitutes taking all reasonable precautions or exercising all due diligence."

Thus, without a definitive answer as to what steps are considered appropriate, online retailers are often left in the dark and choose instead to limit the products sold online. For example, Argos does not sell knives online. While the UK recently launched initiatives to clarify age-verification in offline sales, the new approach did not provide any new guidance as to how to protect children online.[27]

Although reasonable steps are not outlined, the Trading Standards Institute does suggest what steps are unlikely to be accepted in cases where laws are breached, namely those that are unlikely to require some form of external age-verification. Examples of measures deemed inadequate under this view would include self-reporting of age or date of birth, checking a tick-box stating you can legally purchase a good, including a site-disclaimer, or using an e-payment service that does not itself verify a consumer age.[28] While in the offline context, alcohol retailers are required to request a photo ID to check proof of age for anyone who presents as close to the age limit, with online sales, ID checks at the point of delivery may be used but are not required.[29]

Some examples are given of the types of age verification processes that might be used, but no single one of these is required or guaranteed to be adequate. These examples include online checks referencing available public identity databases, or implementation through payment mechanisms. For example, if an individual pays by a credit card, the sites can reasonably assume that the credit card company effectively verified the consumer and thus the purchase is allowed. In January 2013, OfCOM fined Playboy £100,000 pounds for not distinguishing between credit and debit card

---

[26] http://www.tradingstandards.gov.uk/cgi-bin/manchester/bus1item.cgi?file=*BADV674-1001.txt
[27] https://www.gov.uk/government/news/new-code-ends-tick-box-regulation-in-sales-of-age-restricted-products
[28] http://www.tradingstandards.gov.uk/cgi-bin/manchester/bus1item.cgi?file=*BADV674-1001.txt
[29] http://www.wsta.co.uk/publications-useful-documents/42-distance-selling-age-verification-procedures/file

purchases (the latter can be issued to individuals under 18). The penalty was avoided because the service operating the payment processing was based overseas, beyond OfCOM's reach.[30] Verification systems are expected, if not formally articulated. However, the lack of formal expectations coupled with loose regulatory frameworks creates a confusing e-commerce eco-system.

Further complicating the online sales marketplace, age-related legalities are often impacted by pre-Internet legislation that spoke to the sales of certain age-restricted goods. For example, Poland currently forbids online alcohol sales as a result of its historically complex licensing limitations. A recent report by the European Commission argues for greater harmonisation in the sale of alcohol across Europe, recommending measures such as the adoption of 18 as the minimum age for alcohol purchase in all member states, requirement for age checks of all those looking less than five years above the legal minimum, and most notably, the banning of online alcohol sales because of "the lack of effective age verification systems."[31]

Although we are seeing a rationalisation whereby the sale of online goods are increasingly subject to the same age restrictions as offline goods, many countries struggle to outline effective verification strategies, just as we noted in the UK example above. For example, the German "Youth Protection Act" outlines that mail-order businesses, such as online retailers, may not sell age-restricted goods like alcohol or data media to underage consumers, but does not outline what counts as a *reasonable* attempt to verify a consumer's age. [32] Despite the vague legislation, German attitudes towards online sales reflect the country's emphasis on parent-child dialogue around responsible alcohol consumption.[33]   As such, policies on online sales and age-verification focus more on restricted media, such as pornography and violent games. In this context, the German self-regulatory body for tele-media (Voluntary Self-Monitoring of Multimedia Service Providers or FSM) works with the providers of age-restricted content and filtering tools to restrict access. Formal age-verification solutions are only employed with content deemed to endanger minors, such as pornography.[34] This creates inconsistencies about how content is accessed and who holds the power to restrict access – parents or industry. However, Germany is expanding its e-ID schemes, which may change the industry's structure.[35]

Little legislation exists to harmonize e-commerce age-verification techniques across Europe. Countries generally either adopt vague approaches or rely on offline methods, whilst current European contract law does not address age-verification techniques for the sale of online or offline goods.[36] The newly proposed Common European Sales Law attempts to simplify international sales. Currently, online retailers must individually respect the contract law of each member state. The legislation would supposedly create a common, simplified framework to encourage small retailers to enter the e-commerce market.[37] However, the proposed legislation does not reference age-

[30] http://media.ofcom.org.uk/2013/01/16/playboy-fined-100000-for-failing-to-protect-children/

[31] http://ec.europa.eu/health/alcohol/docs/eyes_on_ages_report_en.pdf

[32] http://www.bmfsfj.de/RedaktionBMFSFJ/Abteilung5/Pdf-Anlagen/jschg-englisch,property=pdf,bereich=bmfsfj,sprache=de,rwb=true.pdf

[33] http://iffor.org/sites/default/files/age-verification-white-paper.pdf

[34] http://iffor.org/sites/default/files/age-verification-white-paper.pdf

[35] http://iffor.org/sites/default/files/age-verification-white-paper.pdf

[36] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011PC0635:en:NOT

[37] http://ec.europa.eu/justice/contract/files/common_sales_law/sales_law_general_en.pdf

restricted goods, as these are subject to national variation and the subject of wide cultural sensitivity. Age-verification techniques may not be at the forefront of the Commission's mind, limiting this sector's international growth, but the progress made by small-scale pilots such as the STORK project suggest that there may be scope to increase political appetite in the future.

Social gaming

As noted during the literature review section, social gaming is still an emerging genre. As such, no genre-specific regulation has yet to arise but players and providers are of course still covered by existing regulation concerning e.g. consumer rights, advertising of adult content etc. Given some high-profile media coverage of concerns relating to issues such as high costs incurred by minors, the compelling nature of some games or the perceived similarity to online gambling, there has been vibrant discussion on the desirability of such regulation among stakeholders and some governments. Whilst there has been no new regulation yet, there have been some investigations of the sector in the light of its co-operation with existing legislation, largely in relation to consumer rights. In 2013, the UK Office of Fair Trading (OFT) conducted an investigation into free mobile game apps that are marketed to children and allow for in-app purchases[38], resulting in the publication of eight principles which industry should adhere to, if they wish to avoid being the subject of targeted enforcement action.[39] In similar vein, the US Federal Trade Commission (FTC) recently considered a class-action lawsuit against Apple Inc, on the grounds that they had allowed children make in-app purchases without parental consent. This resulted in a settlement requiring Apple to refund at least $32.5 million.[40]

Further general developments in consumer rights protection at the European level are likely to have an impact on the social gaming sector as it develops. A new European Directive on consumer rights (2011/83/EU) must be implemented in Member States by 13 June 2014, with little flexibility given to member states as to how it can be implemented. Article 6 of the Directive requires service providers to give consumers extensive information, thereby increasing the transparency of online contracts. For example, additional charges and the length of a contract must be communicated clearly to the consumer, as well as technical functionalities or possible issues with software and hardware interoperability. Article 22 prescribes that the service provider must seek the *express consent* of the consumer to any extra payment than originally agreed upon. These specific types of information may no longer be hidden in lengthy end-user licence agreements (EULAs). Article 3(3)(c) explicitly states that this directive will not be applicable to the gambling sector. Recital 31 of the Directive states that "[…] Member States should be able to adopt other, including more stringent, consumer protection measures in relation to such activities."

With regards to *aggressive practices*, the Directive prescribes that purchases must be made freely, without the use of harassment, coercion or undue influence. Recital 18 declares that "[w]here a commercial practice is specifically aimed at a particular group of consumers, such as children, it is

---

[38] http://www.oft.gov.uk/OFTwork/consumer-enforcement/consumer-enforcement-current/childrens-online-games/#.UoVEkpQkK6o
[39] Report: http://www.oft.gov.uk/shared_oft/consumer-enforcement/oft1506.pdf
Principles: http://www.oft.gov.uk/shared_oft/consumer-enforcement/oft1506a.pdf
[40] http://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million

desirable that the impact of the commercial practice be assessed from the perspective of the average member of that group." The recital allows Member States to develop a "list of practices which are in all circumstances unfair a provision which, without imposing an outright ban on advertising directed at children, protects them from direct exhortations to purchase." National courts and authorities are given the discretion to determine "the typical reaction of the average consumer in a given case."

The practical enforcement of consumer rights differs per country. For example, in the UK a strongly decentralised organisation called Trading Standards enforces a wide range of legislation on a local level. When confronted with more systemic failures in a market, the powers previously held by the national Office of Fair Trading will shortly pass to the Competition and Markets Authority. While other European countries have similar national authorities that address market failures or even have the competence to take a case against an individual firm, the regional and local enforcement of consumer rights differs significantly. Denmark, for example, has one main consumer organisation called the Forbrugerrådet (Danish Consumer Council). Spain, France and Italy have a much wider landscape of consumer organisations with diverging interests, competences, methods and procedures. It goes beyond this study to give a full account of the consumer organisations in each country but it remains to be seen whether the often decentralised approach to consumer protection will offer effective protection to online consumers using services which may originate outside national state boundaries.

Consumer rights legislation is not the only regulatory framework likely to impact the development of social gaming responsibilities in relation to the protection of minors. PEGI, the game classification scheme informs parents and children of game content and, in some countries such as the Netherlands and the UK, is used to legally demarcate the minimum purchase age for a game, with consequent legal penalties for retailers if this is disregarded.[41] Game classifications make content-specific recommendations based on explicit sexuality, violence, or other socially-undesirable behavior, although the efficacy and accuracy of such rating systems is not without its controversies. For example, a cursory review through the US's Entertainment Software Rating Board (ESRB) classification listings found that some simulated gambling games were rated E for Everyone with "no descriptors," while others were rated Teen for "simulated gambling." Classification schemes guide parents, even though they may not tackle the complexities of how games impact behavior. Games are also informally classified through gatekeeping bodies like the App store, which segments games based on genre. However, it is challenging (and potentially costly if any sort of liability is involved) for even centralised gatekeepers to keep track of what children access and how games are classified, particularly given the competing pressures of the need to both sell as many games as possible whilst protecting minors. For example, one academic study suggests that of the 65,000 games labeled "educational" on the App Store, very few have been verified for educational potential (Goodwin and Highfield 2012).

Another point of concern for regulators has been the possibility of risks resulting from the 'social gambling' subset of social gaming. The UK's gambling commission recently finished its own review of

---

[41] PEGI. "Pan European Game Information." *PEGI Homepage*. Retrieved from: www.pegi.info

social gambling risks (Parke et al 2013), identifying potential risks related either to problem gambling behavior or consumer exploitation. To the extent that these risks are already recognized in existing regulatory frameworks, the Commission argued that further regulation would be needed only if the identified risks could not be mitigated by responsible self-regulation, consumer protection laws, and the current oversight responsibilities of OfCOM and the Advertising Standards Agency.[42]

VI Technical means of restricting access by age

The challenges of identifying minors

In their review of online child safety, the 2008 US Internet Safety Technical Taskforce concluded that in the face of a wide array of online risks, multiple factors feeding those risks, and numerous different technical platforms, that no one technological solution could protect children online. Instead,

> "Parents, teachers, mentors, social services, law enforcement, and minors themselves all have crucial roles to play in ensuring online safety for all minors – and no one's responsibility to help solve the problem should be under-valued or abdicated." (Internet Safety Technical taskforce 2008: 37)

This doesn't mean, however, that technical solutions might not be feasible within specific contexts. Indeed as the Sparrow report, issues from Harvard at around the same time, concludes in relation to the risks of online gambling for minors:

> "Regulatory mechanisms and technological solutions, many of which are currently used in other jurisdictions and industries, can equip online gambling operators with capabilities to selectively exclude minors from engaging in online gambling. Age verification policies would be less effective in the absence of support from minors' parents and guardians; therefore, a successful regulatory strategy would provide tools with which parents can limit access to gambling websites by their children. We believe that online gambling can effectively exclude minors when it combines cutting-edge technology with a strong regulatory regime." (Sparrow 2008: 23).

Since those two reports were published, developments in identity assurance technology have progressed rapidly, and although some challenges remain in applying these technologies to minors rather than adults, the possibility of using age verification tools for broader online child protection purposes is now a real option, at least in terms of confirming that service users/consumers are over 18. Research carried out to date reveals the challenges of extending this to those under-18, for

---

[42] See http://www.gamblingcommission.gov.uk/gambling_data__analysis/social_media_gaming_and_ga.aspx

example to allow for the purchase of age-restricted goods where the legal minimum is 16, or to support COPPA-style identification of those under 13 for the purposes of data collection and processing. In order to contextualise the findings about age verification practices obtained through our interviews, in the section that follows below we outline some of the main developments in identity assurance technologies, and go on to assess the significant disparities that exist between the quality, rigour, reliability and value to businesses of existing identity and age verification solutions that cater for the adult demographic (aged 18+) and the younger demographic (aged 17-). Note that the majority of information collected here is derived from market reports and industry news rather than academic sources.

Identifying and verifying adults is still easier

There are now numerous databases, such as the electoral role, credit rating databases, address information, against which it possible to corroborate the identity and age information that an individual asserts. One of our interviewees estimated that in the UK, up to 85% of the adult population can be ID validated with good access to data sources. The remainder of the adult population, who may or may not have bank accounts, typically lack a strong credit history or may have recently moved to the UK, and exception-handling processes are required to validate the identity of these individuals. In other European countries where access to datasets against which asserted identity details can be cross-checked is poor, this coverage can drop to 60% of the adult population. Crucially, children and young people are not likely to be listed on the most easily accessible public datasets such as driving license registers, credit reference databases or the electoral roll; nor do they usually have an extensive digital footprint. However, in countries such as Belgium, Denmark and Spain, children aged 12 years old and above, (sometimes younger) have national ID cards and where countries have migrated to eID's children will also have electronic identities. Electronic identities afford children the opportunity to share attribute information such as their age group, in online environments where age gating needs to be applied. (See for example the Belgian STORK Chat research and other alpha projects being conducted across Europe).

To illustrate the other important disparities between age verification processes for the adult and young demographic it is useful to consider instances where it is a legal requirement for commercial entities to corroborate the information a consumer asserts online with respect to their identity and age when wishing to engage in certain activities, e.g. online gambling. Traditionally, data aggregation businesses and /or a Credit Reference Agency (CRA) provide both identity and age verification services and consumer credit information for regulated business sectors targeting adults, for example, banking, telecommunications, gambling, retail and the public sector. There are recognised sets of rules and standards governing the business, legal and technology aspects of the identity and age verification processes for the adult demographic and these apply in different countries around the world, although the level of access to the requisite datasets can vary significantly from country to country. In a UK context, there is clarity with respect to the levels of assurance associated with the validation of identity and age related details. For example, financial services firms are subject to stringent 'know your customer' and 'anti-money laundering' regulations. Furthermore, in the UK the Consumer Credit Act 2006(c 39) stipulates that a Credit Rating Agency (CRA) requires a licence to operate and this level of legal oversight increases the business sectors confidence when using CRA's. In addition, there is clarity around liability issues relating to the use of identity and age verification

services for the adult demographic such that all stakeholders should have a clear understanding of what constitutes strict liability offences.

Perhaps most importantly, there are viable commercial models underpinning identity and age verification solutions for the adult demographic. Businesses can negotiate fees based on the volume of requests and offset the costs incurred either against revenue or the price a consumer pays for a product. For sectors such as the licensed online gambling sector, strict audit and enforcement requirements mean that direct competitors face the same pressures, and investment in establishing high-assurance identity and age-verification processes is worthwhile. In sectors which technically require either identity or age-verification, but where enforcement is patchy and uncertain, the incentives to invest in expensive authentication systems are less clear unless reputational damage is clearly at risk. This is particularly true when the product or service to be purchased may just be a one-off with little possibility of recouping the costs over a longer consumer relationship.

Developments in identity assurance

In addition to these formal, top-down methods for identity assurance and age verification, the past five years have seen a large growth in open source community initiatives, which provide a radically decentralised approach to online identity management, and perhaps, in the future also age verification. In 2005, OpenID[43] was created by an open source community and is an open standard that allows users to be authenticated by certain co-operating sites (known as Relying Parties or RP) using a third party service. OpenID authentication is used and provided by several large websites. Providers include Facebook, Google, Yahoo!, PayPal, BBC, AOL, LiveJournal, MySpace, IBM, Orange and VeriSign. Users may create accounts with their preferred OpenID identity providers, and then use those accounts as the basis for signing on to any website which accepts OpenID authentication. The OpenID standard provides a framework for the communication that must take place between the identity provider and the OpenID acceptor (the "relying party"). The OpenID Foundation was formed in 2007 to assist the open source model by providing a legal entity to be the steward for the community by providing needed infrastructure and generally helping to promote and support expanded adoption of OpenID.

Although OpenID was initially a standard used to assert and authenticate identity, recent innovations mean that it may become much more usable for age verification purposes. Specifically, an extension to the standard (the OpenID Attribute Exchange) facilitates the transfer of user attributes, such as age, from the OpenID identity provider to the relying party (each relying party may request a different set of attributes, depending on its requirements). Vitally, the OpenID protocol does not rely on a central authority to authenticate a user's identity, and may be able to capture the credentials of a wider range of citizens through the large number of authenticating partners that users can choose to create their identity account.

Existing age verification services for minors

Despite the high barriers to entry into the identity and age verification sector and the lack of easy access to datasets relating to the children and young people there are a number of providers of age verification solutions for the young demographic on the market. The value proposition underpinning

---

[43] http://openid.net/

these solutions is improved child safety that will purportedly be achieved by enabling the means to do the following; *'prevent'* children accessing age-inappropriate or harmful content and *'protect'* children from encountering cyber-bullying and the advances of predatory adults operating online. The European Data Protection Directive requires operators to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

Most providers of age verification solutions for the minors require a parent to submit data about themselves, which can be checked against various databases. A verified parent can vouch for a child, confirm the child's age and give parental consent so that other companies can corroborate the age information a child asserts. Both the providers of age verification solutions for the young demographic and child protection advocates have focused on the Internet industry as potential users of these solutions. However, it is not necessarily possible to verify the relationship between a verified adult and the 'child' for whom the adult is vouching. This leads to a number of uncertainties about the level of assurance that can be attributed to both the age-related data about a young person and the legal status of the 'consent' the adult gives on a child's behalf, since both are open to repudiation. When age verification services for the adult demographic are juxtaposed with those for the young demographic the absence of equivalent agreed standards as to the level of reliability of the data checks and the corresponding level of assurance associated with the results is particularly problematic.
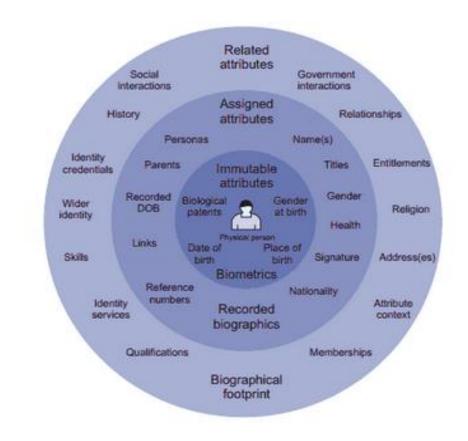
It has proved challenging to develop a viable commercial model for such age verification solutions as so far, the focus has mainly been on websites aimed at children and general audience sites that typically are free to use, which helps to explain why it has been difficult to develop a viable commercial model. Further, unlike age verification processes for the adult demographic where what constitutes strict liability offences is clearly outlined in legal guides for all stakeholders, the same level of clarity and legal oversight does not currently exist with respect to age verification for those under 18. Both of these factors combine to make granular age verification of minors currently an unattractive proposition from a business perspective.

One other oft-raised possibility is that banks might serve as guarantors of identity and age information for minors. Across Europe, legal provisions with respect to 'Know Your Customer' and 'Anti Money Laundering' require banks to check the authenticity of a number of identity documents in a face-to-face setting prior to opening a bank account for a young person. These legal requirements suggest that banks hold age-related information about their customers. However, once again, the absence of clear liability and commercial models and an agreed set of standards and protocols underpinning age verification, renders this a highly unlikely option. Banks have argued that whilst data about young customers' identity and age was checked for the purposes of opening an account, it was not necessarily stored on databases in a manner that could be easily queried. Furthermore, to be 'fit for purpose' that data, most likely, would have to be put through a costly data cleansing process. Against these oft-raised concerns, it is notable that the Danish government and the Danish banking sector do cooperate in the area of identity management. Our interviews with Danish stakeholders suggest that the system is largely considered to be a success, as will be discussed further in the Analysis section.

Future Models of Age Verification for Minors

Within the electronic identity ecosystem are organisations called attribute providers, who are responsible for all the processes associated with establishing and maintaining a subject's identity attributes. Attributes are what make up an identity; the little bits of information about you that say who you are. They fall into three categories:

- Immutable attributes - these are facts which cannot change, i.e. your biological parents and your date and place of birth, as well as certain biometrics such as iris colour and pattern.
- Assigned attributes – this is recorded biographical information, i.e. name(s), titles, personas, gender, health, signature, nationality, reference numbers, links, recorded date of birth, and 'assigned' (e.g. adoptive) parents. Assigned attributes are the ones used for official purposes, like government services.
- Related attributes – these are the details that are deemed to comprise your "wider identity", and result from your interaction with the world. They need to be kept updated because these types of attributes can be changeable. They include your address, your work details, your government/ social/financial interactions, skills and qualifications, the personas you use, memberships, and even your religion, your relationship details, your 'history', and the context of each attribute. Together these details are said to comprise your biographical footprint.

Figure 1.0: Individual attributes[44]

An attribute-based approach provides more than just a flexible model of age verification, making better use of a child's more limited digital footprints, it also addresses privacy concerns, which are a paramount consideration, particularly in relation to children. Age or the age band that applies to an individual is simply an attribute of their identity; e.g., I am over 12 years of age (or 16, or 18, or 21, or 65) or I'm under 12 years of age etc. Similarly, being a student or in receipt of a pension are attributes that may be particularly salient in certain transactions, but vitally, these are not uniquely identifying because they apply to other people too. As such, attribute providers can afford Internet users with a means to reveal certain salient bits of information, which are relevant or required to carry out a transaction. If non-identifying attributes are utilised in a transaction, this has numerous advantages, particularly from a privacy perspective. The concept of Attribute Based Access Control (ABAC), i.e. providing access based on the evaluation of attributes has existed for many years[45] in the corporate and government sectors. The process of working out the assurance levels associated with different attributes when utilised within a citizen centric context and on the wider Internet is in progress.

In the context of the anticipated mass adoption of mobile wallets and the emergence of payment apps, which leverage bank-to-bank payment mechanisms, an attribute-based approach opens up the potential for mobile operators and banks to play the role of trusted identity providers. Mobile operators and/or banks, with the consent of users, could play a broker role authenticating their customers' identity credentials (including age) with replying parties. Despite the concerns outlined earlier in relation to banks' use of credit cards as an age guarantor mechanism, both banks and mobile operators seem more receptive to the idea of introducing age attributes into new and emerging payment protocols. A number of these discussions are already taking place within and the GSMA (Global Speciale Mobile Association) are conducting a pilot project in Q1 2014 to test the feasibility of introducing age attributes into payment protocols.

Crucially, electronic identity ecosystems and in particular attribute providers not only have the potential to re-dress the disparities between identity and age verification solutions for the adult and the young demographic but to develop more efficient, scalable, privacy preserving, viable, low cost solutions, in turn, enabling young people to become active participants in the digital economy. The electronic ecosystems and the related emerging attribute economy may, in the close future – within 2 to 5 years -, meet the growing market need for age verification solutions that cater for minors. Underpinning this technical innovation with appropriate regulatory frameworks internationally recognised standards, robust legal and policy oversight, viable liability and commercial models) will be essential to encourage various business sectors to adopt these solutions win over consumer confidence.

---

[44] Aspects of Identity Yearbook 2011-12 BCS Identity Assurance Working Group https://docs.google.com/viewer?url=http%3A%2F%2Fwww.bcs.org%2Fupload%2Fpdf%2Faspects-of-identity.pdf
[45] NIST Special Publication 800-162 Guide to Attribute Based Access Control (ABAC) Definition and Considerations (Draft) https://docs.google.com/viewer?url=http%3A%2F%2Fcsrc.nist.gov%2Fpublications%2Fdrafts%2F800-162%2Fsp800_162_draft.pdf

VII Analysis

Employing age verification measures: assessments about risk and harm

Against this backdrop of evidence about children's use of online commercial goods and services, and the accompanying risks and harms, we can explore the efficacy of existing measures (regulatory or self-regulatory) initiated to protect minors from accessing goods and services perceived to inappropriate for their age-group. It should, of course be acknowledged that regulation (which in this context covers state interventions as well as co or self-regulatory options) is not necessarily, indeed rarely purely evidence-based, and that there are many important different factors beyond child welfare to be taken into account when determining policy. However, the evidence of risk and harm set out in the previous sections provides an important foundation for regulatory decisions, and indeed for company strategy in entering markets, product design and marketing.

Brownsword (2012) suggests that there are four different challenges facing policy-makers dealing with new technologies: the need for regulatory prudence, regulatory legitimacy, regulatory effectiveness and regulatory connection. In most circumstances, it would, for example, be self-defeating to require the introduction of protective measures with such a high economic cost that the company or industry would cease to be viable, but it would be equally absurd to introduce regulatory measures which were toothless and ineffective. These principles inform the analysis of our data, together with literature on the effectiveness of existing regulatory frameworks protecting children in the activities discussed in earlier sections (e.g. Livingstone et al 2012; Staksrud 2013; Gainsbury & Wood 2011; Nair 2012).

It is worth noting upfront that the three sectors considered here present rather different evidence bases for risk and harm. The literature relating to smoking and alcohol is quite unequivocal in its message that real physical harms result from the use of these products, and that the effects may be greater for minors. The case is somewhat more controversial in relation to other age-restricted goods such as DVDs or games, which rely on the study of media effects, but there is at least a degree of political consensus around the need to protect minors from exposure to heavy sexual or violent content. The same seems to apply to online gambling. In the academic literature reviewed, the concept of problem or pathological gambling has become an accepted concept almost despite the methodological difficulties of identifying the weight and importance of the various factors contributing to the problem, or even the full extent and nature of the harms caused. However in the gambling industry, respondents are very accepting of the concept of risk and harm to individuals, and our interviewees have so far been unanimous in recognising a potential risk of young people developing patterns of problem gambling behaviours. Similarly, in discussions with a children's charities representative about the risks posed by purchasing of alcohol online, the nature of the risks and harms was very much taken for granted, and was juxtaposed by a sense of almost disbelief that in the face of good academic evidence of risk, so little political or enforcement resources seemed to be dedicated to the problem. In the social gaming case, there is as yet no significant empirical evidence suggesting that harms, other than financial harms, are resulting from minors' use of these games. In the few interviews conducted around social gaming, this uncertainty was referred to in the

context of media reports which are quick to provide more inflammatory stories of possible harms.

Measures used to verify age

As noted above, Europe currently lacks a harmonised legislative framework regulating online gambling, and interviewees from across the gambling sector viewed harmonisation as possibly desirable but highly unlikely to arise in the near future. In line with the fragmented picture across Europe, most countries in which online gambling is legal have chosen to apply detailed licensing restrictions with conditions unique to each state, the terms of which impact decisions of operators to have a presence in these markets. Several interviewees suggested that their companies had decided not to seek a license in France, for example, given certain characteristics of its licensing regime.

Interviewees from across 12 online gambling companies and 4 national regulatory bodies described three different approaches deemed to meet both identity and age verification requirements:

1. Purely online systems which leverage existing electronic identity architectures (Denmark, Italy and Spain)
2. Purely online systems which leverage a range of publicly accessible data sets (UK)
3. Offline submission of physical copies of identity documents (France).

Participants noted that no single approach to age verification is 100% reliable in every circumstance, meaning that one or more of these ID and age verification methods may have to be utilised to verify the identity and age of a new customer.

Gambling operators and regulators deemed the first method, i.e. leveraging electronic identities as their preferred method of age verification for a wide variety of reasons. In terms of customer experience it is fast, reliable and convenient, often taking just split seconds to complete, therefore offering a relatively seamless on-boarding process. This method also has clear benefits for online gambling businesses even beyond the positive customer experience. It was noted to offer several operational efficiencies, as well as lower levels of both fraud and identity theft, whilst the costs (although not insignificant) are bearable given the ease of the solution. Furthermore, leveraging electronic identities offers a scalable solution underpinned by clear liability models. The different electronic identity architectures developed in countries around Europe can, in theory, interoperate and the levels of assurance associated with the checks are in the process of being standardised and should soon be mutually recognised. In June 2012 the European Commission published its enhanced proposal for a Regulation on *"electronic identification and trust services for electronic transactions in the internal market"* to enable cross-border electronic authentication services in Europe, ensuring the mutual recognition and acceptance at EU level of notified electronic identification schemes and other essential electronic trust services.

The European Commission has heavily invested in extending to organisations the benefits of secure cross-border electronic authentication and identification while offering them and European citizens new services and solutions based on electronic identity, via the STORK 2.0 (Secure idenTity acrOss boRders linKed 2.0) project[46]. Crucially, in some states, children and young people are also issued with electronic identities, helping to remove a significant barrier to verifying the age of a person

---

[46] https://www.eid-stork2.eu/

aged 17 and below. The benefits of children and young people using aspects of their electronic identities, and in particular, their age attributes, has been tested in STORK pilot projects such as the school e-learning project SaferChat[47] and an Age Attribute Quality Assurance Framework is being developed by the current STORK project.

In countries such as the UK where work is still in progress in terms of developing electronic identities for UK citizens that do not rely on a centralised database, identity and age verification checks are conducted by third party services such as Experian who specialise in querying publicly accessible datasets such as the electoral roll, the drivers' license database or credit rating agencies. A crucial factor here concerns the coverage of these datasets. One industry figure suggested that in the UK up to 85% of all adults are covered by these publicly accessible databases, whilst Experian's own website claims that up to 90% of Betfred customers were passed first time using their services.[48] Whilst none of our interviewees focused on the security of this approach, the lack of reliance upon one single centralised database might also be deemed an advantage. As in the previous case, our interviewees presented this method as a commercially viable and scalable system, trusted by both businesses and customers, although the preference was still for e-ID systems where possible..

The third method of identification and age verification described by our online gambling interviewees requires the customer to complete the process offline by sending in or presenting copies of identity documents. This is clearly appropriate in countries that have not rolled out electronic identities to its citizens or where there isn't easy access to data sets, but it may also result from a cultural or political reliance on notarisation. It's also important to remember that whilst some states were early adopters of electronic identity schemes for online interactions with government, the use of such schemes for corporate compliance is still quite new, and we may well see a shift from more traditional offline means to such newer online schemes as they become more tried and tested. Although we were unable to gain access to the French online gambling sector, several interviewees from other countries noted that many in the industry perceive this approach to be a disproportionately burdensome response to AV and identification requirements. In particular, attention was drawn to the difficulties of breaking the customer experience and inserting possibly lengthy delays before play could begin or winnings be extracted. It does, however, bear some interesting parallels with methods of offline verification applied in the online retail sector, specifically where proof of age is checked physically upon delivery of goods, rather than online at the point of sale. This method will be discussed further below.

Retail Sector

The online retail sector clearly covers a very diverse array of businesses. Whilst we originally set out to interview companies selling alcohol online, it soon became clear that some very interesting challenges also apply for general retailers such as Amazon, Argos or the supermarkets, who sell a number of products with very different age ratings. For this reason we expanded our interviews to include retailers from these other sections of the industry. A number of representatives from the

---

[47] https://www.eid-stork.eu/pilots/pilot2.htm
[48] http://www.experian.co.uk/assets/identity-and-fraud/betfred-case-study.pdf

retail sector were interviewed, including members of various Trade Associations that represent the grocery, DIY and alcohol sectors.

It was obvious from all the interviews conducted that this sector is far less reliant upon sophisticated online identity or age verification methods. The most common reason given for this was cost, but concerns were also raised about potential delays for customers. It is worth noting that the very different business models underlying online retail and online gambling no doubt explain the reliance on different AV procedures. Retail interviewees mentioned the low profit margin on goods sold, and the degree of competition in the market. Sales might be just one-off transactions rather than the start of an on-going commercial relationship meaning that there was less likelihood of recouping the transaction costs of the high-assurance identification and AV methods employed in the online gambling sector, unless these were to decrease substantially in the future. It's worth noting on this point, that it's not clear that it would be necessary for online retailers to gain such a high level of assurance, and that the level required might vary across products (alcohol or knives might be deemed more risky than DVDs, for example.)

Despite the marked absence of reliance upon e-ID databases, our retail interviewees did highlight a range of AV methods employed. The most rigorous methods employed relied upon checking customer details with publicly accessible databases. One online wine company, specialising in the regular dispatch of cases of wine, did employ a third-party database search, as the closest equivalent to methods employed in the online gambling industry. This investment was deemed appropriate in part because of the reputation of the company, but it is also clear that the company's business model of repeated, high-worth transactions meant that this was an affordable decision. Another general retailer noted that they used the same service but without the need for an instant response. This was deemed acceptable because of the delay between purchasing goods and their delivery, and presumably enabled the firm to benefit from lower cost AV transactions. In other cases, a common strategy was to rely upon a combination of tick-box/self-assertion and credit card use, even though the latter is not a definitive proof of age. Where businesses employ their own in-house delivery staff, there is also a tendency to rely upon physical age verification, with the driver expected to check whether or not the recipient is of the appropriate age, and if not, to challenge them for identity and age documents. In practice, it might be expected that the possibility of confrontation or the pressures of a heavy delivery schedule would make such challenges less likely.

Perhaps the most interesting insight was the business model of one company we interviewed, who, by only selling multiple bottles of beer or wine, felt that this would be unattractive to underage drinkers who would usually choose lower-cost sources of alcohol. In addition, this same company had instituted a governance system maximising individual responsibility, whereby local shops were responsible for dispatching deliveries within their surrounding area. The manager of these local shops was awarded a license to sell alcohol by the local authority, and if any cases of under-age selling were revealed, would risk losing his license.

One benefit of focusing on online alcohol sales was that this enabled us to consider the age verification procedures used in the advertisement of 18+ rated goods. Advertising alcohol online through engagement marketing techniques on social media platforms relies on those platforms to age-gate users, i.e. only those platform users who have self-asserted that they are aged 18+ years old should see the alcohol adverts. In this context, our interviewees did recognise that social

networks such as Facebook or Twitter do not currently apply rigorous age verification procedures when accounts are set up, and to this extent such advertising practices may mean that underage social network users are exposed to adverts intended for those aged 18 and over. Our interviewees noted that because of the uncertainty about the SNS user's age, their advertising policy was often revised such that adverts would only be shown to those claiming to be 21+ or even 25+. But a recent small-scale study by the UK ASA noted that minors are being shown age-inappropriate adverts on social media, although there is little evidence that advertisers are not acting in good faith (ASA 2013). The alcohol industry recognises that this current reliance on self–asserted age-related data poses a potential threat to their commercial freedom to advertise their products online and as such there is a developing appetite to explore alternative solutions. This commitment is articulated in a document that outlines the Global Beer, Wine and Spirits CEOs backing of '*New Initiatives to Reduce Harmful Use of Alcohol Commitments on digital marketing, underage drinking, retail activities and drink driving'*[49]

Another area of concern for retailers relates to PEGI age-rated content i.e. films and games, (12+, 16+) where, in a UK context this rating is now underpinned by legislation meaning that it is illegal to sell an age-rated game to someone aged below the stated age-rating. Our interviewees noted the great difficulty of identifying the age of consumers down to this level of granularity when most databases can only prove that a customer is an adult, not that they are of a child, and furthermore, a child age 13 or 15. Despite the legal risks, one interviewee from a large general retailer noted that they didn't worry too much about a 13-year old buying a 16-rated game or film, but that they would take more care when selling 18+ rated products.

Other challenges arise with the evolution of customer shopping habits. For example, more and more customers are buying goods via their mobile device and coming into shops to collect goods, sometimes minutes later, which narrows the time frame available to retailers to conduct identity and age verification checks – compared to the one or two day window before a retailer delivers items to a customer home address. A number of competitors in the retail sector, such as Amazon, are exploring the use of unstaffed locker systems[50] in local shopping centres where customers can collect goods purchased online which removes the scope for delivery people to engage in age verification checks.

Historically, data sets held by credit rating agencies and data bureaus do not contain data with respect to children and young people, largely due to data protection and privacy constraints. Retailers contend that the absence of easy access to datasets that would enable reliable age verification of customers aged 17 years of age and below means that the only feasible approach is to use a tick box reliant on self-asserted age. Interviewees suggested that this part of the retail sector is actively looking for more effective age verification techniques. Existing practice may be less than satisfactory, but it is important to remember the political and economic realities which under-gird decisions to invest in compliance systems. For example, it is hard not to be sympathetic in the UK context where there are few appropriate sources of age data for minors, but the law requires age

---

[49] Global Beer, Wine and Spirits CEOs Back New Initiatives to Reduce Harmful Use of Alcohol Commitments on digital marketing, underage drinking, retail activities and drink driving (Retrieved 25 November, 2013) http://www.icap.org/LinkClick.aspx?fileticket=%2FyL9WsqsP4g%3D&tabid=36

[50] Amazon's New Secret Weapon: Delivery Lockers http://online.wsj.com/news/articles/SB10000872396390044354550457756776382 9784538

verification and an absence of predictable enforcement regimes means that even responsible retailers face unfair competition from companies unwilling to invest in appropriate age verification methods. In countries such as Denmark or Belgium, where there are more extensive databases of children's data that could be leveraged, the case for action seems rather stronger, and further research considering cases such as Estonia where electronic identities are far more widely used in retail transactions would certainly be beneficial.

Some of our retail interviewees noted that despite the lack of easily useable age verification data sources, members of retail trade associations do adhere to the principles of professional diligence as described in the Unfair Practices Directive[51], implying that existing checks need not be 100% accurate so long as appropriate diligence was shown in the method of checking. In a UK context, the retail trade association is actively involved in discussions with both the UK Government and the GSMA's Mobile identity Initiative to explore ways to gain access to reliable data, i.e. age attributes which may in future, for example, be included in online payment mechanisms and which could better support such principles in the future.

Social Gaming

Within the social gaming sector, there are a very wide variety of businesses operating, including companies that primarily produce online gambling products, companies occupying the social gaming space, and businesses developing games targeted at children aged 12 years of age and under. Firm size may range from a one-man/woman app developer to a large international company with many other products. We sought to interview representatives across these different parts of the sector, but it proved remarkably difficult to gain access.

Given the variety of businesses in operation, and the range of products on offer, it is no surprise that there are different approaches taken to age verification. As a new and emerging sector with at present, little evidence of risk or harm to players, there are few regulatory requirements pressing firms to check users' age or identity. The main regulatory framework with implications for AV is the US Children's' Online Privacy protection Act (COPPA) which requires that verifiable parental consent to process a child's personal data is sought in games targeted at players aged 12 or under. Although this law applies just to the US, many games manufacturers design their procedures to work within both the US and other jurisdictions. In effect, this law means that parental consent has to be sought via 'Email Plus' in which an e-mail is sent to the child's parent requesting parental permission for a child to access a game. From a business perspective, one interviewee informed us that in their experience, Email plus is an unreliable method of obtaining consent because there is no way of knowing if a child has provided a parent's email. Furthermore, that individual claimed that over 20% of automated emails the company sends to "parents' end up in a Spam folder resulting in a

---

[51] Professional diligence is defined (in Regulation 2 of the Consumer Protection from Unfair Trading Regulations 2007 as: 'the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers which is commensurate with either — (a) honest market practice in the trader's field of activity, or (b) the general principle of good faith in the trader's field of activity, or both -(Retrieved 25 November, 2013) http://www.oft.gov.uk/shared_oft/reports/consumer_protection/oft931con.pdf

proportion of children not being able to access the games they wish to play or spend money. This results in poor customer experience and loss of potential revenue for the company.

Although recent investigations into consumer protection issues relating to social gaming have shown regulatory concern for the potential exploitation of minors through aggressive or non-transparent selling in *freemium* games, there has as yet been no requirement for games producers to determine whether or not it is a child that is playing. This may change when the new Consumer Rights Directive comes into effect, especially if the social gaming industry chooses not to self-regulate by improving the transparency of procedures for, and costs of, in-app purchases. For this reason, it was not surprising that we found little evidence of age verification procedures in regular use, although it is notable that online gatekeepers for example, Apple App store do group and list games and apps considered to be child-friendly, whilst also age-rating all games for content and declaring the possibility of in-app purchasing. The latter developments, introduced in April 2013, are intended to provide guidance and transparency for parents, but is not accompanied by any requirements to prove a child's age before a download is completed.

One interesting research finding relates to awareness of and interest in age verification procedures. That part of the industry with a history of serving the social gaming community of children aged 12 years old and below has a greater depth of experience with respect to handling regulatory requirements, and perhaps unsurprisingly, representatives of this sector recognise the importance of employing effective age verification techniques. There is evidence that some of these social games developers are already actively seeking viable age verification solutions and understand the potential to leverage both electronic identities architectures and new payment protocols to not only to ensure regulatory compliance but to improve customer on-boarding processes, generate revenue and enable innovation and business development. Initiatives such as the $1.6 million grant issued by the US National Institute for Standards and Technology to privacy company PRIVO for piloting a new Trust framework for minors are helping to drive rapid developments in this field, and we can expect to see the emergence of an expanding range of products that enable retailers and game developers to engage safely with young consumers.

Individual companies in the social gaming arena that design games with mass appeal, were also invited to participate in this programme of research but almost all declined. We did speak to individuals at two companies selling social games as well as a representative from the newly formed International Social Games Association (ISGA). In each case, interviewees were clear that they met whatever regulatory responsibilities required of them in relation to protection of minors, although this did not mean that they were required to implement any sort of age verification. Since the interviews took place, the ISGA has since merged with the Social Gaming Association and now represents Zynga, Slingo, RocketPlay, Plumbee, Playtika, PlayStudios, MGM, IGT, High Five Games, Gamesys, Big Fish Games, Bally Technologies, Aristocrat, Akamon and AbZorba Games. The Association has responded to media and policy concerns about its conduct by developing a set of 'Best Practice Principles' for responsible self-regulation[52].

Given the on-going speculation about the possible effects of social casino gaming, i.e. games that simulate gambling, it is notable that these Principles do make reference to the responsibilities

---

[52] http://www.i-sga.org/best-practice-principles/

associated with the marketing of such games. The ISGA has developed best practice that seems intended to address concerns about social casino gaming as follows:

- Casino style social games should specify that the games are intended for use by those 18 or older **and/or** provide advice to parents and teens on making smart choices online
- Advertisements for casino style games should not be deliberately or explicitly directed at those aged below 18 years.

It would appear that the ISGA has age-rated social casino games as suitable for players aged 18+ years of age, but rather bizarrely, has also included what is effectively an opt-out clause, suggesting that casino style games *can* be targeted at a younger age group if advice is provided. These principles raise questions with respect to which age verification techniques, if any, the ISGA envisages its members applying in a social casino gaming context, for example, will they recommend age-gating on platforms, self-asserted age tick box or pop-ups that indicate to players they must be 18+ to play? These efforts at self-regulation are set against a backdrop where calls for social games to have age certificates similar to films are growing louder, as an Australian state announces plans to rate social games for gambling-like content[53]. In a UK context the statutory status of PEGI age rating system raises an interesting set of issues for both online retailers and possibly parts of the social gaming sector.

Adequacy of these measures

Having explored the nature of risks and harms which underpin age-restricted access to goods and services in our three case studies, we can assess the adequacy of the measures applied. Perhaps most obviously, it's quite clear that the age verification processes developed and applied in the licensed online gambling sector display an admirable level of efficacy in countries where customer details can be checked against public databases offering high levels of ID assurance. It's still not possible to verify 100% of customers through online databases, in part because many databases used (such as national identity registers or electoral rolls) will not necessarily cover foreign nationals, whilst in other cases there may be errors in the data. Both regulators and corporate interviewees stated that they do see instances of customers attempting to lie about age but that these are few in number, for example one regulator claimed to see fewer than 20 reports of underage breaching per year. Further, these are split between minors attempting to access gambling products, and adults pretending to be children in order to attempt to recoup a loss (deposits must be returned to any minors found to have gambled). This low level of attempted age fraud reflects the view of an interviewee from the children's charity sector that implementation of online AV methods, required by law has made a substantial difference in reducing risk to minors:

> "Gambling is in a class of its own, there's no question about that. Since the 1st of September, which is when the relevant provisions of the gambling act in 2005 became operative in the United Kingdom, we have not heard of a single case, literally not one, where a child has been

---

[53] State Government plans to classify gambling apps to protect children from addiction
http://www.adelaidenow.com.au/news/south-australia/state-government-plans-to-classify-gambling-apps-to-protect-children-from-addiction/story-fni6uo1m-1226762792077

able to do what they did before the act, which was tick a box and say I'm 18 and go online and gamble. That's quite, that's quite something."

Importantly, in the licensed states that we investigated, every instance of fraudulent age claims must be reported and will be noted in the annual review and audit that licensed operators undergo to ensure compliance with all legal requirements. As eCOGRA, the main provider of such services, notes on its website, such audits typically cover:

"…player payments and receipts, record retention, internal security requirements, responsible gambling, player and gambling funds and IT security over player information… (h)igh risk areas of anti-money laundering procedures, control over advertising and promotions and probity requirements."[54]

The requirement of regular audit and review is a key feature of the licensed online gambling business model insofar as it imposes an equal (and predictable) burden on all licensed operators. Given that it is costly to establish and operate high assurance ID and AV procedures, it's important that operators know that their investment will be noted and rewarded (by continuation of a license), and equally vitally, that each company can be sure that its licensed competitors will also comply. To that end, one of the biggest sources of irritation for the responsible operators that we interviewed, is the ease with which customers can turn to unlicensed competitors whose operation may be illegal, but very difficult to prevent. Clearly, enforcement doesn't offer the only incentive to provide responsible, reliable AV systems – major international gambling companies undoubtedly also value their reputation as responsible actors within an industry which is regarded by some as morally dubious, and, as will be discussed further below, there are also important business advantages which flow from knowing more about your customers.

Before leaving discussion of enforcement, it's worth noting that this issue has great relevance for the online retail sector. It may be illegal for online stores in different European jurisdictions to sell alcohol or knives to minors below a certain age, but if such legislation is rarely or patchily enforced, then there is little incentive to invest in reliable online AV systems. This is especially true for smaller or less well-known companies who are also less likely to receive reputational damage if any illegal selling is revealed.

It should be noted that not all online gambling operators have access to effective online AV systems, and the adequacy of measures may be very different for those using other methods. Many interviewees from the online gambling sector suggested that procedures are less effective in countries such as France which require offline submission and checking of documentation, not because the procedure is itself less accurate, but rather because it is cumbersome for customers to use, and may therefore drive users to unlicensed operators. Not having conducted interviews in France we cannot confirm this, but it's notable that several interviewees claimed their companies would be unlikely to seek a license in that country.

On this point, the important conclusion to draw is about proportionality. AV systems impose costs both for a company (that has to invest in a new on-boarding infrastructure and possible pay per-

---

[54] http://www.ecogra.org/Services/SafeandFairSeal/SafeFairSealTestingMethodology.aspx

customer fees for age- and ID-checking) and for the consumer (who has to provide information about herself in order to continue with an online transaction). Note that costs need not be just financial – in the case of the French online gambling example, the prospective consumer faces temporal costs (having to take time to send physical documentation) as well as long delays in accessing a service he wants to use. And it should not be forgotten that there is a fundamental cost to giving up personal information simply in terms of a reduction in privacy. Indeed the cost associated with this may be very great for an individual if either they are accessing highly personal and sensitive services or content (such as pornography) or if they have to give up more information than might be strictly required by law, which will then be used for other purposes, such as marketing or advertising, at a later date. If these costs seem disproportionate to the value of the transaction, then there will be little incentive for the consumer or business to co-operate. As Brownsword notes in his analysis of the conditions for information technology regulation,

> "Regulators should not be surprised that regulatees (particularly regulatees with business interests) should think that a calculation of rational economic interest is the appropriate way to determine how to respond to a regulatory intervention." (Brownsword 2012: 263)

In considering the implications of proportionality, it's worth drawing a distinction between legal requirements for age verification, and voluntary efforts. In the first case, the question is what procedures are required in order to fulfil a legal obligation. In the second, the issue is whether or not a business can see enough value in implementing such a system despite the absence of any legal requirement to do so, and whether customers can (or should) be motivated to comply. In the first case, there's clearly a much stronger incentive for both the transacting business and customer to pay the costs associated with AV, although this doesn't automatically mean that a customer will want to give up as much information as a company might want to acquire. In both cases, the combination of attribute-based identity systems and principles of data minimisation mean that it is increasingly conceivable that a business providing access to an online app or service might only need to know that the customer is indeed 18 or over, rather than also their address, credit history, bank details etc. Whether the cost of the AV transaction is covered in part by the collection of more personal information that could be used to leverage further business opportunities is a decision that each company will have to consider very carefully.

Extending these arguments back to our three case studies, we can conclude that the online age verification measures used by white-listed online gambling companies in Italy, Denmark, Spain and the UK offer high assurance of customer age and identity in accordance with the legal requirements of their licenses. In the majority of cases where customer processing and database checking is undertaken in sub-second time, the cost to the consumer is not substantial, except insofar as the law requires the provision of a large quantity of personal information. The systems used seem to offer an effective solution to the regulatory challenge of allowing access to online gambling services whilst protecting minors and preventing fraud or money laundering.

In the case of online retail, the conclusion is rather more mixed. Whilst regulation already prohibits the sale of age-restricted goods such as alcohol, knives or adult DVDs and games to minors in many European countries, the resources devoted to enforcing such laws are minimal. Against this regulatory backdrop, and facing highly competitive market dynamics plus a reliance on one-off

transactions, there is little incentive for even responsible firms to invest in medium to high assurance age verification systems, although should the price of such services continue to drop, these incentive patterns would of course change. This doesn't mean that no age verification is currently taking place, and the big-brand retailers we interviewed were at pains to emphasise that they applied appropriate levels of 'professional diligence', relying on a variety of methods such as self-assertion, credit card ownership, and (in some cases) checking details against the electoral roll. In other cases, stores had made the decision simply not to sell some types of good, such as knives, in order to avoid a potentially very embarrassing scenario where an underage consumer might purchase such an item and use it with criminal intent. However there was also an awareness of risk, that the systems currently employed did not provide high levels of assurance of customer age, and (in some cases such as the sale of PEGI-rated games or BBFC DVDs) that existing processes could provide no guarantee that a consumer was old enough to buy a particular good.

In the case of social gaming, the lack of age verification procedures is undoubtedly a reflection of the absence of regulatory requirements in this area. As this study was focused on European practices rather than American ones, we did not question interviewees about the challenges of complying with COPPA regulation, but had we done so, this might have been one area where more accurate information about customer age could support greater compliance with regulation. We also considered the available research evidence of risks or harms resulting from minors' use of social gaming. Whilst there continues to be media speculation about the potential risks, particularly of games which closely resemble gambling, there is insufficient evidence to suggest that strict age verification is needed to protect minors at this point. Some of the gambling regulators interviewed for this study also suggested that social casino games should ensure consumers are made aware that game-play on social casino games does not reflect the realities of gambling. The ISGA has developed a best practice principle in this regard as follows:

> Social games should not lead players into believing they will be more successful at real-world activities. For example:
>
> 1. Car driving simulators should not deliberately lead people to believe they are acquiring real-world driving skills.
> 2. Casino style games should not deliberately lead players to believe they will be successful at real money gambling games.

These particular 'best practice principles' seem somewhat facetious and are not strictly in keeping with principles of professional diligence but there is clearly a space for responsible self-regulation here which might ultimately recommend the use of AV. If social gaming operators can demonstrate a willingness to act responsibly even in the face of this less than exemplary code of practice then there will be little reason to require state regulation. However, if such responsible behaviour is not widespread, or evidence emerges of harmful effects associated with social games such as simulated gambling, then more regulatory intervention could be justified.

One area where there is unclarity about the adequacy of existing online age verification processes concerns social media advertising. Interviewees from both the online gambling sector and the alcohol sector spoke of their reliance on social media platforms in correctly identifying the age of consumers exposed to advertising on these platforms. Whilst it's not generally illegal for such

companies to provide adverts which may be seen by minors, they must not target under-18s. Given that nearly 40% of US teens claim to have lied about their age on social media (Madden et al 2013), our interviewees noted some concerns about whether or not their adverts might be being seen by large numbers of under-18s, even when the target age is set deliberately high to allow for such deceit. Whilst it would seem heavy-handed to ask for mandatory age verification by social media platforms which would reduce the role of parental discretion in deciding when their children are ready to use such services, it will be interesting to see whether we might see the introduction of voluntary age verification processes that could offer higher assurance of age. This strategy might seem increasingly attractive to SNS if it meant they were able to extract more value from online advertising and the already expanding opportunities to act as identify providers.

VIII Examples of Good Practice and Further Policy implications

Good practice and lessons learnt

A principle aim of this research project was to identify examples of good practice in online age verification, with a view to determining whether lessons could be learnt for practice in different industry sectors. In terms of best practices in age verification, Denmark, Spain and the UK are the markets regarded as good examples of how different systems of identity and age verification develop and operate. The UK is well-regarded because data aggregators and credit reference agencies apparently cover 85-90% of the UK adult population, offering one approach to identity and age verification not reliant upon a single central identity database. Denmark and Spain offer different examples of good practice whereby the regulator allows gambling operators' access to the electronic identity database to cross-check asserted identity details. All respondents repeated the mantra that access to good datasets against which they can cross check self-asserted data is critical to enabling companies to comply with legal requirements, and many suggested that governments play a critical role in ensuring that appropriate data is made available. In other words, governments have a crucial role to play not just in providing legitimate, prudent and effective regulatory frameworks, but in supporting the efficient operation of these by ensuring appropriate e-ID resources are available. This last point will be an important one to consider in the remaining issues, insofar as we ultimately seek to clearly set out the separate but intertwined responsibilities of all the different stakeholders.

In relation to the operations of particular companies, white-listed gambling companies all regard themselves and each other as maintaining very high standards of ID and age verification processes, partly because their licences depend on it. Gambling companies hosted in location like Antigua and Costa Rica - where there isn't an equivalent legal or regulatory regime as there is in Europe - were frequently identified by interviewees as examples of poor practice. It was also suggested that poor regulatory practice – the imposition of burdensome and disproportionate rules in different European countries would aid the proliferation of such bad actors. France, for example, does not allow online

casinos and so French consumers wishing to gamble online have no choice but to use these non-regulated sites.

In the online retail sector, despite the wide disparity of age verification practices, several examples of good practice emerged. Two of the companies approached in our interviews already used some sort of database check to determine the age of their customers, even if this was not applied in every transaction. The first, a high-end online wine shop, specialised in sending regular boxes of wine to customers, meaning that the cost of an initial age check could be recouped over multiple transactions. The second, a general multi-channel retailer, made use of the delay between order and delivery to undertake further checks, meaning that the shopping order itself was not held up, whilst any problems with age-restricted purchases could be dealt with before or at delivery.

In addition to these applications of reasonable assurance methods of online age verification, other examples of good practice emerged, often as pragmatic responses to imperfect conditions. Thus, for example, one major international alcohol distributor described how their social media advertising strategy was targeted not at over-18s, but at over 21s or over 25s. This was intended to compensate for uncertainty around the real age of social media users on platforms such as Facebook. Although not strictly good practice, it's worth noting that even those retailers whose business models did not currently support the use of database checks for AV were open to the possibility of using such services in the future, should either the regulatory situation change, or the costs of such services become significantly lower. The retailers we interviewed were generally concerned about professional diligence and the possible reputational risks to their businesses of not addressing issues such as age verification. To this end, trade associations are already engaged to varying degrees in discussions about leveraging electronic identity solutions to deliver age attributes in payment protocols, and we would strongly recommend that such efforts are expanded to incorporate dialogue with other sectors such as the online gambling industry.

Amongst the few social gaming operators we were able to interview, there was a stark contrast between the views of those operators who routinely work within a regulatory framework and those that do not. Those that do so, regard age verification as a key business enabler, a means to enable regulatory compliance and generate revenue, and ease the customer on-boarding processes. These companies, often with a history of focusing on children's games, are the best examples of good practice in the social gaming sector. In contrast, those for whom the OFT and the FTC have recently explained the parameters of existing legislative frameworks seem to be the furthest removed from understanding the benefits and challenges associated with leveraging existing and emerging age verification techniques. This finding seems plausible, but given the small number of interviews conducted in this sector, it is important not to read too much into such conclusions. A key recommendation of this report is that the social gaming industry should consider convening a number of meetings to enable dialogue with representatives from both their own sector and the retail, gambling, payments, and electronic identity sectors. These meetings would foster valuable avenues of communication and facilitate sharing of good practices between sectors with respect to protecting consumers online, addressing calls for regulation and leveraging the emerging interoperable electronic identities and implications for business models.

Despite initial reservations, gambling operators and regulators now express high levels of satisfaction with opportunities to leverage the architectures underpinning differing electronic identity infrastructures in Denmark, Spain and Italy, enabling them to verify either the identity or age or both of most customers quickly and efficiently. E-identity schemes may help to provide such solutions as well as delivering economic benefits such as fraud reduction, new business services, and lower transaction costs in citizen-government interactions in ways that will more than justify the costs of such schemes. The extent of such benefits can only be maximised if identity schemes are, from the very beginning, underpinned by rigorous trust frameworks incorporating fundamental principles that engender user trust, such as commitments to providing user control, ensuring data quality, transparency over use of data, and agreed data minimisation.

Currently, for example, the UK Government Digital Services Department is working in partnership with a number of companies and stakeholders to develop an electronic identity ecosystem, similar to the US, NSTIC programme. Many public services require citizens to prove their identity as an early and necessary step to accessing government services. The UK's Identity Assurance Service is intended to provide a simple, secure way for people to access public services on GOV.UK. It is grounded in a trust framework of nine core principles, including the four outlined above[55]. The Identity Assurance Programme (IDAP) vision is that a citizen centric electronic identity ecosystem, which doesn't rely on a single centralised database of identities, will be rolled out to UK citizens in 2014 /2015. These electronic identities will also be used on the wider Internet and might eventually enable regulated sectors to conduct age attribute checks. At some point in the future, companies operating in the UK which currently rely on data sources held by data bureaus and credit reference agencies will be able to leverage the electronic identity ecosystem, in similar ways to how Spain, Denmark and Italy does now. This serves as an example of the ways that e-identity and age verification systems are evolving rapidly. Interestingly the view of representatives for the European Commission DG Market is that more could be done to enable the retail sector to leverage the e-ID architectures to enable age verification. A number of representatives from the retail sector, gambling operators and one of the gambling regulators regard this proposition as potentially viable and worthy of further discussion.

There are some more general implications for the future development of national and European consumer regulation and sector-specific legislation. Whilst the online gambling sector is heavily regulated in most European countries with specific requirements to verify the age of a customer, it also experiences competition for non-regulated operators. A lesson the regulated gambling sector has learned is that ID and age verification techniques must be proportionate and balanced and cause minimal disruption to a potential customer otherwise these customers may opt to use non-regulated operator. Retailers' views concurred in a number of respects with these lessons namely that regulatory measures designed to protect consumers such as age verification requirements must be proportionate, scalable, viable, incur low or neutral cost, adhere to a risk based approach, and not negatively impact on a retailers competitiveness.

In terms of the adequacy of existing regulatory measures in addressing the risks and harms identified

---

[55] http://www.publictechnology.net/news/cabinet-office-outlines-its-9-identity-assurance-principles/37845

in each case, there has so far been broad support for more harmonisation of the legal and regulatory frameworks across Europe. A number of interviewees also expressed concerns about how further harmonisation might work out in practice, particularly if this resulted in more burdensome regulations for industry. It was also noted that different sectors display particular cultural and legal sensitivities and member states are a long way from reaching consensus on key issues– for example in the online gambling sector, some countries are comfortable with sports betting but will not allow online casinos.

Instruments such as the Consumer Rights Directive serve as examples of how a degree of national flexibility might be balanced with a simplified and transparent agenda of basic consumer rights. At the same time, we are yet to see any more coordinated approach towards the enforcement of consumer rights, and this is likely to undermine the efficacy of such regulation in an era where cross-border transactions are so common. Some of our interviewees expressed an appetite for the stricter application of such consumer protection legislation. In particular, a number of respondents regard these legal avenues as offering the most viable means to regulate different types of social games, especially those that involve in-app purchases. Suggestions have included the idea that age verification might be required to determine whether or not a player is under 16 (and therefore particularly vulnerable to aggressive selling) or that the only issues requiring attention are concerns of transparency and fair play. However, it is unclear how well this argument stands up in terms of the free-to-play games that gambling companies offer on their sites where the potential for 'transitioning' or 'converting' players to real-money gamblers is far greater. Whilst we are therefore keen to explore further the potential for protection to be ensured via consumer legislation rather than gambling legislation, our interviews to date suggest that the latter cannot so quickly be ruled out.

Recommendations about age verification and identification online should not be discussed without due consideration for privacy and data protection. Interviewees highlighted the challenges of ensuring compliance with data protection requirements, with the example raised of a recent hack of the Danish police system in which Swedish hackers were able to copy all Danish social security (CPR) numbers. Putting sensitive personal data such as national security numbers at risk is a fundamental breach likely to undermine consumer trust and it's essential that effective information security management systems are in place to prevent this from happening. This case also highlights the strengths and weaknesses of different eID ecosystems: whilst the Danish model seems to operate efficiently in the context of online gambling, its reliance on a single centralized database of information may be more vulnerable to attack than eID systems drawing together information from a wide variety of sources.

The most significant conclusion to be reached is that whilst age verification was previously discarded as a useful tool for protecting children online, it seems to offer far greater potential at this point in time. The development of national eID architecture means that an increasing number of European states are seeing the emergence of varying levels of identity and age verification, potentially lower cost options for identification and age-verification. Some of these identity infrastructures hold data on minors, (as in Denmark), and even in states where only adults may be checked this means that at the very least these offer a valuable resource for restricting access to online goods or services restricted to those over 18. As the EU SaferChat pilot also demonstrated, reliable databases holding

information on those under 18 may also provide future opportunities to leverage age data for younger Internet users as well.

We cannot conclude this project without offering some last caveats. Our interest in the potential uses of online age verification systems should not be read as a desire to see every online transaction undertaken by a child subject to age-gating. Children benefit immensely from their explorations of the Internet, whether this be direct educational and informational advantage, or more personal benefit from opportunities to socialise, communicate, play with identity or express themselves online. In most cases, there should be no need for them to prove how old they are. Parents and educators have primary responsibility for ensuring that children behave online in ways that are safe (or at least not very unsafe) and decent. The suggestion here is that when it comes to goods and services which are subject to legal restriction for minors, we would expect providers of these goods or services to apply proportionate means of checking age. Given the expanding opportunities in online age verification, we suggest that they could be much more widely used in such transactions, much as would be the case in offline transactions.

It's also vital that decision-makers are willing to encourage more open-minded public debate about how best to balance minors' interests in relation to balancing their privacy, versus other aspects of their wellbeing. Thus, for example, principles of data minimisation would support age verification systems that only need to determine whether a user is under 18, or indeed, under 16, 12 etc. As the UK and US examples demonstrate, there is no need for a single centralised database of children's data to be established, it is enough to facilitate the exchange of permissioned, verified attribute data, whether these be between services, or across borders. At present, the idea of collating and using minors' personal data for commercial services is regarded in many European countries as simply unacceptable. But if such an ecosystem could conceivably be used to ensure that minors don't illegally access adult goods and services, then it's at least worth asking whether the current balance is optimal. Indeed, if social networks are already being used voluntarily as de facto age verification services for advertising purposes, then there would seem to be good reason to at least consider the pros and cons of higher assurance and possibly more privacy-preserving age verification services.

Final Conclusions

Legislative requirements with respect to age-restricted products and services – including alcohol, tobacco, knives, fireworks, spray paints, solvents and petrol, gambling, film and gaming content – share the common objective of protecting the health, safety and wellbeing of young people. The findings of this one-year qualitative research project undertaken by the Oxford Internet Institute indicate that whilst companies in the licensed online gambling sector are rightly to be praised for taking a strong lead, many businesses in the retail and social gaming sectors have also have adopted a responsible approach to complying with legal requirements relating to the advertisement and sale of age-restricted products and services. In doing so, all these businesses apply a range of age

verification methods that afford differing levels of assurance and are subject to differing levels of enforcement, generating many examples of good practice which should be of interest within and beyond their sectors.

Elite interviews with experts on age verification from across three sectors established that practices of online age verification are (unsurprisingly) most common in the online gambling sector. In those countries where it is possible to do so, gambling operators and regulators regard the practice of leveraging electronic identities as their preferred method of age verification for the following reasons: it provides a reliable, fast, convenient, proportionate approach to age verification that enables operational efficiencies, lower levels of both fraud and identity theft, higher levels of customer satisfaction, convenience, and more effective self-regulatory measures to manage problem gambling. Furthermore for the gambling sector, leveraging electronic identities offers a commercially viable and scalable solution for identity and age verification, which is underpinned by clear liability models. The different electronic identity architectures existing or planned in countries around Europe have been designed to interoperate and the levels of assurance associated with the checks are standardised and will soon be mutually recognised[56]. Crucially, in some of these states, children and young people are also issued with electronic identities, potentially removing a significant barrier to verifying the age of a person aged 17 and below. This means that opportunities for businesses to leverage reliable e-identity infrastructures for age verification will almost certainly grow in the medium term, and there is therefore a great need to identify and build on existing good practices.

As an appropriate foil for the opportunities potentially provided by an expanding attribute exchange ecosystem, representatives from the retail and social gaming sectors highlighted a number of important drivers that underpin a renewed interest in age verification, these include changing business practices and consumer behaviours (including the rise of children as consumers), innovative business models, scope to build both existing and new revenue streams, a persistent concern for protecting minors and anticipated changes to the regulatory environment. The latter includes moves toward harmonisation of identity and age verification techniques across Europe. Together these create a 'perfect storm' of conditions for the development of innovative practices in online age verification. It is too early to predict how and where such practices will evolve most rapidly, but as this report has suggested, one very fruitful area would be the online sale of goods or services currently subject to legal restriction by age.

Our interviews revealed deep pockets of knowledge and expertise within the gambling sector and some parts of the retail and social gaming sector with respect to leveraging the different the electronic identity ecosystems in individual European countries now and in future across all 28 members states. Furthermore the findings of this study highlight the efforts to date of individual sectors proactively engaging with regulators to ensure that proportionate and balanced outcomes are achieved for all stakeholders. In this context, a key recommendation of this study is that there would be clear benefits to creating avenues of communication between relevant stakeholders and across sectors to share best practice principles with age and identity verification and how best to leverage electronic identities ecosystems. Regulators and national governments have a key role to

---

[56] Proposed regulation of electronic identification and trust services for electronic transactions in the internal market

play in supporting innovation in the development of such ecosystems, but should also show forbearance in avoiding heavy new regulation which might impose excessive costs on business and incentivise consumers to turn to unregulated services. Instead, more extensive and predictable enforcement of existing legislation (such as advertising standards and consumer rights protection) should serve to protect Internet service users, whatever their age.

In 2008, when the Internet Safety Technical Taskforce reported on the potential of age verification technologies to protect children online, they concluded that:

> "Age verification and identity authentication technologies are appealing in concept but challenged in terms of effectiveness. Any system that relies on remote verification of information has potential for inaccuracies." (Internet Safety Technical Taskforce: p. 152)

The research conducted for this project has demonstrated that, in the intervening six years, the assurance levels associated with the most trusted age verification procedures have dramatically improved. The interviews we conducted revealed a growing appetite across different online business sectors to explore the broader applications of these tools, and together with the emerging identity infrastructures being developed by western states, there is reason to believe that age verification tools will play a much greater role in protecting minors in the next six years.

Appendix 1

Details of interviewees

Sector	No of interviewees
Online gambling	13 (across 4 countries)
Retail	6
Social gaming and social networks	4
Payment and ID services	5
Government and regulatory bodies	8
Children's charities	2

Appendix 2

Informed Consent Statement

Effective Age Verification Techniques: Lessons to be Learnt from the Online Gambling Industry

Information for Participants

You are being invited to take part in a research study. Before you decide to participate, it is important to understand why the research is being conducted and what your participation entails. Please take time to read the following information carefully. Please ask if there are any aspects of the project that are unclear or if you would like more information before deciding whether or not you would like to take part in this research. Contact details for the research team are given at the end of this information sheet.

What is the purpose of the study?

The purpose of this study is to identify lessons for policy relating to the use of age verification practices online.

What is being asked of me?

We would like to interview you for approximately one hour reflecting on your experience and perspectives of the use of age verification processes online. You will be audio taped so that we have a record of the interview to refer to as we reflect on the key questions central to our research. Please note that your participation is completely voluntary. You can choose to not answer any question or withdraw at any time. Also, if you choose to end the interview early, we will discard any interview materials.

What are the risks of taking part?
No reasonable risks are foreseen from this research.

What are the benefits of taking part?
The benefits of this research are that it will inform scholarly understanding of how online businesses use age verification processes to limit access to age-restricted goods by minors. The findings will inform recommendations for policy-making on an issue of increasing social importance.

Confidentiality
Recordings and transcripts of this interview will be treated confidentially, meaning that only approved members of the research team will be able to see any text and original documents will be stored securely. We will publish quotes anonymously or alter details in order to ensure that you are not personally identifiable. In the unlikely event that we want to attribute a quote to you directly, we will seek further consent to clear this quote and indicate the manner in which you will be identified.

Audio Recordings

Audio recordings may be collected during your participation in this research. This information will be used primarily for research purposes, and only researchers working on this project will have access to the original files storing this information. The PI will retain all data when the project has terminated. If you withdraw from this study, the files containing your data will be destroyed. Edited versions of audio information from this research may be used in instruction, public talks, and publications of this research if you consent to your data being used in this way below. The audio will not be used for any additional purposes without your additional permission. All data will be held in accordance with the 1998 Data Protection Act.

Who is organizing and funding this research?

The research team running this project are Dr Victoria Nash, Dr Rachel O'Connell and Bendert Zevenbergen at the Oxford Internet Institute, University of Oxford. It is supported by a research grant from Bwin.Party Digital Entertainment.

Contact for Further Information or Follow-up

Should you have any further questions about this research, please feel free to contact Vicki Nash (Victoria.nash@oii.ox.ac.uk), Rachel O'Connell (Rachel@technologist.com), or Bendert Zevenbergen (bendert.zevenbergen@oii.ox.ac.uk). It has received ethics clearance from the Oxford Internet Institute's Departmental Research Ethics Committee. You can contact drec@oii.ox.ac.uk for questions or concerns about this study.

Consent Form

1. I have read and understood the information about this study and have had the opportunity to ask questions and get satisfactory answers about this study.
2. I understand that agreeing to take part means that I am willing to be interviewed by a researcher for one hour, and that this interview will be audio-recorded.
3. I understand that my participation is voluntary, that I can choose not to participate in part or all of the project, and that I can withdraw at any stage of the project without being penalized or disadvantaged in any way simply by informing the research of my decision.
4. I consent to anonymised quotes from my interview being used in the report of the study.
5. I am aware of whom to contact should I have questions following my participation in this study.
6. I understand that this project has been reviewed by and received ethics clearance through the Oxford Internet Institute's Departmental Research Ethics Committee.

I hereby agree to participate in this study.

Name:……………………………………………………………………….....(please print)

Signature:…..……………………………………………….………...……

Date: ....

Appendix 3

Interview Schedule

Background information for interviewee

The aim of this programme of research is to explore the issue of age verification from the perspectives of representatives from a number of sectors, including online gambling, social gaming, retail and payment processing.

Within certain sectors, businesses are obliged to conduct both identity and age verification processes to comply with specific legislative requirements e.g. Know Your Customer (KYC) and Anti Money Laundering (AML). However, across sectors there are not only differing levels of assurance associated with a range of identity and age verification techniques but also variations in compliance with and enforcement of legal requirements and self-regulatory good practice recommendations, both online and off-line.

The combination of rapidly evolving technology, legal, regulatory and policy landscapes, alterations in both consumers expectations and business models and the anticipated emergence of electronic identity eco-systems, are having an impact on discussions about identity and age verification. You have been invited to share your organisation's views about the deployment of existing age verification processes for the purposes what, if any, lessons learnt in this regard may be relevant to emerging and future methods of identity and age verification.

> *Prompt:* Description of eID ecosystems: usernames and passwords are insecure, fraud costs billions, governments around the world are exploring opportunities to issue citizens with electronic identities with which to transact with government services online and these may also be used to transact on the wider web.

Specifics of the interview process

- Thank you for agreeing to participate in this programme of research.
- Check status of consent form and discuss the degree of anonymity afforded to respondents.
- This interview will last for approximately 60 minutes and it will be recorded to facilitate the process of information gathering.
- Are you happy to proceed?

Information-gathering

- Name:
- Affiliation:
- Country of residence:
- Position and role description, length of time in this role:

Sector/role /territories role covers

Retail	☐	Business	☐	Legislator	☐	Regulator	☐	Trade Association	☐
				National	☐	European	☐	Global	☐
Gambling	☐	Business	☐	Legislator	☐	Regulator	☐	Trade Association	☐
				National	☐	European	☐	Global	☐
Gaming	☐	Business	☐	Legislator	☐	Regulator	☐	Trade association	☐
				National	☐	European	☐	Global	☐
Payments Provider	☐	Business	☐	Legislator	☐	Regulator	☐	Trade Association	☐
				National	☐	European	☐	Global	☐
Consumer/ Child Protection	☐	Organisation	☐	Legislator	☐	Regulator *(OFT, OFcom, UK charity commission)*	☐	Trade Association *(eg ASA, ISPA has a child protection policy group*	☐
				National	☐	European	☐	Global	☐

We will begin with some general questions about age verification methods and where responsibility lies for protecting minors. *(10 mins)*

- From your organisation' s perspective, who should be responsible for ensuring /overseeing the protection of minors with respect to accessing age-restricted content, goods or services: the European Commission? National governments? Industry bodies? Individual firms? Parents?
- What do you think of the current legal and regulatory framework with respect to identity and age verification as it relates to your business sector – *please state and speak about the legal requirements and regulatory framework with which you are most familiar -* for limiting minors' online access to age-restricted goods or services? (Prompt is it sufficiently clear, flexible enough, or is there scope for improvements?)
- Do the particular legal requirements and regulatory framework in individual markets influence your companies decision to operate in that market? If so, can you please give examples?
- What are your views on harmonizing the legal and regulatory frameworks across Europe for your business sector?
- How effective are companies both in your sector and /or across different sectors, in terms of implementing self-regulatory good practice recommendations and what, if any measures could be implemented to encourage greater compliance?

In this section we would like to explore the Identity and age verification methods employed by your company and the levels of assurance associated with methods required either by law /self regulatory measures *(prompt: in relation to minors)*

- What is the age profile of users across your (specify which) products / services? Target demographic: All, 18+, 13+, 13- (parental consent)
- Can you please describe the ID and age verification methods your organisation currently employs and the points in the customer journey at which these processes are employed?
    - *e.g.* Self-asserted age verification, e.g. tick box
      Adult demographic: ID checking – electoral role, address verification, CRA, KBA,
    - Point of registration process / or payment process
    - Children and young people: Guarantor model, parental permission

- Are the particular ID/age verification procedures your organisation uses standard across your business sector – are there many bad actors who do not comply? *(If regulation not mentioned, prompt on this)*
- What are the potential risks a business might incur if age verification procedures are not implemented and what risks of harm might there be to consumers?
- Do *you* think these procedures are necessary?

The following questions explore in greater depth your organisation's views on the perceived efficacy of current age verification procedures at an operational level (if any used)

- How do the ID/Age verification processes employed by /overseen by your organisation work in practice? For example, for a typical Internet user, what is the time frame /costs involved in verifying his/her age/identity?
    - Does it achieve its aim?
- As business models evolve e.g. freemium, new products come on the market – social casino gaming, omni-channel retailers, new payment mechanisms are these The liability and commercial models that underpin identity and age verification may not always be clear, what are your views on these issues?
- Have the ID and age verification methods employed by your organization evolved over time?
- Are there any lessons that your own and other online sectors – both existing and emerging - could learn from your organisation's experience
- Could the efficacy of the identity and age verification procedures be improved, and /or do you expect methods to evolve in the near future and if so, how?
- Prompt: introduction of age verification into payment protocols?
- Ask about the experience in each market?

The following questions explore the issue of enforcement, transparency and cross industry collaboration.

- Are there audits conducted by your sector to assess levels of compliance with identity and /or age

verification procedures.
- Does your sector file its audits of the verification method? If so, where and are they publicly accessible?
- Are there effective enforcement mechanisms to address non-compliance with identity and age verification legal requirements /self-regulatory recommendations?
- Are your competitors' using/promoting similar verification methods? To what extent, if any, does cross industry collaboration exist vis a vis id/age verification procedures or more broadly good practices? (*Prompt social casino games*)
- Impact assessments are critical to both business and regulatory processes. On what factors, if any, do you measure the impact of ID/age verification processes? Can you please rate the following in terms of importance as follows:

	Very Important 1	Important 2	Neither important or unimportant 3	Unimportant 4	Very Unimportant 5
Child Protection					
Impact on Revenue					
Legal ramifications					
Impact on Innovation					
Company Reputation					
% of completed registrations /transactions					
Customer experience					
Competitive advantage					
Proportionality					
Other					

In this section we will explore possible future scenarios:

- With respect to identity and age verification what anticipated legislative /regulatory measures concern you most? (Prompt: Various proposed EU Directives including the Consumer Rights Directive, Article 8 of the Data Protection Directive, proposed legislation of electronic identities, distance selling and unfair commercial practices)
- What, if any, self-regulatory measures have been implemented in the past that would mitigate the concerns that proposed future regulatory and legislative measures are seeking to address?
- Electronic identity ecosystems aim to introduce privacy preserving, age verification methods that would allow your organization to *reliably* identify consumers that fall into specific age bands e.g. 7 years old, 12 years, 16 or 18 -that correspond to the Pan European Game Information (PEGI) content rating scheme – see below – or similar age bands applied in different countries to specific products,

goods and services.

- What do you anticipate might be the impact of the introduction to the market, of age verification methods on your business models etc?

In this final set of questions we would like to explore a couple of issues relating to policy making/shaping/influencing:

- Who has been influential in your sector in the development of the age verification laws/ regulatory measures / good practice recommendations?
- How has industry shaped the regulatory process and can you please describe the techniques you employ to influence and shape policy?
- What, in your view are the major impediments to effective policy making with regard to identity and age verification?

Final comments

- Are there any other general points you would like to add?
- Can you direct us to any resources or information that would be useful for this study?
- Could you recommend any other experts in your field that we should interview for this study?
- Next steps

References

Abbott, Max., Binde, Per., Hodgins, David., Korn, David., Pereira, Alexius., Volberg, Rachel., Williams, Robert. (2013). *Conceptual Framework of Harmful Gambling: An International Collaboration*. The Ontario Problem Gambling Research Centre (OPGRC), Guelph, Ontario, Canada.

Anderson, J., & Rainie, L. (2012). Millennials will benefit and suffer due to their hyperconnected lives. *Pew Internet & American Life Project*. Retrieved from: http://www.pewinternet.org/2012/02/29/millennials-will-benefit-and-suffer-due-to-their-hyperconnected-lives/ (Accessed 5th February 2014)

ASA (2013). Children and advertising on social media websites. Available at: http://www.asa.org.uk/News-resources/Media-Centre/2013/~/media/Files/ASA/Reports/ASA%20Compliance%20Survey_Children%20and%20advertising%20on%20social%20media%20websites.ashx (Accessed 5th February 2014).

BBA (2013) https://www.bba.org.uk/news/press-releases/age-of-the-app-children-spending-online-before-getting-money-lessons-at-school/

Bellman, S., Kemp, A., Haddad, H., & Varan, D. (2014). The effectiveness of advergames compared to television commercials and interactive commercials featuring advergames. *Computers in Human Behavior*, *32*, 276–283. doi:10.1016/j.chb.2013.12.013

Blaszczynski A, Collins P, Fong D, Ladouceur R, Nower L, Shaffer HJ, Tavares H, Venisse JL. (2011). Responsible gambling: general principles and minimal requirements. *Journal of Gambling Studies.* 27(4):565-73.

Bouchery EE, Harwood HJ, Sacks JJ, Simon CJ, Brewer RD. (2011) Economic costs of excessive alcohol consumption in the United States, 2006. *American Journal of Preventative Medicine* 41:516–24.

Boyd, d., Hargittai, E., Schultz, J. and Palfrey, J. (2011). Why parents help their children lie to facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act'. *First Monday*. 16 (11).

Brownsword, R., (2012). The shaping of our online worlds: getting the regulatory environment right. *International Journal of Law and Technology*. 20(4)

Buckingham, D., Whiteman, N., Willett, R., & Burn, A. N. (2007). *The impact of the media on children and young people with a particular focus on computer games and the internet*: prepared for the Byron Review on children and new technology

Burgess, A., (2004) *Cellular Phones, Public Fears, and a Culture of Precaution*. Cambridge: CUP

Byron, T. (2008). *Safer children in a digital world* The report of the Byron Review

Caoilli, E. (2012, Apr. 4) Study: Teens losing interest in traditional games, prefer social/mobile experiences, *Gamasutra.* Retrieved Jan 2013, from: http://www.gamasutra.com/view/news/168007/Study_Teens_losing_interest_in_traditional_games_prefer_socialmobile_experiences.php

Clark, D.B.; Lynch, K.G.; Donovan, J.E.; and Block, G.D. (2001) Health problems in adolescents with alcohol use disorders: Self-report, liver injury, and physical examination findings and correlates. *Alcoholism: Clinical and Experimental Research* 25:1350–1359, 2001

Consalvo, M. (2009). Hardcore casual: Game culture Return (s) to Ravenhearst. In *Proceedings of the 4th International Conference on Foundations of Digital Games* (pp. 50-54). ACM

Delfabbro, P. & Thrupp, L. (2003). The social determinants of youth gambling in South Australian adolescents, *Journal of Adolescence,* Volume 26, Issue 3, Pages 313-330

Dweck, C. (2006). *Mindset: The new psychology of success*. Random House Digital, Inc.

Fidgeon, T. (2012, Mar. 26) Social Gaming: a usability perspective, *Spotless Interactive.* Retrieved from: http://www.spotlessinteractive.com/articles/usability-research/social-gaming-usability-perspective.php

Gainsbury, S. M., & Derevensky, J. L. (2013). *What do we currently know about the impact of social media gambling games upon current and future gambling among young people?* Paper presented to the 15th International Conference on Gambling and Risk-Taking, Las vegas, Nevada, 27-31 May. Retrieved from: http://epubs.scu.edu.au/cgi/viewcontent.cgi?article=3866&context=tourism_pubs

Gentile, D. A., Anderson, C. A., Yukawa, S., Ihori, N., Saleem, M., Ming, L. K., Sakamoto, A. (2009). The effects of prosocial video games on prosocial behaviors: international evidence from correlational, longitudinal, and experimental studies. *Personality & Social Psychology Bulletin*, *35*(6), 752–63.

Goodwin, K., & Highfield, K. (2012, March). iTouch and iLearn: an examination of "educational" Apps. In *Early education and technology for children conference.* Retrieved from: http://www.academia.edu/1854816/iTouch_and_iLearn_An_examination_of_educational_apps

Graham K, West P. Alcohol and crime. In: Heather N, Peters TJ, Stockwell T, eds. (2001). *International handbook of alcohol dependence and problems.* London: John Wiley and Sons: 439–70.

Grant, B.F., and Dawson, D.A. (1998) Age at onset of drug use and its association with DSM–IV drug abuse and dependence: Results from the National Longitudinal Alcohol Epidemiologic Survey. *Journal of Substance Abuse* 10:163–173.

Griffiths, M. D. (2013). Social Gambling via Facebook: Further Observations and Concerns. *Gaming Law Review and Economics*, *17*(2), 104-106.

Griffiths, M. D., and Parke, J. (2010). Adolescent Internet Gambling: A Review. *Journal of Adolescent Medicine and Health* 22(1): 58-75.

Grunbaum, J.A.; Kann, L.; Kinchen, S.; et al. (2004) Youth risk behavior surveillance—United States, 2003. *Morbidity and Mortality Weekly Report Surveillance Summary,* May 21; 53:1–96.

Holloway, D., Green, L. and Livingstone, S. (2013). *Zero to Eight. Young Children and their Internet Use*. LSE, London: EU Kids Online. Available at: http://eprints.lse.ac.uk/52630/1/Zero_to_eight.pdf (Accessed 3rd February 2014)

Internet Safety Technical Taskforce (2008). *Enhancing child safety and online technologies: final report of the internet safety technical task force to the multi-state working group on social networking of state attorneys general of the United States*. Cambridge: Berkman Center.

Ipsos Mori, Social Research Institute. (2011). *Underage Gambling in England and Wales: A research study among 11-16 year olds on behalf of the National Lottery Commission*. Retrieved from: http://www.natlotcomm.gov.uk/assets-uploaded/documents/ipsos-mori-report-on-behalf-of-the-commission_1316537803.pdf

Ito, M., Baumer, S., Bittanti, M., boyd, d., Cody, R., Herr-Stephenson, B., Horst, H., Lange, P. G., Mahendran, D., Martinez, K., Pascoe, C. J., Perkel, D., Robinson, L., Sims, C. and Tripp, L. (2010). *Hanging Out, Messing Around, and Geeking Out*. Cambridge, MA: The MIT Press.

Ivory, J. D., & Kalyanaraman, S. (2007). The Effects of Technological Advancement and Violent Content in Video Games on Players? Feelings of Presence, Involvement, Physiological Arousal, and Aggression. *Journal of Communication*, *57*(3), 532–555. doi:10.1111/j.1460-2466.2007.00356.x

Juul, J. (2012). *A casual revolution: Reinventing video games and their players*. Cambridge: The MIT Press.

King, D. L., Delfabbro, P. H., Kaptsis, D., & Zwaans, T. (2014). Adolescent simulated gambling via digital and social media: An emerging problem. *Computers in Human Behavior*, *31*, 305–313.

D King, P Delfabbro, M Griffiths, (2010) The convergence of gambling and digital media: Implications for gambling in young people, *Journal of Gambling Studies* 26 (2), 175-187

Kopp, C. B. (1982). Antecedents of self-regulation: a developmental perspective. *Developmental Psychology*, *18*(2), 199

Kuittinen, J., Kultima, A., Niemelä, J., & Paavilainen, J. (2007, November). Casual games discussion. In *Proceedings of the 2007 conference on Future Play* (pp. 105-112). ACM, p. 106

Kypri, K.; Voas, R.B.; Langley, J.D.; et al. (2006) Minimum purchasing age for alcohol and traffic crash injuries among 15- to 19-year-olds in New Zealand. *American Journal of Public Health* 96:126–131.

Lange, P. G. (2011). Learning Real-Life Lessons From Online Games. *Games and Culture*, *6*(1), 17-37.

Lenhart, A., Madden, M., Smith, A., Purcell, K., Zickuhr, K., and Rainie, L. (2011). *Teens, Kindness and Cruelty on Social Network Sites*, Pew Internet and American Life Project. Online. Retrieved from: http://pewinternet.org/~/media//Files/Reports/2011/PIP_Teens_Kindness_Cruelty_SNS_Report_Nov_2011_FINAL_110711.pdf (accessed 15 August 2012).

Lesieur, H. R, & Rosenthal, R.J. (1991). Pathological Gambling: A review of the literature (prepared for the American Psychiatric Association task Force on DSM-IV Committee on Disorders of Impulse Control Note Elsewhere Classified. *Journal of Gambling Studies*. 7(1)

Livingstone, S., (2010). *e-Youth: (Future) Policy Implications: Reflections on Online Risk, Harm and Vulnerability*. Paper presented at e-Youth: Balancing Between Opportunities and Risks, 27–28 May

2010, UCSIA and MIOS University of Antwerp, Antwerp, Belgium. Retrieved from <http://eprints.lse.ac.uk/27849/> (accessed 28 August 2012)

Livingstone, S. and Bulger, M. (2013). *A Global Agenda for Children's Rights in the Digital Age*. UNICEF Office of Research: Florence. Available at: http://www.unicef-irc.org/publications/pdf/lse%20olol%20final3.pdf (accessed 3rd February 2014)

Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). *Risks and Safety on the Internet: The Perspective of European Children. Full Findings.* London: EU Kids Online, LSE.

Livingstone, S., Ólafsson, K., O'Neill, B and Donoso, V. (2012) Towards a better internet for children: findings and recommendations from EU Kids Online to inform the CEO coalition. London: EU Kids Online, LSE. Available at: http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/EUKidsOnlinereportfortheCEOCoalition.pdf (Accessed 14th February 2014)

Lovell, N., (2011, Jan. 11) What is a social game?, *Games Brief*. Retrieved from: http://www.gamesbrief.com/2011/01/what-is-a-social-game/

Madden, M., Lenhart, A., Cortesi, U., Duggan, M., and Smith, A. (2013) *Teens, Social Media and Privacy* Pew Internet and American Life Project. Online. Available at: http://www.pewinternet.org/Reports/2013/Teens-Social-Media-And-Privacy.aspx (accessed 1 July 2013).

Namrata Raylu, Tian P.S Oei, (2002) Pathological gambling: A comprehensive review, *Clinical Psychology Review*, Volume 22, Issue 7, Pages 1009-1061.

Nikken, P., Jansz, J., & Schouwstra, S. (2007). Parents' interest in videogame ratings and content descriptors in relation to game mediation. *European Journal of Communication*, *22*(3), 315-336.

OfCom. (2012). *Children and Parents: Media Use and Attitudes Report*. London. Available at: http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/oct2012/main.pdf (Accessed 3rd February 2014)

O'Neill, B. (2013). Who cares? Practical ethics and the problem of underage users on social networking sites. *Ethics of Information Technology*. 15: 253-262

Parke, J., Wardle, H., Rigbye, J., & Parke, A. (2013) *Exploring Social Gambling: Scoping, Classification and Evidence Review*. London: Gambling Commission.

Pearl, R. (1926). *Alcohol and Longevity*. New York: Knopf.

Phonepayplus (2012) http://www.phonepayplus.org.uk/for-business/research/~/media/Files/PhonepayPlus/Research/Consumer%20Research/PhonepayPlus%20Online%20Gaming%20and%20Payment% (Accessed February 15th 2014)

Phonepayplus (2013) Children as Connected Consumers http://www.phonepayplus.org.uk/News-And-

Events/News/2013/1/~/media/Files/PhonepayPlus/Corporate_and_Governance/PhonepayPlus_Children_as_Connected_Consumers_2013.pdf (accessed February 15th 2014)

Rehm J, Room R, Graham K, Monteiro M, Gmel G, Sempos CT. (2003) The relationship of average volume of alcohol consumption and patterns of drinking to burden of disease—an overview. *Addiction*; 98: 1209–28.

Room, R., Babor, T., and Rehm, J. (2005) "Alcohol and Public Health". *The Lancet*. 365: 519-30.

Shin, W., & Huh, J. (2011). Parental mediation of teenagers' video game playing: Antecedents and consequences. *new media & society*, *13*(6), 945-962.

Shuler, C. (2012). iLearn II: An Addendum An Analysis of the Games Category of Apple's App Store.

Shontell, A. (2012, Feb. 22) How To Get 60 Million Users Without Using Any Social Media, *Business Insider*. Retrieved from: http://www.businessinsider.com/how-to-get-60-million-users-without-using-any-social-media-2012-2#ixzz1pZkyGZl4

Smith, G.S., Branas, C.C., and Miller, T.R. (1999) "Fatal nontraffic injuries involving alcohol: a metaanalysis". *Annals of Emergency Medicine*, 33 (6): 659-68.

Sparrow, M.K. (2008) *Can Internet Gambling be effectively regulated? Managing the risks.* Cambridge: Harvard University

Staksrud, E. (2013). *Children in the Online World. Risk , regulation, rights*. London: Ashgate

Torres, C. A., & Goggin, G. (2014). Mobile social gambling: Poker's next frontier. *Mobile Media & Communication*, *2*(1), 94-109.

University of Adelaide SA Center for Economic Studies and Department of Psychology (2005). *Problem Gambling and Harm: Towards a National Definition*. Melbourne: Office of Gaming and Racing, Victoria Government Department of Justice. Available at: http://www.adelaide.edu.au/saces/gambling/publications/ProblemGamblingAndHarmTowardNationalDefinition.pdf. Accessed 2 July 2013.

Van Reijmersdal, E. A., Jansz, J., Peters, O., & van Noort, G. (2010). The effects of interactive brand placements in online games on children's cognitive, affective, and conative brand responses. *Computers in Human Behavior*, *26*(6), 1787–1794. doi:10.1016/j.chb.2010.07.006

Wallace, M., & Robbins, B. (2006). Casual games white paper. *IGDA Casual Games SIG,* Retrieved from: http://www. igda. org/casual/IGDA_CasualGames_Whitepaper_2006. pdf

Waller, P. F., Hill, E. M., Maio, R. F. and Blow, F. C. (2003), Alcohol Effects on Motor Vehicle Crash Injury. *Alcoholism: Clinical and Experimental Research*, 27: 695–703.

Williams, R.S., & Ribisl, K.M. (2012). Internet Alcohol Sales to Minors. *Archives of Paediatrics and Adolescent Medicine*. 166(9):808-13.

Wohn, D. Y. (2011). Gender and Race Representation in Casual Games. *Sex Roles*, *65*(3-4), 198–207