From legitimacy to informed consent: mapping best practices and identifying risks

A report from the

Working Group on Consumer Consent

May 2009

PEN paper 3

About the Working Group

The Working Group on Consumer Consent is a project convened by the Information Systems & Innovation Group of the London School of Economics and Political Science and administered by 80/20 Thinking Ltd, based in London UK.

The Working Group aims to bring together key industry players, consumer experts and regulators to achieve the following goals:

- To better understand the implications of the Article 29 Working Party Opinion on data protection issues related to search engines (April 2008) and its potential impact on the processing of personal information in the non-search sectors.
- To foster dialogue between key stakeholders to map current practices relating to notification and consent.
- To inform regulators about limitations and opportunities in models and techniques for informed consent for the processing of personal information.
- To help inform all stakeholders on aspects of the pending Article 29 Opinion on targeted advertising planned in 2009.

Membership

The members of the Working Group included: AOL, BT, Covington & Burling, eBay, Enterprise Privacy Group, Facebook, the Future of Privacy Forum, Garlik, Microsoft, Speechly Bircham, Vodafone, and Yahoo!

We also sought comments from a number of privacy commissioners and regulators from across Europe.

Methodology, Meetings, and Outreach

We have been actively engaging with policy-makers and regulators since the creation of the group. This networking not only enhances the quality of the research, but also goes some way to identify and prepare the audience for our discussion papers. We have liaised with Parliamentarians in Europe and in the UK, staff members of regulators offices across Europe, and spoken at more than a dozen conferences and countless meetings since our last update.

We have also met with nearly every group member, often on-site, and sometimes involving in-depth discussions regarding privacy practices across their services, to discuss the pressing problems, the key experiences, and lessons.

All of the feedback from these experiences has fed into our own work, resulting in our discussion papers.

The sections on the Article 29 Opinion and on the general issues relating to online Consent were drafted primarily by the teams at LSE and 80/20 Thinking. The section on 'informed consent' was drafted by Speechly Bircham, and the section on children and consent was drafted by Covington & Burling. All drafts were circulated to the full membership for their review and commentary, and comments were fed back into the final versions.

Table of Contents

Executive Summary

In April 2008, Data Protection Regulators from across the European Union released their opinion on the processing of personal data by search engine providers. In that document, the Article 29 Working Party recommended that search engine providers must obtain consent from their users before engaging in any data collection or profiling. This was a controversial conclusion and stirred a vigorous debate across industry and civil society organisations. A more subtle and yet interesting controversy arose from the Working Party's requirement for service providers to enable both authenticated and non-authenticated users to provide consent. They signaled this requirement while also hinting that it should apply to all 'information society' services and utilities.

The Consent Working Group was established immediately afterwards, bringing together academia, industry, and civil society, with the goal of bringing forth ideas to regulators and policy-makers to inform future policy-making. The Working Group is not a lobbying exercise, however, and was established to be a research initiative. The research objective is to explore the contextual nature of consent together with its inherent complexity. This report is the culmination of our research.

We start by reviewing some of the challenges that surround obtaining online consent from technical and legal perspectives. As most consent forms resemble in one way or another electronic contracts, their effectiveness and ease of use depend on their readability and linguistic clarity. Privacy policies remain difficult for many users to comprehend and a number of initiatives have tried to simplify them while still conveying the necessary information needed for users to make an informed decision. We review the opportunities offered by layered privacy policies, aiming at simplifying the legalistic nature of the texts, and privacy enhancing technologies (PETs), aimed at providing the necessary tools for users to exercise control over their privacy settings.

For online consent to work, however, companies may need to make sure that the person who is expressing his or her will is in fact the relevant user and not someone else. Thus some form of credential verification (as examples, relative uniqueness of identity, and age) is needed. The controversy around children's representation online also needs to be resolved as children are an increasingly active group in today's Internet economy and ignoring their relationship with businesses could have serious overall consequences.

Yet, in the process of garnering consent in order to protect the privacy of individuals, we may be first requiring users to disclose information about themselves. In this sense, the remedy destroys the protections. The Article 29 Working Party requires that consent be managed even for anonymous users, thus creating a conundrum for service providers.

Probably the most contested issue surrounding online consent is the way the process is expressed, or "signaled" by users. Despite the similarities with e-contracts, users do not always enter actual contractual agreements when simply browsing the Web. Thus, obtaining meaningful consent from non-authenticated users for the purpose of data collection, as recommended by the Working Party, remains contradictory. One way of addressing this challenge has been to

offer users the option to opt-out of data collection for the purposes of behavioural targeting or profiling. This is still an ambiguous process. Despite the fact that the industry standard is currently set to opt-out, it is debatable to what extent opt-in or opt-out are more appropriate given the current level of user sophistication and awareness of data mining practices. We review the experiences of companies like Facebook, AOL, eBay, Microsoft, Bluekai and Google to inform our work in this domain.

In order to provide background for a meaningful review of industry practices, section II of this report studies the legal qualification of 'informed consent'. Some important points we revisit include the purpose and method of data collection, fair processing, and the possibility for data subjects to object to data being used for certain purposes, such as advertising and third-party processing. Some of the most significant legal challenges faced by website operators remain associated with data exports and further complicate the publishing of personal data online, as the latter can easily be accessed from third countries. We then discuss the challenges associated with company ownership and the issue of legal accountability when an operator's site is hosted by a third party or when a website operator is taken over. In all of these cases the operator remains responsible for processing personal information securely and is advised to adopt appropriate technological and organizational measures to secure information under all foreseeable circumstances. In practice, however website operators vary widely in how they comply with their duties and data protection legislation. As evidence, we provide an analysis of the practices and policies of Disney, Expedia, MSN, Electronic Arts, PayPal, Pipex, Fidelity, and others.

In section III of this report we report on how securing consent from children remains central to the debate on obtaining meaningful consent online. While the EU Data Protection Directive provides that consent can serve as a legitimate basis for the processing of personal and even sensitive personal data, it offers virtually no guidance on how these terms should apply to cases where consent is sought from children. National legislators have thus adopted differing approaches, which make data protection compliance for international companies challenging, and often quite costly. Many institutions are working to remedy this situation by offering unified guidance on collecting consent from children. One such example is the European Commission's Safer Internet Program, which aims at promoting safer use of the online technologies and the recently released a public consultation on "Age Verification, Cross Media Rating, and Classification and Online Social Networking". There are other initiatives at the national level, which we look into, alongside applicable lessons learned from the US Children's Online Privacy Protection Act. A number of different methods for obtaining consent online illustrate the current inadequacy of age verification systems and prove that extra efforts are required to solve issues of interoperability and to ensure that an infrastructure for identity technologies to becomes more reliable.

In order to place the different legal and policy challenges in context, the report is interspersed with industry examples. These are also used to review opportunities in the area of online consent management, as exhibited by the efforts of private companies to facilitate, simplify, and inform the process of giving and obtaining meaningful and lawful consent on the Web.

Background to this Project

The Working Party Opinion on Search Engines and Information Society Services

The Article 29 Working Party Opinion of April 2008 relates primarily to search engine providers. But like so many of its recent opinions, the Article 29 Working Party's decision has a wider application. This briefing outlines the key components of the opinion, and the implications for online service providers and has been prepared for the Working Group on Consumer Consent (hereinafter referred to as the *Consent Project*).

The Article 29 Working Party developed its opinion in response to a number of developments in the search sector. First, in view of the sensitivity of personal information contained in search logs, the Article 29 Working Party believes that search engine providers have insufficiently explained the nature and purpose of their operations to the users of their services. Second, as search engine providers also perform the role of content providers through helping to make publications on the Internet easily accessible, the Working Party contends that the services' representation and aggregation capabilities (e.g. the creation of personal profiles) can significantly affect individuals, especially if the personal data in the search results are incorrect, incomplete, or excessive.

It is important to note that the Working Party's reasoning for calling for changes in compliance practices may well be applied to many other **information society services**[1]. That is, the Working Party declares that in the context of the Directive on Electronic Commerce (2000/31/EC), search engines are a type of information society service (Directive 98/34/EC)[2], namely information location tools[3]. Therefore the issues that the Working Party raised could very well apply to all information society services.

In our analysis of the opinion, the implications across sectors are as follows:

Regulators will require greater transparency. Data collectors will need to be clearer about what information is collected, how it is processed, and why it is retained. In the opinion, the Working Party calls for 'comprehensive and detailed justifications'. The opinion also declares some relatively firm barriers to these justifications. *As interfaces shrink in size and profiling regimes become more sophisticated, the Consent Project notes that further challenges will emerge for communicating transparency practices, and identifying the qualities and*

---

[1] See Recital 18 of the Directive on Electronic Commerce (2000/31/EC): Information society services span a wide range of economic activities which take place on-line; these activities can, in particular, consist of selling goods on-line; information society services are not solely restricted to services giving rise to on-line contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data; information society services also include services consisting of the transmission of information via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service.

[2] Defined in Directive 98/34/EC as amended by Directive 98/48/EC.

[3] See Article 21.2 in connection with Recital 18 of the Directive on Electronic Commerce (2000/31/EC).

characteristics of good practices. We must also better understand and communicate justifications for extended processing of personal information.

We must devise more effective regimes and mechanisms for consent and access. Individuals must be able to use information society services without having to authenticate themselves. However if any processing of their personal information is conducted consumers must be provided with mechanisms to consent to this processing. Such mechanisms must allow consent without the need to identify oneself ahead of time. Consequently, individuals must also be able to access their profiles, particularly those that are generated for the purpose of targeted advertising. *The Consent Project decided that it was essential to review existing consent and subject access models, as well as identify the likely challenges and technological constraints.*

We need to consider methods of reducing the processing of personally identifiable information in such services. The Opinion qualifies IP addresses and unique identifiers as personal information that can be linked back to individuals through other stakeholders. The Working Party calls for meaningful anonymisation techniques. *We therefore need to encourage discussion and research on what qualifies as meaningful anonymisation techniques, and other technological protections that can be considered to ensure that processing of personal information is kept to a minimum, particularly as industry moves into location and behavioural targeting.*

Legal Framework

The Working Party opinion provides further guidance on application of the definitions of "personal data" and "controller" to search engine providers. The primary focus is on search engines whose business model is based on online advertising.

The Directive generally applies to both EEA-based and non-EEA based providers where the latter have an establishment in a Member State or make use of equipment on the territory of a Member State. Non-EEA based search engine providers should inform users about the conditions in which they must comply with the Directive, whether by establishment or by the use of equipment.

The Directive does not apply to the processing of personal data by information society services that act as mere information intermediaries.[4] However, search engine providers do not always

[4] In this briefing we are limiting discussion to the Data Protection Directive. The Working Party also notes that search engine providers may also have to adhere to Directive 2002/58/EC (ePrivacy Directive) and Directive 2006/24/EC (Data Retention Directive), though search engines fall outside of the scope of "electronic communications service" as defined in Article 2(c) of the Framework Directive 2002/21/EC. However, additional services offered by search engine providers, such as publicly accessible e-mail services may fall within the scope of an electronic communications service. If so, both directives could apply. The ePrivacy Directive offers general provisions on cookies, spyware and unsolicited communications, which are applicable to any services when these techniques are applied. The Data Retention Directive does not apply to the task of providing responses to search engine queries.

limit themselves to an intermediary role.[5] The Directive applies when a search engine performs value-added operations on personal data (profiling, advertisements triggered by an individual's name) or act as controllers of the personal data contained in the cached publications. Therefore, it is essential that search engine providers respect search engine and caching opt-outs expressed by website editors. This point will likely extend to cross-site advertising schemes.

Summary of Relevant Points raised in the Opinion

Processing of Personally Identifiable Information: The Article 29 Working Party believes that search queries do not need to be attributable to identified individuals in order to improve search services. Similarly, any personal data processed and stored for system security, fraud prevention or accounting purposes must be subject to strict purpose limitations. Therefore, data stored for security purposes may not be used to optimise a service for instance. The Working Party has a clear preference for anonymisation of personal data used for the above purposes. In addition, while search engine providers will need to comply with valid legal orders for the purpose of crime detection and prevention, this compliance should not be mistaken for a legal obligation or justification for storing such data solely for these purposes.

Retention periods – for each purpose a specific limited retention period should be specified. A29 does not see a basis for a retention period beyond 6 months. However, the retention of personal data and the corresponding retention period must always be justified and reduced to a minimum, to improve transparency, to ensure fair processing, and to guarantee proportionality with the purpose that justifies such retention. Organisations retaining personal data longer than 6 months must demonstrate comprehensively that it is strictly necessary for the service. If search engines provide a cache in which personal data is made available for longer than the original publication, they must respect the right of data subjects to have excessive and inaccurate data removed from their cache. Search engines should respect website editor opt-out requests, indicating that their website should not be crawled and indexed or included in the search engine's caches. Once the data no longer match the actual contents published by the controllers of the website(s) publishing the information, and the search engine provider receive a request from a data subject, they must act promptly to remove or correct incomplete or outdated publication. Such services should be offered free of charge.

Further processing for different purposes – The Working Party is aware that full disclosure about the further use and analysis of user data could result in increased vulnerability of search engine services to abuse, however such considerations cannot be used as an excuse to not comply with applicable data protection laws. Furthermore, search engine providers cannot claim that their purpose in collecting personal data is the development of new services whose nature is as yet undecided.

---

[5] In this opinion search engine providers are seen as having two roles. First they are data controllers, in the traditional sense of the data protection law, meaning a body that determines the purposes and means of the processing of personal data, in this case the search engine responds to users' search queries. Second, they are also content providers in that they retrieve and group widespread information about a single person, and conduct other activities such as the republishing of data in "cache".

Cookies – The responsibility for processing cannot be reduced to the user for taking or not taking precautions through their browser settings. The search engine provider determines if a cookie is stored and for what purposes it is used, thus an appropriate lifetime should be defined and users should be fully informed, especially in view of default browser settings. This information should be more prominent than search engine privacy policies. Flash cookies should only be installed if transparent information is provided about how to access, edit or delete them.

Anonymisation – If there are no legitimate grounds for processing of personal data beyond the well-specified legitimate purposes, search engine providers must delete personal data, or alternatively anonymise it. Anonymisation must be fully irreversible in order for the Data Protection Directive to no longer apply. **Anonymisation of data should exclude any possibility of any individuals to be identified even when combining data held by search engine providers with data held by other stakeholders, such as ISPs.**

Data correlation across services – when search engine providers also provide personalized services, such as e-mail, chat, social networking sites, etc. the obligations upon providers become more onerous. Correlation of personal data across services and platforms for authenticated users can only be done based on informed consent.

Consent - Any profiling of natural persons or other value-added services should only be performed after expressed consent has been obtained from the user. Registration with a search engine provider in order to benefit from a more personalized service should be voluntary. As it is possible to conduct correlation for non-authenticated users, based on IP and unique cookies that can be recognized by all services offered by a search engine provider, organisations should be very clear about the extent of correlation of data across services and only proceed on the basis of consent. Similarly, consent would have to be garnered from non-authenticated users prior to their personal data being processed or stored for any other purpose than acting upon a specific request with a list of search results.

Obligation to inform data subject - If users are unaware that processing of personal data takes place, they are unable to make an informed decision. Thus, the A29 opinion places the following obligations on search engine providers:

- Search engines must provide a basic description of the use of personal information when collected, with a more detailed description provided elsewhere.
- They must inform users of the organisations identity and location. Non-EEA based search engine providers should inform users about the conditions in which they must comply with the Data Protection Directive, whether by establishment or by the use of equipment.
- They must inform users about software, such as cookies, and how these can be refused or deleted.
- They must ensure easy access to the privacy policy before conducting any search, including from the search engine home page.

The A29 opinion notes deficiencies with regard to data subject rights of access or deletion included in Articles 12, 13, and 14 of the Directive.

Transparency and Subject Access - Enrichment of user data with data provided by third parties might be unlawful if the data subjects are not informed at the time of collecting their personal data and if they are not granted easy access to their personal profiles and the right to correct them or delete certain elements that are incorrect or superfluous. This applies particularly to authenticated users. However these rights also apply to non-registered users, who should have the means to prove their identity with a statement from their access provider regarding the use of specific IP or/and by registering for access to future data. Search Engine providers are thus expected to provide the necessary technical tools for the exercise of these rights, such as a web-based tool that allows registered users direct access to their profiles and allows them to oppose certain data processing.

Conclusions

As the Article 29 Working Party moves on to other internet policy domains including behavioural targeting, this decision from April 2008 provides an insight to the reasoning of regulators. The opinion's elaboration on the obligations placed upon search engines could be placed upon any 'information society service', or online service. It is therefore essential that we prepare the required documentation, reporting structures, research and thought-leadership to consider these dynamics of consent, transparency, and the processing of personal information.

SECTION I: Problems with Consent

The Article 29 Working Opinion on search engines reaffirmed the applicability of European data protection law, recommending a maximum retention period of 6 months and indicating that web users must be able to provide consent to the exploitation of their data - in particular for profiling purposes. This report focuses on the implications of that second point about the provision of consent.

The main reason behind this call for change was the belief of the Working Party that search engine providers have insufficiently explained to users the nature and purpose of their operations. Thus, the Article 29 Working Party recommends that consent mechanisms must be devised to provide consent without users having to identify themselves ahead of time, thus enabling authenticated and non-authenticated users to explicitly consent to data collection.

In this section of the report, we explore the nature of consent as pertaining to the use of online services in general, or as termed in the Directive of Electronic Commerce (2000/31/EC), "information society services"[6].

Consent cannot be viewed as a freestanding concept. While its early adoption is associated with medical practice and the right of patients to be informed about the risks of medical procedures that might affect their wellbeing, today its scope has broadened to include, amongst other elements, the right of online service users to be informed of the way their personal information is used. According to some, the complexity of consent stems from its implication in the right to privacy, the right to confidentiality, and the right against discrimination, the benefit of which the rights-holder may consent to wave.[7] While Black's Law Dictionary[8] frames consent as "an agreement, approval, or permission as to some act or purpose", the latter remains contextual by nature, as indicated by differing court decisions in consent-related cases[9].

In addition to the traditional requirement for disclosure of risk[10] associated with medical practices, service provision in online environments has created a new and different set of challenges for the obtaining and provision of informed consent. Web-based services have

---

[6]See Recital 18 of the Directive on Electronic Commerce (2000/31/EC): Information society services span a wide range of economic activities which take place on-line; these activities can, in particular, consist of selling goods on-line; information society services are not solely restricted to services giving rise to on-line contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data; information society services also include services consisting of the transmission of information via a communication network, in providing access to a communication network or in hosting information provided by a recipient of the service

[7] Roger Brownsword , 'The Cult of Consent: Fixation and Fallacy', King's College Law Journal, 15:2004, 223.

[8] Black's Law Dictionary 323 (8th ed. 2004)

[9] DoubleClick Inc. Privacy Litigation, 154 F. Supp 2d 497, 507, 519 (S.D.N.Y. 2001); Pharmatrak Inc, Privacy Litigation, 220 F. Supp. 2d 4, 15 (D. Mass. 2002); Inc. v. Bidder's Edge, Inc. eBay. 100 F. Supp. 2d 1058 (N.D. Cal. 2000); Moore v Regents of the University of California 793 P2d 479; Greenberg v Miami Children's Hospital Research Institute, Inc 208 F.Supp. 2d 918 (ND Ill. 2002).

[10] Nora Moumjid, Marie-France Callu, 'Commentary: informed consent and risk communication in France', BMJ, 327, Sept. 2003.

raised questions about the adequacy of information provided by online advertisers, search engine providers, and social networking websites. How much do users need to know about company data protection practices? Do they need to know within which jurisdiction their data is stored? Do they need to be informed of internal auditing procedures? These are all questions that contribute to the emerging debate on online consent. The design principles of the Internet itself may be based on a norm of implied consent, to enable a functioning communications system, but when individuals are subject to monitoring and profiling by private companies, human rights concerns and governance issues simultaneously arise. That is, individuals are subjected to profiling and detailed analysis of their habits and activities, and yet they are not even aware that this activity is occurring. Even if they are aware of the practice, they are often unable to even trace the activity back to an identified data processor. Therefore, these concerns arise not because targeted advertising, for example, is harmful in itself but because users are not necessarily aware of the fact that it is taking place, let alone aware of the possible consequences of personal data loss or misuse. Secret or hidden processing and storage of data is generally outlawed in the EU. This is why the Working Party has recommended that online service providers obtain consent from both authenticated and non-authenticated users before collecting their personal information. However, this proposition poses a number of challenges that need to be addressed and resolved before a truly workable solution can be found.

Challenges of managing consent online

Readability & Usability

Often, the readability of digital contracts is different from that of paper ones. For informed consent to work, users must be presented with comprehensive but clearly written information in accessible language. Studies show that privacy policies are hard to read, are read infrequently, and do not support rational decision-making, while often being the only source of information available to users. Systems should ideally be logical and transparent to users. Policies therefore present an important challenge in terms of finding the best way to convey complicated but critical information without overwhelming users.

Currently there are a number of industry initiatives that attempt to fill this gap. As early as 2001, Abrams and Crompton from the Center for Information Policy Leadership (CIPL), Hunton & Williams, proposed the use of layered policies as a way of achieving completeness and improved readability of privacy notices[11]. In an attempt to make privacy policies more readable and also enforceable, others have tried to tackle the same issue through privacy enhancing technologies (PETs). Two privacy policy specification languages have emerged: Privacy Preferences Project (P3P) and a P3P Preference Exchange Language (APPEL), both designed

[11] A multi-layered notice has two or more layers that work together to give the individual complete information in a manner in which one can understand information use and make choices. Layered notices were first suggested by the Center for Information Policy Leadership (CIPL), Hunton & Williams in December 2001 at a workshop sponsored by US Financial Services Regulatory Agencies.

by the W3C's[12]. P3P enables websites to encode their data-collection and data-use practices in a machine-readable XML format, known as P3P policies. In turn, APPEL allows users to specify their privacy preferences. Ideally, through the use of P3P and APPEL, a user's agent should be able to check a website's privacy policy against the user's privacy preferences, and automatically determine when the user's private information can be disclosed. Both policy languages are designed to enable users to play an active role in controlling their private information and depend heavily on user cooperation.

While these might seem to provide viable solutions, as research in the area shows[13], a number of challenges, such as the need for well-defined semantics for P3P, still remain. Experts[14] also claim that existing languages for specifying privacy policies are limited in expressive power and lack enforcement and auditing support. Furthermore, these solutions fall short of the universal and default expectations favored by regulators.

Moreover, the burden placed upon the individual to read these policies stretches the limits of acceptability. A recent study[15] points out that the additional time spent by users for comparing policies between multiple sites in order to make informed decisions brings the social cost well above the market for online advertising itself. This leaves us with the same question: how can companies provide the information users need to make informed choices in simple terms while remaining transparent about the often quite complex company data collection practices? Disclosure legislation may sound promising but prove insufficient, as adding more text to policies that most consumers do not read does increase transparency, but may otherwise be of limited practical utility[16].

Verifiability of consent

Once users have been provided with an adequate level of information about data collection and processing practices (however we define "adequate"), they are sometimes given an option to check a box as an expression of their consent to the privacy policies. Frequently however their consent is inferred, whereby if the user continues to surf a site, or completes a purchase, they are considered to have agreed to the privacy practices. Even where there is a checkbox, in online environments it is difficult to know who is checking that box, his or her age, or the relevant identity. While some age verification mechanisms exist, the reality is that for the most part companies make assumptions. The problem is further aggravated in the case of mobile

---

[12] World Wide Web Consortium: http://www.w3.org/

[13] Ting Yu, Ninghui Li, Annie I. Antón, 'A Formal Semantics for P3P', ACM Workshop on Secure Web Services, October 29, 2004, Fairfax VA, USA; Annie Anton, Elisa Bertino, Ninghui Li, Ting Yu, 'A roadmap for comprehensive online privacy policy management', Communications of the ACM, July 2007/Vol. 50, No. 7.

[14] Annie I. Antón, Elisa Bertino, Ninghui Li, and Ting Yu, 'A Roadmap for Comprehensive Online Privacy Policy Management', Communications of the ACM, July, 2007/Vol. 50, No. 7.

15 Aleecia M. McDonald, Lorries Faith Cranor, 2008, 'The cost of reading privacy policies', Carnegie Mellon University, Revised September 26, 2008 for the Telecommunications Policy Research Conference. The report also tried accounting for the costs of reading these policies, and approximated the cost of time in the order of $365 billion (US nationwide) per year or about $2,949 annually per American Internet user.

[16] Id.

telephones, where young children access services outside of the environment of the home, and thus beyond parental oversight.

Creating mechanisms for age verification is directly linked to another issue, not yet resolved at the international level, thus inapplicable to a borderless online environment: the legal capacity to consent. Can a child of any age consent to behavioral targeting? Can a child of any age create an account on Facebook or MySpace? Under English common law, for example, a child can exercise legal rights when he or she has sufficient understanding and intelligence to comprehend what they are doing. There is also a general presumption that a child has sufficient understanding and intelligence to exercise a right (such as under data protection law) when that child is aged 12 years or over. Unfortunately, as a study conducted by Vodafone shows, the rules governing children's legal capacity to consent are not harmonized across Europe[17], an issue that we revisit in later sections in this report. This makes the offering of standardized privacy policies, abiding simultaneously by differing national laws, challenging, to say the least.

As a child has a right to privacy and autonomy, one can argue that whether a child can provide lawful consent or not should be determined not by their age but rather by their level of maturity and proven ability to exercise that right of autonomy alone. In WP147 on the protection of Children's Personal Data[18] the A29 Working Party provides direction on this issue: "as the guidance of legal systems in different countries is quite divergent on the issue of age, the maturity of a child needs to be considered when determining the need for representation".

Identity verification is however rarely discussed in the context of the different levels of anonymity available to users. Online service providers vary widely and with them vary the types of data they request from users in order to provide a service, as well as the time period for which PII is retained and the way it is anonymised (or not). As privacy regulations generally apply to all companies that collect and process personal information, the latter have no compliance incentive to reduce the identifiability of the data they hold. Recognizing that depending on the level of anonymity and thus identifiability of data, users are exposed to different levels of risk, and adjusting regulatory compliance expectations accordingly, might provide a stimulus for data controllers to make that extra step in anonymising customer data. If this principle is accepted it might provide a potential platform for industry, policy makers and regulators to investigate how better to manage consent dependent upon how 'identifiable' the data (and therefore the user) is.

Custodianship of data

In addition to verifiability of identity and age, online firms are struggling with the notion of custodianship of the children's data they collect and manage. With the advent of online health management platforms such as Microsoft Health Vault and Google Health, new types of questions need to be answered regarding children's right to autonomy. At what age can a child revoke access to their health records, held in an account originally created by their parent? If

17 'Children's' Legal Capacity to Consent to the Processing of Their Personal Data', Stephen Deadman, Vodaphone Group Services Limited, June 2006.

18 Working Document 1/2008 on the protection of Children's Personal Data, available at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm

such platforms do not offer certain granularity of options for access control, could this result in a violation of the doctor-patient privilege to which everyone is entitled?

While as mentioned above, the Article 29 Working Party provides some guidance on children's capacity to consent, WP147 fails to recognize children's increasing interaction with the private sector. Thus privacy law needs to be adapted to recognize that type of new commercial relationship, which is often quite different from children's interactions with the public sector.

Again in WP147, it is pointed out that when very personal rights are concerned - as for instance in the health field - children could even ask their doctors not to disclose their medical data to their representatives, the criteria for the conditions of access being not only the age of the child, but also whether or not the data concerned were provided by the parents or by the child. Furthermore, while in theory parental consent mechanisms offer an alternative means of obtaining consent where the user is incapable of giving a valid lawful consent, these are often not suited to online or distance relationships.

Data custodianship brings up another important issue, that of users' new ability to control their own data. Control here means not only giving free consent after having been informed of risks but the actual use of tools that determine how and by whom personal data is used. Health Vault and Google Health only show part of the picture. Social networking sites provide an even more illustrative example. They enable users to control not only their own data but often that of their friends by providing the tools to upload videos and photos of others and tag them, though only to some extent. Thus users, similarly to corporate data controllers, are now empowered with processing capabilities that enable the creation, publication, and dissemination of personal information. If this is increasingly the case, will we soon need to reconsider the existing consent model? If a company merely provides the tools for users to determine the use of personal data, should it be the one held accountable? Should it be the one that needs to obtain consent? What control mechanisms would be suitable for this new and fluid data ownership model given that there is no existing privacy framework regulating consumer behavior? These are just some of the most pertinent questions raised by evolving data sharing models. Whether the appropriate solution will come from legally binding agreements or technology itself is yet to be seen.

Facebook recently updated their terms of use[19] to address precisely this conundrum but received harsh criticism for trying to increase their control over user content by retaining certain types of information, such as copies of messages sent to others, even after the deactivation of an account. The networking site argues that the update of its terms was necessary as currently there is no system that allows users to freely share information with others and at the same time control how this information is used by those they have entrusted with it. This however is just the beginning of an important privacy debate where cultural and social norms will play important roles in redefining the importance and nature of online consent itself.

[19] http://www.facebook.com/terms.php#/terms.php?ref=pf

Third party accountability

Online services that are increasingly offered by multiple partners and transitioning from one website or platform to another is often not as obvious as walking from one store to another is in real life. This somewhat confusing web of relationships, at least to the average user, is typically governed by contractual agreements, such as developers' terms of service or service level agreements. While those ensure that third-party service providers abide by the rules and the applicable laws, privacy protections vary from one provider to another and they might not always meet the requirements or preferences of the individuals who are subject to data collection. What users are typically left with, if they want to be informed of data collection and processing practices, is having to read individual partner terms of service and privacy policy statements and, as mentioned above, this could be a time consuming and costly task.

Furthermore, media consolidation means that multiple sites may share one privacy policy, which is often ineffective in communicating the different data practices to which the users of those sites might be subjected. Thus, a new method of communicating privacy policies of complex online partnerships is needed in order to enable users to make informed choices about how, where, and when their personal data are or might be used.

Signaling of consent

There are a number of different ways to express consent online. Some of the techniques used, especially in the US, are "shrink-wrap" (requires clicking on an icon) and "browse-wrap" (there is a link to the terms of the contract at the bottom of the page) e-contracts. However, the reliability of these procedures as adequate means of expressing one's will has been widely debated. While certainly relevant to consumer behavior online, those types of digital contracts are not always representative of the types of interaction people have with websites when simply browsing the Internet, whether as authenticated or unauthenticated users. As European policy makers encourage search engines (and imminently other information society services) to obtain consent, the question of identification becomes central to the signaling of consent. Exactly how practicable it is, however, to obtain consent from non-authenticated users without verifying their identity remains to be discovered. The most promising development in this regard is Credentica's U-Prove technique of selective disclosure of personal information for the purpose of authentication, but for this to meet the needs of all EU citizens, every consumer and company would have to sign up to this service.[20]

Mobile phone operators offering web-based services face similar consent-related issues. There is growing consensus amongst those companies that privacy policies displayed on mobile phones need to be multi-layered, comprehensible, legally compliant, consistently formatted, and brief[21]. Obtaining consent for the purpose of m-advertising makes providing disclosure about

---

[20] In an interesting development, Microsoft purchased Credentica in March 2008. While this will advance the likelihood of Credentica's techniques being embedded within the infrastructure of electronic commerce and services, it may also give rise to competition concerns amongst EU authorities.

[21] Nancy J. King, 'Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices', 60 Fed. Comm. L.J. 229 2007-2008.

information processing practices in an appropriate manner even more pertinent. Current practices used by m-advertisers are similar to e-contracts used online and include browse-wrap and shrink-wrap contracts. There are other emerging techniques for obtaining consent in m-environments, responding to some extent to the criticism of browse-wrap agreements (click-wrap require the actual checking of a box), which do not require an action to signify agreement. Those include the possibility of mobile phone users to make a call to the service provider or send a text message.

Given the importance of informed consent, more in depth evaluation of the efforts of companies to bring the contractual clauses to the attention of users could be beneficial. Much can be learned from innovative techniques, such as the use of privacy layered policies, user friendly notices, educational videos, and the overall management of visual spaces. A reasonable trade-off however between the extent to which contractual clauses are brought to the consumer's attention and the space and efficiency of electronic contracting should be reached[22].

Opt-in versus opt-out

The options of allowing users to opt-in or opt-out of personal data collection, be it personal information or anonymised data, are key to the issue of consent. While the industry standard is currently set to opt-out, recent initiatives prove the need to find a better workable solution.

Cookies are very useful in streamlining transactions by reducing the need for repeated transfer of redundant information during interactions between clients and servers over the Internet. Their use is also an enabling factor for behavioral targeting, which in turn, together with search advertising, fuels the Internet economy. Behavioral targeting companies, such as DoubleClick, BlueLithium, and aQuantive collect user data by using cookies they drop on users' hard drives when the latter browse the Internet. Based on this data used to conduct sophisticated analysis of online behavioral patterns, users are assigned to different pre-determined advertising categories (cars, flowers, insurance, hotels). Thus, a widely accepted opt-in approach to user consent in advertising and profile building is considered by some to threaten the business model of these advertising companies, as well as the overall prosperity of the Internet economy, mostly driven by advertising revenues.

In addition, cookies have direct implications for the management of online consent. In general, browsers would not accept cookies unless they have been set to do so. However, most browsers are set to accept cookies by default. Thus, one might ask: if a user's browser is set to accept cookies by default, can this be considered equivalent to "consent"? We would recommend against taking such a view particularly as, in the interests of advancing privacy protections, industry should pursue the role of educator rather than merely benefit from default settings and a lack of user understanding. Contract law provides some guidance on consent and contractual agreements, whereby we expect the law to decline to enforce agreements that have supposedly crystallized by virtue of the offeree's silence or inaction[23]. Nonetheless it

---

[22] Vincent Gautrais, 'The Color of eConsent', U. Ottawa L. & Tech. J. 189 2003-2004.

[23] Roger Brownsword , 'The Cult of Consent: Fixation and Fallacy', King's College Law Journal, 15:2004, 223.

remains to be decided whether cookie placement does in fact signify the entering into a contractual agreement. The Working Party's opinion on this issue clearly states that:

"The general assumption that a user enters into a de facto contractual relationship when using services offered on their website, such as a search form, does not meet the strict limitation of necessity as required in Article 7(b) of the Data Protection Directive" (WP148).

What's more, the possible perceptual disconnect between the parties to a cookie transaction needs to be considered as well. The party setting the cookie knows that the cookie may not be set unless the recipient's computer gives permission to do so, but the recipient may not know how their computer is configured. Although consent may be implied from actions, there must be a reasonable belief that the action is meant to convey consent. Under the current state of user sophistication, it does not appear that the action of accepting cookies carries the necessary implication of consent in the absence of specific, conspicuous notice[24]. Furthermore, opt-outs might not suffice because they are arguably unreliable signaling procedures and presume consent on the basis of an omission[25].

How justifiable is then the consent model in an increasingly ubiquitous world where the only way for users to give informed consent is to fully understand the intricate technologies behind modern communications services? Putting the burden on consumers through the mechanism of consent is a well-known, widely accepted, and fervently recommended practice. It is viewed as a free and informed expression of the acceptance of risk. As long as users are aware of company data processing practices, the argument goes, understand the risks, and are given the tools to accept or reject them, they should be the decision-makers. However, as the complexity of technology grows, and with it the importance of technology enabled services in our every day lives, this burden will only become heavier. If privacy policies are still difficult to read, behavioral tracking too complex to explain, reliable identity and age verification tools non-existent, then aren't matters bound to get even worse? If consumer consent is getting to the untenable stage, we need to start searching for new models of shared responsibility.

Managing consent online: opportunities

Enabling the meaningful provision of informed consent online is critical to the process of technological innovation and evolution of services offered to consumers, as well as to their safety as citizens, entrusting companies with their personal data on a daily basis. However, as new opportunities for easy interconnection between services emerge, greater care needs to be taken to ensure that users not only consent but also understand what they are consenting to. And this would require parallel and may be even greater efforts in the area of children's consent as children take an increasingly active part in the digital economy.

---

[24] Oppenheimer, Max Stul, 'Cookies: When is Permission Consent?', Neb. L. Rev. 85:2006-2007, 383.

[25] Roger Brownsword , 'The Cult of Consent: Fixation and Fallacy', King's College Law Journal, 15:2004, 223.

Facebook: From Beacon to Connect

Companies are now competing to implement new features and thus show that they have learned from past mistakes. After the introduction of Beacon, a controversial service that was publishing user activity from other websites to their Facebook profiles without prior consent, the social networking company is now making a renewed effort to develop a more robust and secure approach to privacy. Facebook recently introduced a new service called Connect. It allows users to "connect" their Facebook profile data with external websites[26], connect with friends that are already on those external sites, and finally import information generated there back to Facebook as a Feed story[27] (Fig. 1). What makes Connect different from Beacon is the real time consent to story publishing and the dynamic privacy feature. Dynamic privacy[28] ensures that the same rules that users set on Facebook, if they so wish, are applied throughout Connect partner sites, using dynamic privacy controls, so anything that is not visible to a user on Facebook also isn't visible on a Connect partner site. This means that a user must provide explicit consent before an action they take on a Connect enabled site can generate a story.

Figure 1. Facebook Connect.

---

[26] Facebook has released a sample site that shows how Facebook Connect works. It's an application called The Run Around, which lets you track how much running you've done lately and informs your Facebook friends through a story feed. Visit: http://www.somethingtoputhere.com/therunaround/index.php

[27] Facebook has created a sample Connect enabled site called "The Run Around," which allows you to record your runs and publish them as stories to your Facebook Wall. Access: you can access here: http://www.somethingtoputhere.com/therunaround.

[28] http://developers.facebook.com/connect.php

Currently, Facebook carefully reviews the privacy policies and data collection practices of all sites before granting them access to Connect (some examples of groups using Connect are CNN's The Forum, MoveOn.org, and the Obama campaign). In the future, though, the social networking site intends to make Connect available as a self-service product, which will allow any site to use it as long as it complies with their Developer Terms of Service. Connect is not an ad product and it is completely free for sites to use.

Google and Yahoo have launched similar services in the past year, called Google Friend Connect and Yahoo Open Strategy. These similarly focus on extending the reach of social networking sites to the web by using users' social graphs, a term used by Facebook to describe their social network. As more and more similar services emerge, online companies will need to start reflecting on the provision of adequate technological tools ensuring safe social network data portability. The main challenges in this process will likely be providing sufficient information about data aggregation and empowering users to make choices about whom they share their personal information with, while recognizing the new trend towards data decentralization and complexity of online media partnerships.

Enhanced opt-out cookies?

In the world of cookie management there is a most perplexing conundrum: a user can only opt-out of personal information collection online by having an "opt-out" cookie placed on their computer stating that preference. However, if a privacy-concerned user decides to delete all cookies, the "opt-out" cookie will most likely be deleted, once again subjecting the user to monitoring. One major provider has considered using ETags as an alternative to traditional opt-out cookies. ETags could deduce that the user must have had an opt-out cookie but has deleted it, and then reinstate it. This is done by arranging that when users who currently have an opt-out cookie visit a website, that website will return a piece of content with a particular ETag. If they subsequently visited the website, they were to request the content without any cookie, but with the ETag value they previously received. The website could then reset the opt-out cookie.

While this technology was promising as a means of reducing the invasiveness of cookie technology, it was likely to introduce new problems. Older browsers were likely to fail to return the ETag value and if the requested content were no longer available, it would have been fetched without the provision of an ETag. There was also the possibility of unexpected interactions with web proxy caches. Another potential side effect could have also been the use of caches for tracking purposes and a general user perception that ETags are a form of spying technology, as in the end ETags are very similar to cookies.

The provider concluded that while the proposed persistent cookie would at least deal with a significant number of users who use more recent browsers, and who manage their caches in a more traditional and predictable manner, the danger of secondary effects was still too large to ignore. Furthermore, the introduction of such a technology would require the full disclosure of its presence, as well as a mechanism for users to refuse its use. Current privacy statements would thus have to be updated and users re-educated, possibly making online privacy management even more complicated.

eBay: On ad notice for increased user awareness

eBay recently introduced a new user privacy preference program for targeted advertising, called Ad Choice. Ad Choice was developed in an attempt to mitigate the higher risks of delivering targeted advertising to users that have shared more personally identifiable information than is normally collected for the purpose of ad serving. As eBay collects real names, addresses and bank information in order to conduct its online business, it allows it to also recognize registered users wherever they might be on the web. Thus the e-commerce platform has taken greater care in ensuring that its users may exercise choice both on the eBay site and when browsing partner websites.

Figure 2. Note the "AdChoice" link displayed on the ad itself.

This is achieved through both prominent notice (Fig. 2), which eBay can afford to display because it owns the ad space, and an opt-out button. Users may choose to prohibit eBay from using customer data for targeted advertising on the eBay website from eBay's partners, or prohibit eBay from serving their own ads on third party sites they partner with (Fig. 3), thus preventing any possible correlation of data.

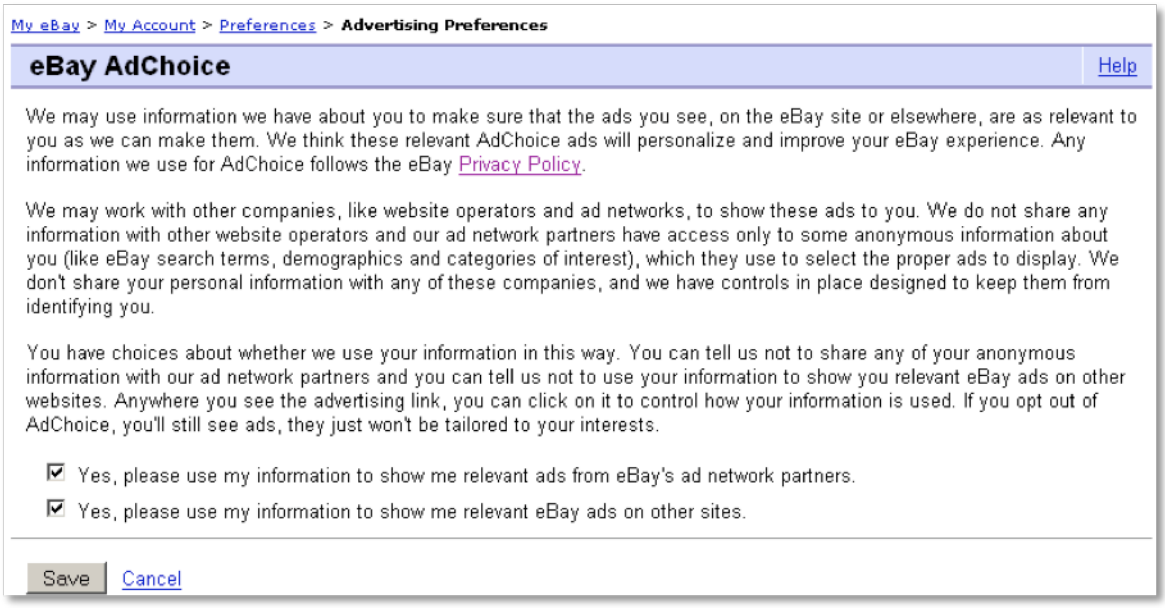

Figure 3. eBay notice and consent options.

Given the complexity of behavioural targeting and the different methods of data collection it entails, eBay's efforts to give additional prominence to its advertising practices and ensure the

informed consent of its customers and users is commendable. It also might bring us a step closer to eliminating the danger of perceptual disconnect between the parties involved in the use of cookie technology, which is the foundation of behavioral targeting. Many have argued in the past that the fact that there is no proof of user awareness of the use of cookies, combined with browsers being by default set to accept the latter, raises questions about the validity of consent. Preference programs like Ad Choice might thus be a possible solution as they persistently remind users of the fact that they are being served targeted ads, informs them who is doing this, and most importantly, allows them take control and opt-out of the process.

Microsoft Health Vault: Granularity of access

Launched in beta in October 2007, Microsoft's Health Vault is an online repository of personal health data. It allows users to store and share their health records digitally with their physicians, pharmacists, hospitals, and insurance companies, as well as with family members.

The value of such services is significant. However, it raises important questions in terms of access to and control of sensitive data. In an attempt to offer flexibility to its users, Microsoft is working on offering an increased granularity of options, allowing them to grant different levels of access to different people or institutions with whom they decide to share their health records.

One arising challenge in this general domain is the right of children to revoke access to their account, which might have initially been created by a parent or a guardian. While the policy implementation team of Health Vault is currently aiming to find the appropriate solution to this, the challenges of age verification and the lack of a harmonized approach to the age at which children have the right to express lawful consent remain. And as much as companies might be able to find alternative solutions through granting complex account privileges, the issue needs to be tackled at an international level by both industry and policy makers.

Bluekai: User control over advertising categories of interest

Bluekai[29] is a new company that is trying to create a preference database of personally non-identifiable information about user browsing patterns obtained from third parties, which they call "preference data". Preference data allows Bluekai to put users into different groups and create segments, the general characteristics of which can later be sold to advertisers. Their business model is based on that collection of anonymous customer preferences that would allow advertisers and publishers to serve ads to Internet users that better match their interests.

What is noteworthy about that service is that Bluekai allows users whose preference data it holds within its database to view the categories of interest into which they have been placed and modify them by either deselecting the existing criteria or selecting new ones that better reflect their topics of interest. As a member of the National Advertising Initiative (NAI), Bluekai also allows users to opt-out of their preference directory (Fig. 4).

[29] http://www.bluekai.com

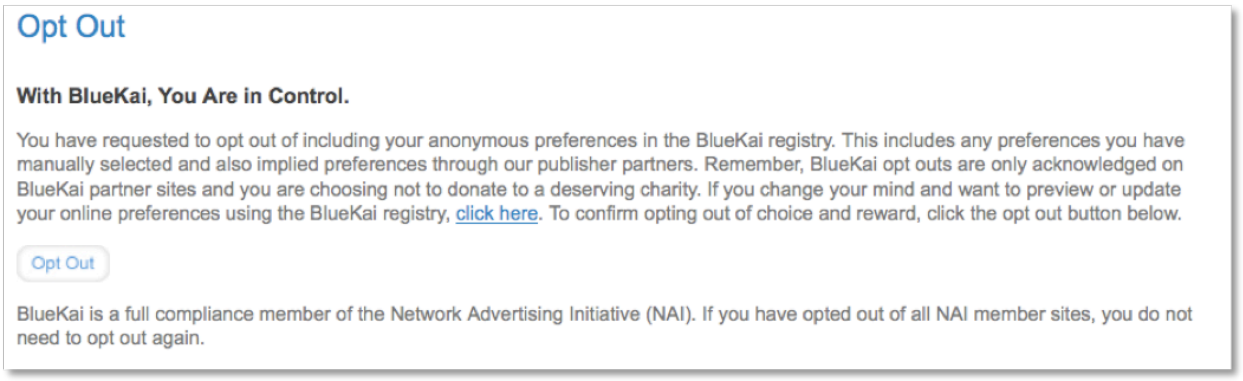

Figure 4. BlueKai opt-out window.

Google dashboard

In 2007 Google began discussing publicly the idea of a 'privacy dashboard'. The envisioned use of this dashboard was to enable users to view how Google was processing their information.[30] This would also help consumers understand the functionality of their user settings. At the time of the announcement of the idea, Google admitted that it "would be hugely complicated to build".[31] At the time of publication of this report, the privacy dashboard has not been publicly released.

Conclusion

Some companies are leading innovation and debate on these pressing problems surrounding consent. But greater regulatory certainty may be required, as well as a greater dialogue between industry and regulators as to what measures are necessarily, possible, and feasible. And we believe through engaging across communities and sectors we may be able to generate better forms of knowledge about current, good, and best practices.

[30] 'Google considers privacy dashboard', David Meyer, ZDNet UK, June 13, 2007.

[31] 'Anonymizing Google's Server Log Data — How's It Going?', Danny Sullivan, Search Engineland, October 10, 2008.

SECTION II: Key principles of 'informed consent'

In this section we review the qualification of 'informed consent' from a legal perspective. We offer practical advice to companies in terms of design of privacy policies, their prominence on websites, and the additional challenges associated with the use of personal data for tracking.

We further explore the intricacies of obtaining consent in situations where personal information is being processed for a previously unspecified purpose. These situations include sending unsolicited marketing messages, data transfers to third countries, or when a company that has been taken over has previously assured it users that their information will not be shared. We then proceed to compare the above legal requirements with the practices of a number of leading organizations. This allows us to clearly identify good and not so good practices in the application of data protection rules and regulations. The comparison of privacy notices, their placement and prominence, as well as their often differing content can serve as the basis of further recommendations to both policy makers and industry.

1. Identification: make sure the individual knows who is collecting data from them.

2. Make sure there is a 'privacy policy' on the website in a clearly identifiable place which sets out:

    (a) The purposes the data is being collected for (unless obvious or the individual already knows);

    (b) The method by which the individual can object to the information being passed to third parties for marketing purposes;

    (c) How the individual can object to the information being used for direct marketing;

    (d) An address to which objections can be made. If this is a terrestrial address then the data collect must respond to objections writing in 21 days stating that the objection will be complied with;

    (e) Any further information needed for the processing to be fair (e.g. if it is to be transferred outside the EEA).

    Be upfront about intentions for the data. Customers will appreciate honesty.

3. It is not enough just to have a privacy policy: in addition there must be a link to that information at the point of collection. A multi layered approach may be appropriate. For example:

    (a) A detailed policy containing references to the legal framework (for example the Data Protection Act 1998); and

    (b) A condensed notice with the main information under sub headings (at the point of data collection).

4. If it is intended to use tracking technology such as cookies on the website this must be flagged up at the time of collection and the individual told certain details including who is collecting the information, the purpose of collection and how it is collected. An opportunity must be given to refuse this.

5. If information is collected otherwise than directly from individuals, for example from other website operators or 'harvested' from a website the website operator has a duty to make sure the subsequent processing is fair. This means it must make sure the individual knows you have it and for what purpose.

    (a) This can be done through the privacy statement (stating that information is collected about individuals from other sources).

    (b) Alternatively they may have been told by the other website operator (this could be highlighted in the privacy policy as getting information from 'carefully selected third parties').

    (c) If the individual does not know someone has their information they must be informed:

        i. As soon as possible after they get it; and

        ii. If it is intended to disclose the information no later than when it is first disclosed.

        There is an exemption if this would require 'disproportionate effort' but to rely on this the decision must be documented and the decision maker ready to explain it to anyone who asks. This is unlikely to apply to website operators because of the ease with which an automated email can be sent.

    (d) 'Scavenging programmes' which collect personal information from other sites on the internet must be used carefully. Unless the data is to be used for the same purposes as it was originally collected it may breach data protection rules.

6. If the information will be used to send unsolicited marketing messages the individual should positively opt-in to receive them unless it is collected in the course of negotiations for the sale of a product or service and the individual is given a chance to unsubscribe. Once positive consent is given a confirmation email setting out what the person has signed up for, the purpose of collection, how the person can opt-out or correct data and giving a telephone number for customer queries should be sent. In each subsequent email there should be a reasonably prominent opt-out function.

7. If personal information is published on a website it may be transferred to other countries when someone accesses the website from abroad. Therefore it may only be published if this is fair to the individuals involved considering the potential impact.

    (a) Sometimes the risk will be negligible, for example if no contact details are given or if the information is about a well known achievement.

(b) In other cases informed and freely given consent will be needed. This means the individual must understand the consequences of publishing information, that there is no penalty for them declining to do so and that the individual can refuse consent at any time. For example this would apply if a club had previously published a leaflet of members contact details and wanted to put that information on the internet.

8. If another company is used to host an operator's website, the operator remains responsible for complying with data protection regulations if it determines how and why the personal information is processed. There must be a written contract which:

    (a) States the processor must only act on the website operator's instructions; and

    (b) There must be appropriate technical and organisational security measures in place.

9. If a web based company is taken over it is likely it will be able to share the information it has collected with the new owner since he is essentially carrying on the same business. The reasons the information was originally collected must be considered as well as the expectations of the individuals concerned. Personal information may not be disclosed without express consent where:

    (a) The company has previously assured an individual that their information will not be shared;

    (b) There is a duty of confidentiality; or

    (c) If the data would be processed in a way that would have a markedly different effect on the individual.

10. The website operator is responsible for processing personal information securely and should adopt appropriate technical and organisational measures to protect the information it collects. An encryption-based transmission system may be appropriate.

11. Information must only be used for the reasons it was collected for. To use it for other purposes it is not enough to change the privacy policy. Operators must consider exactly what they intend to do with the information:

    (a) If the new use is not for a new purpose or is close to that in the privacy statement, it is enough to tell the individual and give them a chance to opt-out.

    (b) If the new use is within the privacy statement the individual does not have to be told specifically although those who object should be respected.

    (c) If the new use is substantially different even if it is within the privacy statement the individual's reasonable expectations should be considered. If the new use is well outside of these customers should opt-in rather than opt-out.

(d) To use the information for a new purpose or disclose it to different organisations than those stated in the privacy statement an operator must tell the individual of this proposed change and get their positive consent. Not replying to an email does not suffice as consent.

12. Collecting information from children requires extra considerations.

    (a) Language must be adapted to reflect a child's lower level of understanding. It must be clear and appropriate to the age group the website is aimed at. Their lack of understanding should not be exploited.

    (b) To collect personal information a website must get the consent of their parents or guardian unless it is reasonable to think the child understands the decision and its implications. Taking personal information from those under 12 requires parental consent.

    (c) No personal data about adults should be collected from children.

    (d) An example of actions likely to breach this duty would be to collect personal information in exchange for winning a prize.

    (e) To share a child's personal information with third parties there must be verifiable consent from the parent or guardian (a button signifying that the parent has given consent is not enough) or from the child if it is of an age to understand the decision and the implications of publishing information on the internet.

Industry examples (commercial in confidence)

In practice website operators vary in how they comply with their duties under data protection legislation and how far they follow the principles set out above.

Disney

This website is primarily directed at children. Its privacy policy is easily accessible at the bottom of its home page.

1. In the first paragraph Disney identifies itself, its associated companies (paragraph 3) and that it controls information it collects.

2. The type of information collected is identified. The user is warned that by registering or using the site he is consenting to the policy.

3. The purpose is identified – 'marketing and market research purposes' among others.

4. Other sources of information that are used about an individual are identified

5. Situations where information will be disclosed are identified.

6. Circumstances where international transfer of data will take place are identified – 'for maintenance purposes' and the standards to which it will adhere.

7. Children: Disney identifies how it will get permission to collect information about children. It will check with the parent that the information a child supplies is correct.

8. Disney explains how to remove your information on registration.

9. It explains how cookies are used – 'to make our sites more interesting and useful for you'.

10. It explains that if the privacy policy is changed, it will only use the information gathered prior to that for a different purpose with consent.

This is a very good example of an operator following the appropriate principles.

Phorm

Phorm's technology allows it, with the co-operation of the user's ISP, to match addresses and content of websites that users visit against predefined advertising categories.

There is a prominent link to an on-line video privacy overview on the top left hand corner of the home page. The key points highlighted are that the technology does not identify individuals, where they have browsed and users can opt-out at any time.

The link to the full policy is at the bottom of the home page. There are two sections: the site privacy policy and the service privacy policy. The former has a helpful overview of the policy's main points at the start. It covers what information is collected, the purpose of collection (and if information is collected for another purpose Phorm requests permission), when that information will be disclosed to third parties, user choices and option in relation to cookies. There is clear guidance on how individuals can find out what information Phorm has about them. There is no mention of a fee for this.

Furthermore, there is a pledge to use 'reasonable efforts' to keep information accurate.

Changes to the policy are updated on line, and the onus is on the individual to check for changes each time they submit personal information. To comply with the principles there should be a link to this at the time the information is submitted.

The ICO's comments on Phorm's services are instructive of what they consider the main concerns in data protection. They conclude that Phorm's technology will comply with data protection legislation.

Significant factors in this decision include:

(a) The ISP will not create lasting records of browsing habits or seek to link living individuals to the information sent to Phorm;

(b) Phorm will not need any information from an ISP which would link a user ID to a living individual;

(c) The user will be presented with a clear choice at contact about the product and will be able to opt in and out easily;

(d) The user will be able to refuse cookies; and

(e) The information will only be used to target advertising.

Facebook (TRUSTe verified – an independent organisation which promotes fair information policies to customers)

This is a good example of an operator dealing with highly sensitive personal information. The privacy policy is available on the home page before registration and in the site itself under 'account settings – privacy'.

1. There is a link to 'safe use of Facebook' where parents and children can get appropriate information. Facebook's policy is that no-one under 13 can have an account. This accords with data protection principles.
2. The policy explains what information Facebook collects from the individual and through cookies. It deals with the use of cookies by third parties.
3. Information is used to be 'presented back and edited to you' and anonymously by third parties for market research and personalising adverts.
4. Facebook states that it uses information about individuals from other sources too – the user can block this.
5. There is a very detailed section on third party access to personal information. For example 'Facebook beacon' allows the site to publish what sites individual's access on-line. This can be blocked by the user.
6. It deals with privacy if Facebook was taken over by another company.
7. The policy states how a user can remove information. An email address is provided for users to request removal of cached data.
8. The policy states that users consent to their information being transferred to the US.

Expedia

The privacy policy link is on the home page. It covers:

1. Information collected, including specific instances when it is collected, for example when a customer 'completes a traveller profile'. For each instance there is a description of exactly what is collected.

2. A detailed description of how cookies are used by Expedia and third parties.
3. Detailed use of information is provided.
4. Expedia has an area of their website where customers can tailor promotional material they receive.
5. Expedia details specific instances when it will contact customers – for example on a request to close an account.
6. What information Expedia must, as a travel agent, give to the U.S. authorities about passengers flying to the U.S and other related queries.
7. Although the privacy policy will be updated online, the privacy policy in effect at the time the user signs up will apply to that data.

Ecclesiastical

The privacy policy is accessible from the bottom of the home page.

1. Ecclesiastical identifies itself clearly, including its company registration number and affiliates.
2. An individual's consent to the policy is deemed by submission of personal data.
3. Changes to the policy are notified on the policy page. There is no mention of any other consent being sought.
4. It states that it may collect information about an individual from another source.
5. It sets out its use of personal data.
6. It states that it collects information through cookies to monitor use of its website.
7. It clearly sets out the circumstances it will share personal information with third parties.
8. It states how an individual can find out what information Ecclesiastical holds. It charges a small fee for this. An individual can also contact this address to unsubscribe from marketing emails.
9. The onus for correcting inaccurate data is put on the individual. An email address is provided.
10. The user consents to international transfer of his information if he accesses the website from abroad. The policy states Ecclesiastical's obligation of confidentiality in relation to personal data.

Electronic Arts (TRUSTe verified)

The policy is accessible from the home page. It includes:

1. Data will be stored in the U.S and elsewhere worldwide.
2. The policy lists exactly when data is taken for each service.
3. If a friend is referred to the services their details will only be used to send them an email inviting them to join.
4. Children: information is not collected from children under 13. There is no other mention of arrangements for them.
5. Information collected by third party advertising companies is subject to their terms and conditions – the user is directed to their privacy policy. There is no easy way to unsubscribe from this site.
6. If Electronic Arts was taken over customer information would be transferred.
7. The customer must opt-in to be contacted by other companies. If he does so he can opt out through Electronic Arts or through the third party website.
8. If Electronic Arts uses a third party contractor, for example for research, that party is bound by these privacy conditions and cannot use the information for any other purpose without the customer's explicit consent.
9. Opt-out options are provided extensively in the site and on each marketing email the customer receives.
10. Changes to the policy will be notified online or by email (if material). Continued use of the website signifies assent.

MSN

There is a link to the general Microsoft privacy policy on the home page. This is an example of the use of 'layered' privacy notices. The first page sets out policy highlights and covers personal information collected, uses of information, how an individual can control the marketing information he receives and contact addresses.

The full privacy statement covers many of the principles outlined above including:

1. What information Microsoft collects through registration, through use of website analytic tools (including keywords and search engine used) and through other companies (for example general geographic area from the IP address used).
2. The purpose of collecting the information – 'to operate and improve its site and services', to contact the individual and to display personalised advertising.

3. It states information will be transferred to the United States and other countries Microsoft has affiliates.
4. It provides perimeters for sharing personal information and when information will be disclosed.
5. There are guidelines for children. It states no personal information will knowingly be collected from under 13's and where age registration is required under 13's will be blocked or parental consent required. It states on some products there are further privacy settings for children which can be activated.
6. There is a web form through which customers can complain.

However:

1. There is no mention of a way customers can choose not to have their information collected.
2. Although the policy states that material changes to it will be posted online or sent directly to customers, there is no mention of whether customers can object to such changes and what happens to information already gathered.
3. There is also no mention of a way individuals can find out what information Microsoft stores about them.

Second Life

The policy is accessible from the home page. Accessible prose is used throughout.

1. Information collected is detailed under sub headings by type of website user.
2. Linden Lab use 'reasonable efforts' to tell customers of changes to the policy.
3. Only over-13's may register.
4. Information may be transferred to the U.S.
5. Circumstances when personal information will be disclosed are detailed.
6. Contact details are provided.

However the policy does not cover all the principles above. In particular there is no mention of how customers can get cached data removed and no reassurance that information will not be used for other purposes than those stated. Further rules on use by children can be found in the Terms and Conditions (Clause 2.2). Although the website restricts access to those over 13 it puts the onus of the child's understanding of the terms and conditions onto the child and its guardians. This does not allow for differing understandings between children.

This is the only site accessed where the operator stated it would sell personal information to a company if it sold its business or was taken over.

Home Office

The privacy policy is accessible from the home page under 'Terms and Conditions'. It is very brief and covers the use of cookies, why information is gathered and that the Home Office will comply with the Data Protection Act.

It does not state the circumstances in which information will be disclosed to third parties or if information will be transferred abroad. Although it states the Data Protection Act will be followed, it gives no further details about what this entails.

Paypal

The privacy page is accessible from the home page. It covers:

1. The information collected and the reason for this.
2. A ban on selling personally identifiable data to third parties.
3. Information collected about an individual from third parties.
4. A detailed policy on disclosure of information (particularly to other customers to whom an individual is transferring money) including the names of major third parties.
5. Paypal states some communications will be compulsory (for account maintenance, etc) but others can be blocked.
6. It states that cached data will be retained 'to deter fraud'.

However:

1. Paypal posts changes (minor or major) to the privacy policy on the website. There is a deemed acceptance period of 30 days. No personal notification is sent to customers and if a customer objects to the new purpose his only choice is to close his account. There is no mention of what happens to data collected before the change.
2. Children are 'requested' not to submit personal information. There is no other provision to stop them.

Pipex

There are separate privacy policies for residential and business users under 'Terms and Conditions'. The business user policy valid until 5 December 2008:

1. Details information it collects from users and from third parties and how it does so

2. How it uses data: to ‘provide and improve’ the service and for direct marketing.
3. Warns users that information will be transferred abroad.
4. Details the disclosure policy: only shared within the group or to third parties in defined circumstances (e.g. for delivery).
5. Details customer rights in relation to deletion or amendment of data and gives a contact address for this purpose.
6. Although it posts changes to the policy on the website, there is no mention of a personal notification to customers.

The business user policy effective thereafter is similar but also details the use of cookies and states that information will be collected about transactions customers enter with third party partners. This policy states that a profile of customer interests and preferences will be built up – although customers can opt-out of this. Children are advised to get parental permission to use the services but no other protective procedures are mentioned.

There is no mention of which policy terms information collected before a change is made will be held.

AOL

The privacy policy is accessible through ‘Safety and Security’ on the home page. AOL use layered notices. The policy is drawn very wide. It includes:

1. When a customer registers there is a link to the privacy policy.
2. An overview of the key principles with links to further information.
3. A statement that information will not be passed onto third parties without consent unless required by law. However it also states that ‘not objecting’ counts as consent.
4. Why the information is collected – this includes information about a customer’s online habits. Information may be obtained from third parties ‘to better understand you as a customer’. This seems very wide.
5. The use of information. This states if that personal information may be disclosed to ‘potential’ buyers. This seems excessive.
6. Changes to the policy will be notified on line. It appears it applies retrospectively.
7. Details of how long information will be kept. This includes a ‘reasonable period’ after a customer ceases to use the service.
8. AOL uses other companies to advertise on its sites. Their activities are subject to their own privacy policies. It is not clear whether a customer could consent to use AOL but object to another policy.

9. The use of cookies is explained, including how to turn them off. However the sites 'may not work very well' if a user does so.

10. Customers can opt-out of marketing emails but to do so they must send an email to AOL. It is not clear whether this is prominently marked on other parts of the site.

11. When a customer leaves AOL their information will continue to be used for a 'reasonable period' by AOL and for 6 months by third parties unless a specific email is sent.

12. There are strict conditions in place for use by children.

Royal Bank of Scotland

The privacy policy is easily accessible from the home page. It explains the use of cookies on the website. It identifies the uses for which information is collected and that third parties collect data for research into the use of the site and the effectiveness of the RBS's advertising. It explains that cookies can be blocked but refers the user to their internet browser's help section for how to do this.

The individual is referred to individual product terms and conditions for how the Bank processes its data. Unlike Disney privacy information is not all in one place. A link to product terms and conditions ('the Terms') is available for each product on its information page under 'Legal'. There are several documents to open. The terms and conditions are set out in small type. Clause 1 refers to 'Your information'. This sets out purposes, disclosure policies, international transfer and change of purpose policies. The document then moves on to account specific conditions, including ones for children. The language is adapted to children, but it says that the child should review the conditions with its parent or guardian. The onus is put on the individual. Although copies of the Terms are available to the child it is questionable whether the child would actually read them.

'Website terms and conditions' on the home page repeat some information found in the Terms. At point 12 the Bank explains why it would share information within the group and when it would transfer information outside the group. It states its procedure when the purposes for which the information is collected changes – but note that if the Bank asks permission to change the purpose (where the user would not 'reasonably expect' the new use) it states lack of response in 60 days constitutes deemed consent. This is contrary to the principles outlined above.

Overall, the privacy information is not easily accessible in one location and the principles are not always followed.

Fidelity

There is no easy link to a privacy policy on the website, and no way to search for one. The privacy policy can be accessed by entering one of the specialist sites – 'About us' – 'Fidelity and you'.

It covers the use of personal information, when third parties have access to it, direct advertising (which requires specific permission), how customers can find out what information holds about them for a small fee and explains the use of cookies.

However:

1. It refers to limited exceptions to the customer's right to find out what information Fidelity has about them but does not explain further.
2. It provides very little information about how Fidelity interacts with third parties.

Conclusions

Through this review of practice, we were able to identify good and not so good practices in the application of data protection rules and regulations. The comparison of privacy notices, their placement and prominence, as well as their often differing content shows that much work remains to be done on getting even the most basic statements of practices made available, even while those on the cutting edge try to move forward with more accessible means of explaining and 'informing'.

SECTION III. Minors and Online Consent

Introduction

This section examines the issue of securing consent from children or minors in the online context, and considers how, if at all, current data privacy rules address the issue. Industry, regulators and privacy practitioners continue to grapple with this difficult subject, and the absence of targeted laws or regulations in this area continues to prove problematic. Here, we explore different methods for obtaining consent online, highlight European practices and age verification techniques, and briefly discuss the U.S. Child Online Privacy Protection Act ("COPPA").

'Consent' under European Framework Legislation

The EU's Data Protection Directive 95/46/EC (the "Directive")[32] regulates the processing of "personal data" by organizations that qualify as "data controllers," and imposes various controls on the handling of such data. In particular, the Directive requires that any processing of personal data be "legitimate," and then establishes a set of legitimate grounds for the processing of such data. A more restricted list of "legitimate" purposes exists for the processing of "special" or "sensitive" data, which includes data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning their health or sex life.

Critically, the Directive provides that consent can serve as a legitimate basis for processing personal data, regardless of whether it is mere personal or sensitive personal data. That said, the Directive does distinguish between the two: whereas non-sensitive data may be processed legitimately where the data subject has "unambiguously given his consent,"[33] sensitive personal data can be processed with an individual's "explicit" consent.[34] The Directive further embellishes the notion of consent by defining it to mean "any freely given specific and informed indication of [the data subject's] wishes, by which the data subject signifies his agreement to personal data relating to him being processed."[35] Despite this clarifying language, there continues to be active disagreement among Member States on the appropriate form that

---

[32] Directive No. 46 of 1995, Official Journal of 23 November 1995, L281, p. 31.

[33] Article 7(a) of the Directive. Other conditions for processing personal data include where it is necessary for the purpose of the legitimate interests pursued by an organisation; where it is necessary for the performance of a contract to which the data subject is a party; and where processing is necessary for compliance with a legal obligation to which the data controller is subject.

[34] Article 8(2)(a) of the Directive. Stipulated conditions for processing sensitive data include (among others): where the processing is necessary for carrying out the obligations and specific rights of an organisation; where processing is necessary to protect the vital interests of the data subject; and where the processing relates to data which are manifestly made public by the data subject.

[35] Article 2(h) of the Directive.

consent must take in various contexts and how to interpret such key terms as "explicit" and "unambiguous."

Meanwhile, and unhelpfully, the Directive offers virtually no guidance on how these terms should apply in circumstances where consents are sought primarily from children. There continues to be ongoing debate among regulators, industry and others over whether, and to what extent, it is possible to obtain valid consents from a child and what such consents might require in practice. At a minimum, because consents need to be adequately "informed" in any circumstance, all organisations are obliged to furnish both adults and children with appropriate informational disclosures. It is generally held that those disclosures, both in terms of their content and presentation, must be appropriately modified where they are targeted to a child, as opposed to an adult.

As discussed in more detail below, Member States continue to be afforded some latitude when applying the Directive, and therefore the law regarding consent remains inconsistent across the EU. National regulators also adopt differing approaches, with certain regulators, such as Spain's, being known to be more demanding than others, such as the UK's. These national-level variations cause problems for industry, as organizations must consider the approach taken in each country rather than respond to a clear body of pan-European data protection law.

The Article 29 Working Party and the European Data Protection Supervisor

Frustratingly, there continues to be scant regulatory guidance to serve as an aid for organizations seeking consents from children online. The Article 29 Working Party on search engines in April 2008 helped fuel the current debate over obtaining consents online, but stopped short of suggesting a suitable method for obtaining such consent and did not examine what that might mean when the user was a child.

By contrast, the group did consider children's privacy in a separate paper, WP147, which discusses circumstances where parental consents might be required before an organization processes personal data relating to children. The A29 Working Party resisted establishing a set age at which parental consent must be sought as a protective measure; instead, it argued for a more flexible standard that took into account a child's maturity and the complexity of the issue at hand.[36] For example, the Working Party felt that collecting data from an 8-year-old for the purpose of receiving a free magazine would not require parental consent, whereas it would be required to take part in a live TV appearance. The A29 Working Party also stressed the need to provide a clearly labelled privacy notice in "simple, concise and educational language that can be easily understood."[37] Recently, the A29 Working Party further considered the capacity of a child to provide valid consent, and explained how the existing rules of the Directive could best

---

[36] WP29, Working Document 1/2008 on the protection of children's personal data (general guidelines and the special case of schools), 18 February 2008, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_en.pdf.

[37] *Id*. at p.10.

be applied to ensure that children's privacy is adequately and effectively protected.[38] Again, however, the Working Party did not address the narrower issue of obtaining online consents from children.

Two other Working Party papers touch upon the issue of online consent, but neither offers the kind of detailed guidance that industry have sought for some years. Opining on direct marketing via email and disclosures of personal data to third parties, the Working Party stipulates that individuals should be able to indicate their consent via a "click box online."[39] In a separate paper examining privacy on the internet, the A29 Working Party proposes the same method as a means of opting out of receiving spam mail when supplying an email address.[40] Neither of these papers, however, discusses consent specifically as it relates to children.

Finally, guidance provided by the European Data Protection Supervisor ("EDPS")[41] confirms that the Directive applies equally to the collection of personal data online -- including the "invisible" collection of data through the use of cookies -- as to "visible" collection such as when a person actively submits information online. The EDPS states that where "visible" collection of data occurs, it is arguable that an individual provides implied consent to its processing as long as the risks involved are made clear, usually via a detailed privacy notice available on the site. On the other hand, where the personal data are sensitive, the EDPS advises that it is necessary to obtain "explicit" consent. As with the Article 29 Working Party, the EDPS refrains from focusing on the unique problems associated with collecting consent from a child.

Illustrative Member State Approaches

Member States, and more particularly their national privacy regulators, have to date refrained from releasing much if any guidance on securing a child's consent online (or in virtually any other context). At present, the Dutch DPA is one of only two national authorities to provide guidance on how to obtain consent online, and suggests that ticking a box in an electronic form constitutes clear proof that the user has explicitly given his or her consent to the processing of their data. The Dutch regulator also advises that a detailed privacy notice must be provided in order for consent to be "informed" and that a user must freely consent to a specific processing of data in order for consent to be "unambiguous."[42]

---

[38] WP29, *Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools)*, 11 February 2009, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp160_en.pdf.

[39] WP29, Recommendation 2/2001 on certain minimum requirements for collecting personal data online in the European Union, p. 9, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp43en.pdf.

[40] WP29, *Privacy on the Internet - An integrated EU Approach to On-line Data Protection,* adopted 21 November 2000, p. 37, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37en.pdf.

[41] The European Data Protection Supervisor, *Data Protection in the European Union,* available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/guide/guide-ukingdom_en.pdf.

[42] *Guidelines for Personal Data Processors,* available at: http://english.justitie.nl/images/handleidingwbpuk_tcm75-28677_tcm35-15485.pdf?refer=true&theme=purple.

Meanwhile, other regulators, such as the Finnish and Irish, provide slightly contrasting advice. The Finnish regulator maintains that "inferred" or implied consent is insufficient and believes that online businesses should require individuals to tick a box before being submitting information.[43] The Irish regulator advises that it is unnecessary to ask individuals to expressly indicate their consent before processing their data online, as long as the website provides a detailed privacy notice explaining how the data protection principles are applied to data that are processed on the site. While many regulators, like the U.K.[44] and Swedish, follow the Irish approach, there is no consistency among European regulators regarding this issue.[45] Again, organizations hoping for more explicit guidance on how to secure a child's consent online will be disappointed.

EU-Level Initiatives

The absence of any detailed guidance or recommendations on collecting consents from children online is surprising given that protecting children on the internet remains a high priority policy issue in Europe. For example, the European Parliament and Council recently announced a multinational European Community program on protecting children using the internet and other communication technologies,[46] and the European Parliament and Commission recognise that they must provide guidance and issue recommendations for Member States. Several European bodies and task forces, discussed below, have been set up to discuss the issue. Many Member States also have launched their own local initiatives. One particular concern surrounds the increasing use of online social networks.

Regulators and policy makers in Europe continue to struggle with two issues in particular -- verification mechanisms and age classification discrepancies. First, it remains a generally recognized legal principle that children of a certain age may lack the capacity to validly consent, either to the disclosure of their personal information[47] or otherwise. For that reason, the legal category of minor appears in nearly every domestic legal regime, generally so that additional legal or other protections can be bestowed on such persons. In Europe, for instance, regulators

---

[43] This information reflects guidance provided in an email from the Finnish data protection agency.

[44] The U.K. Information Commissioner's Office also advocates the use of "layered notices", which entails providing condensed notices wherever personal information is collected, in addition to a comprehensive privacy policy located elsewhere on the website. WP29 also promotes this practice, *see Opinion 2/2009 supra* n.9 at p.10, section B.2.d.1 ("Right to be informed").

[45] Other sources of guidance include the University of Leicester, which maintains a research program focusing on online consent. The program concludes that the nature or expression of the consent should vary with the context. For example, it argues that private websites should always obtain informed consent, whereas public sites, such as chat rooms or internet blogs, should be allowed to infer consent from the fact an individual used a site. The program suggests a suitable method of obtaining informed consent would consist of a highly detailed privacy policy (addressing all necessary issues under the Directive) combined with an equally detailed consent form that refers an individual to the purpose(s) for which their data are being collected, and requires them to tick an electronic box.

[46] Decision No. 1351/2008/EC, Official Journal of 24 December 2008, L348, p.118. The "Safer Internet" program includes a number of measures that will require a response from ISPs and website operators in the form of increased filtering tools and quality labels to indicate that they subscribe to a code of conduct.

[47] *See, for example,* ICO Issue Paper, *Protecting Children's Personal Information,* available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/issues_paper_protecting_childrens_personal_information.pdf.

have noted that companies must consider the context in which data are collected when deciding whether to accept consent from a child, and presumably be particularly cautious when doing so.

For that reason, the notion of confirming a child's consent, often by seeking verification from an adult or guardian, has arisen and is popular with many policymakers. That said, requesting that a child's parent or guardian send a confirmatory email may not guarantee that valid consent will be obtained given the anonymous nature of the internet and the opportunity for abuse. Similarly, a "click-button" confirming an individual is over the relevant age remains a notably weak form of age verification. Online services that are aimed at children therefore face a difficult task, and may simply be required to engage in a risk-benefit analysis by adopting methods that lend some additional protections, but are not foolproof.

Second, another major challenge facing companies operating online in Europe (and elsewhere) is the discrepancy across Member States regarding the age at which an individual can be classified as a minor. For example, the relevant age in Belgium is between 12 and 14 (depending on the context), while in Finland there is no set age limit, although persons under the age of 15 may not receive direct marketing materials. Ireland classifies a child as a person under 16 in connection with health data, and under 14 for marketing purposes. Spain sets the age at 14, while the UK considers a child to be anyone under 12, though the UK Information Commissioner stipulates that it is incumbent on an organization to assess each situation in which it is collecting information, and decide whether an individual older than 12 is able to grant consent.[48]

The EC's Safer Internet Program

Established in 2005, this European initiative aims to promote safer use of the internet and new online technologies, particularly for children, and to combat illegal online content. A key objective is to implement an industry code for self-regulation, and the European Commission recently convened a Social Networking Taskforce, which held two meetings in 2008 with several operators of social networks, including MySpace, Bebo and Facebook. The Taskforce will continue to meet throughout 2009 and explore effective age verification schemes, as well as mechanisms for obtaining online consent.[49]

In September 2008, as part of the Safer Internet Program, the European Commission released the results of a public consultation on "Age Verification, Cross Media Rating and Classification

---

[48] A recent case in Spain highlights the need for a data controller to exercise discretion. The Spanish DPA imposed a €270,000 fine on a company that collected data from a 9 year old using an online registration system that required users to enter their date of birth before they were granted access. The child entered "95" instead of "1995" and the system subsequently registered the child as being 1,911 years old and therefore some way above the necessary age limit. *Privacy, Laws and Business Data Protection and Privacy Information Worldwide*, Issue 94, August 2008, p.7.

[49] The Taskforce's immediate priority is the implementation of Safer Social Networking principles to which social networking services ("SNS") are expected to adhere, *see* Social Networking Taskforce, *Safer Social Networking Principles for the EU,* draft, 17 December 2008. These include a range of good practices and a process of self-declaration by which SNS providers will indicate how they consider the principles relate to their behaviour. Although the principles do not expressly address methods of obtaining consent from a child, they demonstrate the Commission's commitment to children's online safety.

and Online Social Networking."[50] The consultation asked interested parties to provide views on current age verification technologies. The following is a summary of some of the responses it received.[51]

Ofcom

Ofcom, the independent regulator and competition authority for the UK communications industries, noted the importance of securing verifiable consent in the context of converging technologies and an Internet-dominated environment, yet stopped short of suggesting a method of achieving this and admitted that "age verification remains problematic in that it needs to be ascertained in a reliable way." The agency argued that credit cards could be helpful as they prove someone is over 18, but acknowledged that many service providers do not wish to charge membership or other upfront fees.[52]

Microsoft

Microsoft suggested that trusted "off-line" systems should be digitalized to allow online verification of identity and age. Because children do not carry a driving licence or social identity cards, Microsoft has proposed that other identity documents are used, such as birth certificates or school enrolment forms. Alternatively, government departments could take the initiative by providing digital identity cards, although such a development naturally would be controversial.

Yahoo!

Yahoo! identified a number of issues with existing age verification techniques, including excessive false positives, lengthy delays, and vulnerability to manipulation. It differentiated "on-line" from "off-line" verification, stating that although the former can be a simple process for the majority of adult users by using electronic databases such as the electoral register or credit rating services, equivalent databases for children do not exist. Even if they did exist, Yahoo! considered that any proposal to allow online providers access to such databases would be unlikely to gain public acceptance.

---

[50] The replies submitted in connection with the consultation are available at: http://ec.europa.eu/information_society/activities/sip/public_consultation/index_en.htm.

[51] Fox Interactive summed up the general consensus: "identity verification on the Internet is difficult because it is virtually impossible to know whether the individual user supplying the information is indeed the individual whose information is being supplied. Although a user may provide certain information when registering with a website, there is no efficient or effective way to ensure that this information has been entered truthfully. *Fox Interactive Media Response to the European Commission's Safer Internet Public Consultation on Age Verification, Cross-Media Rating and Classification and Online Social Networking,* 31 July 2008, p. 2, found at: http://ec.europa.eu/information_society/activities/sip/docs/pub_consult_age_rating_sns/results/foxinteractivemedia.pdf.

[52] Ofcom praised the mobile phone industry for developing effective age verification systems that require users to "prove their age." However, O2, the mobile provider, uses credit card details to verify a user's age before allowing access to adult material, which is not a possibility for children. Amberlight Partners, *WAP Age Verification: Adult Content on Your Phone,* available at: www.amber-light.co.uk/resources/whitepapers/wap_age_verification_amberlight.pdf.

Regarding "off-line" verification systems, Yahoo! discussed the method it employed under the BT Yahoo! service, which requires a parent to act as the primary account holder and to verify their child's age when setting up their account. Yahoo! noted drawbacks in other age verification systems in terms of usability and openness to fraud.

UK Initiatives

On September 29, 2008, Prime Minister Gordon Brown launched the UK Council for Child Internet Safety. The Council aims to work with over 100 organisations, representing both public and private sectors, to develop a Child Internet Safety Strategy to be delivered in early 2009. Among its targets, the Strategy aims to establish a comprehensive "one-stop shop" on child internet safety, and a self-regulatory code of practice for user generated content sites, including social networking sites. Until the Strategy is published, the Home Office Task Force on Child Protection on the Internet has provided guidelines for social networking operators that offer practical solutions that include:

- placing a cookie onto a user's computer to prevent the user from attempting to re-register with false age details;
- using search algorithms to identify words typically used by under-13s; and
- offering free downloadable parental controls to help parents manage their child's use of the service.[53]

The Home Office admits these measures vary in robustness. Some service providers do not consider the Home Office's measures to be feasible, however.[54]

The U.S. and COPPA

Introduced 10 years ago, the U.S. was one of the first jurisdictions to introduce legislation protecting children online. In a 2007 report to Congress examining COPPA, the Federal Trade Commission ("FTC") concluded that the Act is effective in protecting the security of children without unduly burdening website operators.[55] However, it also noted that because age verification technology is not widely available, age verification falsification remains a risk for general content websites not specifically aimed at children.

---

[53] UK Home Office, *Good practice guidance for the providers of social networking and other interactive services,* 2008, available at: http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance.

[54] In addition to these measures, The Online Purchasing of Goods and Services (Age Verification) Bill received its first reading in the House of Lords on January 14, 2009. The Bill would require businesses engaged in online sales to take reasonable steps to determine whether a customer met a relevant age restriction, and would make it an offence to fail to comply with this requirement. Because it is a Private Members' Bill, however, it is unlikely to become law. See http://www.publications.parliament.uk/pa/ld200809/ldbills/016/09016.1-i.html#top.

[55] *Implementing the Children's Online Privacy Protection Act: A Report to Congress*, Federal Trade Commission, February 2007, found at: http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf.

COPPA requires websites targeting children to obtain verifiable parental consent before collecting any personal information. There are certain exceptions to this rule, but these fall outside the scope of this paper. In brief, verifiable consent is not needed when: (1) responding to a one-time request from a child; (2) collecting information in order to send the child periodic communications such as newsletters; (3) where necessary to protect the safety of a child participating in the site; or (4) where necessary to protect the security/integrity of the site, respond to a judicial request or other public investigation.

Under COPPA, "verifiable parental consent" means that the consent method must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. In its FAQs, the FTC cite specific methods of obtaining verifiable consent where the information is going to be disclosed to third parties or made publicly available through social networking or similar sites. These include:

- providing a form the parent can print, fill out, sign and post or fax back;
- requiring the parent to use a credit card in connection with a transaction (this could include a membership or subscription fee, or simply a charge to cover the processing of the card);
- maintaining a free-phone (toll free) number staffed by trained personnel for parents to call in their consent; or
- obtaining consent through an email from the parent or guardian, if that email contains a digital signature, or other digital signature obtained through one of the methods above.

Where the information is not going to be disclosed or made publicly available, a method known as "email-plus" can be used. This involves the site operator obtaining consent through the receipt of an email from the parent, plus a further step. Either the service provider can request a postal address, telephone or fax number for the parent and follow up directly with the parent, or it can, after a reasonable delay, send another email to the parent to confirm their consent.

In its report to Congress, the FTC noted that industry feedback on COPPA was generally positive, with the Direct Marketing Association, Motion Picture Association of America, Nickelodeon and Scholastic all expressing satisfaction with the legislation.[56] The FTC's report emphasises the difficulties general content sites face in obtaining verifiable consent. This is understandable given that these sites are not marketed at children, therefore the operators are less inclined to invest in safeguards such as those mentioned above. COPPA provides for this by only imposing penalties on general content site operators when they receive "actual knowledge" that a child is using their site, but do nothing to rectify the situation.

Suggested precautions operators may take include introducing a requirement whereby all users must enter their birth date before they can access the site. However, website operators must

---

[56] *Children's Online Privacy Protection Rule,* Federal Trade Commission, 16 CFR Part 312, p.15, available at: http://www.ftc.gov/os/2006/03/P054505COPPARuleRetention.pdf. Only Aftab believe COPPA has had a negative effect, and even it conceded that this was during the dot-com bust of 2000, when it would be difficult to single COPPA out as the main cause.

not make it obvious that a person must be above a certain age to use the site. For this reason, making it impossible to input an age before a certain year, e.g., 1995, will not satisfy FTC requirements as this would encourage the user to provide false information. The FTC prefers an approach that allows any birth date to be entered. However, if the date given proves the user to be under a certain age, the system should not allow them access, and furthermore, a cookie should be placed on their computer preventing them from returning to the data entry page and providing a false birth date.

COPPA in Practice

Imbee.com

Imbee.com was promoted as a "free, secure, social networking, and blogging destination specifically designed for kids aged 8 to 14." According to the FTC, Imbee.com collected and maintained information from children under 13 years of age without obtaining verified consent from their parents. Over 10,500 children were allowed to create Imbee.com accounts by submitting their first and last names, dates of birth, personal e-mail addresses, parents' email addresses, gender, user names and passwords prior to the site providing notice to their parents, or obtaining consent. In February 2008, Imbee.com was ordered to pay a $130,000 civil penalty, delete all personal information it had collected, and circulate the FTC's "How to Comply with the Children's Online Privacy Protection Rule" to company personnel.

Imbee's homepage now displays a prominent link to its privacy policy, which is divided into information for children and adults, the former written in language accessible to a child. It provides detailed information on what personal data Imbee collects, and the circumstances in which parental approval is sought. Imbee lists three acceptable methods of age verification: credit card details; telephone confirmation; or a valid, government-issued form of identification.

Xanga.com

In September 2006, social networking site Xanga.com paid a $1 million civil penalty for breaching COPPA by creating over 1.7 million accounts for children under 13 without first notifying their parents that they were collecting this information or allowing them access and control over their own child's personal data. Similar to Imbee.com, Xanga was ordered to circulate FTC documentation and delete all collected information.

Following this penalty, Xanga's privacy policy now contains a prominent warning that children under-13 are not allowed to register for accounts. It also provides a link for parents, which contains information about children's privacy online and instructions on how to close their child's account. Details of their verification scheme to check both the child's identity (through offline methods -- e.g., driving license, passport, birth certificate, or daytime or evening telephone number) and the parent's identity (provision of the child's details, telephone number, email address and signed statement that the guardian is over 18 and the child's parent) are also made available.

Sony MBG Music

On 11 December 2008, Sony equalled the largest payout ($1million) under COPPA since its conception when it settled a claim brought by the FTC. The case marked the 13th enforcement action taken by the FTC. The FTC brought the action because Sony BMG Music posted, and made available for viewing on the Internet, items of information submitted by at least 30,000 children under 13 including photos, gender, age and location.

Sony BMG Music's privacy notice now contains a provision warning users under the age of 13 that they should not post personally identifiable information on Sony's site. Further, certain areas of the site require users to input their date of birth before access is granted. If the date supplied reveals that a user is under 13, a cookie is placed on their computer to prevent further access attempts.

Age Verification Methods - Some Examples

In preparing this paper, our research revealed two recent age verification schemes that were sufficiently unique to warrant a brief description. Whether either will be commercially viable is yet to be seen, but they do demonstrate two different models for addressing the age verification problem. Further, advances with Identity 2.0 may provide some solutions in future.

e-Guardian

eGuardian requests that parents submit the date of birth, address, school and gender of a child to the company, and then asks the child's school to confirm that these details are correct. Schools effectively become trusted third parties in the scheme. This process is slow and not well suited to general content websites, but it has proved appealing to website operators providing services for children. The way in which eGuardian generates revenue has proven to be controversial, however. As an incentive to sign up to the service, eGuardian offers financial inducements to schools if they can successfully persuade a parent to place their child in the scheme.[57] eGuardian proposes to then sell the information they gather to website operators to facilitate targeted advertising. This has understandably given rise to serious privacy concerns, even though eGuardian claims parents can opt out of having data sent to advertisers. The New York Times claims that eGuardian has pitched the idea to Facebook and MySpace, whilst Microsoft will give users the option of signing up to the service.[58] Critics maintain that website advertisers should not be able to target children, and the Attorney General of Connecticut claimed that while targeted advertising may have its place, it should not be at the expense of, or pose a threat to, children's safety.

---

[57] B. Stone, Online Age Verification for Children Brings Privacy Worries, *The New York Times*, November 16, 2008, found at: http://www.nytimes.com/2008/11/16/business/16ping.html?_r=1&sq=stone&st=nyt&adxnnl=1&oref=slogin&scp=5&adxnnlx=1226930549-uGDZZke3jPEN/rGGHce7lg.

[58] Id.

VerificAge

A company called VerificAge uses developments in biometric technology to create a product that can verify a child's age.[59] Aimed at parents and other end-users, the device utilizes a low frequency ultrasound scanner to scan the physiological properties of a user's finger to determine his or her approximate age. The company claims that the device is highly accurate and able to distinguish between children up to 12 and adults with an accuracy rate of 98%.[60] The accuracy reduces to 96% between adults and children aged 12-13. There are clear downsides to this method and the company itself admits that there are "issues" in accurately predicting whether a user is a child or adult around the age of 14. An additional flaw is that an online service provider needs to incorporate VerificAge's Javascript code onto their website before the device will function, and, more fundamentally, it ceases to function as soon as the child moves onto another computer that does not use the device.

Identity 2.0

Identity 2.0 is the name given to anticipated advances in online identity verification technology, which are designed to prove a user's identity without requiring additional information. Using digital signature technology and the Uniform Resource Locators (URLs), current Identity 2.0 systems including "Information Cards" and "OpenID" allow users to login and verify their identity on enabled sites without needing to remember a password or username. This could be particularly useful for a young child who may not have the capacity to use traditional methods.

Unfortunately, because the online infrastructure has not developed as quickly as had been anticipated, these systems will not be widely available for several years. Neither are they likely to provide a solution for general content sites that do not target children, as these sites are unlikely to be enthusiastic about implementing costly additional solutions. That said, leading companies are now exploring the technology -- Microsoft, Google, Paypal and others recently founded the Information Card Foundation, a non-profit organisation committed to fostering a simpler, transparent and secure digital identity system on the internet. If interoperability and infrastructure problems for Identity 2.0 technologies can be resolved, then they may well prove to be an effective solution to current verification problems.

Conclusions

The purpose of this exposition of practices and regulation was to show how industry, regulators and privacy practitioners are continuing to grapple with this difficult subject of children and consent, and the absence of targeted laws, regulations, and guidance in this area continues to prove problematic.

---

[59] *See*: http://www.verificage.com.

[60] *See* http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Verificage_ISTTFTAB_submission.pdf, p.2.

Conclusions and Further Work

By reviewing all the work that has gone into issues around consent within academia, industry, regulators and policy-makers, it has become clear to us that while getting this far was indeed an accomplishment, everyone is in great need of more guidance to navigate through this complex and complicated domain.

Although many of the examples raised in this report are linked with mostly traditional web services, though with some discussion of cases involving domains such as internet advertising and web 2.0, we believe that many of the challenges and implications that we identified will be just as relevant as we consider other internet privacy issues. For instance, the managing of personal preferences and personal information in a 'cloud computing' environment may benefit from some of the policy and technology tools identified in this paper. Similarly, the authentication challenges that exist in all the cases above are certainly not limited only to consent issues but to general data management issues when we are dealing with sensitive information, and particularly sensitive personal information.

In fact, so many of these problems return to the issue of authentication and the management of the means of stating a preference, or in the cases above, the signaling of consent. The conundrum that arises is that if individuals wish to state a preference do they have to give up the right to privacy and authenticate themselves to a service provider? Similarly, if the processing of personal information is not conducted based on the linking of that personal information to an authenticated identity, we can never be certain that we aren't processing the personal information of a child.

If not properly managed, these authentication challenges can pose serious threats to transparency principles and subject access rights. That is, if individuals must be able to see the profile that is being developed based on their personal information, then each individual must be able to authenticate to gain access to that profile. If the means of authentication are too strong, then the individual may be compelled to strongly identify him or herself. However, if the means of authentication are too weak, then malicious third parties could gain access to the profiles of individuals and use that data for further, and possibly nefarious, purposes.

In many senses, this is the foundation problem. On top of those shaky grounds we have further problems highlighted in section II regarding the qualification of 'informed' consent. Particularly in the realm of online advertising there must be some means of informing users that their personal information is being processed for advertising purposes, informing the nature of that processing and the risks therein, and offering the means to give consent, without overburdening the consumer or introducing new risks.

More guidance is required, and it is now the task of regulators to provide this new information to the other players. If regulators are informed about the leading opportunities in the technological field, and the good practices in industry, we would hope that this will enhance the nature of the guidance and protections that follow. This is perhaps too great a task for regulators alone. We recommend there be a regular engagement across these sectors about the practices and policies around consent. This 'engagement' would provide an opportunity for everyone to share

ideas, experiences, and concerns. Then we can start resolving some of these problems in our midst, identify new ones to tackle, and identify the best practices that must be pursued.

The lessons here can then be applied across other domains. We therefore point you to the research that we are doing on the privacy issues in Internet Advertising, and the privacy and security opportunities for Cloud Computing issues. The research was conducted in a manner similar to here, where engagement with industry and academia was essential. Both reports are due out in the summer of 2009.

Appendix I: Children's consent to data-sharing and processing

Introduction

The purpose of this section is to give further indications of current legal thinking on children's ability to give informed consent to information sharing, both in the UK and more widely in the EU.[61] This is an extract of a larger report written by Action on Rights for Children (ARCH) and funded by the Nuffield Trust. ARCH conducted research in the UK with specialist academic and practising lawyers and organisations[62] in order to establish the legal basis for claims about children's capacity to give valid consent, in particular to data-sharing, and conducted a comparative study of seven EU countries.

Though many of the cases discussed below are about medical and legal services, they do not involve the issue of information sharing, it is essential to understand the circumstances in which children can give informed consent to data processing so that we can develop good practices while also identifying some of the pitfalls and dangers in processing information on children.

Children's consent in the UK

It is important to remember at the outset that the common law jurisdictions of England, Wales and Northern Ireland have an entirely separate legal system from that of Scotland, which is based in Roman law.

Scotland:

Prior to 1991, girls reaching the age of 12, and boys the age of 14, achieved the legal status of 'minority', which made it possible for them in certain circumstances to enter into legally-binding contracts.

---

[61] This section is part of a research projected conducted by Action on Rights for Children (ARCH).

[62] The research was conducted through interviews with a number of individuals and experts at relevant and influential organisations. From within academia, the research team met with researchers and lecturers at the University of Cambridge; the University of Manchester; the University of Hull; Pembroke College, Oriel College, and Exeter College, Oxford; the University of Sussex; the University of Leeds; King's College London; the University of Leicester; the University of Bristol; and the University of Liverpool. Law firms that were consulted include Morgan Cole and Matrix Chambers. Finally, the institutions who informed the research include the British Medical Association, the Family Law Bar Association, the General Medical Council, and the Information Commissioner's Office.

In order to rationalise and restrict the legal capacity of children under 16 in Scotland, the Age of Legal Capacity (Scotland) Act 1991[63] was enacted. It provides that those aged under 16 cannot normally enter into contracts, and any contract entered into by a person aged 16-18 can be subject to review by the courts. The Act also provides for a presumption of competence, in limited circumstances, from the age of 12, and section 66 of the Data Protection Act 1998[64] extends this presumption to the exercise of data protection rights. It should be noted that this is not a fixed age of consent, and we are advised by the General Medical Council and the Scottish Child Law Centre that it does not absolve practitioners of the responsibility for ensuring that a child is competent to consent.

England, Wales and Northern Ireland:

The situation in the rest of the UK is far more complex. The ordinary rule is that one cannot make any assumptions about a person under 16 because they lack legal capacity. However, a body of case law has developed on the circumstances in which children can consent to specific services, such as medical treatment or legal representation, and the principles established by such cases have been expanded into other areas.

No case specifically about children's consent to data processing and sharing has yet been before the courts and thus it is to a large extent uncharted territory. Indeed, there is no categorical answer to the question of whether a child can give consent to information-sharing; merely a selection of opinions and 'best theories' that would be argued in court.

The law has developed from the 1986 House of Lords' decision in the case of *Gillick v. West Norfolk and Wisbech Area Health Authority,*[65] to which we shall hereafter refer as '*Gillick'.* Mrs Gillick had sought a declaration from the court that it was unlawful for a doctor to prescribe contraception for a girl under 16 without the consent of her parents. She lost at first instance, won before the Court of Appeal and then lost again in the House of Lords.

'Gillick' still provokes much discussion, but the key message of it is set out in the form of guidelines taken from Lord Fraser's speech in which he set out the following criteria

[63] Age of Legal Capacity (Scotland) Act 1991 (c. 50). Crown copyright.

[64] Data Protection Act 1998, CHAPTER 29. Crown copyright.

[65] Woolf, J [1984] Q.B. 581, Court of Appeal [1985] 2 W.L.R. 413, House of Lords [1986] 1 AC 112

under which a doctor could lawfully provide contraception to an under 16 year old without being under a duty to inform her parents:

1) that the girl (although under 16 years of age) understands his advice;
2) that he cannot persuade her to inform her parents or to allow him to inform them that she is seeking contraceptive advice;
3) that she is very likely to begin or to continue having sexual intercourse with or without contraceptive treatment;
4) that unless she receives contraceptive advice or treatment her physical or mental health or both are likely to suffer;
5) that her best interests require him to give her contraceptive advice, treatment or both without parental consent.

These have become known as the '*Fraser guidelines*' and a child who meets the criteria is said to be *'Gillick competent'.* The guidelines are narrowly drawn and medically focussed, but subsequent cases have built upon *Gillick,* developing the idea of young people being involved in and consenting to that which affects them.

Children's rights to confidentiality, to have their views considered and to give consent have also been expanded by legislation, such as the Data Protection Act 1998; the Human Rights Act 1998; and the UK's ratification of the United Nations Convention on the Rights of the Child in 1991, while the Children Act 1989 enshrined the principle that the welfare of the child is *'the court's paramount consideration*'[66],

Gillick is still highly significant. In 2006, when the case of *Axon v. The Secretary of State for Health*[67] came before the courts, Silber, J effectively reiterated the guidelines given by Lord Fraser, and concluded that *'Gillick remains good law'.*

Interpretation of Gillick

The majority of lawyers whom we interviewed agree that *Gillick* established a common law principle that under-16s can sometimes consent to certain things. However, they were adamant that there is no scope in English law for a presumption of competence at any fixed age. *Gillick* did not proceed on that basis, and in his speech Lord Scarman specifically warned against attempting to fix any age:

> *'Certainty is always an advantage in the law, and in some branches of the law it is a necessity. But it brings with it an inflexibility and a rigidity which in some branches of the law can obstruct justice, impede the law's development, and stamp upon the law the mark of obsolescence where what*

[66] s1(1) Children Act 1989

[67] [2006] EWHC 37 (Admin)

is needed is the capacity for development. The law relating to parent and child is concerned with the problems of the growth and maturity of the human personality. If the law should impose upon the process of "growing up" fixed limits where nature knows only a continuous process, the price would be artificiality and a lack of realism in an area where the law must be sensitive to human development and social change.'

There is not in any case a clear consensus that *Gillick* can be applied to situations where a child's consent is sought to share data. While some believe that *Gillick* established a common law principle in the matter of young people's consent generally, others believe that it is questionable whether *Gillick* can be mapped onto the largely abstract and intellectual matter of information-sharing.

There is also a range of views amongst lawyers as to whether the default position established in the *Fraser guidelines* – that parents should be involved in decisions unless the child herself specifically objects – applies to situations other than where the child is seeking sexual health advice. Although the majority of lawyers believe that parental involvement is a matter of good practice rather than of law, it is significant that the Family Law Bar Association disagrees because, in their view, parents have parental responsibility for their minor children. Thus it is a matter of law that they should at least be informed and consulted unless the child flatly refuses such involvement. According to Andrew Bainham, a Reader in Family Law and Policy, Faculty of Law at the University of Cambridge and Fellow of Christ's College, Cambridge *Gillick*:

'…does not support a view that [parents] can simply be routinely by-passed. It rather supports a form of participatory decision-making in which it would be normal to try to persuade a child to inform parents and bring them into important decisions. Cases subsequent to Gillick have made the important point that parents retain their parental responsibility until the child attains majority at 18 and this is so whether or not the child has capacity for decision-making. In other words, children's capacities and parental responsibility co-exist or are concurrent.'

Considerable confusion has been created by the UK Government guidance on consent to information sharing that states:

'Children aged 12 or over may generally be expected to have sufficient understanding'[68]

There is quite simply no basis in English law for this assertion.

[68] Information Sharing Guidance for Practitioners and Managers, HM Government 2008.

Ambiguous wording in the Information Commissioner's guidance on s66 of the Data Protection Act 1998 (the exercise of rights in Scotland by children)[69] has also muddied the waters because it implies that the presumption of competence at 12 in Scotland also applies throughout the UK. We understand that this guidance is currently being revised to make the legal position clear.

Although children may be capable of exercising some data protection rights, such as subject access, from a relatively young age, there is a difference between accessing one's records or issuing an instruction that maintains the status quo of confidentiality, and taking an active decision to release information that may have long-term consequences. Legal experts have pointed out to us that information sharing is a more complex issue than subject access, while Joan Loughrey, a Senior Lecturer in Law at the University of Leeds, argued:

> *'Choosing to have your confidentiality breached is much more of an autonomy right. You need to have the capacity to make an autonomous decision regarding the release of information.'*

Competence is not a fixed state that a child attains: it is issue-specific and relates to the nature of the information and the gravity of the potential consequences of the decision. The fact that a child may, for instance, consent to antibiotic treatment does not mean he is capable of consenting to long-term steroid use. Similarly, being competent to forbid certain people access to confidential information does not mean that a child is competent to waive that confidentiality where it may have consequences that the child is not sufficiently mature to understand.

The elements of competence

To say that competence cannot be presumed at any specific age is not in any way to imply that a person under 16 could never offer valid consent to the sharing of their personal data, or that a child of 12 – or younger – may not be competent to consent to certain things. However, the child must meet the *Gillick* criteria and, once any possibility of a 'rubber-stamp' decision based on age has been removed, it becomes necessary for the person seeking consent to engage in a far more subtle process of information-giving and assessment.

Competence will depend upon the individual child's maturity, intelligence and understanding in relation to the particular decision. This is not simply an issue of

[69] Data Protection Act 1998, Legal Guidance. http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf

cognitive capacity, as courts have spoken of 'psycho-social maturity' in judgments concerning a child's refusal of consent to medical procedures.

If a particular child possesses that maturity, he must then be given sufficient information about the implications of the proposed course of action to weigh up the relative risks and benefits in order to reach a decision, and it will be for the practitioner seeking consent to ensure that this information has been fully understood.

In the UK Information Commissioner's view, a child needs to know exactly what information is being talked about and what will be shared in as much detail as possible. The child must be told with whom the information will be shared and why, what the people receiving it will do, and how long it will be held for:

> *'We are adamant that consent is linked to Fair Processing. It's not just what the information is but what the consequences of sharing or not sharing might be. When talking to a child, it's not just 'can we share with this person for this', but the difficulties which might arise either way – that some people who see it may for example have to tell teachers or parents.'*

The child also needs to be made aware of data protection rights and information security arrangements, including any risk that data may be lost or stolen. The majority of lawyers whom we interviewed believe that a practitioner must be trained in seeking consent from children. Indeed, the Family Law Bar Association was emphatic that the process requires a high level of skill.

The lawyers whom we interviewed have made it clear that the standards for obtaining children's consent are high. Because the default position is that children under 16 do not in general have legal capacity, each exception must be judged according to the criteria laid down in *Gillick* (which includes a requirement that a proposed course of action is in a child's best interests) and developed in common law. As some of our interviewees suggested, it may even be that issues of data-sharing and processing are beyond the scope of *Gillick,* although there can be no definitive answer until a case goes through the courts. The alternative is that the Government brings forward legislation to clarify the position. As Lord Scarman opined:

> *'If certainty be thought desirable, it is better that the rigid demarcations necessary to achieve it should be laid down by legislation after a full consideration of all the relevant factors than by the courts confined as they are by the forensic process to the evidence adduced by the parties and to whatever may properly fall within the judicial notice of judges.'*

Children's consent in the EU

Data protection laws on the Continent are generally strict about what constitutes valid 'free, specific and informed' consent - be this of an adult or a minor. In all the countries examined below, valid consent can only be given by someone (adult or minor) if that person was fully aware of, and could appreciate, the consequences of giving his or her consent, which in itself means that consent can only ever relate to clearly-defined processing for very specific purposes.

It is also expressly recognised, not just by the data protection authorities but notably also by the courts, that minors are 'adults in the making', who require extra protection of their fundamental rights, and thus also extra data protection. In other words, data protection rules are applied with special rigour in the case of minors.

While there is no agreement on a specific age when a minor can consent to the processing of his or her personal data - indeed, the consensus is that this is not a matter that lends itself to such a simple rule – there is a degree of convergence. In the Continental-European countries examined below, a young person will often be able to consent to the processing of his or her data from somewhere between the age of 14 to 16.

The question of whether a particular minor is competent and can give valid consent in a particular context will depend upon all the circumstances, including both subjective matters such as the maturity of the minor and more objective matters such as whether the matter for which consent is sought is in the direct interest of the minor or not, and also whether the parents were, or should have been involved. For trivial matters which do not have any significant effect, the age in some countries may be lower, sometimes perhaps as low as 12, but even then the requirements about the validity of consent remain to be met, and are especially strictly applied.

Germany

In Germany consent as a basis for processing of personal data, especially by public authorities, is of limited relevance. More important are the requirements that any processing by such authorities may only take place for a narrowly-defined purpose and on the basis of a specific, strictly-worded legal provision, and that they may only seek and use personal data that are strictly necessary, therefore, they can only process personal data on the basis of consent to the extent that that is expressly allowed in the relevant rules, or clearly compatible with them.

Data protection rules and principles must be applied with particular rigour when it comes to children and young people. While the general rule is that they should in principle be seen as competent from the age of 14, the more important consideration is the professional duty of care. Accordingly, in the (quasi-) public sector, for children under 12, the parents should always be consulted; for children between 12 and 14, this must always be considered; and for minors over 14, it can still be considered where a professional believes that it is necessary to consult the parents and not rely solely on the wishes of the data subject.

France

The French authorities take a more administrative-regulatory approach to data protection, in that they seek to lay down (at least for the public and semi-public sectors) detailed rules setting out the requirements for each specific context. The French data protection authority, the National Commission for Informatics and Freedoms (CNIL) plays a central role in this, not just in monitoring compliance with data protection rules and principles laid down by the legislature, but by playing a strong role in the formulation of those rules themselves.

As in Germany, considerable emphasis is placed on the need to enforce data protection rules especially strongly where children are concerned, and the best interests of the child are paramount. In various contexts, CNIL has emphasised the need to involve parents in data protection matters relating to young people. In 1983, the CNIL ruled that questionnaires should not be handed out to students in a secondary school without the prior written consent of the parents. It has also required the prior written consent of parents for placing photographs of minors on a school website, and for the passing on of contact data on minors for the purposes of direct marketing.

CNIL has also held that all collecting of data from minors on their family circumstances, their parents' lifestyle and their social and professional status is 'excessive and unfair', and thus unlawful; and that the recording of sensitive data on minors is prohibited, unless the controller can provide proof that the parents have expressly consented to this.

The sharing between public bodies of personal and sensitive data on minors would require a clear, specific legal basis, which should spell out the precise purposes and limitations of the data sharing. The CNIL would be highly doubtful of the legitimacy of basing any such sharing on consent, and would be likely to find that consent could not be relied upon in the absence of such provisions. Where, exceptionally, it might be allowed, it would appear that the CNIL would require such consent to be given by the

minor's parents, at least as far as minors under the age of around 15 or 16 are concerned.

Belgium

The issue of consent by minors to the processing of their personal data has been addressed in some detail in Belgium in an Advice by the Belgian data protection authority in relation to the protection of the privacy of minors on the Internet.[70] The Advice notes that children are in a weak position when using the Internet because they are more easily manipulated, less suspicious, and less aware of rights than adults.

On the question of when a child comes of age, the Advice notes that although under Belgian law, the general age of maturity is 18, in reality - and law - there is a gradual development, with minors gaining more independence as they grow up, in particular in adolescence, which is broadly considered to be 13 – 16.

Data collected online from any minor cannot be used for purposes other than those for which they were collected, and cannot be passed on to others. Parental consent is required in all circumstances where a child is not yet mature enough to understand the implications of the solicited consent. (This is generally considered to be younger than 13 or 14, but for complex cases may be 15.) Parental consent is also required whenever sensitive data are sought from minors under 16, and in all circumstances when the processing may not be in the direct interest of the child.

Portugal

Although Portugal has had a data protection law since 1998 the standards have not yet been fully developed, and there is little specific law on its application to minors.

Parental consent must be sought for the processing of personal data on a child under 12. Children between the ages of 12 and 14 may be able to exercise some data protection rights in their own name, perhaps even without involving parents at all, if the matter is relatively trivial. If the issue is serious and may affect the interests of the child, parents should be informed and consulted, and are likely to be given an overriding right to decide. If children are over 14, their views will be given more weight, and may be decisive, but the data protection authority is still likely to feel that, without good reason,

---

[70] *Advies Nr 38/2002 van 16 september 2002 betreffende de bescherming van de persoonlijke levenssfeer van minderjarigen op Internet/Avis N° 38/2002 du 16 septembre 2002 relatif à la protection de la vie privée des mineurs sur l'Internet* (Advice No. 38/2002 of 16 September 2002 concerning the protection of the private life of minors on the Internet). The full text can be found on the Privacy Commission's website at: http://www.privacycommission.be/nl/docs/Commission/2002/advies_38_2002.pdf (Dutch); http://www.privacycommission.be/fr/docs/Commission/2002/avis_38_2002.pdf (French).

the young person's consent cannot be considered valid if the parents have not at the very least been consulted. Overall, the data protection authority will place great emphasis on the need to consider what is in the minor's best interests.

Spain

Data protection regulations in Spain contain specific rules on the question of consent for the processing of data on minors. The provision, contained in Article 13 of the Regulation,[71] reads as follows:

> ***Article 13 – Consent for the processing of data on minors***
>
> *1. Data pertaining to data subjects over fourteen years of age may be processed with their consent, except in those cases where the law requires the assistance of parents or guardians in the provision of such data. The consent of parents or guardians shall be required for children under fourteen years old.*
>
> *2. Under no circumstances may data be collected from the minor regarding information about any other member of the family unit, or about its characteristics, such as data relating to the professional activity of the parents, financial information, sociological or any other such data, without the consent of the persons to whom such data refer. The aforesaid notwithstanding, data regarding the identity and address of the father, mother or guardian may be collected for the sole purpose of obtaining the authorisation set out in the previous subsection.*
>
> *3. When processing refers to the data of minors, the information aimed at them shall be expressed in easily understandable language, with express indication of the provisions of this Article.*
>
> *4. The data controller is responsible for setting up the procedures that guarantee that the age of the minor and authenticity of the consent given by the parents, guardians or legal representatives have been effectively checked.*

Denmark

There are no specific rules in the Data Protection Law as to its application to minors. A general rule that young people are legally competent from the age of 15 is usually taken as a rule of thumb in the data protection context; parents are generally consulted about

[71] 'Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. ' https://www.agpd.es/portalweb/canaldocumentacion/legislacion/estatal/common/pdfs/RD_1720_2007.pdf

the sharing of data on their children under the age of 15. However, the authorities stress that all relevant matters should be taken into consideration, including the nature of the data, the seriousness of the issue in the context of which the data are processed or shared, and where appropriate the maturity or otherwise of the young data subject. All of these may imply a need to involve the parents, even if a child is over the age of 15, rather than relying solely on the consent of the young person.

Sweden

In Sweden, the basic rule is that children of 14 or 15, and sometimes 13, are normally capable of giving consent for the processing of their data - but this is always subject to a test of whether the individual child in question is mature enough. Professionals may never simply rely on the age of the child; rather, they must always take the context and the maturity of the particular child into account. Moreover, even if a child is deemed to be capable of giving consent, the parents must still be informed of the fact that the child consented to any specific processing or data sharing (unless there are special reasons not to do so, as in cases of suspected child abuse).

It should be noted that a review is currently taking place of data sharing arrangements in Sweden, in particular in the public sector, and the report on this review is due in the autumn of 2009.

Conclusions

There is so much that remains unresolved in the area of children and consent. The purpose of the research project that led to this briefing was to give an indication of current legal thinking on children's ability to give informed consent to information sharing, both in the UK and in other EU countries.

Despite all the findings in the report, and the key points have been flagged in this briefing and excerpt, so much still remains to be understood. The research focussed mostly in the domain of information sharing, but could very well be applied to general processing of personal information, by both the public and private sectors.

The lack of legal guidance in this domain is startling. Parliaments around the world need to consider legislating, particularly in the domain of children and the use of their personal information by the private sector. Otherwise, under the current legal landscape it could be said that every child under the age of 16 who wishes to apply for a social networking account would have to be individually assessed.

Legislation would also clarify the practices on data retention, deletion, and the applicability of profiling techniques. Most importantly, it will bring these issues into the public domain so that we can all discuss and debate these important issues. Otherwise we are relying on adaptations of 20-year old rulings that hardly considered some of today's pressing challenges.