



CREATe Working Paper 2014/15 (October 2014)

# The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services

---

## Authors

Lilian Edwards  
University of Strathclyde  
Lilian.Edwards@strath.ac.uk

Wiebke Abel  
Pangloss Consulting  
Wiebke.Abel@googlemail.com

---

CREATe Working Paper Series DOI: [10.5281/zenodo.12506](https://doi.org/10.5281/zenodo.12506).

This release was supported by the RCUK funded *Centre for Copyright and New Business Models in the Creative Economy (CREATe)*, AHRC Grant Number AH/K000179/1.

## Contents

<b>1</b>	<b>EXECUTIVE SUMMARY .....</b>	<b>1</b>
<b>2</b>	<b>Introduction and purpose of report.....</b>	<b>4</b>
<b>3</b>	<b>Examples of iconography.....</b>	<b>5</b>
	3.1 Introduction .....	5
	3.2 Offline example: EU Energy Label .....	7
	3.3 Offline example: laundry labels.....	9
	3.4 Online example: Creative Commons .....	10
<b>4.</b>	<b>Privacy initiatives.....</b>	<b>11</b>
	4.1 Platform for Privacy Preferences (P3P) - machine readable privacy statements .....	11
	4.1.2 "Privacy Bird" - graphical P3P extensions.....	14
	4.2 Modern iconography approaches.....	14
	4.3 Academic projects .....	15
	4.4 Privacy Icons (PIS).....	18
	4.5 Labelling for privacy policies .....	19
	4.6 The Privacy Wheel .....	20
	4.7 Assessment and optimisation of privacy icons and labelling .....	21
<b>5.</b>	<b>Summary.....</b>	<b>23</b>
	5.1 Detail versus accessibility.....	23
	5.2 Information about site policies, or information about legal compliance ? ....	24
	5.3 Jurisdictional issues .....	24
	5.4 Would labelling or icons showing more than legal compliance promote greater or higher-priced uptake by consumers? .....	24
	5.5 General issues to be highlighted: competition, critical mass, audit .....	25
<b>II.</b>	<b>Standard Contract Templates for Customers Facing Digital Services...</b>	<b>27</b>
	.....	
<b>1.</b>	<b>Introduction.....</b>	<b>27</b>
<b>2.</b>	<b>EU Data Export Clauses.....</b>	<b>28</b>
<b>3.</b>	<b>Model Service Contracts for EU Cloud Computing Suppliers .....</b>	<b>29</b>
<b>4.</b>	<b>Licenses for Europe.....</b>	<b>30</b>
<b>5.</b>	<b>Summary .....</b>	<b>31</b>

## 1 EXECUTIVE SUMMARY

In the wake of the Snowden revelations about covert state access to consumer data stored in the cloud, consumer confidence about the handling of their personal data in the Cloud in particular, and in digital services in general, has suffered a severe blow. This is particularly true in Europe, where in general consumers expect a higher standard of privacy protection than in the US, both by law and as a matter of cultural norms.

Accordingly this report was commissioned to examine two possible paths for UK industry to re-establish consumer trust and confidence in the cloud, and in consumer digital services in general.

First, we consider the use of **icons and labelling** as a means to more effectively communicate complex and lengthy privacy policies to consumers.

Secondly, we assess the use of **standardised contract terms or templates** in relevant business-to-consumer (B2C) markets, and ask if these might be helpful in relation to industries which collect and use personal data.

### *Iconography and labelling*

In the first section, this report surveys existing examples where iconography and labels have been used to support consumers to make informed decisions about complex factual or legal matters. In particular, we survey prominent use-cases where information about personal data collection and use has been made more accessible to consumers by representing privacy policies via icons and labels.

The key findings and recommendations from this part of the analysis are:

- Icons and labels both have a long history of helping communicating complex factual information in an easy-to-grasp way to consumers. This is true in “off-line” contexts, such as, notably, energy use by applications, laundry instructions and nutritional labelling; and in the digital world, such as the use of Creative Commons icons to indicate the permissions given by the creator of a copyright work.
- Empirical research about applying these techniques to *privacy policies* is mainly limited to academic work, but some detailed icon sets have already been devised eg Prime Life, Privacy Icons Software.
- There is some evidence that user understanding of privacy policies is enhanced by using icons and labels as well as conventional legal text (a “multi layered” privacy notice approach). However this hypothesis has not really been tested “in the wild” due to lack of uptake of existing schemes to date.
- Hard choices have to be made about exactly what features a privacy icon scheme indicates, given the need to provide simplicity at the expense of legal detail. Furthermore, existing offline schemes largely provide descriptive information (eg “number of calories”), not legal assessments (“processing fair and lawful”). Existing schemes vary from one very simple icon to complex sets involving up to 30 icons in various states.
- Labelling schemes can give more information than icons, but may become correspondingly more confusing with information overload for users.
- Icon sets or labels can be devised for discrete industry sectors (eg email, social networks) rather than all data processing, which may help reduce the icon set or information overload.

- Entirely market-driven self-regulatory schemes such as the Platform for Privacy Preferences (P3P) have failed in the past, because of lack of sufficient incentives for both consumers and industry to take part, leading to a crucial failure to achieve critical mass. Achieving consumer mass for consumer recognition would be crucial to the success of any icon scheme for privacy. No current scheme has (yet) achieved this visibility. Governmental involvement in (co-)promoting schemes might help overcome this market hurdle. “Iconifying” privacy policies (and maintaining such) is also time consuming for industry: automatic generation tools as with CREative Commons may help.
- “Offline” examples have found that a standardised graphical approach across multiple national jurisdictions is best for successful implementation and consumer recognition. This may be difficult to achieve in a field such as privacy, where laws (and regulatory oversight) are very different globally, and yet access to services is multi-jurisdictional.
- If a system was to indicate legal (or more than minimum legal) compliance to EU users to increase trust and confidence, then again difficult issues of jurisdictional locality (both of user, and service) would arise.
- Some kind of independent audit and/or complaint process, with appropriate sanctions, would also help instill trust by guaranteeing that service providers were actually implementing their privacy claims. This might be provided by working with the existing DPAs (the Information Commissioner in the UK) or by putting an independent industry ombudsman in place.

### *Standard contracts*

The second section of this report surveys proposals for standard contract templates or “regulated privacy policies”.

The key findings are:

- Standard contracts or clauses are a recognised means to ensure that consumers are sufficiently protected against industry standard terms or service level agreements that are unfair and/or significantly weighted in favour of the provider. In the EU, control of unfair terms in B2C contracts by law is already an accepted norm.
- Standard terms and contracts are already used to implement data protection guarantees into contracts where there is export of personal data outside the EU. While only one strategy to achieve legal compliance in this area, this is by far the most popular industry choice. Standardised privacy policies have also been partly introduced in the US in the area of financial services.

- These privacy strategies were both initiated by government intervention (mandatory law). However it is also possible that industry “soft law” could create such regulated privacy policies for industry sectors, with sufficient incentives.
- However, standardisation of contracts and terms, in the context of global data flows, probably has the greatest impact if it is harmonised at international level. This again might be done by law (international treaty), by industry groups, or by standard setting bodies such as ISO.

## 2 Introduction and purpose of report

In the wake of the Snowden revelations about covert state access to consumer data stored in the cloud, consumer confidence about the handling of their personal data in the Cloud in particular, and in digital services in general, has suffered a severe blow.

This is particularly true in Europe, where, in general, consumers expect a higher standard of privacy protection than in the US, both by law and as a matter of cultural norms. Yet EU consumers now see themselves as disempowered to protect their personal data when it is disclosed to or collected by US-controlled services eg Google, Facebook et al. The emerging backlash against data exports into the Cloud in particular has already been predicted by the Cloud Security Alliance, a US industry body, to lose US cloud computing firms between \$35bn and \$45bn over the next three years.

A similar backlash may also follow against UK domestic digital services, given general uncertainty over where data is stored; who is the data controller; and general fears over lack of control over personal data. Even pre Snowden in 2010, Eurobarometer found that only 30% of UK respondents trusted Internet companies to protect their personal data.

The UK export market for services which involve the collection and processing of personal data may also be affected, both within the EU and elsewhere if home-country data protectionism takes root. The German government has called for home-grown email and internet providers, and France is also investing to create a “local” cloud industry. Russia is working to introduce a new law that would force tech firms such as Facebook, Google and Microsoft to build data centres in Russia to ensure citizen data stays in Russia. While so far this activity mainly deleteriously affects US industry, it may soon also affect the UK.

Accordingly this report was commissioned to examine two possible paths for UK industry to re-establish consumer trust and confidence in the cloud, and in consumer digital services in general.

First, we consider the use of **icons and labelling** as a means to more effectively communicate complex and lengthy privacy policies to consumers.

Such icons or labels, as currently implemented, merely convey existing company privacy policies with greater clarity – allowing consumers more effectively to exercise “notice and choice”. They do not allow consumers greater control over their service provider.

Secondly, we assess the use of **standardised contract terms or templates** in relevant business-to-consumer (B2C) markets, and ask if these might be helpful in relation to industries which collect and use personal data.

In B2C markets, suppliers invariably unilaterally dictate standard terms and conditions. In quasi-monopolistic markets, such as search in Europe, there is little market alternative to accepting such conditions. Since data collection and processing is typically legalised by such contracts, they play an important role in restricting what suppliers can do with consumer personal data, and thus in reassuring consumers.

One approach to generating trust and confidence for consumers, is thus to regulate the shape of contracts. Such “regulated contracts” might apply to all or certain B2C industry sectors eg social networks, energy suppliers, marketing companies. Mandatory clauses might require that service providers provide certain remedies, not collect certain data (eg children’s data; health data), not retain data beyond a certain time, etc. These terms might merely comply with data protection law, or might go further, providing greater protection.

### **3 Examples of iconography**

#### *3.1 Introduction*

Almost all websites and service providers engaging with consumers in digital or digital-assisted markets now offer privacy policies. These were originally driven by compliance actions by the Federal Trade Commission (FTC) in the USA, but have also become ubiquitous in Europe to establish compliance with data protection obligations. The UK Data Protection Act (DPA) requires every data controller to have a “privacy notice”.

Privacy policies form part of the contract or license between consumer and service provider and so are binding legal agreements. Consumers are usually made aware of the privacy policy during a sign up or registration procedure, often by hyperlink, and registration then constitutes acceptance of the policy. Accepting the privacy policy gives consent by the consumer to the collection and use of their data, as detailed in the policy. Compliance of a company with its privacy policy is typically overseen by a privacy regulator, such as the FTC in the US, or a DP Authority (DPA) in the EU. In the UK, this DPA is the Information Commissioner.

Privacy policies are known to be problematic as a means for consumers to understand and control the processing of their personal data. Privacy policies are typically long and convoluted, and frequently written in complicated “legalese”. Much empirical research has shown that data subjects rarely read privacy policies, and, even if they do, comprehension is limited<sup>1</sup>. An online survey of over 700 participants that tested policies from six different companies in three existing formats found “participants were not able to reliably understand companies’ privacy practices with any of the formats” and “all formats and policies were similarly disliked”.<sup>2</sup>

Time and convenience also mitigate against any concerted effort to truly engage with privacy policies: McDonald and Cranor calculated that if an individual were to read the privacy policies at every website she visited even once per year, she would spend, on average, an estimated 244 hours per year.<sup>3</sup> Privacy policies also often frequently change from time to time, since service providers typically give themselves the power to make unilateral changes by notice after initial acceptance of the contract. Typically, they become longer and ever more complex as time goes on, eg, by 2010 the Facebook privacy policy had famously become longer than the US Constitution and when all the surrounding policies, guidelines and user statements of responsibilities were added, was longer than the typical novel. This further de-incentivises reading privacy policies and increases the user experience of lacking control over what happens to their personal data.

In general, therefore, data subjects do not read privacy policies, do not understand them if they do, and do not have control over when they change. They do not see privacy policies as giving them rights and therefore their presence when noted (eg, after a controversial change is mentioned in the media) tends to instil anger and confusion not trust. The problem is exacerbated on mobile sites where reading long policies is impractical<sup>4</sup>. The conventional “notice and choice” approach (where users are presented with information about their privacy risks and options, assess it and make informed choices whether to enter the contract) is thus arguably broken.

In recognition of the failure of privacy policies, different approaches have been developed to try to make privacy policies and terms more accessible to the layperson. Ideally, data subjects (consumers) would be able to make informed choices as to their privacy and data protection risks without having to read the privacy policies in full at every site they visit, or service they engage with.

---

<sup>1</sup> See for summary, Edwards L “Privacy , law , code and social networking sites” in Brown I ed *Research handbook on governance of the Internet* (Edward Elgar, 2013) 309.

<sup>2</sup> A M MacDonald, R W Reeder, P G Kelley, L F Cranor, “A Comparative Study of Online Privacy Policies and Formats” (2009) in *Privacy Enhancing Technologies, 5672 Lecture Notes in Computer Science*, 37-55.

<sup>3</sup> A M McDonald, L F Cranor “The Cost of Reading Privacy Policies” (2008) 4 *Journal of Law and Policy for the Information Society* 540-565.

<sup>4</sup> See *ICO Guidance on Privacy in Mobile Apps*, 2013, at [http://ico.org.uk/for\\_organisations/data\\_protection/topic\\_guides/online/mobile\\_apps](http://ico.org.uk/for_organisations/data_protection/topic_guides/online/mobile_apps) .

One approach to reach this goal is the representation of legal text by icons or pictures, ie, iconography. Similar to icons are labels. These, drawn from the concept of nutrition labelling in food, tend to give more information than icons, and may not be pictograms. Both approaches have been trialled successfully in the offline as well as online world, but almost exclusively so far in non-privacy domains. Their utility is thus untested in relation to privacy policies.

Below, we first look at existing examples of iconography from:

- (i) the “offline” world, in a domain other than privacy/personal data
- (ii) the online world, in a domain other than privacy/personal data

before turning to look at attempts to communicate *privacy policies* more successfully. In particular, we examine several recent research attempts to produce “privacy icon” schemes.

### 3.2 *Offline example: EU Energy Label*

The EC introduced a mandatory energy consumption labelling scheme in 1992<sup>5</sup> to provide consumers with standardised information on energy consumption and performance criteria for major household appliances. The energy label allows consumers to identify the most efficient and cost saving appliances without having to read an instruction manual or possess an understanding of the technology of the appliance.

The most prominent and recognisable part of the scheme is the set of energy efficiency classes, ranking originally under the Council Directive from A to G on the label, with A being the most energy efficient and G the least efficient. These are combined with a colour code ranging from green (most energy efficient) to red (least energy efficient) with light green, yellow and orange in the middle. The 2010 EU Directive has updated the energy efficiency classes with grades A+, A++ and A+++ to keep up with development in energy efficiency.

While labels for different appliances, cars, or light bulbs each vary slightly (e.g. labels for refrigerators have icons showing capacity of fresh and frozen food in litres, and the noise in dB) the uniform design characteristics for energy efficiency remain identical, and have, apart from the addition of new grades, remained untouched under the new Directive.

---

<sup>5</sup> Council Directive 92/75/EEC of 22 September 1992. This Directive was replaced by the Energy Labelling Directive in May 2010.

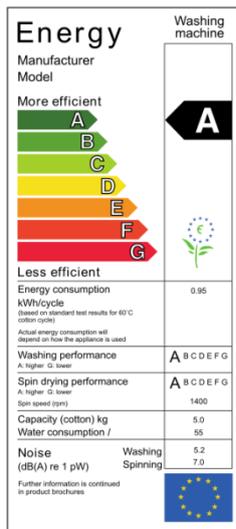


Figure 1: Old energy label

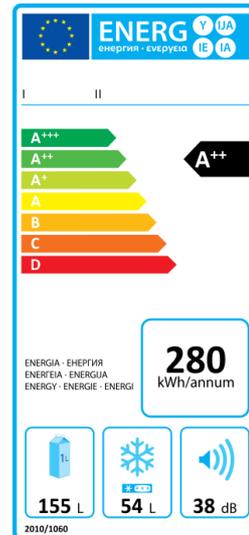


Figure 2: New energy label

Significantly, the new label is language-neutral. Country-specific text is replaced by pictograms as seen above.

The intention of the labelling scheme was to make consumers aware of the relative energy-efficiency of appliances and associated potential cost savings through the provision of observable, uniform, and credible standards.<sup>6</sup> In addition, given that major household appliances account for 35% of total EU residential end-use electricity consumption, the labelling scheme is one of the key components to achieve the energy efficiency targets set by the EU climate and energy package.<sup>7</sup>

Various studies evaluating these schemes have come to the conclusion that they are successful in terms of energy and carbon reductions, since consumers are more likely to purchase appliances with good energy-efficiency ratings.<sup>8</sup> The major criticism is that consumers rely on a limited amount of information to make their decision. A recent study, for example, suggests that improvements to the scheme could be made by including information on relative efficiency of appliances (eg how much is saved by choosing a grade A rather than grade B appliance).<sup>9</sup>

<sup>6</sup> J Truffer et al., “Eco-labeling of electricity - strategies and tradeoffs in the definition of environmental standards” (2001) 29 Energy Policy 885-897.

<sup>7</sup> B Mills, J Schleich, “What’s driving energy efficient appliance label awareness and purchase propensity?” (2010) 38 Energy Policy 814-825.

<sup>8</sup> See e.g. Sanchez et al., “Saving estimates for the United States environmental protection agency’s ENERGY STAR voluntary product labelling program” (2008) 36 Energy Policy 2098-2108; K Lane, “Evaluating the impact of energy labelling and MEPS—a retrospective look at the case of refrigerators in the UK and Australia” (2007) in European Council for Energy-Efficient Economy (Paris): Proceedings of the ECEE Summer Study, 743-751; P Waide, “Monitoring of energy efficiency trends of refrigerators, freezers, washing machines and washer-driers sold in the EU”: Final report, PW Consulting for ADEME on behalf of the European Commission (PW Consulting, 2001).

<sup>9</sup> Mills and Schleich, *supra* n 7.

### 3.3 Offline example: laundry labels

Laundry instructions are coded worldwide by a series of icons which are owned by and registered trade mark of an international association, Ginetex. GINETEX, the International Association for Textile Care Labelling, was founded in Paris in 1963 following several international symposia for Textile Care Labelling at the end of the 1950's<sup>10</sup>. The symbols have also been embodied internationally in an ISO standard 3758:2012. In the UK, these symbols are managed by the UK Fashion and Textiles Association (UKFT).

ASTM GUIDE TO CARE SYMBOLS									
 <b>Wash</b>	<b>Machine wash cycles</b>  normal  permanent press  delicate / gentle	 hand wash	<b>Warning symbols for laundering</b>  do not wash  do not bleach  do not dry (used with do not wash)  do not iron						
	<b>Water temperatures (maximum)</b> symbol (s) dots & °C. <table border="1" data-bbox="558 817 837 918"> <tr> <td>very hot (140F)</td> <td>hot (120F)</td> <td>warm (105F)</td> <td>cool/cold (65-85F)</td> </tr> <tr> <td>60 •••</td> <td>50 •••</td> <td>40 •••</td> <td>30 •</td> </tr> </table>			very hot (140F)	hot (120F)	warm (105F)	cool/cold (65-85F)	60 •••	50 •••
very hot (140F)	hot (120F)	warm (105F)	cool/cold (65-85F)						
60 •••	50 •••	40 •••	30 •						
 <b>Bleach</b>	 any bleach when needed  only non-chlorine bleach when needed								
 <b>Dry</b>	<b>Tumble dry cycles</b>  normal  permanent press  delicate / gentle	 line dry / hang to dry  drip dry  dry flat	<b>Additional instructions (in symbols or words)</b>  do not wring  do not tumble dry  in the shade (added to line dry, drip dry, or dry flat)  no steam (added to iron)						
	<b>Tumble dry heat setting</b>  any heat  high heat  medium heat  low heat  no heat/air								
 <b>Iron</b>	<b>Iron when needed—dry or steam</b> maximum temperature  200°C (390F) high  150°C (300F) medium  110°C (230F) low								
 <b>Dryclean</b>	<b>Dryclean - normal cycle</b>  any solvent  perchlorethylene or petroleum solvent  petroleum solvent only	<b>Dryclean - modified cycle</b>  	 do not dryclean						

Figure 3: Laundry care instructions

<sup>10</sup> See <http://www.care-labelling.co.uk/aboutus.html>.

While symbols vary a little from country to country eg use of Chinese and Japanese number symbols in those countries, they are basically harmonised across the world.

### 3.4 *Online example: Creative Commons*

Another prominent use of iconography is the Creative Commons (CC) list of icons depicting the CC copyright license options.

CC licenses allow creators to distribute copyright works that would normally by default appear to be “all rights reserved” to anyone who tried to copy, publish, perform or remix them.<sup>11</sup> The philosophy of CC is that users may wish to distribute their works with only “some rights” reserved, thus increasing social benefit and minimising permissions clearing. To this end it has developed an automated licensing platform that allows authors, while retaining copyright in their respective works, to authorise as many uses of the work as they choose. The licensing process is standardised and automated at both the drafting and licensing end.

Drafting a license is automated as a user-friendly process explained in plain language.<sup>12</sup> Authors make choices depending on their needs but do not require extensive legal knowledge about copyright. They can choose any combination of the following standardised terms: “Attribution” (requiring credit to the author), “Non-commercial” (uses only for non-commercial purposes), “No Derivative Works” (no changes to be made to the work) and “ShareAlike” (new creations must be in turn licensed under the same terms ).

The license is released in a “three-layer” design:<sup>13</sup> first, a legal version, intended to ensure the license will stand up in court; secondly, a human readable version that communicates in plain language its contents; and thirdly, a machine-readable license, which provides computer-readable code, which can be embedded into a website, and which also allows search engines and other software to understand the terms of the licensing. These three layers ensure that the creator’s license specifications are implemented correctly and can automatically be recognised; and that users appropriating CC works can fully understand their rights (eg to copy, play, distribute, remix, etc).

Most pertinently, the “human readable” CC license selected can be depicted as a set of standardised icons. These can be downloaded and attached to the CC-licensed work. The icons appear clear and concise, and communicate otherwise complex intellectual property and copyright concepts in an easy to understand way.

---

<sup>11</sup> See Creative Commons, at <http://creativecommons.org/>.

<sup>12</sup> See Creative Commons, *Choose a license*, at <http://creativecommons.org/license/>.

<sup>13</sup> Ibid.

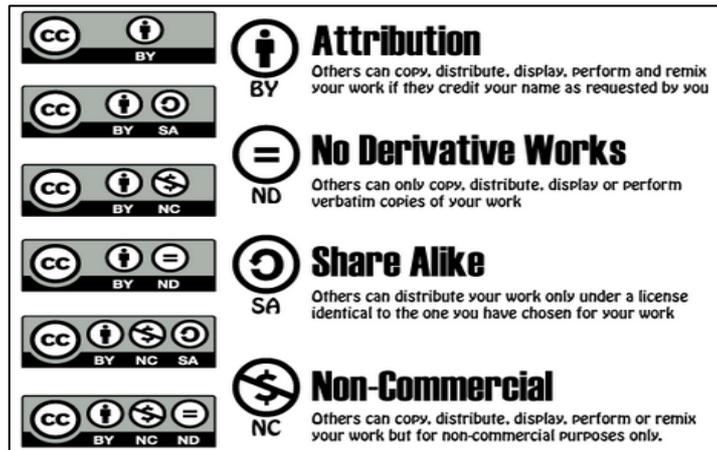


Figure 4: CC Licenses

The success of the icon approach of CC has not been formally assessed. The scheme is generally regarded as a success, albeit mainly within the limits of non-profit uses. Around 400 million CC licensed works had been released as of end 2010<sup>14</sup>. Recent cases in Germany, USA and other countries have shown that CC licenses can be enforced in court<sup>15</sup>, which lends credibility to its use by creators. The widespread use of CC by large commercial websites such as Flickr, Mozilla and Google, and many governments and universities, shows that the scheme is internationally and institutionally accepted.<sup>16</sup>

CC licensing as a global project requires a great deal of institutional effort. Renegotiating the core license suite to keep up with changing laws and needs is a major endeavour. The global scope of CC has required setting up an international infrastructure which requires huge amounts of mainly volunteer effort and fundraising. CC currently operates in around 70 countries with c 100 designated associates. In principle, CC offers a suite of six licenses compliant with international copyright treaties but also enables “ported” local licenses to allow for local law variation; around 50 of these ported licenses exist.

## 4. Privacy initiatives

### 4.1 Platform for Privacy Preferences (P3P) - machine readable privacy statements

Historically, the first attempt to simplify making privacy choices for users online (though not an iconographic project) was P3P, which was developed by the World Wide Web Consortium (W3C) in 2002. P3P was developed at the height of the first “dot.com” boom, in response to Congressional and FTC concern that

<sup>14</sup> [http://wiki.creativecommons.org/Metrics/License\\_statistics](http://wiki.creativecommons.org/Metrics/License_statistics) .

<sup>15</sup> [https://wiki.creativecommons.org/Case\\_Law](https://wiki.creativecommons.org/Case_Law) .

<sup>16</sup> See e.g. list of government use, at [http://wiki.creativecommons.org/Government\\_use\\_of\\_Creative\\_Commons](http://wiki.creativecommons.org/Government_use_of_Creative_Commons) .

user privacy issues might inhibit the development of online commerce<sup>17</sup> and as a plausible self-regulatory alternative to forestall state regulation on privacy<sup>18</sup>.

P3P is a protocol and architecture, developed to allow users to determine whether a website's privacy policy meets their requirements.<sup>19</sup> P3P provides tools for both user requirements and site privacy policies to be expressed as machine readable code. When a P3P user visits a website providing a P3P machine-readable compact privacy policy, the user's privacy requirements can be compared with the website's policy, and the user can be informed of any incompatibility. The user can then at least in theory decide to take action, eg engage with the site anyway, disclose limited information, bargain, or block it.<sup>20</sup>

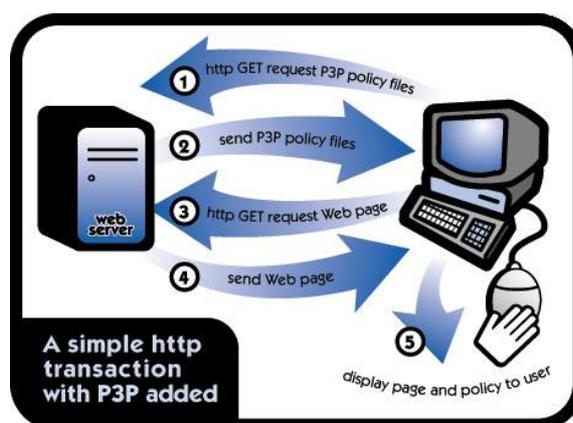


Figure 5: P3P Protocol

P3P is generally regarded as a landmark failure. It is no longer updated due to a lack of market uptake. Even though an extension was developed for Microsoft's web browser Internet Explorer (IE), not many users have implemented it.<sup>21</sup> It has not been incorporated into more modern browsers such as Firefox or Chrome. Most commercial websites do not operate a P3P compact policy. Google even goes beyond non-implementation by tricking IE into believing that it is "about to send a P3P compact policy", when in fact it sends the information that "This is not a P3P policy".<sup>22</sup>

Why P3P failed is highly significant for current attempts to improve privacy information or labelling in the online environment. User failure to adopt P3P was partially blamed on user ignorance and inertia and also on poor interface design: it was too complex for unskilled end users to fully understand and adopt<sup>23</sup>. Service providers also lacked incentives to uptake P3P, given lack of consumer demand, which in turn meant that consumers had relatively few P3P

<sup>17</sup> L F Cranor, "Necessary but not sufficient: Standardized Mechanisms for Privacy Notice and Choice" (2012) 10 *Journal on Telecommunication & High Technology Law*, 273-307, 279.

<sup>18</sup> M S Ackermann, "Privacy in Pervasive Environments: Next Generation Labelling Protocols" (2004) 8:6 *Journal of Personal and Ubiquitous Computing*, 430-439, note 14.

<sup>19</sup> *What is P3P?*, at <http://www.w3.org/P3P/>.

<sup>20</sup> <http://www.p3ptoolbox.org/guide/section2.shtml>.

<sup>21</sup> Cranor, *supra*, n 18.

<sup>22</sup> Cranor, n 18 at 298.

<sup>23</sup> H Hockheiser, "The Platform for Privacy Preferences as a Social Protocol: An Examination Within the US Policy Context" (2002) 2 (4) *ACM Transactions on Internet Technology*, 276-306.

enabled services to pick from. It might also be doubted if service providers at the time had much incentive to cut themselves off from data as a valuable source of extra revenue, given widespread user (at that time) apathy as to personal data collection.

An important issue was how to handle defaults in a state of emergent market failure. P3P envisaged a culture evolving of online automated “bargaining” over data exchange between users and service providers, both equipped with P3P policies. However this causes problems when many service providers have not yet chosen to adopt P3P; so that neither compatibility nor incompatibility could be established. A user with P3P-enabled browser could choose by default to regard a service provider not offering a P3P policy as invisible, or as compliant. If the former default was set, the Internet largely went away; if the latter, the P3P protections became largely redundant. In practice, this issue of lack of a critical mass of P3P enabled service provider sites lead to the demise of P3P.

Another key problem, which continues to affect all self-regulatory industry schemes, was that a service provider might simply not obey the P3P preferences of the consumer, either overtly or covertly, whatever his compact privacy policy said.<sup>24</sup> Similarly in the recent “Do Not Track” controversy, many US sites which received “Do Not Track” tags from users seeking to opt out of behavioural tracking, simply ignored them, since US law did not compel them to take notice<sup>25</sup>. In contrast to “Do Not Track”, both in the US and EU, regulatory action *can* be taken where providers act in breach of their privacy policies, as misleading trade practices or breach of contract; but such action is still very rare.

Finally, in practice, P3P could only become a true marketplace or negotiation space for personal data if there was a marketplace of privacy choices for users, eg, some trading specified benefits for personal data for different considerations, some discarding personal data collected at various dates, some restricting collection of personal data to that absolutely necessary for service delivery, etc - something which has to date never happened. Effectively, as with privacy policies in general, competition has failed to deliver a market for bargaining over personal data where users have any choice other than to accept or reject the service provider entirely - something which is often implausible due to network effects, as in the social network services market. Instead a *de facto* norm of trade of unlimited amounts of personal data for “free” services has been established (although of course many services requiring payment also collect personal data as a “free gift”).

Thus in the end, P3P could only act as a system of notice for users, not as a means by which users could control the practices of service provider. Similarly, probably because of the market-driven bargaining and anti-regulatory ethos, P3P was never implemented to require a *minimum* standard of privacy

---

<sup>24</sup> Y Beres et al, “On the Importance of Accountability and Enforceability of Enterprise Privacy Languages” (2003) *W3C Workshop on the long term Future of P3P and Enterprise Privacy Languages*.

<sup>25</sup> See <http://www.forbes.com/sites/eliseackerman/2013/02/27/big-internet-companies-struggle-over-proper-response-to-consumers-do-not-track-requests/>.

protection from providers. It was never, therefore, used to indicate compliance with EC data protection (or even US “safe harbor”) standards.

#### 4.1.2 “Privacy Bird” - graphical P3P extensions

It was envisaged that P3P might be made more user-friendly by the addition of “user agent” software<sup>26</sup>. One example of such, “Privacy Bird”, was released in 2006. It was also developed by W3C<sup>27</sup> and is available as a plug-in for Microsoft’s Internet Explorer. The plug-in consists of a small bird that is added to the browser’s menu bar and changes colour (red, yellow and green) and has a speaking bubble that changes depending on the (mis-)match of the user’s privacy preferences with the website’s policy. As with P3P generally, it requires the user to define their privacy preferences so that matching can take place.



**Figure 6:** *Privacy Bird*

#### 4.2 Modern iconography approaches

The success of the CC icons (3.4 above) has inspired several similar schemes in the privacy realm. Although most schemes have been pure academic explorations with no expectation of practical implementation, the Privacy Icons Software (PIS) project at 4.4 below seems to have wider aspirations. PIS has just been launched in 2014 and seems to show a new interest in icons after an apparent subsidence in attention after the demise of P3P and lack of uptake of several academic projects<sup>28</sup>.

Recent developments at EU level also seem to indicate some renewed interest in the benefits of iconography for consumer protection in fairly simple privacy related areas. The recent implementation of new EU-wide technical standards introduced a uniform RFID label for easy identification of goods including RFID tags (see below).<sup>29</sup>

---

<sup>26</sup> See B van den Berg and S van der Hof, “What Happens to my Data? A Novel Approach to Informing Users of Data Processing Practices” (2012) 7:2 *First Monday*.

<sup>27</sup> <http://www.privacybird.org>.

<sup>28</sup> For example, the US FTC announced in 2012 its intention to move to “nutrition labels” for privacy (see below). In fact this never transpired.

<sup>29</sup> [http://europa.eu/rapid/press-release\\_IP-14-889\\_en.htm](http://europa.eu/rapid/press-release_IP-14-889_en.htm).



**Figure 7 :** *RFID Icon*

In addition, the European Parliament Committee of Civil Liberties, Justice and Home Affairs suggested amendments during the passage of the proposal of the EC Data Protection Regulation reform<sup>30</sup> to introduce standardised icon-based representations of privacy policies.<sup>31</sup> In the draft Data Protection Regulation (at time of writing not yet complete and not expected to be so till around early 2016) an article 13a(2) (“Standardised information policies”) added some while into the process does stipulate that privacy policies shall also be presented “in an aligned tabular format, using text and symbols”. The reference is clearly to an iconic presentation. The fate of this amendment is as yet not secure however.

Icons and labelling schemes are sometimes used to supplement a full, traditional privacy policy, combining the detail of the traditional policy with a more accessible version for consumers : this is sometimes called a “layered” privacy policy. Layered privacy policy approaches were popular around 2009-2010; again, they seem less prominent now, which may coincide with the apparent lack of success of self-regulation in the privacy marketplace<sup>32</sup>.

#### 4.3 *Academic projects*

Mary Rundle, as part of the identity project at London School of Economics, proposed a set of CC-like icons for the depiction of privacy policies and terms. This icon set was developed as a start for discussion and aims at (a) bridging jurisdictional requirements, (b) offering simple choices and (c) allowing multiple combinations according to context, while offering consumers clear and easy information on privacy policies.<sup>33</sup>

---

<sup>30</sup> <http://ec.europa.eu/justice/data-protection/> .

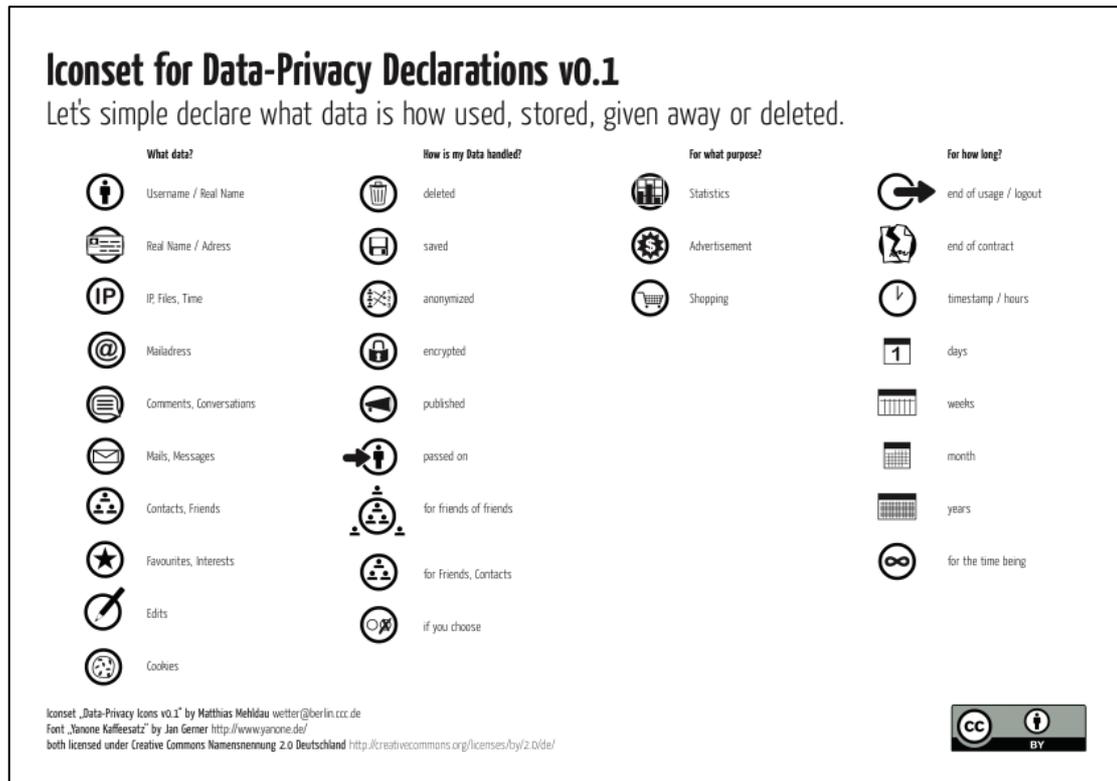
<sup>31</sup> European Parliament, Amendment 71, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARG+PE-501.927+04+DOC+PDF+V0//EN>, at p. 55.

<sup>32</sup> More commonly a layered privacy policy involved a full “legal” privacy policy; a short privacy policy accessible to non lawyers; and sometimes a machine readable version of the policy. Short policies were, again, in vogue with both the ICO and the FTC c 2009-2012. The “layered approach” is still promoted by the ICO in its current guidance on *Privacy notices code of practice (December 2010)*.

<sup>33</sup> M Rundle, “International Data Protection and Digital Identity Management Tools” presentation at *IGF 2006, Privacy Workshop I, Athens, 2006*, at <http://ssrn.com/abstract=911607> .

Matthias Meldau independently developed a set of 30 icons that aimed at answering the questions:

- “What type of data is collected?” (eg, real name, IP address, contacts/friends)
- “How is my data handled?” (eg ,deleted, saved, available to friends of friends)
- “For what purpose?” (eg statistics, advertising, shopping) , and
- “For how long?” (eg, end of session, end of contract, 6 weeks, forever).<sup>34</sup>



**Figure 8:** Iconset, M Meldau

While working at Mozilla, Aza Raskin developed a set of 4 privacy icons inspired by the CC icons. The aim of this set is, again, to simplify complex privacy policies so they can be scanned in seconds. Raskin went on to work on Privacy Icons Software, below, 4.4.

<sup>34</sup> M Meldau, “Iconset für Datenschutzerklärungen” (2007) *netzpolitik*, <https://netzpolitik.org/2007/iconset-fuer-datenschutzerklaerungen/>.

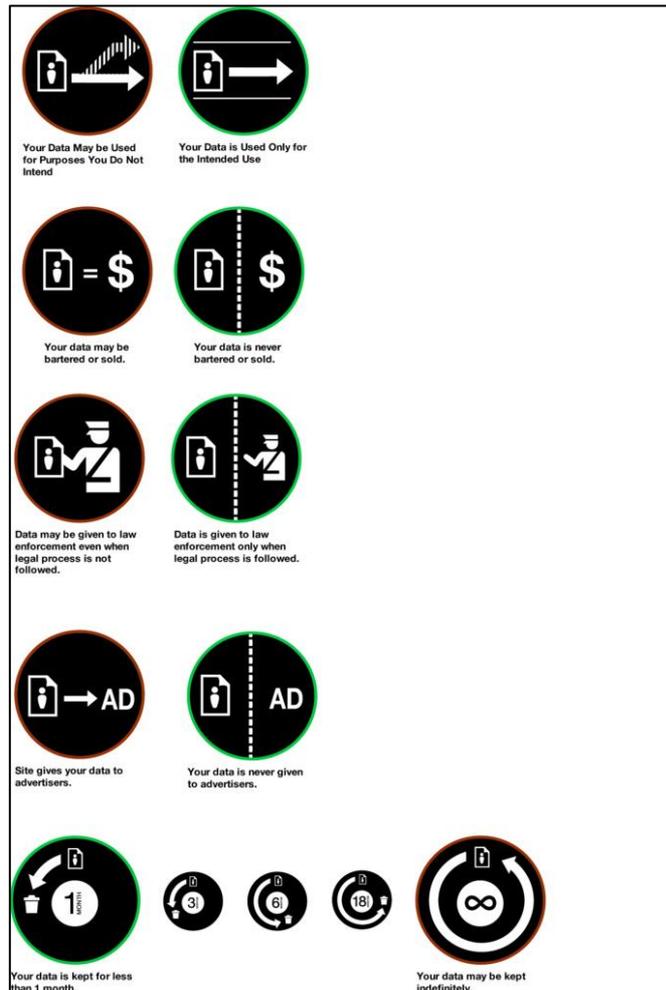


Figure 9: Iconset, A Raskin

## Prime Life

While all these projects were US based, a major EU project examining the whole question of better interfaces for privacy enhancing technologies was the *Prime Life* project, an FP7 project on privacy and identity, which ran 2008-2011. Prime Life also extended the P3P protocol, providing 3 extensions for browsers, including one which allowed the user to an easy interface to see if the site visited matched the user's privacy preferences (akin to Privacy Bird above)<sup>35</sup>.

The Prime Life set included two detailed sets of icons (one for general use, one for social networks only) which communicated privacy information in considerable detail, eg, whether or not a Web site was tracking users' behaviours, facilitating anonymisation, and whether or not the data were passed on to third parties. Even very complex issues as whether or not data were aggregated with personalized third-party information, and whether or not the

<sup>35</sup> See <http://www.w3.org/2011/D1.2.3/> and <http://primelife.ercim.eu/results/documents/> .

processing practices of the company fall under EU law or equal protection were captured in icons<sup>36</sup>.

### PrivIcons<sup>37</sup>

PrivIcons were developed by researchers from the Prime Life project, Stanford University and other researchers. The aim was to develop an iconset simply to convey preferences as to how emails should be handled by the recipient. Six icons were developed as below. Icons can be incorporated into emails and user agents can help recipients handle emails received according to the embodied preferences. PrivIcons were designed deliberately to be very simple by sticking to one small use case. “Think of it as washing tags for email privacy.”



**Figure 10:** *PrivIcons*

None of these projects have (to date) been widely implemented in practice. Hence, no empirical data on their success “in the wild” exists.

#### 4.4 Privacy Icons (PIS)

In June 2014, TRUSTe<sup>38</sup>, the well known privacy/trust seal, released together with Disconnect (a privacy-advocacy and open source software company) a set of privacy icons (Privacy Icons Software - PIS) to “help people quickly understand how websites handle their data”.<sup>39</sup> Although at an early stage, this is, it seems, intended to be a working commercial solution, not just an academic experiment. PIS is available as a desktop browser extension for Chrome and Firefox, with versions for other browsers and mobile devices to follow. PIS shows users a set of 9 icons in the browser for every site they visit, and for every search result, to inform consumers about the most important data practices of a given website. The icons indicate information about:

- Expected use of data

---

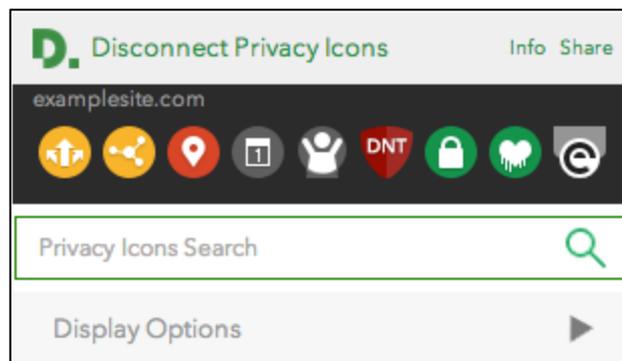
<sup>36</sup> See M. Hansen, 2009. “Putting privacy pictograms into practice: A European perspective,” GI Jahrestagung, volume 154GI, pp. 1,703–1,716. The iconset does not seem to be available on the free to air Internet as a whole; however some icons can be seen in, Leif-Erik Holtz, Harald Zwingelberg, and Marit Hanse “Privacy Policy Icons” in Camenisch, Jan, Fischer-Hübner, Simone, Rannenber, Kai (Eds.) *Privacy and Identity Management for Life* (Springer, 2011) at [http://link.springer.com/chapter/10.1007%2F978-3-642-20317-6\\_15#page-1](http://link.springer.com/chapter/10.1007%2F978-3-642-20317-6_15#page-1). There are at least 17 icons.

<sup>37</sup> See <http://www.privicons.org/>.

<sup>38</sup> <http://www.truste.com>.

<sup>39</sup> <http://www.truste.com/about-TRUSTe/press-room/news-visual-icons-introduced-help-privacy-policies>.

- Expected collection (ie who are disclosures made to , third parties et al)
- Whether precise location of user is tracked
- Data retention periods
- Children’s privacy
- Do Not Track compliance
- SSL support
- Heartbleed vulnerability
- TrustE certified



**Figure 11:** *PIS Iconset*<sup>40</sup>

However as with P3P, the icon assessments are simply derived from the service providers privacy policies, hence consumers cannot assess how far websites are really living up to the standards displayed.

#### 4.5 Labelling for privacy policies

Labelling applies the idea of labels on food packaging, or, as shown above, energy ratings, to the privacy realm.<sup>41</sup> Privacy labels, based on a design similar to nutrition labels, have been developed showing information in a grid with colours and providing simplified information.

<sup>40</sup> Full notes at <https://disconnect.me/icons> .

<sup>41</sup> M Abrams and M Crompton, “Multi-layered privacy notices: A better way,” (2005) 2 (1) Privacy Law Bulletin 1-4; G Kelley et al., “Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach” (2010) Carnegie Mellon University, CyLab, Technical Reports, CMU-CyLab-09-014, at <http://www.cylab.cmu.edu/research/techreports/2009/tr-cylab09014.html> ; P Kelley et al., “A ‘nutrition label’ for privacy,” (2009) , *Symposium On Usable Privacy and Security (SOUPS) 2009*, at <http://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf> .

information we collect	ways we use your information				information sharing	
	to provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information	dark red	opt in		dark red	opt out	
cookies	dark red			dark red		
demographic information	dark red	opt in		dark red	opt out	
financial information						
health information						
preferences	dark red					
purchasing information	dark red	opt in		dark red	opt out	
social security number & gov't ID						
your activity on this site	dark red	opt in		dark red	opt out	
your location						

Access to your information  
 This site gives you access to your contact data and some of its other data identified with you  
 How to resolve privacy-related disputes with this site  
 Please email our customer service department

bell.com  
 5000 Forbes Avenue  
 Pittsburgh, PA 15213 United States  
 Phone: 800-555-5555  
 help@bell.com

**Figure 12:** Example of Privacy Label (<http://www.openlawlab.com/2013/06/03/privacy-nutrition-labels/>)

#### 4.6 The Privacy Wheel

In 2012, Van den Berg and Van der Hof developed a graphical representation of privacy policies known as the “privacy wheel”. This project, which is thus far merely an academic thought exercise, but was informed by user group consultation, was based on the OECD Guidelines on the *Protection of privacy and transborder flows of personal data*, also known as *Fair Information Principles*.<sup>42</sup> It tries (according to the authors) to find a balance between schemes that either provide too much information at a single glance for end users (such as “nutrition labelling” for privacy) or too little (icon approaches, such as Privacy Bird).<sup>43</sup> The wheel can be placed on a website and users can click on the different spokes to receive more information on a topic (such as consent, or data quality).



<sup>42</sup> Van den Berg, and van der Hof, supra n 26.

<sup>43</sup> Ibid.

**Figure 13: Privacy Wheel**

consent		you have consented to data processing for the following purposes		change consent? check each purpose for which you wish to give or revoke consent	
purpose 1: customer identification	<input checked="" type="checkbox"/>	1 Jan 2010	<input type="checkbox"/>	enter date	
purpose 2: direct marketing (newsletter, special offers etc.)	<input checked="" type="checkbox"/>	1 Jan 2010	<input type="checkbox"/>	enter date	
purpose 3: medical treatment	<input checked="" type="checkbox"/>	15 May 2010	<input type="checkbox"/>	enter date	
purpose 4: third party research (blood group only)	<input checked="" type="checkbox"/>	30 June 2010	<input type="checkbox"/>	enter date	

submit

**Figure 14: Consent Choice and History Privacy Wheel**

The Privacy Wheel also contains tools which a consumer can use to document consents given to the service provider (see Figure 14 above).

#### 4.7 Assessment and optimisation of privacy icons and labelling

Given the low uptake “in the wild” of privacy icons, a limited amount of academic research has been done on assessing how well icons work to explain complex concepts about privacy to consumers, and how best to do this, usually based on fairly small user sample groups.

The Prime Life project (discussed above, 4.3 ) is perhaps the leading EU source on this. Holtz et al found that privacy icons should allow for quick comprehension regardless of the social and cultural background of users. Social factors, such as education and age, should not restrict their user-friendliness, and it should be possible to understand the icons within different legal frameworks.<sup>44</sup> Another paper by Holtz et al suggests that clear icons with few details are preferred over more complex and detailed ones.<sup>45</sup> Holtz’s group working on Prime Life exposed their icon sets to small different language user groups, and a larger online focus group, and found some were immediately voted as intuitive, easy to understand - “clear and helpful” said both Swedish and Chinese student focus groups – while others struggled to convey more complicated concepts such as “visible to friends of friends” on social networks. The Prime Life icon set included at least 17 icons, which was found to be unduly complex. This was partially met by splitting the icons into two sets, a “basic” set and a “specialist” set for social network users.

<sup>44</sup> L-E Holtz, K Nocun, M Hansen, “Towards Displaying Privacy Information with Icons” (2011) 352 *IFIP Advances in Information and Communication Technology* 338-348, 342.

<sup>45</sup> Holtz et al, supra n 36.

Van den Berg and van der Hof surveyed as preparatory work c 560 respondents from 3 countries to find out what information they wanted conveyed in online transactions, and *when* they wanted to be given that information, as well as demographic and personality characteristics. They did not however (yet?) trial the user-friendliness of their Privacy Wheel construct.

The PIS team in the US developed their icons via academic work, blog posts as outreach, workshops, Hack groups and engagement with W3C<sup>46</sup> as well as input from their original Mozilla-led working group that included some of the most prominent privacy organizations, like the Electronic Frontier Foundation, Center for Democracy and Technology, and W3C. The final list includes 9 icons on which variations can be made<sup>47</sup>, although the pre-commercial alpha release only apparently had 4 icons (with variations)<sup>48</sup>. This project is still in its infancy, hence no empirical data on consumer satisfaction and success has been generated so far.

The general consensus seems to be that as few icons as possible is best, but this limits the subtleties and complexities that can be conveyed. This lead Van den berg and other players such as the FTC to turn to “nutrition labelling” instead. However here the problem seems to be information overload.

In a study by Kelley in 2010, privacy “nutrition labels” were rated by users as better to understand and more enjoyable than natural language notices.<sup>49</sup> Accuracy and speed of uptake were also better. Abrams found that, ideally, privacy labels should be short, present no more than seven issues, use everyday speech, and have common graphical interfaces.<sup>50</sup>

One way to limit the complexity of an icon set (and presumably the overload of a label set) is to create iconsets or labels restricted to particular technologies or industries. This was the approach eventually taken by Prime Life, and by PrivIcons, who restricted themselves only to email privacy.

Finally persuading service providers to translate their privacy policy into icons is itself an overhead in time. Lack of critical mass among service providers is a key pitfall to avoid, and may need support by any icon-promoting scheme. PIS claim to have “over 5000” sites displaying PIS icons. It is not clear if this work is done by PIS/Disconnect, by TrustE or by the individual service providers. An early report in 2012 noted that an early workshop of lawyers tried to “iconify” 1000 privacy policies in one day and succeeded only in creating 235<sup>51</sup>.

---

<sup>46</sup> See <http://www.azarask.in/blog/post/privacy-icons/> .

<sup>47</sup> <https://disconnect.me/icons> .

<sup>48</sup> <http://www.legaltechdesign.com/privacy-icons-a-legal-communication-design/> .

<sup>49</sup> Kelley et al, supra n 42.

<sup>50</sup> Abrams et al, supra n 42.

<sup>51</sup> See [http://bits.blogs.nytimes.com/2012/11/19/building-an-iconography-for-digital-privacy/?\\_php=true&\\_type=blogs&r=1](http://bits.blogs.nytimes.com/2012/11/19/building-an-iconography-for-digital-privacy/?_php=true&_type=blogs&r=1) .

## 5. Summary

Icons and labels have both been explored in some depth in both the US and EU as means to communicate privacy policies written in “legalese” more effectively to lay users. Most schemes have explicitly been academic exercises, or if commercial are very recent and so far unproven. Empirical research assessing their success “in the wild” is thus extremely limited but what there is seems to show that end-user understanding of privacy policies can be improved by such initiatives.

The offline literature highlights that a standardised graphical approach implemented across multiple state jurisdictions works best for consumer recognition and uptake. In addition, attempts at standardising consumer information may be improved by government mandate or co-sponsorship, as in the EU Energy example. Other ways of securing such standardisation and international harmonisation may however be to work with standards bodies such as the W3C, browser writers such as Mozilla, Safari (Apple), Chrome (Google) etc; or to look for support from ISO standards (cf laundry symbols<sup>52</sup>).

However while there is clear empirical evidence that some offline implementations of icons/labels, in non-privacy contexts such as energy and nutrition labelling, have, at least to some extent, successfully promoted consumer literacy and social/environmental goals, in the privacy domain, there are a number of difficult issues to be resolved.

### 5.1 *Detail versus accessibility*

Van den Berg and Van der Hof note that the use of icons to depict privacy policies, involving “capturing complex, detailed material such as data protection legislation in one single image, or a (relatively) limited set of images is incredibly difficult”. They cite the Prime Life icon set (above) as involving “rather complicated drawings” with “several, rather small elements”. The “tracking” icon was particularly difficult. Hansen similarly notes that the attempt to convey such specified, detailed information becomes too complex to understand at a single glance.

“Nutrition labelling” provides more information than icons, but suffers from the opposite problem, that too much information is provided all at once for the user to absorb. Value judgments (eg “unexpected uses”) have to be made in ways very different from traditional “nutrition labelling” of unambiguous facts, such as number of calories. The simpler the icon – eg Privacy Bird, RFID icon – the less nuanced information is conveyed.

It turns out there may be reasons why traditional privacy policies have become so long. The solution used by PrivIcons and Prime Life – to concentrate on one particular sector of industry , or technology – however seems helpful.

---

<sup>52</sup> See above, 3.3.

Furthermore PIS emphasise that their icons are intended to be “bolt ons” to the “real” legally-complete, textual privacy policy<sup>53</sup>. They merely highlight key points and are not meant to be complete. This raises the issue however that the picture a user gains from the “icon” privacy policy may be very different from the one given by the entire written, legal policy<sup>54</sup> – and of possible consumer complaints and legal disputes. Raskin describes this as the “bad icons” problem.

## 5.2 *Information about site policies, or information about legal compliance ?*

Most the projects described above were created in the USA where no mandatory omnibus privacy protection laws akin to EU DP laws existed (or indeed, exist now.) Perhaps because of this, the projects were universally conceived as “neutrally” translating privacy policies, not making legal assessments. As a result, these projects do not indicate if a site is compliant with the law (of whatever jurisdiction); merely (at best) that it is, or is not, compliant with the user’s specified requirements in the area (the P3P paradigm). For an EU implementation, it would seem useful to indicate if a site does or does not comply with basic data protection guarantees eg a traffic light implementation. No work on this seems yet to have been done.

## 5.3 *Jurisdictional issues*

A key problem with icon or label schemes will be their international scope. Consumers buy digital products and services globally not locally; while an icon /labelling system might be developed only for use by UK service providers and aimed at UK consumers only , its usefulness might then be limited to industry sectors strongly tied to national borders (eg energy suppliers). Given differences in privacy laws, especially between the EU and the US, but also between the UK and many other EU states, and the disparity of laws throughout Asia, a system that tried to label compliance, or even “factual” privacy features, might be very difficult to build on an international scale.

Creative Commons points to the possibility of an international icon scheme but it relies heavily both on the high level of international harmonisation of copyright law by international treaty , and on volunteer effort for local “porting” of the CC suite to locally tailored licenses. Privacy is decidedly not harmonised at international level; however there might be a possibility as per van den Berg and van der Hof<sup>55</sup> to use the OECD principles, as global guidelines, to develop a basic international icon/labelling system.

## 5.4 *Would labelling or icons showing more than legal compliance promote greater or higher-priced uptake by consumers?*

---

<sup>53</sup> See <http://www.azarask.in/blog/post/is-a-creative-commons-for-privacy-possible/>.

<sup>54</sup> Holtz et al, supra n 36 at 285.

<sup>55</sup> Ibid.

It remains another largely unanswered question if users are willing to pay for more privacy than the mere basics of legal compliance. Some work has been done by privacy economists but mainly in the US, or in the EU but with little conception of legal difference. A study by Egelman et al. at Carnegie Mellon in the US showed that if presented with a choice, consumers will pay for increased privacy when they see privacy indicators.<sup>56</sup> In another study, it was found that consumers opt for the least expensive website if no privacy icons are shown. However, where privacy icons were present, a significant number of participants paid extra to buy the items at a more privacy-protective site.<sup>57</sup> However, timing is crucial because consumers will be particularly willing to pay more if privacy indicators are shown alongside search results and before the consumer has chosen a website.<sup>58</sup>

### 5.5 *General issues to be highlighted: competition, critical mass, audit*

As noted above, almost universally icon or label schemes have merely tried to translate privacy policies. Thus, they share the same basic problem as privacy policies: does giving users clearer notice really empower the user any more? The problems of user failure to pay attention to privacy policies may not go away simply by making policies more readable, if a non-competitive market does not differentiate by privacy as a selling point of value. In comparison, energy appliance labelling has been a success, because many thousands of very different white goods are on sale and the user can then make a meaningful choice based on energy rating as well as price and other factors. If more competition develops as to terms re personal data collection (within the UK or internationally) or in particular market sectors (say - smart energy delivery; mobile fitness apps), then icons and labels will become correspondingly more useful.

Icons and labels need universal recognition from consumers, and a critical mass of acceptance from service providers, to become successes. The lesson of P3P and most the schemes surveyed above is that these are both very difficult to obtain without adequate incentives. One incentive is, of course, for the law to demand – by legislation or some kind of co-regulatory strategy - that industry engage with such schemes. However, law is not the only incentive and the success of laundry labels in the international mass market shows clear industry and consumer incentives to partake in such schemes without legal compulsion. ISO or BSI standards are another approach. Another strategy for consumer uptake and enhancing choice would be to encourage the development of comparison sites to assess similar websites on their privacy policies, cf “switching” price comparison engines.

Finally the history of privacy policies and trust seals in the US shows that schemes representing privacy guarantees need policed. TRustE failed to adequately sanction several privacy breaches by its members in the dot.com era

---

<sup>56</sup> S Egelman et al., “Timing Is Everything? The Effects of Timing and Placement of Online Privacy Indicators” (2009) *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 319-328, 322.

<sup>57</sup> Cranor, *supra* n 15, at 292.

<sup>58</sup> *Ibid*, at 293; Egelman, note 36, at.

leading to considerable loss of credibility. An icon or labelling scheme need not guarantee legal compliance by its members – that is the job of the privacy regulator - but it still arguably needs audit to make sure what its participants represent in their icons is accurate. Such audit could be supplied by working in hand (in the UK ) with the Information Commissioner or , arguably, by providing an independent auditor or ombudsman. It would need to be considered what sanctions if any were needed for failing to implement an icon representation accurately (or more likely, perhaps, failing to maintain it after changes to the policy).

## II. Standard Contract Templates for Customers Facing Digital Services

### 1. Introduction

In online environments, consumers interact with a variety of digital services. Users have to make decisions about the level of trust they put into these services, and the amount of data they entrust the service with. This is particularly crucial, as data processing by, and exporting to, third parties becomes increasingly common.

Standard terms contracts are an inevitable part of everyday transactions between consumers and businesses. They contain terms, which are not negotiated, but imposed as a whole by one party (the business party) on the other party (the consumer). The significant imbalance of power and information tends to lead to unfair terms being imposed on the weaker party. To protect consumers from such unfair terms, the EU enacted the *Unfair Terms in Consumer Contracts Directive* 93/13/EC in 1993.<sup>59</sup> The 1999 *Unfair Terms in Consumer Contracts Regulations* have implemented this Directive into UK law. Unfair terms can be challenged in court by a regulator, in the UK, the Office of Fair Trading (OFT); this makes up for the fact that UK (and EU) consumers rarely go to court to assert their rights.

The notion that freedom of contract is subject to legal constraint to protect consumers from unfairness is therefore well established in the EU and UK.<sup>60</sup> The US, by contrast, has no omnibus Federal legislation regulating standard terms contracts and businesses are generally free to impose contract terms on consumers without legal constraint. Some US states do allow challenge to consumer contract terms on common law grounds of “unconscionability” but these challenges are rare. In general, in all countries, B2C contracts are often written knowing they might not survive challenge in court, but expecting such challenge to be unusual.

The notion of “regulated contracts” is that certain terms have to be written into contracts, or sometimes, are not allowed in contracts. Such occasions are rare but seen as appropriate in some industries or circumstances to protect the vulnerable. One well known example is the UK Sale of Goods legislation which mandates for example that certain guarantees of fitness of purpose and quality must be read into any sale to a consumer. Similarly some terms in employment contracts are illegal eg terms breaching minimum hours or minimum wage protection.

---

<sup>59</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31993L0013:EN:HTML>.

<sup>60</sup> Freedom of contract can be defined as “the freedom of the parties to the contract to bargain and create the terms of their agreement as they desire without interference from government”: see *Legal Information Institute*, [http://www.law.cornell.edu/wex/freedom\\_of\\_contract](http://www.law.cornell.edu/wex/freedom_of_contract).

Such regulation has not generally been applied to privacy policies. In the EU, terms relating to personal data collection should reflect the guarantees of the data protection legislation – but as consent is a ground for fair and lawful processing, it is very easy to put any data protection practice into a contract (privacy policy) and have it legitimised by acceptance thereof (which in digital services, as we have seen, is very often a rather routinised and automatic consent.) In the US, similarly, the FTC audits companies to see if their practices match their privacy policies; but it does not regulate what goes into those policies. Challenges to privacy policies as unfair terms are clearly possible, and have been mounted in some Continental countries eg against iTunes and FB – but no such challenge has been yet mounted with any publicity in the UK.

Thus in the privacy domain, the idea of a “regulated contract” is akin to the idea of a regulated privacy policy. As we have seen, representing privacy policies as icons merely gives consumers greater or clearer *notice* – it does not give them more *control*. Regulating privacy policies on the other hand – whether by law or by “soft law” industry agreement – can provide minimum guarantees of privacy protection and can therefore, arguably, engender greater trust from consumers in the market. Ideally regulated privacy policies would also be represented by clear multi-layered notices which might combine full legal details, plain English short notices and iconic representations.

Such regulated policies might be omnibus, or more likely, sectoral. So, for example, a regulated privacy policy for the social network services sector might require no data to be collected concerning under 13s; might demand that data collected was not retained beyond certain time limits; might demand that data was not disclosed to certain third parties (eg employers, certain advertisers); was not used for certain uses (eg behavioural profiling relating to sensitive data around health, alcohol, anorexia etc).

The nearest to such a concept of a regulated privacy policy is probably the short privacy notice mandated for some financial institutions in the US by the Gramm–Leach–Bliley Act (GLB) of 1999. This Act provides a template form for the required short privacy notice<sup>61</sup>. While not exceptional by EU standards, it does at least show a short privacy policy model can be drafted for certain sectors.

In a number of areas, the EU is currently exploring initiatives to develop standardised or template contracts in the privacy and digital arenas, intended to create fairer contracts, protect minimum consumer rights and/or instil trust and confidence in consumers. We discuss these below.

## **2. EU Data Export Clauses**

Increasingly, businesses share customer data with third parties when outsourcing business functions. In addition, businesses increasingly operate on an international basis. This is particularly true with the rise of cloud computing.

---

<sup>61</sup> See [http://www.ftc.gov/system/files/documents/rules/privacy-consumer-financial-information-financial-privacy-rule/privacymodelform\\_optout.pdf](http://www.ftc.gov/system/files/documents/rules/privacy-consumer-financial-information-financial-privacy-rule/privacymodelform_optout.pdf).

This means that personal data of customers is often processed outside of the UK, and even the EU.

To ensure that personal data is adequately protected during such transactions, the European Commission has published model contractual clauses based on the EU Data Protection Directive (DPD).<sup>62</sup> Article 26 (2) DPD requires member states to “provide adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights”.<sup>63</sup> This means that personal data may only be exported outside of the European Economic Area (EEA) if it is as well protected there, as it is within the EU.

Companies processing personal data of individuals therefore must include these model clauses in contracts with companies outside the EEA that process data on their behalf, unless they pass an adequacy test taking one of the other routes.<sup>64</sup> These clauses thus are intended to safeguard the data protection rights of EU consumers.

The Commission has so far published two sets of contractual clauses with the latest version published in 2010.<sup>65</sup> One set governs controller-to-controller transfers and the other controller-to-processor transfers<sup>66</sup>. The Decision 2010/87/EU updated the latter set of clauses to include sub-processors. In essence, these model contractual clauses oblige all parties involved in the transfer and processing of personal data to comply with the data protection standards set out by the DPD.

Both data exporter and importer must accept liability to data subjects for breach of those standards (Article 6 Decision). Enforcement of standards in outsourced transactions however remains an issue.

### 3. Model Service Contracts for EU Cloud Computing Suppliers

Cloud computing services often operate with complex standard contract terms or service level agreements with extensive disclaimers.<sup>67</sup> A major study in 2011 found these standard terms to be significantly weighted in favour of the provider, and many to be potentially non-compliant with unfair terms or other

---

<sup>62</sup> [http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index\\_en.htm](http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm) .

<sup>63</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> .

<sup>64</sup> See for other assessment means: ICO, “Assessing Adequacy - International Data Transfers, [http://ico.org.uk/for\\_organisations/data\\_protection/the\\_guide/~media/documents/library/Data\\_Protection/Detailed\\_specialist\\_guides/assessing\\_adequacy\\_international\\_data\\_transfers.ashx](http://ico.org.uk/for_organisations/data_protection/the_guide/~media/documents/library/Data_Protection/Detailed_specialist_guides/assessing_adequacy_international_data_transfers.ashx)

<sup>65</sup> <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF> .

<sup>66</sup> “Data controller” and “data processor” are terms of art in DP law. Roughly, the controller is the company which decides how, why and what data shall be processed; and the processor is any agent who does the actual data crunching for the controller. The cloud has unhelpfully muddied this distinction.

<sup>67</sup> EC, “Unleashing the Potential of Cloud Computing in Europe” (2012), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF>, 11.

EU laws.<sup>68</sup> Such contracts often, for example, disclaim all liability for security breach, data confidentiality or service continuity.<sup>69</sup> This leads, arguably, to consumer insecurity and hesitant use of cloud computing infrastructures.

Accordingly the EC established an expert group on cloud computing contracts to assist the Commission in identifying safe and fair contract terms and conditions for cloud computing services for consumers and small companies.<sup>70</sup> The first results, as of June 2014, are guidelines on governance of Cloud Service Level Agreements (Cloud SLAs) developed by the industry working group.<sup>71</sup>

The guidelines include a glossary of uniform principles and terms designed to allow customers to evaluate and compare cloud SLAs more effectively. They also define SLA standards for cloud computing, performance service level objectives, security service level objectives, data management service level objectives and personal data protection service level objectives.

Interestingly, the EC has signalled that to instil consumer trust, the EC cannot set standards alone. They are currently investigating how to standardise SLAs at an international level, e.g. through international standards, such as ISO/IEC 19086.<sup>72</sup>

#### **4. Licenses for Europe**

The “Licenses for Europe” initiative of the European Commission, launched in 2012 is another example of attempting to develop general clauses and agreements for consumer rights in a digital space within the EU. It aims at creating a single market for Intellectual Property Rights (IPR) in Europe and making more digital content available through practical industry-led solutions.<sup>73</sup> One particular aim was to enable cross-border access to creative works and portability of services within the EU.

To achieve such harmonisation, one of the aims was to create multi-territorial copyright licenses.<sup>74</sup> While the substantive scope of copyright has been largely harmonised, rights are still largely licensed on a national basis. In a digital single market, this is an enormous hurdle to efficient copyright licensing and revenue distribution.

---

<sup>68</sup> S Bradshaw, C Millard, I Walden, “Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Services” (2011) 19 (3) *International Journal of Law and Information Technology* 187.

<sup>69</sup> Article 29 Working Party, *Opinion on Cloud Computing*, [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf).

<sup>70</sup> [http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index\\_en.htm](http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm).

<sup>71</sup> <http://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines>.

<sup>72</sup> *Ibid.*

<sup>73</sup> European Commission, “A Single Market for Intellectual Property Rights Boosting Creativity and Innovation to Provide Economic Growth, High Quality Jobs and First Class Products and Services in Europe” (2011)

[http://ec.europa.eu/internal\\_market/copyright/docs/ipr\\_strategy/COM\\_2011\\_287\\_en.pdf](http://ec.europa.eu/internal_market/copyright/docs/ipr_strategy/COM_2011_287_en.pdf).

<sup>74</sup> [http://europa.eu/rapid/press-release\\_IP-11-630\\_en.htm?locale=en](http://europa.eu/rapid/press-release_IP-11-630_en.htm?locale=en).

The initiative ended in 2013 as a failure: the end result was no more than a set of pledges setting out broad principles or points of interest for future debate.<sup>75</sup> The participants failed to agree on more specific agreements and solutions for a copyright reform in the digital single market.

Crucially, the Licenses initiative fell apart because, while set up very firmly to be a multi-stakeholder endeavour, it was seen as dominated by large industry interests to the detriment of stakeholders representing the research sector, SMEs and open access publishers. Accordingly they withdrew from the project in its early stages as they felt the focus was purely on increasing commercial exploitation, ignoring aspects such as wider access to science, culture dissemination and the efficient use of public funds.<sup>76</sup>

## 5. Summary

Standard contracts or clauses can be an effective means to ensure that consumers are sufficiently protected against industry standard terms or service level agreements that are unfair and/or significantly weighted in favour of the provider. In this domain, standard contracts can be seen as “regulated privacy policies”.

Standard terms and contracts are already widely used to implement data protection guarantees into contracts where there is export of personal data outside the EU. While only one strategy to achieve legal compliance in this area, they are by far the most popular industry choice. Standardised privacy policies have also been partly introduced in the US in the area of financial services.

Both these strategies were initiated by government intervention (mandatory law). However it is also possible that industry “soft law” could create such regulated privacy policies for industry sectors, with sufficient incentives.

However, standardisation of contracts and terms, in the context of global data flows, probably has the greatest impact if it is harmonised at international level. This again might be done by law (international treaty), by industry groups, or by standard setting bodies such as ISO.

---

<sup>75</sup> [http://europa.eu/rapid/press-release MEMO-13-986\\_en.htm?locale=en](http://europa.eu/rapid/press-release_MEMO-13-986_en.htm?locale=en) .

<sup>76</sup> See letter of withdrawal:

[http://www.eblida.org/News/Letter\\_of\\_withdrawalL4E\\_TDM\\_May%2024.pdf](http://www.eblida.org/News/Letter_of_withdrawalL4E_TDM_May%2024.pdf) .



RCUK Centre for Copyright and  
New Business Models in the  
Creative Economy

College of Social Sciences / School of Law  
University of Glasgow  
10 The Square  
Glasgow G12 8QQ  
Web: [www.create.ac.uk](http://www.create.ac.uk)

