Appendix H: Shepherd and Wedderburn LLP comparative industries and regulations research

Nominet commissioned law firm Shepherd and Wedderburn LLP to undertake an examination of the practices and disclosure requirements in comparative sectors including Royal Mail PO Boxes, the Electoral Roll and telephone directory services and assess the legal and regulatory drivers for disclosure. We also requested an examination of the existing legislative provisions covering disclosure and e-commerce including the E-Commerce (EC Directive) Regulations 2000, the Companies (Trading Disclosures) Regulations 2008 and the provision of Services Regulations 2009 to provide clarity regarding the information that registrants are required to disclose in order to comply with existing regulation and whether those requirements are materially different to the information disclosed on the .uk WHOIS. We also requested an assessment of whether the definitions set out in the above regulations could be applied to Nominet's definition of "trading" for the .uk WHOIS opt-out eligibility criteria.

Their regulatory assessment of Nominet as a data processor of personal information supplied by registrants under the contract of registration and Nominet's disclosure of that data on the .uk WHOIS (subject to that data not being opted-out) concluded that Nominet is currently compliant with the Data Protection Act.

Additionally Nominet requested a review of the forthcoming reform of the EU data protection framework (set out in Annex 1 of Appendix H) particularly in relation to obtaining specific consent to process data separately from contractual consent. This was in order to ensure that we can, as far as possible, develop a policy that is fit for the future and takes into consideration legal and regulatory developments.

Following assessment of the specific areas set out above Shepherd and Wedderburn LLP proposed six potential policy options which were developed within the narrowly defined scope of the research brief relating to the WHOIS opt-out. These options provided useful input and background to inform our own development of options for consideration internally and for consultation with our stakeholders that could also be assessed against our strategic objectives, public purpose commitment and potential impact on stakeholders.

Research highlighted the importance of balance in relation to the public policy concerns regarding reliability, accessibility and privacy of data. The full report is set out below:

SHEPHERD+ WEDDERBURN

WHOIS opt-out

Different policy options

11 September 2014

Shepherd and Wedderburn LLP
Condor House
10 St. Paul's Churchyard
London
EC4M 8AL
DX 98945 Cheapside 2
T: +44 (0)20 7429 4900
F: +44 (0)20 7329 5939
www.shepwedd.co.uk

EXECUTIVE SUMMARY

1. Overview

1.1 Nominet is currently reviewing its policy on the use and supply of privacy services. As part of that review, Nominet wishes to consider how its current policy on the WHOIS opt-out impacts the views and expectations of stakeholders in relation to domain privacy.

1.2 You have asked us to:

1.2.1 review the WHOIS opt-out clause and consider whether continuing to restrict the WHOIS opt-out to "consumers" still fulfils the purpose and needs of different stakeholders;

1.2.2 assess whether the personal information supplied by registrants to Nominet under the contract of registration between Nominet and a registrant (**Contract of Registration**) creates any risks under the Data Protection Act 1998 (**DPA**);

1.2.3 identify the information disclosure requirements domain holders face under existing legislative or regulatory provisions. We have reviewed the E-Commerce (EC Directive) Regulations 2002 (**E-Commerce Regulations**), the Companies (Trading Disclosures) Regulations 2008 (**Disclosure Regulations**) and the Provision of Services Regulations 2009 (**POS Regulations**);

1.2.4 review the way privacy and information disclosure is treated in other industries. We have reviewed the information disclosure rules for PO Boxes, the electoral register and telephone directories; and

1.2.5 identify different policy options.

2. Policy options

2.1 In our analysis, we considered **six** different policy options, including:

2.1.1 retaining the current definition of "consumer" in the Contract of Registration as the criteria for whether a registrant can opt-out of the WHOIS;

2.1.2 adapting the opt-out clause to adopt the eligibility criteria used in the E-Commerce Regulations;

2.1.3 expanding the opt-out clause to all types of registrants;

2.1.4 amending the registrar agreement for .uk between Nominet and registrars (**Registrar Agreement**) to require that:

(i) all registrars must register a domain in the name of their customer; and

(ii) a registrar may elect to provide its details instead of the details of its customer for the purpose of data that is to be published by Nominet on the WHOIS;

2.1.5 expanding the opt-out to include a mechanism by which "sensitive" non-consumers can apply to Nominet to opt-out of the WHOIS; and

2.1.6 introducing a CAPTCHA which allows a person accessing the WHOIS to securely contact a registrant, while not disclosing any personal information about the registrant in the process.

2.2 The benefits and risks of the six policy approaches are considered in detail in paragraph 19.

CONTEXT

3. WHOIS opt-out

3.1 Nominet's terms and conditions of domain name registration require all registrants to provide Nominet with accurate and up-to-date details. Under clause 4.1 of the Contract of Registration, a registrant must notify Nominet of its correct name, postal address and any phone, fax or e-mail information (and information of any agent or representative appointed under clause 5).

3.2 Under clause 11.2 of the Contract of Registration, Nominet is entitled to publish the information supplied by a registrant under clause 4.1 on the WHOIS, which enables anyone to look up any .uk domain for free and identify any relevant information stored on the WHOIS. Under clause 11.2, Nominet is only entitled to publish a registrant's name and postal address (but not phone, fax or e-mail information).

3.3 Nominet enables certain registrants to "opt-out" from having their postal address displayed on the WHOIS. Currently, only registrants that are "consumers" can opt-out from having their postal address published on the WHOIS. Clause 1 of the Contract of Registration defines a "consumer" as "an individual not registering, using or planning to use the domain name as part of a business, trade or profession".

4. Nominet's review of privacy services

4.1 Nominet is currently reviewing its policy on the use and supply of privacy services. Broadly speaking, privacy services are used to conceal a registrant's name and postal address from being shown on the WHOIS by replacing that information with generic information about a registrar or third party privacy service (**Privacy Service**). In effect, the Privacy Service will be recorded on the WHOIS as the registrant, instead of the actual domain holder. As part of that review, Nominet wishes to consider how its current policy on the WHOIS opt-out impacts the views and expectations of stakeholders in relation to domain privacy.

4.2 Rather than providing Nominet with information about the domain holder, Privacy Services generally use their own company details to complete the registration. As a result, Nominet (and any individuals using the WHOIS to look-up a .uk domain) are unable to identify the actual individual or business which holds the domain. We summarise the impact of this in paragraph 19.

4.3 Nominet first introduced the expanded WHOIS service in 2002, following policy development and dialogue with the Information Commissioner's Office (**ICO**). To address concerns the ICO had about disclosing the home or postal addresses of individually identifiable registrants, Nominet introduced an opt-out mechanism for "consumers". We also note that ICANN is currently reviewing its WHOIS policy to "assess the extent to which the WHOIS policy is effective and its implementation meets the legitimate needs of law enforcement and promotes consumer trust".[1] Full details of the review are available here.

5. Purpose of the WHOIS

5.1 The WHOIS has a range of functions for both Nominet and third parties.

5.2 On its website, Nominet provides non-exhaustive guidance on the "proper purpose" of the WHOIS. Nominet states that the WHOIS is intended to:[2]

5.2.1 identify whether or not the domain name is registered;

5.2.2 identify the person or host responsible for a domain name (e.g. to confirm that this matches the apparent provider of a website, email or other service related to the domain name);

5.2.3 allow registrants of .uk domain names to see information about their domain name;

5.2.4 show publicly if a domain name is in a special status; and

5.2.5 locate and contact the registrant and/or host of the domain name in relation to the prevention or detection of systems use, or to establish or defend legal rights.

CONTRACTUAL MATRIX

6. Contract of registration

6.1 The contract of registration between Nominet and a registrant provides the contractual basis for registrants opting-out of the WHOIS database.

6.2 Specifically, clause 11.2 states that:

[1] https://www.icann.org/resources/pages/whois-2012-02-25-en

[2] http://www.nominet.org.uk/uk-domain-names/about-domain-names/domain-lookup-whois/contract-terms

"[Nominet] will make your personal data available in the following ways, but not release it for any other purpose to any other person. [Nominet] may: [...] include it on the WHOIS (which is also available outside the EEA) and PRSS. For these purposes we will publish your name and (unless you are a consumer and choose to opt out) your address, but not your phone or fax number or e-mail address".

6.3 Clause 1 defines a consumer as "an individual not registering, using or planning to use the domain name as part of a business, trade or profession." There are two limbs to the test for whether a registrant is a consumer:

6.3.1 first, the registrant must be an individual; **and**

6.3.2 secondly, the registrant must not use (or plan to use) the domain name as part of a business, trade or profession.

7. .UK Registrar Agreement

7.1 The Registrar Agreement states that a registrar must register a domain name in the name of its customer, unless the customer explicitly consents to register the domain name in an alternative name (such as the registrar's name).

7.2 Specifically, clause B.1.8 states that:

"Regardless of Tag Classification, as a Tag user, you must [...] only register a domain name in the name of Your Customer unless you or your Reseller have Your Customer's explicit prior consent to register it in a different name, such as your name, your organisation's name or your Reseller's name".

8. Registration terms of sample Privacy Service

8.1 We have reviewed the WHOIS privacy terms and conditions of a sample Privacy Service, (**Sample Privacy Service**).

8.2 The terms and conditions of the Sample Privacy Service state that:

"Subscribers to the WHOIS Privacy Service who activate the service have elected to remove the following information on the publicly available WHOIS Registry:

- *Registrant and Contacts name(s);*
- *Postal address and assigned email address and telephone number on behalf of the Registrant and the Contact(s)."*

8.3 In addition, the terms and conditions state that:

"Subscribers to the WHOIS Privacy Service who activate the service have elected to display the following information on the publicly available WHOIS Registry:

- *The primary and secondary nameservers shall be those [of the Sample Privacy Service];*
- *The original date of registration and the expiration of each domain name;*
- *Registry Domain ID;*
- *Registrar Abuse Contact Email;*
- *Domain Status;*
- *Registry Registrant ID;*
- *Registry Admin ID;*
- *Registry Tech ID;*
- *DNSSEC;*
- *Last update of WHOIS database."*

9. Interaction of contractual terms

9.1 Taken together, the interaction of the three contracts means that:

9.1.1 a “consumer” (i.e. a person who satisfies the two limb test described in paragraph 6.3) may elect to opt-out of having their postal address displayed on the WHOIS database;

9.1.2 a person who does not satisfy the “consumer” test is unable to elect to opt-out of the WHOIS database. That person’s postal address will be displayed by Nominet on the WHOIS database;

9.1.3 a registrar must register a domain name in the name of its customer, unless the customer explicitly consents to the domain name being registered in a different name; and

9.1.4 a customer (including both consumers and non-consumers) that purchases privacy services from a Privacy Service is likely to explicitly consent to having their domain name registered in the name of the Privacy Service, rather than their own.

INFORMATION DISCLOSURE REQUIREMENTS ON DOMAIN HOLDERS

10. Overview

10.1 In this section, we provide a summary of information disclosure requirements that may already apply to individuals or entities that hold websites or domains. The three relevant regulations are the:

10.1.1 Electronic Commerce (EC Directive) Regulations 2002;

10.1.2 Companies (Trading Disclosure) Regulations 2008; and

10.1.3 Provision of Services Regulations 2009.

11. Electronic Commerce (EC Directive) Regulations 2002

Overview

11.1 The E-Commerce Regulations implement the E-Commerce Directive (2000/31/EC). Regulation 6(1) of the E-Commerce Regulations establishes a number of information disclosure obligations on a person providing an “information society service”.

Key definitions

11.2 **Information society services:** Services provided for remuneration, at a distance, by electronic means and at the request of the end-user. This definition includes the selling or advertising of goods or services online; video-on-demand services; and services consisting of the transmission, hosting or provision of access to a communication network.

11.3 **Service provider:** Any person providing an information society service.

11.4 **Enforcement authority:** Any person authorised to take enforcement action (but does not include the courts).

Information that must be disclosed

11.5 Under regulation 6(1) of the E-Commerce Regulations, a person providing an information society service must provide the following information to the recipient of the service and any relevant enforcement authority, in a “form and manner which is easily, directly and permanently accessible”:

11.5.1 the name of the service provider;

11.5.2 the geographic address at which the service provider is established;

11.5.3 the contact details of the service provider (including an e-mail address);

11.5.4 if the service provider is a corporate entity, its company registration number;

11.5.5 where the provision of the service is subject to an authorisation scheme, details of the relevant supervisory authority; and

11.5.6 if the service provider undertakes an activity that is subject to VAT, its VAT registration number.

Comparison with the WHOIS opt-out

11.6 The disclosure requirements apply to any person that provides an information society service, which is defined as a service which is provided for remuneration, electronically, upon request.

11.7 This differs from the WHOIS opt-out because:

11.7.1 it applies to any "person" (which includes both individuals and entities); and

11.7.2 the service only needs to be supplied for a remunerative purpose, which is broader than using a domain as part of a business, trade or profession. We consider that the E-Commerce Regulations will apply to individual bloggers who incorporate paid advertising on their blog, whereas the same bloggers are unlikely to be considered "consumers" under the Contract of Registration.

12. Companies (Trading Disclosures) Regulations 2008

Overview

12.1 The Disclosure Regulations, which were made under section 82 of the Companies Act 2006 (**Companies Act**), create a number of disclosure obligations for companies on their websites.

Key definitions

12.2 **Website:** Under regulation 1(1) of the Disclosure Regulations, a reference to a company's website includes a reference to any part of a website relating to that company which that company has caused or authorised to appear.

Information that must be disclosed

12.3 A company must include the following information on its website:

12.3.1 the company's registered name (regulation 6(2));

12.3.2 the part of the United Kingdom in which the company is registered (regulation 7(2)(a));

12.3.3 the company's registered number (regulation 7(2)(b));

12.3.4 the address of the company's registered office (regulation 7(2)(c));

12.3.5 where a limited company is exempt from the obligation to use the word "limited" as part of its registered name under section 60 of the Companies Act, the fact that it is a limited company (regulation 7(2)(d));

12.3.6 where a community interest is not a public company, the fact that it is a limited company (regulation 7(2)(e)); and

12.3.7 in the case of an investment company, the fact that it is such a company (regulation 7(2)(f)).

Comparison with the WHOIS opt-out

12.4 The disclosure regulations only apply to companies incorporated in the United Kingdom. These companies will not be able to utilise the WHOIS opt-out as they will not satisfy the definition of "consumer".

13. Provision of Services Regulations 2009

Overview

13.1 The Provision of Services Regulations 2009 (**POS Regulations**) implement the Services Directive (2006/123/EC). Under Part 2 of the POS Regulations, all "service providers" operating in the UK must comply with a number of information provision requirements.

13.2 According to the Department for Business Innovation & Skills, the aim of these requirements is to:[3]

"[...] ensure that service recipients have access to a minimum amount of information and to a complaints procedure. This should enable recipients to make more informed decisions when considering whether to buy services from a particular provider and should widen the choice of providers available to them."

Relationship with the E-Commerce Regulations and the Disclosure Regulations

13.3 The obligations in the POS Regulations overlap with certain information disclosure obligations in the E-Commerce Regulations and the Disclosure Regulations.

13.4 Under regulation 6 of the POS Regulations, the obligations in the POS Regulations do not apply if, or to the extent that, a service provider cannot comply both with that obligation and with a requirement applying to the provision of services in existing legislation. In practice, this is not likely to cause any issues for businesses as many of the information requirements overlap.

Key definitions

13.5 **Service provider:** A service provider is an individual **or** organisation providing a relevant service for which they normally charge (regulation 4).

13.6 **Services:** Services are defined as any economic activity which is normally provided for remuneration and which is not an excluded service (regulation 2(1)). The provision of online retail services is not an excluded service.

Information that must be disclosed

13.7 A service provider must make the following information available to all customers (among others):

- 13.7.1 contact details (regulation 7);
- 13.7.2 formal name and legal status (regulation 8(1)(a) and (b));
- 13.7.3 geographic address of where the business is established (regulation 8(1)(c));
- 13.7.4 contact details for rapid and direct communication (e.g. e-mail address) (regulation 8(1)(c));
- 13.7.5 if the service provider is registered in a trade register, the name of the register and the service provider's registration number (regulation 8(1)(d));
- 13.7.6 if the service is subject to an authorisation in the UK, details of the relevant competed authority;
- 13.7.7 where the service provider is registered for VAT, the VAT number (regulation 8(1)(g));
- 13.7.8 general terms and conditions, if any (regulation 8(1)(i));
- 13.7.9 the existence of any after-sales guarantee in addition to that which is legally required (regulation 8(1)(k));
- 13.7.10 the price of the service (if pre-determined) (regulation 8(1)(l));
- 13.7.11 the main features of the service (regulation 8(1)(m)); and
- 13.7.12 details of any professional indemnity insurance or guarantee (if relevant) (regulation 8(1(n)).

13.8 Regulation 8 states that information must be made "available" to a customer. A mechanism by which information can be made available under regulation 8(2)(c) is electronically, e.g, on a service provider's website.

Comparison with the WHOIS opt-out

[3] http://webarchive.nationalarchives.gov.uk/20090609003228/http://www.berr.gov.uk/files/file53100.pdf

13.9 Similar to the E-Commerce Regulations, the disclosure requirements apply to any individual or organisation that provides a service for which it normally charges. A service is defined as any economic activity which is normally provided for remuneration.

13.10 This differs from the WHOIS opt-out because:

13.10.1 it applies to both individuals and organisations; and

13.10.2 the focus is on whether or not the service is provided for remuneration, which is broader than using a domain as part of a business, trade or profession.

INFORMATION DISCLOSURE RULES IN OTHER INDUSTRIES

14. PO Boxes

Royal Mail Terms and Conditions

14.1 The terms and conditions for application for a Royal Mail PO Box state:[4]
"Disclosure of information

We reserve the right to give the address (and title) of the PO Box holder to any enquirers, (and you consent to this) and this information will be added to our national address database – the Postcode Address File (PAF). Information on the PAF is used to produce a number of Address Management products that are available to the public."

14.2 In its group privacy policy, Royal Mail states that:[5]
"We will also share your information with carefully selected third parties outside the Royal Mail group. We may do this for the following reasons:

To provide you with a service. Some of our services are provided in conjunction with our business partners, and we'll need to disclose your information to them to provide you with the services. We make it clear in the terms and conditions for each service whether information will be passed to third parties or not.

To protect the Royal Mail group or others. We may share your information with third parties when we believe it is necessary to comply with the law or protect our or another person's rights, property, or safety. This includes exchanging information with third parties to protect against fraud and reduce payment risks. Your information may be processed outside the European Economic Area (EEA) where privacy laws may not provide protection to the same level as in England, but if so, we ensure that the processing is carried out to standards equivalent to our own.

We will only deal with third parties that we trust to act in our customers' best interests and who treat our customers' information with the same stringent controls that we apply ourselves."

Legal basis for disclosure

14.3 Before Royal Mail was privatised in April 2014, individuals could make requests for disclosure of information under section 1 of the Freedom of Information Act 2000 (**FOIA**). The FOIA gives any person, including foreign nationals and companies, access to any information held by public authorities.

[4] http://www.royalmail.com/sites/default/files/PO-Box-Application-Form-with-Terms-and-Conditions-Jun-2014-Web.pdf
[5] http://www.royalmail.com/cy/node/19353843

14.4 In an example response to a request for information under the FOIA, Royal Mail noted that disclosure is subject to the exemption in section 43 of the FOIA which is designed to protect Royal Mail's "commercial interests".[6] Effectively, section 43 exempts trade secrets and other information the disclosure of which would, or would be likely to, prejudice the commercial interests of any person (including the public authority itself). In its response to the information request, Royal Mail stated that:[7]

"Royal Mail is a commercial company which relies on revenue from products such as PO Boxes. Terms and conditions in place for PO Boxes only specify that the geographical address may be disclosed to customers who request information. They do not state that the name of the owner, whether this is a company or an individual, will be disclosed. We believe that by disclosing the requested information about a third party, which they do not expect to be released, would be likely to impact upon any future business with this customer, and other customers.

Section 43(2) is a qualified exemption, therefore we are required to consider the 'public interest test' when applying this exemption. We appreciate that you have a particular interest in the requested information however we do not consider that the release of this information would significantly serve the interests of the public as it does not relate to the provisions of public postal services or business decisions directly affecting the public."

15. Electoral register

Information collected

15.1 Regulation 23 of The Representation of the People (England and Wales) Regulations 2001 (**Electoral Regulations**) makes it compulsory to provide information to an electoral registration officer for inclusion in the full electoral register. The details include a person's name, address, nationality and age. The full register is updated every month and published once a year, and is used by electoral registration officers across the country for purposes related to elections. Political parties, MPs and public libraries also have the full register.

Disclosure of the electoral register

15.2 Under the Electoral Regulations, the Electoral Registration Officer must publish two versions of the register:

15.2.1 the full register, which lists the names and addresses of everyone registered to vote. Circulation of this version is strictly limited to individuals and organisations listed in the Electoral Regulations. Recipients of the full register may only use it for the purposes specified by the Electoral Regulations, which will be for electoral purposes, the prevention and detection of crime, safeguarding national security or checking the identities of individuals who have applied for financial services. It is a criminal offence for any recipient to disclose information from the full register or to put it to any other purpose than that for which they receive it; and

15.2.2 the edited register, which omits the names and addresses of those electors who have requested on their applications to register that their names be excluded from this version. The law requires that the edited register must be made available for purchase by anyone for a statutory fee. Such recipients are then permitted to use the information for whatever purposes they choose.

15.3 It should be noted that a copy of the full register can only be sold to those organisations listed in regulations 113 and 114 of the Electoral Regulations. These organisations are:

[6] https://www.whatdotheyknow.com/request/170255/response/413724/attach/3/Philips%20290713.pdf
[7] Ibid, pp. 1-2.

15.3.1 government departments (including the Environment Agency, the Financial Services Authority and any body which carries out the vetting of any person for the purpose of safeguarding national security); and

15.3.2 credit reference agencies.

15.4 The Electoral Regulations, therefore, give electors the option to opt-out of the edited register. This means that their personal electoral information will not be available to third parties who may choose to purchase the edited register.

16. Telephone directories

Disclosure of directory information

16.1 Condition 19 of the General Conditions of Entitlement (**General Conditions**) requires that all providers that have been allocated phone numbers ensure that details of the numbers which are issued to end users (directly or through sub-allocations to other providers) are made available to other organisations which wish to compile telephone directories or operate directory enquiry services.[8]

16.2 Under condition 19.3 of the General Conditions, a provider must supply directory information on terms which are fair, cost-orientated and non-discriminatory, and in a format which is agreed between the provider and the person requesting the information.

Directory services opt-out

16.3 Under BT's code of practice for residential customers and small businesses (**Code**), a BT customer can choose how its phone number is listed. BT offers three options:[9]

16.3.1 a customer's name, address and number can be printed in The Phone Book (BT's telephone directory), with the customer's number also available from directory enquiry services;

16.3.2 a customer's name, address and number can be kept out of The Phone Book, but still be available from directory enquiry services; and

16.3.3 a customer's name, address and number is not printed in The Phone Book or available from directory enquiry services.

16.4 The underlying policy rationale behind this is to protect an individual's privacy and, specifically, to prevent persons from obtaining information about a directory member's physical address.

16.5 If a customer chooses the third option, BT will make the customer's name and address, but not the customer's telephone number, available for the purposes of providing directory enquiry services. This includes services on the internet as well as those available from 118xxx providers. BT will not reveal the customer's name and address to any user of these services but, when searching for the customer, they will be told that the customer's listing was found but that the customer is "ex-directory".

PRIVACY AND DATA PROTECTION

17. Data Protection Act 1998

17.1 An important question for Nominet when considering whether, and to what extent, customer information may be disclosed on the WHOIS is whether this creates any risks for Nominet under the DPA.[10] The DPA applies to the "processing" of "personal data".

17.2 To help Nominet assess this, we provide a brief overview of:

---

[8] http://stakeholders.ofcom.org.uk/binaries/telecoms/ga/GENERAL_CONDITIONS_AS_AT_16_MAY_2014.pdf

[9] http://www.btplc.com/Thegroup/RegulatoryandPublicaffairs/Codeofpractice/Consumercodeofpractice/BTResidentialCodeofPractice-Oct13.pdf

[10] The DPA implemented the EU Directive 95/46/EEC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

17.2.1 when data is considered "personal data" under the DPA;

17.2.2 any obligations that Nominet has in relation to controlling or processing personal data under the DPA; and

17.2.3 whether disclosing data through the WHOIS creates any risks for Nominet.

Key definitions

17.3 **Data controller:** The data controller is required to meet obligations relating to personal data under the DPA. The data controller is defined as the person who determines the purpose for which or manner in which personal data is processed. Nominet is the data controller because it determines the manner in which personal registrant data is processed through the terms of the Contract of Registration.

17.4 **Data subject:** This is defined as any individual about whom personal data is processed. In this case, the registrant will generally be the data subject (unless the Privacy Service is registered as the registrant).

17.5 **Personal data:** Section 1(1) of the DPA defines "personal data" as:

"data which relate to a living individual who can be identified –

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual".

The definition of personal data clearly includes data collected by Nominet about registrants (for example, a person's name, postal address, telephone number and e-mail address).

Processing

17.6 The DPA imposes obligations on those who process personal data. Processing is broadly defined in section 1(1) of the DPA to include obtaining, recording, holding, using, disclosing or erasing data.

17.7 To ensure that data is processed properly, Schedule 1 of the DPA sets out eight data protection principles:

17.7.1 **Principle 1**: Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

(i) at least one of the conditions in Schedule 2 of the DPA is met; and

(ii) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Generally speaking, Principle 1 will be met if the data controller has the specific, informed consent of the data subject to process the data. A registrant consents to the processing of their data by agreeing to the terms of the Contract of Registration.

17.7.2 **Principle 2**: Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

17.7.3 **Principle 3**: Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

17.7.4 **Principle 4**: Personal data shall be accurate and, where necessary, kept up to date.

17.7.5 **Principle 5**: Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

17.7.6 **Principle 6**: Personal data shall be processed in accordance with the rights of data subjects under the DPA.

17.7.7 **Principle 7**: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

17.7.8 **Principle 8**: Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

17.8 Overall, a key focus for Nominet under the DPA is to ensure that it complies with Principle 2. In essence, Principle 2 requires that Nominet only process data for the stated, explicit purpose for which that data was originally collected. (We describe the purpose in paragraph 5.2).

MENU OF POLICY OPTIONS

18. Overview

18.1 In this section, we summarise the benefits and risks of six different policy options:

18.1.1 **Option 1: Status quo.** In this option, Nominet retains the current definition of "consumer" in the Contract of Registration as the eligibility criteria for whether a registrant can opt-out of the WHOIS.

18.1.2 **Option 2: E-Commerce Regulations.** In this option, Nominet adapts the opt-out clause to adopt the eligibility criteria used in the E-Commerce Regulations. This will mean that a person is only entitled to opt-out if they are not supplying an "information society service" (as defined in the E-Commerce Regulations). This option does not propose to amend the current information that Nominet requires registrants to disclose in the WHOIS under the Contract of Registration.

18.1.3 **Option 3: All registrants.** In this option, Nominet abandons the distinction between "consumers" and non-consumers and expands the opt-out to all registrants. This means that all registrants may opt-out, if they wish. In effect, this means that Nominet will be providing services similar to the services supplied by Privacy Services. For example, a business (or non-consumer) may now choose to opt-out of the WHOIS rather than purchase separate services from a Privacy Service.

18.1.4 **Option 4A: Amend Registrar Agreement.** In this option, Nominet amends the terms of the Registrar Agreement to require that:

(i) all registrars must register a domain in the name of their customer. (Effectively, this involves removing the "explicit consent exception" referred to in paragraph 7.2); and

(ii) a registrar may elect to provide its own details for the purpose of data that is subsequently provided on the WHOIS. This may involve including an additional clause in the Registrar Agreement which distinguishes between data supplied by the registrar for the purpose of publication on the WHOIS and data supplied by the registrar to enable Nominet to enforce its contract with the registrar's end-customer.

Effectively, this creates two data separate streams: on the one hand, data that is supplied to Nominet so that Nominet can enforce its contract with the registrant; and, on the other hand, data that is supplied to Nominet for the purpose of supplying on the WHOIS. The second data stream can be generic details of a Privacy Service.

18.1.5 **Option 4B: Amend both the Registrar Agreement and the Opt-Out.** In this option, Nominet amends the terms of the Registrar Agreement as described in

paragraph 18.1.4 and changes the terms of the current opt-out. In this hybrid approach, we consider two alternatives:

(i) **Option 4B(i):** First, maintaining the current definition of "consumer" in the Contract of Registration but removing a registrant's name from the WHOIS if the registrant has successfully opted-out; or

(ii) **Option 4B(ii):** Secondly, adapting the opt-out clause to adopt the eligibility criteria used in the E-Commerce Regulations (as described in paragraph 18.1.2) and removing a registrant's name from the WHOIS if the registrant has successfully opted-out.

18.1.6 **Option 5: Sensitive Cases.** In this option, Nominet expands the opt-out to include a mechanism by which "sensitive" non-consumers can apply to Nominet to opt-out of the WHOIS. In effect, the definition of consumer is retained, but a side mechanism is created for sensitive cases.[11] For example, Nominet could weigh up the public interest in disclosure against the non-consumer's interest in having the data excluded from the WHOIS.

18.1.7 **Option 6: CAPTCHA.** In this option, Nominet introduces a CAPTCHA (or some other technical mechanism) for persons wishing to contact a registrant that has opted-out of the WHOIS. For example, Nominet may enable a person to contact an anonymous registrant (e.g. through clicking a CAPTCHA or form on the WHOIS display page). The CAPTCHA or form will not disclose any information about the registrant; however it will enable the person to contact the registrant directly. This option could be used separately or in conjunction with any of the other five options described in paragraphs 18.1.1 to 18.1.6.

19. Benefits and risks

Options	Benefits	Risks
Option 1: Status quo	• No requirements to alter the terms of the Contract of Registration.	• The risks to Nominet under the DPA appear to be low (please see paragraph 17.8). We note that the Data Protection Directive (95/46/EC) is currently under review at the EU level. We provide a summary of the key features of this review in **Annex 1**. • Non-consumers may continue to utilise Privacy Services to avoid having their postal address displayed on the WHOIS. This may create flow-on issues for Nominet, e.g.: ▪ Nominet cannot communicate directly to registrants as any communications must be made through a registrant's Privacy Service; and ▪ Nominet may have difficulties enforcing its contract with end-users (e.g. dispute resolution settlements, contacting a

[11] These may include situations, for instance, where the registrant has a strong personal interest in avoiding the public disclosure of their postal address (e.g. to avoid an ex-partner).

		registrant about a domain name's expiry).
Option 2: E-Commerce Regulations	• Brings Nominet in line with the UK government's policy under the E-Commerce Regulations. A consistent policy approach is positive because it: ▪ provides a policy basis for Nominet to delineate between different types of registrants. E.g. a registrant that must disclose certain information under the E-Commerce Regulations should not be allowed to opt-out of supplying the same information under the WHOIS; and ▪ places the burden on the UK government to enforce the E-Commerce Regulations rather than on Nominet. It also ensures that Nominet is not regarded as a proxy for the UK government to enforce the E-Commerce Regulations. • Substantially narrows the opt-out (as the focus is now on whether the person's domain has a remunerative purpose). • Sends a strong signal that the opt-out cannot be used to avoid any other disclosure obligations registrants' face.	• Does not resolve the risk of individuals or entities using Privacy Services. It may, in fact, increase the use of Privacy Services as fewer individuals and entities will be entitled to opt-out.
Option 3: All registrants	• Substantially expands who is eligible to opt-out. This may, in turn, reduce the use of Privacy Services and enable Nominet to capture more information from registrants and enforce its contract with end-users. • Indicates that Nominet is focused on protecting registrants' personal data. From a policy perspective, the shift in approach can be justified by arguing that "information service providers" must provide information under the E-Commerce Regulations irrespective of whether that information is also disclosed	• Less information on the WHOIS may lead to a more "stagnant" registry. (E.g. a prospective purchaser of a website may not be able to identify the current registrant and therefore may have difficulty negotiating the purchase of a domain). We consider that this risk is small. • In addition, it may create barriers for registrants to "self-verify" (i.e. check the status of their own registration). However, there are alternative routes available for them (e.g. contacting Nominet or their registrar). • Reduces the ability of

	on the WHOIS. • May improve Nominet's ability to respond to requests for information from law enforcement agencies.	consumers to discover the person or entity that is responsible for a domain name. Nominet has, in the past, indicated that consumer protection is a legitimate policy objective of the WHOIS.
Option 4A: Amend Registrar Agreement	• Nominet gets complete registrant information from registrars. This reduces any risks Nominet currently experiences in enforcing its contract with registrants (e.g. dispute resolution settlements, contacting a registrant about a domain name's expiry etc.) • Registrants can still utilise Privacy Services to avoid having their personal data supplied on the WHOIS. • Clearly delineates between data required to enforce the Contract of Registration and data which is supplied on the WHOIS. This helps illustrate that Nominet is complying with the DPA, as the two data streams are treated separately and for different purposes.	• Creates an imbalance between consumers that legitimately opt-out of the WHOIS under the Contract of Registration and non-consumers that utilise Privacy Services to avoid having their personal data displayed on the WHOIS. • Under this option, an opted-out consumer's name will show on the WHOIS whereas a non-consumer's name will not. Arguably, however, a genuine consumer has a stronger privacy interest. • We present two options to address this problem in Option 4B(i) and Option 4B(ii) below.
Option 4B(i): Amend Registrar Agreement / opt-out; maintain definition of "consumer"	• The same benefits apply as in Option 4A. • Additionally, the imbalance described in Option 4A between consumers and non-consumers is removed. A consumer that is opted-out will not display any personal data on the WHOIS.	• Reduces the amount of information that is available on the WHOIS / devalues the WHOIS for interested stakeholders. •
Option 4B(ii): Amend Registrar Agreement / opt-out; adopt the eligibility criteria used in the E-Commerce Regulations	• The same benefits apply as in Option 4A and Option 4B(i). • Additionally, the opt-out is narrowed as the focus is now on whether the person's domain has a remunerative purpose. • This means that only persons that use a domain for non-remunerative purposes can opt-out of the WHOIS at no cost, whereas any other person will have to purchase Privacy Services from a registrar or third party privacy service if they wish to remove	• See Option 4B(i).

	their personal data from the WHOIS.	
Option 5: Sensitive Cases	• Creates a subjective mechanism for Nominet to manage sensitive cases. This is particularly important because sensitive cases can create 'bad news' stories.	• The "consumer" test is currently largely objective. This is easy to measure and enforce. A subjective test, however, creates uncertainty and requires in depth interpretation and consideration. • May require an appeal mechanism.
Option 6: CAPTCHA (this option may be considered separately or in conjunction with other options described in this paper).	• Allows a person accessing the WHOIS to securely contact a registrant, while not disclosing any personal information about the registrant in the process.	

ANNEX 1

20. Reform of the EU data protection regime

20.1 The European Commission published a package of proposals in January 2012 aimed at reforming the existing EU data protection regime. The main feature of the reform package is a proposed new General Data Protection Regulation (**Regulation**) which will replace the existing rules set out in Directive 95/46 (**Directive**).[12]

20.2 The proposed Regulation involves a number of substantive changes to the existing rules. These include:

20.2.1 Extending the scope of the rules to cover not only data controllers and data processors established within the EU, but also data controllers established outside the EU that supply data subjects located in the EU or that monitor the behaviour of such data subjects (e.g. through cookies or other tracking devices);

20.2.2 Requiring that, where a data subject's consent is needed, it must be given explicitly (rather than impliedly);

20.2.3 Introducing a "right to be forgotten", which will give data subjects the right to request that their personal data is deleted if there is no legitimate grounds for retaining it;

20.2.4 Improving data subjects' access to their personal data, for example by creating a "right to data portability" which will allow data subjects to move their personal data between service providers;

20.2.5 Introducing a new "accountability" principle requiring data controllers and data processors to implement measures to ensure and be able to demonstrate compliance with the Regulation, including appointing a data protection officer, keeping records of processing activity, implementing data security requirements and notifying breaches to the national data protection authority and, in some cases, the data subject;

20.2.6 Introducing a new one-stop shop principle for the approval of binding corporate rules (**BCRs**), i.e. rules which relate to the transfer of personal data between companies within the same corporate group and which have been approved by the national data protection authority. Under the new rules, BCRs will only need to be approved by one national authority in order to be valid across the EU;

20.2.7 Introducing new rules aimed at ensuring greater co-operation and consistency between national data protection authorities, including making measures adopted by the data protection authority in one EU Member State enforceable in all EU Member States; and

20.2.8 Increasing sanctions for non-compliance, for example a company in breach of its data protection obligations may face a fine of up to 2% of its annual worldwide turnover.

20.3 On 21 October 2013, the European Parliament's Committee for Civil Liberties, Justice and Home Affairs voted in favour of certain amendments to the proposed Regulation. These include:

20.3.1 Introducing a new requirement to notify and seek the approval of the relevant national data protection authority prior to disclosing data to a non-EU country, in circumstances where the data controller or data processor has been requested by a court or authority in that country to disclose the data;

20.3.2 Tightening the requirements for obtaining consent, so that the conclusion of contracts cannot be made conditional on consent being given to the processing of data where this is not necessary for the provision of the service. Processing of personal data by internet service providers would also require explicit consent; and

20.3.3 Increasing the maximum penalty for non-compliance to €100 million or 5% of annual worldwide turnover, whichever is the greater.

[12] http://ec.europa.eu/justice/data-protection/index_en.htm

20.4 On 12 March 2014, the European Parliament voted strongly in favour, to approving the amended draft text of the Regulation. There were 621 votes in favour out of a total of 653 votes. The vote means that the European Parliament is no longer able to change its position on the Regulation, even if the composition of the Parliament changes following the parliamentary elections in May 2014. Before the Regulation can pass into law, it must be adopted by the Council of Ministers using the “ordinary legislative procedure”. This means that both the European Parliament and the Council of Ministers must agree on the final legislative text.

20.5 Unlike the existing Directive, the Regulation will be directly applicable in the UK, without the need for implementing legislation. As currently drafted, the Regulation will not apply until 2 years after it enters into force.