The ICANN-Law Enforcement Due Diligence Recommendations and fundamental Rights

A commentary in the context of the 1950 Convention and European Union law

Nigel Roberts LLB*

1 Background

The *ICANN Law Enforcement Due Diligence Recommendations* is a document that was a jointly issued in 2009 by several law enforcement agencies, including the US Department of Justice's *Federal Bureau of Investigation* ("the FBI"), the United Kingdom's *Serious and Organised Crime Agency* ("SOCA") and the *Royal Canadian Mounted Police.*

The Recommendations are addressed to ICANN (the *Internet Corporation for Assigned Names and Numbers*) - a private, not-for-profit company established as a Californian Public Benefit Corporation, which has an centre-stage role in the management of Internet names and addresses.

Although ICANN does have a very significant Governmental input (among others from various government departments from nearly all Member States of the Union and members of the Council of Europe as well as from Canada, the USA, and others), channeled through a separate-but-closely-associated Government Advisory Committee ("GAC"), it is a private company.

Thus the essential nature of ICANN is that it appears to be *"an arrangement between undertakings"*.

However, ICANN has bound itself, in its *By-laws* to comply with international law[1].

2 The Law Enforcement Recommendations

The *Law Enforcement Recommendations* appear to make a number specific (regulatory-style) requirements upon ICANN, domain registries, registrars and the domain name market; amonst other things, suggesting the inclusion of conditions, that intended to be contractually

*http://nigel.je

[1] see *ICM Registry -v- ICANN* ICDR Case 50 117 T 00224 08

legally binding, upon registries and registrars of 'generic Top Level Domains' in the course of ICANN's work, which regulates the operation of the domain name market for domains such as .COM, .NET etc.

2.1 Purpose of the Recommendations

The purpose of the *Law Enforcement Recommendations* is order to assist in the prevention and detection of crime.

The concept of 'prevention and detection of crime' is a golden thread which runs through various parts of the law of the Union. For example it may be seen appearing in the exemptions from certain prohibitions in the Data Protection Directive[2], in the Data Retention Directive[3], in the exemptions to the Treaty prohibitions of Quantitative Restrictions (and of measures having equivalent effect)[4] and indeed in the overriding aims of the Treaties[5].

Another way of putting this might be: **'discouraging bad guys from doing bad things, and making it easier to catch them when they do'.**

Although not explicitly stated in the 2009 *Recommendations*, their context seems to make it clear that they are addressed to the regulation of 'generic' Top Level Domain Registries and Registrars, that is to say, domain names that are not associated with countries or territories, such as those ending in .COM, .ORG etc), rather than towards the managers of the 'country-code' top level domains (such as *.UK*, *.FR* or *.DE*).

Country-code domain registries within Europe are principally regulated by the domestic law of the Member State in which they are established.

They also subject to applicable European law by virtue of the *acquis communitaire* (registries established in Member States of the Union), the EEA Agreement (in other members of the EEA[6]), Protocol 3 to the Treaties (in territories for which a Member State is responsible[7]) or bilateral agreements (the Swiss Confederation). Among other things European law includes the freedom to supply services within the Single Market on an equal footing.

It is probably correct to say that very many of the challenges and issues that are faced by the various police and law enforcement agencies around the world in respect of domain names and the DNS are similar, whether they are 'generic' or 'country-code' TLDs, but on some occasions, the answers to those challenges may differ because of the lack of local accountability for 'generic' domain names that exists in the ccTLD context.

It can often be easier to enforce the law in respect of criminal activity involving holders of country-code domain names (in those countries where the Rule of Law obtains) since ccTLDs are rooted in the legal system of the Member State concerned and are not extra-territorial

[2] Directive 95/46/EC
[3] Directive 2006/24/EC
[4] Article 30 of the Consolidated Treaty on European Union, promulgated in the Official Journal,C321 E/27 on 29.12.2006
[5] Article 2 of the Consolidated Treaty on European Union, promulgated in the Official Journal,C321 E/27 on 29.12.2006
[6] EU Members plus Liechtenstein, Iceland and Norway
[7] (for example) San Marino, Farœ Islands, the Channel Islands, Andorra

or (apparently) supranational in nature, such as .COM, .NET and other 'global' top level domains sometimes appear to be.

In overview, the *Law Enforcement Recommendations* seems to the author to be to be a collection of tactical measures, designed to help the police and judicial authorities track and trace criminals, and help discourage their activity.

It is submitted that, in view of democratic principle of the Rule of Law which embodied, among other places in Art. 2 of the Treaty, *it cannot be doubted that it is desirable that the purpose of the Recommendations should be achieved.*

The rest of this paper therefore focuses on whether the measures proposed may be effective and proportionate and looks at this by way of some examples.

3 Enforcement of the criminal law.

Law enforcement is a fundamental part of the constitution of a democratic society.

Without a functional and efficient police force invesigating and prosecuting crime, operating within the context of a an independent judicial system, citizens rights' to private life and to property, for example, may be restricted. Indeed, in European Convention jurisprudence, Member States have the *positive obligation* to protect these (and other) rights.

The creative tension between pragmatic measures designed to combat harmful activities and the protection of citizens' constitutional and fundamental rights is a feature of modern democratic societies. And whilst in full accord with the aim to be achieved, it seems to the author that are some potential pitfalls with the *Recommendations* where they endorsed by public authorities (if adopted without further discussion and modification), as binding rules for gTLDs (and as a persuasive example for ccTLDs).

The purpose of this paper, therefore is to consider some aspects of this in more detail, using a rights based approach in the context of European Law (that is to say, both Community Law, and Conventional law), and to suggest some perhaps as-yet-not-fully-explored avenues by which the purpose of the Recommendations can be further promoted.

4 The Fundamental Rights

4.1 What are the rights referred to above anyway?

Specifically, they are those rights, which all people within or under the jurisdiction of a signatory State have as fundamental rights, and are set out in the 1950 *European Convention*[8]

[8] The Convention on the Protection of Human Rights and Fundamental Freedoms done at Rome, 4th November 1950

For countries and territories without a written constitutional document (in particular, the British Islands[9]) these rights are the closest thing to constitutional rights and are directly effective as domestic legal rights[10]. But Fundamental Rights are important within all the High Contracting Parties (i.e. all member countries of the Council of Europe) as they provide a further guarantee of respect for fundamental human rights even in States where there exists a written and entrenched Constitution embodying them. Furthermore the Convention rights originated within the post-WW2 background and the context of the UN *Universal Declaration on Human Rights*[11]. They have a similar purpose and form to the Universal Declaration, so it can be said that that the fundamental rights are relevant in *all* democratic countries, not just Europe, and especially so in countries having a Charter or constitutional guarantee of fundamental rights (such as Canada[12] and the United States).

4.2 Importance

At the date of writing, Conventional rights are binding in total of 47 countries.

And they are binding upon upon all government authorities including police agencies and judicial authorities in

- all Member States of the Council of Europe, which includes . . .
- all Member States of the European Economic Area, which includes . . .
- all Member States of the European Union.

Furthermore, under *Article 17* of *Protocol 14* to the Convention, these same fundamental rights are now to be binding on the European Union itself (and all its institutions). These fundamental rights are regarded as so important that it is a condition of membership of the European Union that a candidate state must have ratified the Convention before being considered for Accession.

The guardian of the Convention is the *Council of Europe* (http://www.coe.int) - not to be confused with 'the Council' or 'the European Council'). It is an International Treaty Organisation in its own right. Following the *Declaration of the Committee of Ministers on 26 May 2010*, the Council of Europe participates as an observer to ICANN's Governmental Advisory Committee (GAC)..

It is to be expected that through the mechanism of the public policy advice given to the ICANN board by the GAC and by raising the awareness of fundamental rights within all stakeholders, whether from the private sector or public authorities, European Citizens' fundamental rights shall be taken more into account by ICANN in all its work relating to internet naming and addressing, not just in the context of the *2009 Recommendations*. (One obvious example where this could occur is in the consideration of rights of people seeking to create new

[9] This term-of-art was created by the Interpretation Act 1948 as meaning the UK, Channel Islands and Isle of Man

[10] (*The Human Rights Act 1998* (1998, c.42), *The Human Rights (Bailiwick of Guernsey) Law 2000* (Ordres en Conseil XIV) and parallel legislation in Jersey and the Isle of Man).

[11] Universal Declaration of Human Rights, of General Assembly of the United Nations , December 10, 1948

[12] The Canadian Charter of Rights and Freedoms, enacted as part of the Constitution Act 1982.

forms of expression, such as new top-level domain names - but that is a subject for another paper).

4.3 Qualified Rights and Absolute Rights

Before examining the 2009 *Law Enforcement Recommendations* in terms of the Convention rights, it must be borne in mind that there are two distinct categories of fundamental rights:

1. those rights which a governmental authority may never interfere with under any circumstances *('infringe'* is the term-of-art normally used*)*, and
2. rights that, in clearly defined circumstances, a public authority might legitimately restrict or infringe.

The first category contains the 'absolute rights'.

Examples of absolute rights are as the right to life, and freedom from slavery and from torture. (It can be seen on a cursory examination that such rights should never be expected to be engaged, anywhere in ICANN or the DNS industry.)

The rights that are most likely to be engaged in the public policy aspects of ICANN's work according must be those in the second category (qualified rights), and in particular:

1. the right to private and family life (*Art. 8*)
2. the right to free expression (*Art. 10*)
3. the right to property[13] (*Article 1* of *Protocol 1*)
4. the right of non-discrimination (*Article 13*)

4.4 How Convention rights apply

They apply 'vertically'. This means that is they are binding upon government or public authorities (including law enforcement agencies). They can be relied upon, by individuals and companies.

They do not often apply 'horizontally'. That is to say, it is a general principle that no cause of action arises between private individuals or companies simply on the basis of Conventional rights. However, that is not the end of the story, since judicial authorities are strictly bound by Convention rights and in the Strasbourg jurisprudence it is clear that all three branches of government (executive, legislative and judicial) in the territory of the High Contracting Party have a *positive obligation* to protect the Convention rights. The effect of is that rights may sometimes be applied indirectly between (legal or natural) persons such as individuals and companies[14].

[13] Including intellectual property!
[14] e.g. Campbell v MGN [2004] UKHL 22, MGN v United Kingdom (Application No 39401/04)

4.5 Enforcement

Fundamental rights are enforced

- by the domestic courts, and (if domestic remedies have been exhausted);
- by the *European Court* at Strasbourg.

Sometimes, for example, Convention rights come into conflict with each other.

So one party is legitimately claiming one right, and another party legitimately claiming another, apparently conflicting right.

The most common example of this, outside the context of the DNS, is the creative tension that exists between Article 8 and Article 10, usually in the context of regular clashes between the freedom of the press (a necessary part of a democratic states) and personal privacy (a right of the citizen).

In that case there has to be a balancing act, which is the responsibility of the legislative and judicial authorities in the country concerned to undertake.

5 Application of the fundamental rights to the Law Enforcement Recommendations

If we apply the Convention Rights, which every European Citizen, and every third-country national lawful resident of the territory of a Member State, and every corporate body has of automatic right to some of the prescriptions of the *ICANN Law Enforcement Recommendations* we appear to get some interesting results.

5.1 The Recommendation that personal data of registrants, their employees and contractors must be open and published widely on the Internet using the WHOIS protocol

The promotion, by any organisation bound by the Convention rights, of a condition that European registrants and registrars must submit to *'unrestricted and public access to information about domain registrations'* clearly engages *Article 8*.

The conditions on which any public authority proposing such infringement need to fulfill in order to be acting lawfully and Convention-compliant are :-

that the interference (with the *Article 8* right to privacy) is :

- in accordance with law;
- is necessary
  - in a democratic society; and
- is proportionate.

These are the tests of lawfulness, necessity and proportionality.

The first question to ask is is a proposed infringement *'in accordance with law'*?

When a dispute involving a Convention right usually comes to a domestic tribunal (or even as far as the Court of Human Rights itself), it is most often the case that there is a specific domestic law that is complained of, and the argument before the Court will need to consider the tests of necessity and proportionality (of which more later).

However, where a public authority (such as a police or judicial authority from any of the 47 countries, or even a GAC member for the member state concerned, or an agency of the Union) endorses an infringement of a Convention right apparently unsupported by a legal rule, it appears possible that this is not in compliance with the first requirement; which is that the infringement (where a qualified right is engaged) is in accordance with law.

And it is not clear to the author, where such authority lies when, for example, a European, ICANN-accredited, Registrar is required, under the presumptions of a *Recommendation* of or action by the various public authority acting through the GAC are compelled (using ICANN's contractual powers), to force personal data to be published on the Internet about domain registrants (whether private citizens or commercial entities).

A close analogy, perhaps, is that in most countries, certain information about company registrations and the owners/directors of companies must be publicly available.

This requirement has to be set out in legally binding rules. An example of the effect of Convention rights on such law, the UK recently amended its *Companies Acts* to remain compatible with *Article 8* concerns in a 21st century context (since the Convention is a *'living instrument'*). Henceforth, company directors in England and Wales - although they continue to be required to be on the public record and supply an address for legal service - are now no longer required to have their home address published widely on the Register.

Another example is that the E-Commerce Directive mandates website owners to include, a statement of the owner of the business, and their contact details (i.e. an *Impressum*).

Both of the above examples are examples of the State acting in 'accordance with law' where an *Article 8 right* is engaged.

Incidentally, the E-Commerce Directive applies to operators of websites, and does not appear to be addressed to domain registrations despite the common conflation of the two concepts (which are *not* coterminous).

It does not seem to this author that this Directive (or any local transposition thereof) is a proper source of lawful authority for imposition of a requirement on a domain registrant, although it seems that such a requirement could perfectly legitimately be made by the legislature. (It is clear that the registrant of the domain name *example.com* may not even be the same person as the operator of a website at `http://www.example.com` - for reasons of internal company organisation, the use of an IP holding company etc.)

But let us assume that first issue, that the interference must be 'in accordance with law'. had been successfully complied with.

It seems that this *Recommendation* may not be compliant with the tests of *necessity* and *proportionality.*

The reason for this, is that it seems clear on a cursory examination of the problem to be solved, that the aim to be achieved can be met in a way which respects registrants' *Article 8.* rights, irrespective of whether the inquiring law enforcement concerned is located inside or outside the European Economic Area.

Where law enforcement need access to domain name registration data or other unpublished information, it seems obvious this can be provided by registries and registrars providing law enforcement with speedy access to such information as is needed, just in the same way as, when law enforcement needs access to telephone subscriber data, such data be swiftly obtained in accordance with defined procedures laid down, such as in the UK Regulation of Investigatory Powers Act (RIPA[15]), even if the number sought is 'ex-directory' or unlisted.

In order to fully respect *Article 8* rights, what seems to be required - and seems to be missing - from the practices of gTLD registries or registrars (many of whom are subject to *directly applicable* EU law) is a right of a person to withhold their personal information from publication on the Internet in the same way a person or company has a right to an unlisted telephone number.

Clearly such a right must of course, be balanced by a framework by which law enforcement both inside and outside the EU (subject to European data protection rules and exemptions) may quickly and conveniently access the data when this is both necessary and proportionate.

However, making the information required to be broadcast and published widely on the Internet (as distinct from making it available to legitimate inquirers) without the informed consent of the person concerned, and/or even against their will, can result in problems and difficulties to the registrant, such as spamming and even stalking and, it is submitted, may contravene European Data Protection law.

Such indiscriminate publication of personal data appears to be disproportionate and therefore also would seem to infringe Convention rights without a saving justification and, accordingly, seems to be unlawful, where such infringement endorsed by a public authority to which the Convention rights apply.

5.2 Only accredited proxy registration services to be allowed

This Recommendation would appear to - at a stroke - prohibit the right of a person (whether a legal or natural) to carry out lawful activities that are entirely legal under the law of the country concerned. In particular, the effect of this recommendation would appears at a stroke to strike down the entire law Equity and trusts, on which a large amount of legitimate business is founded in common-law countries.

Such a recommendation appears to prohibit a trustee from holding a contract for registration of a domain name for the beneficiaries of a trust.

It would also appear, on its face, to purport to infringe upon legal professional privilege - a lawyer would seem to be prohibited under this provision from registering a domain name to 'XYZ Advocates Client Account'

[15]The Regulation of Investigatory Powers Law (RIPL) in the Channel Islands

Such a Recommendation also clearly engages Art 8, where a public body to which the Convention rights apply are promoting it, and similar considerations of lawfulness and proportionality must apply.

5.3 Registries, registrars etc. to be required to publicly display enhanced data and carry out 'enhanced due diligence'

Article 8 is clearly and obviously engaged. It seems to the author, that this recommendation is so widely drawn, it fails the test of proportionality immediately. The criminal checks such as those proposed will involve the parties carrying them out in what is known under EU Data Protection Law as not just personal data but *'sensitive personal data'*, and is expected to be transferred to organizations outside the European Economic Area.

What safeguards are proposed to be used here? Has ICANN entered the 'Safe Harbor' agreement? These are questions must be answered before such a scheme should be considered.

5.4 Validation of contact data

All European registries require accurate data in their Registration Agreement.

The approach in .EU, which is exemplified in EU law in the *.EU Domain Regulation* [16] take the approach that validation of contact data shall be done after registration and not before.

European ccTLD registries already take reasonable mechanisms to keep their data correct, and have procedures in place to take immediate corrective action when receiving reports of bad data.

6 Perspective

European registries and registrars do want to help the good guys catch the bad guys.

And don't want unnecessary formalities to get in the way of that goal.

It is now well known that for a Law Enforcement agency outside the EU to request data via a Mutual Assistance request, can take many months. This is an eon in cybercrime terms. So new protocols and systems are required on exchange of information.

Domain name Registries and registrars have to work with the police and judicial authorities, from other jurisdictions, as well as the national authorities (procedures for which are well understood locally).

Just because there are different perspectives does not mean that that registries/registrars and police authorities are on different sides. But it must be the reality that no-one wants to see

[16] *Regulation (EC) No 733/2002 of the European Parliament and of the Council of 22 April 2002 on the implementation of the .EU Top Level Domain*

convenience and pragmatism create a situation whereby fundamental rights are not taken into account or may even be disregarded.

That after all would conflict with very *raison d'être* of the Convention and the Council of Europe.

And in pragmatic terms, to do so would be counterproductive, since infringing fundamental could conceivably in the future provide a defense, or grounds for appeal for a bad guy. It would be 'fruit of a poisoned tree' to use the American idiom.

It seems that the first issue that must be resolved in a rights-based culture is that of excessively public WHOIS.

The law enforcement community have historically stated that want this because they think it is the only way to get fast information in an investigation. But publishing personal information on the Internet is too broad and causes as many problems as its solves. The proposed solution in itself causes bad things, such as encouraging spamming, and worse, the rise of cyberstalking through the use of WHOIS records

The author believes that that police authorities, engaged in legitimate investigations could access the data it wanted, quickly, without the requirement for publishing personal data (within the meaning of the Data Protection Directive) world-wide on the Internet.

It is submitted that can indeed be done, by means of a bilateral information exchange agreements between registries and relevant police and judicial authorities in non-EU countries. (Between EU states there should be no issues in releasing personal data anyway, as every Member State is presumed to have *adequacy* of their Data Protection regime).

It seems that such a model for information exchange would be entirely lawful under European Data Protection Law and convention rights, in the same way that agreements on information exchange have been concluded on tax matters.

That being so, the alternative of requiring publication of personal data of European citizens and companies, must be disproportionate and thereby an impermissible infringement of registrant's Convention Rights.

7 Conclusion

It seems that the optimal way forward would appear to be for the relevant people in the registries, registrars, and law enforcement, and other bodies to come together to produce a framework which allows the police and judicial authorities to carry out their assigned tole of protecting our rights without undue difficulty or inconvenience, whilst not allowing convenience to override fundamental rights.