I am submitting these comments in my capacity as founder and Managing Director of Blacknight Internet Solutions Ltd (IANA ID:1448).
Blacknight is a hosting company and ICANN accredited domain name registrar in Ireland. We have wide experience in dealing with ccTLD domain name registrations and are the largest registrar for .ie domain names in the world.

I am also a member of the Working Group that drafted this initial report (https://www.icann.org/public-comments/ppsai-initial-2015-05-05-en ) .

ICANN's track record around privacy, in particular with respect to whois, is far from stellar. Repeatedly there have been calls from both privacy advocates and data privacy professionals to address the gaps between ICANN's policies and contracts and national law. While ICANN acknowledges that it cannot "trump" national (local) law via contract or policy, it has made it very difficult for affected parties to get waivers to their contracts and allow them to comply. Our own experience in dealing with this matter is illustrative. It took us several months and thousands of Euro in legal fees before we were finally granted a waiver. While this may seem to be an unrelated topic to the matter in hand, it goes to the heart of the matter in question – privacy.

Before addressing the specific questions that the PPSAI's initial report raise one should pause and ask simply why proxy and privacy services came into being in the first place.

One could rely on anecdotal evidence, but as a service provider of whois privacy services,, as well as dealing with a customer base that is primarily Irish and European, there are certain expectations of privacy from our customers.

When you register a .ie domain name, for example, you need to provide as much if not more information than you do during the registration of a gTLD domain. However, while the collection of registration data might be more onerous, the amount of data that is made available to the public is limited.
In the case of a domain name registered to an individual, taking as an example one of my own domain names:

domain: michele.ie
descr: Michele Neylon
descr: Sole Trader
descr: Registered Business Name
admin-c: AIQ120-IEDR
tech-c: AAM456-IEDR
registration: 12-January-2009
renewal: 12-January-2017
holder-type: Billable
wipo-status: N
ren-status: Active
in-zone: 1
nserver: ns1.blacknight.com
nserver: ns2.blacknight.com

source: IEDR

person: Michele Neylon
nic-hdl: AIQ120-IEDR
source: IEDR

person: Blacknight.ie Hostmaster
nic-hdl: AAM456-IEDR
source: IEDR

Or in the case of a domain name registered to an Irish limited company (the equivalent of an LLC):
domain: blacknight.ie
descr: Blacknight Internet Solutions Limited
descr: Body Corporate (Ltd,PLC,Company)
descr: Corporate Name
admin-c: AAE553-IEDR
tech-c: AAM456-IEDR
registration: 21-August-2003
renewal: 21-August-2015
holder-type: Billable
wipo-status: N
ren-status: Active
in-zone: 1
nserver: ns.blacknightsolutions.com
nserver: ns2.blacknightsolutions.com
source: IEDR

person: Blacknight.com Hostmaster
nic-hdl: AAE553-IEDR
source: IEDR

person: Blacknight.ie Hostmaster
nic-hdl: AAM456-IEDR
source: IEDR

In both cases the amount of data that is available to the public is limited and the contact details for the domain holder or any of the other related contacts (NIC handles) is not made public, nor is it possible to query them via any online method.
You cannot, for example, see my home address, email address or mobile phone number.

Only Irish law enforcement can access the underlying data. Anyone else would need to serve the registry (or the registrar) with a court order to access it.

I could cite examples of registrations from many other ccTLD registries based in the European Union, and while the amount of data made public will vary, in most cases there is a “baked in” privacy protection afforded to all registrants regardless of their legal status.

None of these domain name registrations are lurking in the shadows, as the public Whois database is respectful of privacy.

It should also be noted that in most cases ccTLD registries do not differentiate between commercial and non-commercial registrations. This within the framework of national law, which the bulk of country code managers would, by their very nature, need to comply with or risk losing their ability to operate.

On the substance of the Working Group's recommendations in this initial report:

Definitions & Terminology
I have no issue with the definitions and terminology. These were discussed in detail and are non-contentious.

Availability of Privacy / Proxy (P/P) Services
Privacy / Proxy services should be made available to all registrants no matter how they use or plan to use a domain name.
Expecting registrars or other intermediaries to police domain name usage would put a ridiculous burden on them. Bear in mind that a very large portion of the internet resides "below the surface" ie. You need to have a username and password to access the content. It would be impossible for a service provider to verify domain name usage.
At a more practical level, in our experience many of our customers opt to use whois privacy on their .com domain name registration in order to prevent mining of their data by automated systems (bots). At the same time as they seek this protection in the public whois they often publish their full contact details on their websites. It should also be understood that in many cases the entity that manages the domain name might not be the entity who runs the website or whose products and services are being advertised via the website. For example, in the Irish market there is a well known online service that offers e-commerce services to restaurants and takeaways. The company that runs this service has registered domain names for some of their client restaurants and simply points them at the page on their site.

Labels in Whois
While I can understand why adding labels to the whois output might be beneficial, I'm not convinced that it will truly benefit anyone. How would that benefit anyone? Are there unintended consequences of adding a label? Could this, for example, have a negative impact on an associated website's SEO? Google and other search engines have a track record of assigning certain "weights" to aspects of a domain's whois record and this could have a detrimental impact. If, for example, labelling a P/P record scored negatively registrants would be incented to provide non P/P data, but the overall quality of the data would probably be lower.

Publication / Disclosure & Abuse Complaints
No legitimate provider should have any interest in knowingly or through their own negligence allowing for abuse of the DNS.
The DNS is a precious resource that empowers millions of individuals and businesses worldwide and any attack on its stability or trust should be repelled where possible.

Registrars, hosting providers and other service providers should respond to valid abuse complaints. (I discussed the concept of a "good" abuse complaint in a recent blog post here: http://blog.blacknight.com/what-makes-a-good-abuse-report.html )
However, there is a big difference between responding to a complaint and taking any punitive action or breaching a client's privacy.

Intellectual property owners and their advocates are stakeholders, but their wishes and desires should not trump due process or local law.
As stated previously, Blacknight is an Irish company and we are bound by Irish and EU law. ICANN policies cannot take precedence over local law. So any policy that would require us to divulge our client's information in the absence of either a request from law enforcement, Irish consumer protection agencies or a court order with jurisdiction over us is incompatible with Irish law.

Law Enforcement Requests
A valid law enforcement request would need to be processed by the Irish law enforcement authorities – An Garda Síochána. Blacknight is a member of the ISP Association of Ireland (ISPAI – http://www.ispai.ie) and supports the Irish Hotline (http://www.hotline.ie/) . As part of our membership of ISPAI we have agreed to voluntary self-regulation and will act on requests presented by Irish law enforcement that follow the agreed process and have registered a point of contact with An Garda Síochána to facilitate this.

While we are sympathetic to the issues that law enforcement agencies may face when dealing with cross-jurisdictional issues, it is not up to us to resolve these matters. Such issues need to be dealt with by governments.

We would, however, suggest that the Working Group look to established policies around disclosure that are already used by some country code managers, such as CIRA, who run the Canadian (.ca) country code. In the case of CIRA they have their policy as outlined in "Request for Disclosure of Registrant Information for Law Enforcement and National Security Agencies - Rules and Procedures"
(http://cira.ca/sites/default/files/attachment/policies/disclosurelaw_-en.pdf)

Other comments have been submitted by various industry colleagues that cover other aspects of the report, and we are broadly supportive of their stance. One, however, stands out, namely Mark Jeftovic from EasyDNS: http://forum.icann.org/lists/comments-ppsai-initial-05may15/msg11144.html