Perception

Winter 2018

Com Laude

In this issue

Unlocking WHOIS post-GDPR

Also:

- Impacts of the Temporary Specification for WHOIS on domain infringement
- The journey to round 2
- Domain Industry News

Hello

Welcome to the latest Com Laude newsletter, where we share the latest developments and news from around the domain industry. This is the first newsletter featuring our new brand, which we were proud to launch earlier in the autumn.

In this issue we start with an examination of what's happened to the WHOIS now that GDPR and ICANN's Temporary Specification have come into effect. We then take a closer look at the impacts on brands who want to take action against domain infringement activity. We also look at the specific challenges that are presented in UDRP cases.

Although you might feel that you have only just recovered from the arrival of the new gTLDs, it was actually six years ago, in 2012, that the Application window opened. Now the Sub Pro Working Group of ICANN – the team planning what Round Two will look like – has reached a critical moment in its work. We report on the major issues for brands and the possible launch date.

In our look at the latest industry news we hear how some brands are eschewing platforms such as Facebook in the wake of data scandals and we conclude with a brief look at the latest on the impacts of Brexit for .eu domain name holders.

We hope you enjoy the newsletter and look forward to hearing from you if you have comments or questions. Please email: nick.wood@comlaude.com

Nick Wood and Lorna Gradden

WHOIS after GDPR – the story goes on

Unable to agree a method to make the full WHOIS database compliant with the General Data Protection Regulation (GDPR), most contact data for domain name registrants began to be redacted from 25 May 2018, leading to IP practitioners seeking alternative solutions for identifying infringers.

As we reported in our special GDPR Newsletter in May, ICANN created the Temporary Specification for gTLD Registration Data, which permitted registries and registrars to mask the majority of the contact data for many domain name registrants.

The Temporary Specification sets the rules for how registry operators and registrars should collect and display registrant data post-GDPR, for a maximum of one year. It specifies that the name, email address and physical/ postal address of the registrant should be hidden from public display. Only the country/region has to be shown.

Then, in June ICANN stakeholders gathered together and, acting within the Bylaws under mandate from the GNSO, created an EPDP - Expedited Policy Development Process – with the aim of establishing permanent Consensus Policy. It features 31 representatives from all sides of the privacy and IP protection debate – IP and Business interests are balanced against Contracted Parties (Registries and Registrars), with representatives of Civil Society somewhere in-between – the group meets twice a week by telephone. An insider has told us they receive over 100 emails a day.

The impact of GDPR on WHOIS records – and therefore brand owners and their advisers – understandably took centre stage at the 62nd Public Meeting of ICANN, held in Panama City in June and again at ICANN 63 in October in Barcelona.

Even as the EPDP team gathered together in robust debate, forces behind the scenes were attempting to step around ICANN. A group of internet security and consumer safety organisations launched the Coalition for a Secure and Transparent Internet (CSTI) with the aim of saving "a critical tool that protects internet users and consumers: WHOIS data."

We can't confirm it, but we believe CSTI are the driving force behind proposed legislation in the USA designed to bring back WHOIS. Called the Transparent, Open and Secure Internet Act of 2018 (TOSI), it would require registries and registrars to publish full WHOIS information, as if GDPR had never happened. Furthermore, failing to maintain accurate up to date WHOIS would be an "unfair or deceptive act or practice".

Could this ‘temporary’ solution become permanent?

While the Temporary Specification bought some much-needed time by demonstrating to the European data protection authorities that ICANN was working as a community to find solutions, the mandated maximum 12-month duration for such measures imposes a heavy burden on the EPDP working group. There remains plenty that still needs to be agreed, particularly on the difficult question of access.

The working group published its initial report on 21 November 2018 and opened it up for public comment. The Initial Report responds to the call to answer a set of questions and determine if the Temporary Specification for gTLD Registration Data should become a General Data Protection Regulation (GDPR)-compliant ICANN Consensus Policy as is, or one with modifications.

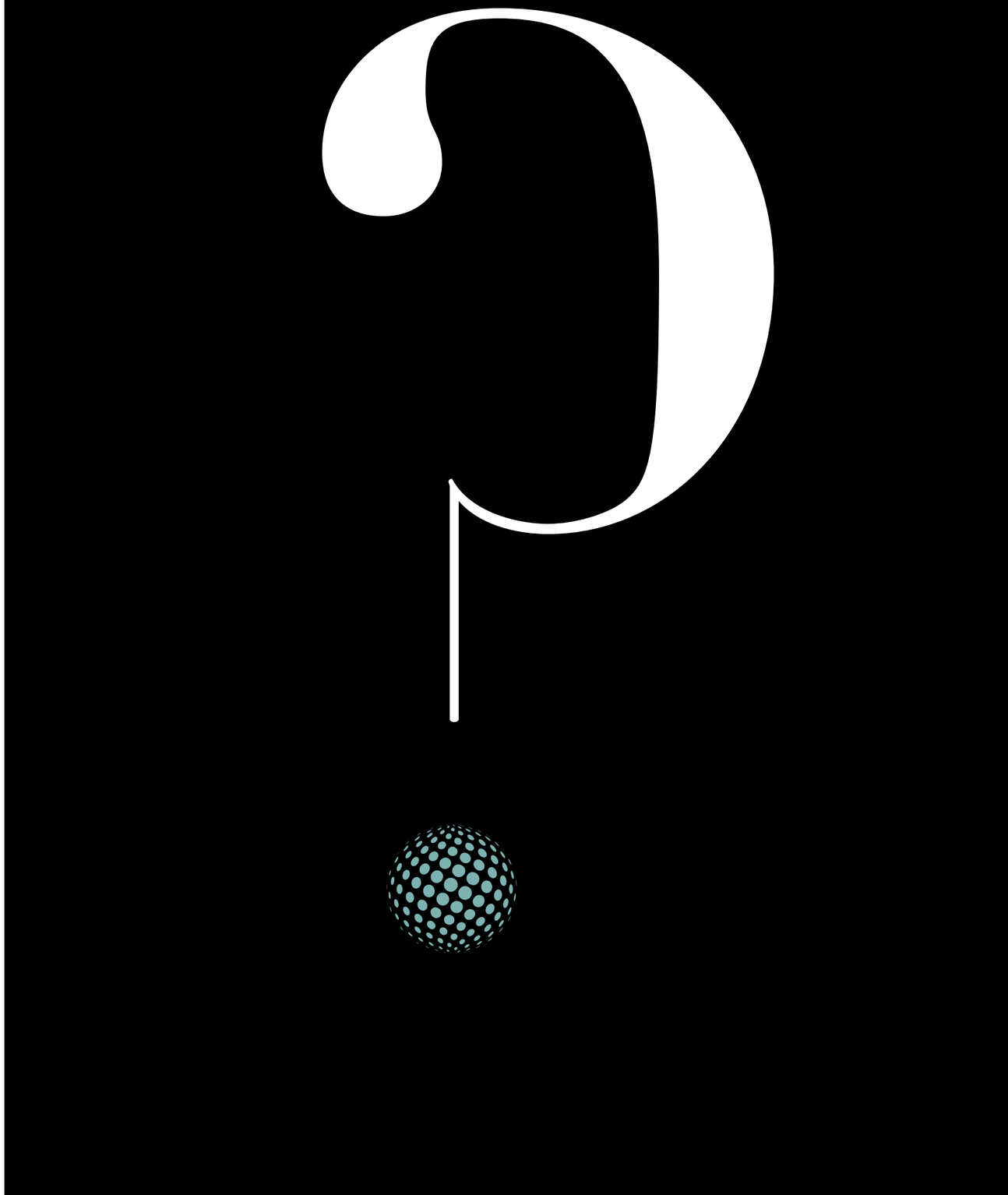
The EPDP working group have been working tirelessly in face of tremendous time pressures, outside scrutiny and entrenched opinions. This initial report is very welcome, but is still the first stage of a long and arduous process. The Temp Spec expires on 25 May 2019. Consensus on key matters has to be achieved in order for ICANN’s GNSO policy making body to make a recommendation to the Board. The divisive nature of some of the discussions so far does not make consensus a foregone conclusion. The registries and registrars are ranged to the left, seeking to limit their exposure and be compliant with whatever local interpretation of GDPR their courts apply; civil society representatives want very strong privacy to protect netizens; brand and law enforcement representatives argue that timely access to accurate information is essential to protect consumers and brand values; and Governments speak from both sides of their mouths – they want their citizens’ data to be nurtured whilst their agencies have unfettered access.

Many of the difficult issues remain to be decided after the public feedback has been received, including whether there can or should be a distinction made between the treatment of registrants depending on their geographic location, and whether the (optional) organisation field should remain open or whether the risk that some registrants may have included personal data in this field warrants requiring it to also be redacted. There is also little to please trademark owners yet. Whilst there is a recommendation to keep the Temp Spec’s existing “reasonable access” obligations in place, the lack of criteria or guidance on what is reasonable has led to fragmented handling, which has hampered access, in practice, to the WHOIS information vital to enforcing against abusive registrations; and brand owners must wait for the next stage of the EPDP’s work to conclude before we know how this will be addressed.

We are not optimistic on access, and hope that ICANN itself might help discussions along by creating and operating a universal WHOIS so at least the process of accessing data is simpler for trademark owners, law enforcement and others who have a legitimate need for accurate registrant information in a timely fashion. In Barcelona, the contracted parties expressed their cautious support for this notion, and ICANN staff seemed to be in favour of exploring further, but recent correspondence to the EPDP working group on identifying controllership suggests that ICANN Org may not be willing to assume this level of potential liability. At best, ICANN Org seems to be considering operating a centralised mechanism for handling data requests, but this is still at an early stage.

To read the full report and comment, please see:

https://www.icann.org/public-comments/epdp-gtld-registration-data-specs-initial-2018-11-21-en



Impacts of the Temporary Specification for WHOIS on domain infringement

"Our domain data has been stolen for years"

It was predicted that the removal of the data from the WHOIS as required by the Temporary Specification would have a very negative impact on brand enforcement. Brand owners and the IP practitioners working with them have enjoyed ready access to up-to-date WHOIS records for nearly 20 years.

Search and watch companies have provided bulk lookups and historical registration data. Many lawyers became expert at reading between the lines of abusive registration records, looking for connections that the fraudsters, the counterfeiters and other bad guys failed to hide. When a false or incomplete address, or a discontinued phone number closed off a line of enquiry, a common set of servers or an email address might open a way forward. Law enforcement agencies and security-threat monitoring companies commonly started their investigations with a WHOIS lookup, before cross-matching to other data points to uncover a pattern or infringing activity.

At first, despite the dire warnings, it didn't seem that bad. Sites offering historical WHOIS data flourished and the European ccTLDs still served up data, though only after validating the legitimacy of the access request. Then a cold wind blew. At the ICANN meeting in June in Panama Elliot Noss, President of Tucows, one of the world's largest registrars, declared to a packed meeting on GDPR that "Our domain data has been stolen for years". He continued, "Access to our customers' data, which we have collated and nurtured for years, is not going to be given away for free ever again".

By the end of August, WHOIS data was drying up. Where a quick free WHOIS look up once sufficed, now records were diminished, revealing very little. Lobbied from all angles, ICANN realised that something had to be done.

The answers to many questions remain unclear: Will the EPDP ever get registrars, registries, civil libertarians and IP and security factions to agree on an access model? Will the Temporary Specification simply become permanent by default? Will TOSI pass the scrutiny of Congress? While we wait to see what happens next, here are our tips of how to cope without full WHOIS:

1 Investigate the source

While it will require additional internal and external resources, it is still possible to find registrant data via analysis of a website's IP (Internet Protocol) address. Such analysis will also help to identify the true location of the website which may be different to the region listed in the WHOIS record and whether the IP address has been blacklist-ed for spam or phishing.

It is also worth checking domain name servers against the data still held on WHOIS (e.g. registrar, registration date) to identify inconsistencies, patterns or repeat offenders.

If you are enquiring about a corporate registration as opposed to a registration made by an individual, remember that ICANN's Temporary Specification still requires the name of the legal entity to be displayed, where this has been included in the WHOIS record.

To track an IP address, try tools such as ip-tracker.org and solarwinds.com

2 Identify the infringer

If you have legitimate grounds for concern, you will be in a position to request the data that has been masked in WHOIS. ICANN's Temporary Specification requires registry operators and registrars to grant access to non-public WHOIS information on the basis of 'legitimate interests', except where they may be overridden by the fundamental rights of the data subject. There is uncertainty about what this will mean in practice: for example, how will registrars assess if the registrant's fundamental rights override the request? However if you are able to show that the registrant is clearly committing illegal or infringing activity, then the registrar should fulfil your request. If it does not, it will be in breach of ICANN's Temporary Specification.

In the short term, answers may also be found in copies of historical WHOIS data (as hosted by a number of brand-monitoring companies). Domaintools.com is not a bad place to start, though a Washington court has told it to remove all the New Zealand records it owns after the New Zealand Domain Name Commissioner brought an action against them for unlawfully harvesting .nz domains.

If neither of the above solutions work, then you will have to consider the cost vs. the value of legal action in order to identify the infringer.

3 Enforce your rights

Here, the same channels for stamping out infringement or abuse are at your disposal as pre-GDPR; for example, pursuing the registrant for redress through the registries, hosting providers or ISPs, or choosing to file a Uniform Domain Name Dispute Resolution Policy (UDRP), Uniform Rapid Suspension (URS) or similar complaint (for more on this, see page 8).

Don't forget that registrants can also be contacted 'directly', as the Temporary Specification requires the public WHOIS to include an anonymised email address or web form to enable such contact. You may get lucky and the registrant might respond, although there is no mechanism in place to ensure or track a response.

Contacting the registrar through its abuse contact email address should work in theory but in practice registrars are developing their policies and processes in response to such requests. Under the Registrar Accreditation Agreement they have with ICANN, they are obliged to take reasonable and prompt steps to investigate and respond to reports of illegal activity and abuse. The problem is that absent clarification from ICANN, "reasonable" and "prompt" are terms open to interpretation.

The uncertainty around permitted access to registrant WHOIS data certainly adds an extra challenge to filing a case under the Uniform Domain Name Dispute Resolution Policy (UDRP). Fortunately, WIPO has issued guidance on how it expects the UDRP to work procedurally moving forward.

The UDRP has been in existence for nearly 20 years, during which time it has provided brand owners with a quick and cost-effective route to address bad faith registration of domain names, rather than having to resort to the courts. The procedure applies to all gTLDs (as well as a number of ccTLDs which have voluntarily adopted the UDRP, or a variation of it).

GDPR+UDRP

Background: pre-GDPR
The UDRP requires the complainant to prove three elements:

i) The domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights;
ii)The registrant has no rights or legitimate interest in the domain name; and
iii) The domain name has been registered and used in bad faith

Clearly, if you don't know who the registrant of a domain name is, then you are going to have more difficulty establishing elements ii) and iii).

You are also potentially going into any complaint blind of the defences that the registrant might be able to raise, and which, if you were aware of them, might cause you to conclude:
– that the domain registration is not of concern after all; or
– that this is not a case for which the URS or UDRP is going to be appropriate.

For example, the registrant might have a very good "nickname" defence.

Substantive challenges have become much harder. Although the procedures and associated rules are not exhaustive on how you establish a lack of rights, legitimate interest and bad faith, there are some specific areas where the loss of access to the WHOIS data is having a negative impact:

For example, it is now much harder for a complainant to show a pattern of bad faith/abusive registrations. If you can demonstrate such a pattern, it is strong evidence of bad faith, but if you do not have registrant details you cannot make connections across multiple registered domains to build evidence.

There are also procedural difficulties where the UDRP either expressly or implicitly relies on WHOIS records for the conduct of the case. The rules permit complaints to be brought against multiple domain names, where registered by the same domain name holder (UDRP Rules 3(c)). However, the complainant will not necessarily have the information to determine the value of consolidation, resulting in increased cost for separate actions and the likelihood that some of them may not be sufficiently egregious to justify the resources involved.

Post-GDPR: WIPO responds WIPO's Brian Beckham, Head of the Internet Dispute Resolution Section, has issued guidance to allay such concerns. In an 'informal' Q&A on the GDPR's relation to the UDRP he sprinkles his wisdom to bring clarity:

– In principle brand owners' ability to file a UDRP case should not be foreclosed by the GDPR;
– As with cases filed previously against a WHOIS privacy/proxy service, if a UDRP complaint contains all available registrant information (even if 'Name Redacted'), then such a complaint would be accepted by WIPO for processing and compliance review;
– Once a UDRP complaint has been filed, WIPO expects to be provided with WHOIS data on the registrant by ICANN-compliant registrars (as required by ICANN's Temporary Specification);
– In order to give effect to the UDRP, complainants in pending UDRP proceedings can expect to receive registrar-confirmed WHOIS data, so as to make substantive and/or procedural amendments to its complaint, given that UDRP providers have a reasonable and legitimate reason to provide this (this is already an accepted practice where privacy/proxy services are named as respondents);
– The provision of such data may also serve to facilitate party settlements (WIPO reports that roughly 20% of cases filed with them settle prior to panel appointment, saving the parties time and money);
– If the relayed information results in withdrawal of the UDRP complaint (e.g. the registrant is the brand owner's own licensee or employee, or if the identification of the registrant indicates that they do have a right or legitimate interest to the name after all), WIPO will refund the unused panel fee, as has been the case if the parties settled before a panel was appointed;
– ICANN's Temporary Specification identifies for future action, the need to develop "methods to provide potential URS and UDRP complainants with sufficient access to Registration Data to support good-faith filings of complaints";
– Separate from WIPO's UDRP provider function, WIPO is involved in stakeholder discussions on a possible Unified Access Model, including a potential role to certify IP owners' rights for such access.

The journey to round 2

What can brand owners expect next from ICANN's new gTLD process? After three years of work by over 180 people, the Subsequent Procedures Working Group has finally completed its review of Round One, which back in 2012 brought us 1936 applications for new registries. Although only 1200 survived conflicts or evaluation to get to launch, their impact on brand owners was significant. Registrations to communicate or defend, Sunrise Schemes, Premium Names and the Trade Mark Clearing House – there was pressure on budgets, teams and strategies.

The aim of the SubPro Development Working Group was to make recommendations on the detail in the Round One Applicant Guide Book including the rules of eligibility, the application process, timing and costs. We were pleased when our SVP for the USA, Jeff Neuman, was selected as co-chair of the Working Group because we wanted to ensure that the disruption and expense of Round One for brands was minimised in Round Two. After a first report was published in the summer, a Supplemental Report was released in November and is open for comment until 12 December.

We have summarised key issues and solutions of particular relevance for those brands who might be interested in applying in the future and all those who want a predictable, transparent process.

Application Process
Although larger brands can cope with a first come, first served permanently open application process, we prefer a permanently open application system with predictable rounds. For example, this might feature a three-month window of application in any year followed by a nine month closed period before the window opens again. We believe that all applications submitted in the open window should be treated equally (e.g. not on a first come first served basis). We think this offers all brands, large and small as well as governments and members of civil society the best opportunity to monitor applications.

Processing & Categorising Applications
We believe that there should be a uniform application process for all, to maintain fairness and because business models change over time. However, within this uniform process each applicant should be directed down a path which facilitates participation and fair evaluation. Thus a brand applying for a single entity (Closed Brand) registry exclusively for their own purposes – as one third of all Round One applicants did - should not be required to submit all the information that an Open Registry has to (for example on operating budget, directors, Sunrise plans etc).

Closed Generics
We believe it is important that the allocation of a TLD does not distort competition. Having said that, a retailer should be allowed to apply for Dot Retail because application itself is not anti-competitive but it should be required to submit a Public Interest Commitment stating that the TLD will not be used in an anti-competitive manner.

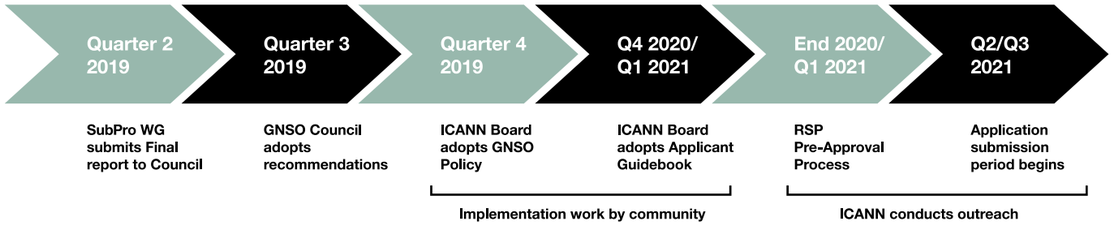
String Similarity
Naturally, we think that that international trademark law should be followed: rights should not be awarded in a TLD that are not available under trademark law though we don't think that the singular and plural of the same string should be allowed.

Objections
It is important that conflicts are resolved with transparent processes. More care needs to be taken in selecting panellists or objectors for Round Two to ensure they are free from conflicts of interest. Objections from Governments must include clearly articulated rationale including the national or international laws they are based upon as well as merit-based public policy reasons. Governments should not have an automatic veto right over applications. To minimise objections, we have championed the idea that all applicants should be given the option of submitting a "Second Choice" alternative string. Where there is an Objection or direct conflict, resolution could thus include abandoning the first choice string and moving to the second choice.

Fees
The new gTLD programme was designed by ICANN to operate on a cost-recovery basis. However, the $185,000 application fee in Round One deterred many interested brand applicants. To enhance brand participation we have suggested that there is a base application fee in the region of $50,000 which all applicants should pay for standard evaluation with supplementary / top up fees paid for more detailed evaluation. Thus the fee for a simple Closed Brand Registry, where the evaluators do not need to review a business plan should be lower than for an Open Registry where there is considerable potential for harm.

What happens next is that the ICANN staff produce a revised SubsPro Report incorporating all comments such as ours. This is submitted to the GNSO (Generic Names Supporting Organisation) where policy is made in ICANN. When they reach agreement it will be passed to the ICANN Board. In light of this process, we believe the timetable to launch is as set out above.

A lot could change. The GNSO could recommend to the Board that there should be a fast-track application round to get things moving or a dedicated round for brands and geographic communities. What is certain, is that another landmark on the road to new gTLDs has been reached.



Industry News

Is Facebook a ‘safe space’ for your business?

Concerns over privacy and fake news is leading some brand owners to close their corporate Facebook accounts.

It had more than 2.2 billion monthly active users as of January 2018, yet reports about Facebook’s approach to personal privacy and tax avoidance, the Cambridge Analytics data scandal, and its lack of action against counterfeiting and fake news are leading many to become disenchanted with the tech company. Brand owners are also turning against the platform citing concerns over data security.

Japanese stationery company Itoya is one such brand owner. Its Facebook account, set up seven years ago, had more than 50K followers; however, following a data leak, the company began to re-evaluate its use of the social networking site.

According to trend.nikkeibp.co.jp, the prevalence of ‘fake news’ in its feed, along with that data leak, led it to decide that Facebook was no longer a trusted or ‘safe’ space for the business. There were just too many people using the platform in bad faith. It wouldn’t want such people in its shops, so why accept them in its online accounts?

Trending on Facebook

Itoya has not written off returning to Facebook if or when it is better policed. Itoya is a well-known brand in the Japanese market and its decision has been high profile enough to prompt enquiries from other companies in Japan considering such a move.

.BRAND or .COM – which ranks better in a Google search?

Concerns over the visibility of .BRAND domains in organic searches has left some businesses investigating how they can completely move away from their .com sites.

Brands that applied in the first new gTLD round did so for a number of reasons: to protect IP, to enhance control and therefore to minimise risk, to support innovation – whatever the reason, it needed to be sufficiently strong to justify $250,000 in application and management fees.

Only a small number, including some not in possession of a .com matching a key brand, planned to move their primary web presence onto a .BRAND. Issues around the practicality of migration from .com to .BRAND whilst maintaining search ranking in Google seemed overwhelming. Web users might “click” on a .BRAND new gTLD, but would they “type” it?

According to SEO expert Bill Hartzer (www.billhartzer.com) all this is changing. Citing the .Tech ngTLD, he claims websites under new TLDs have just as good a chance to rank highly as under .COM. Similarly, ccTLD domain names, such as .UK, .FR and .ES will tend to rank highly in each respective country.

Not just as good, but also potentially better

Now other experts suggest that .BRAND domains are not only as good as traditional gTLDs when it comes to Google rankings, but also potentially better when it comes to maximising SEO.

In an article on MakeWay.World, Matt Dorville, Content and SEO Strategist at Major League Baseball, argued that switching to a .BRAND can actually improve SEO rankings, so long as you take the right approach to link building and keyword targeting.

.BRAND (or ‘vanity’) domain names are, by definition, shorter, customised URLs that are designed to be easy to remember and simple to search for. While vanity URL redirects historically led to a loss of link strength, Dorville argues that changes to the Google search algorithm in 2016, driven in part by the growth in the .BRAND space and the trend towards https use, mean that is no longer the case.

He encourages .BRAND owners to make the most of the marketing and link building potential of vanity URLs within their own domain name extensions.

No-one knows exactly all the factors that go into Google’s search algorithms. What Google have been clear about themselves, is that the choice of Top Level Domain has no positive or negative impact on its own in search ranking. We know that age of domain can play a role and keywords in the domain can also have an impact, but generally they’re both factors that are way down the influence list in comparison to quality of content, frequency of update and quality of backlinks into your site.

At the very least, it’s good to see evidence that there’s little negative impact from an SEO perspective when it comes to new Top Level Domains. What really matters if you’re transitioning to a new domain, be it a .BRAND, a .com or anything else is thorough planning, meticulously mapping your old site to the new one. 301 re-directs will make sure all your amazing content which has supported your search ranking to date can still be found by the Google bots. Simple.

Number of domains rises to over 340m

According to the latest data from Verisign’s domain name industry brief the third quarter of 2018 saw the number of registered domains across all top-level domains (TLDs) rise to 342.4 million, an increase of approximately 11.7m domain name registrations, or 3.5%, compared to the same time in 2017.

Total country-code TLD (ccTLD) domain name registrations were approximately 149.3m at the end of the third quarter of 2018, a decrease of approximately 0.5 million domain name registrations compared to the second quarter of 2018. Nevertheless, this was a rise of approximately 4.6 million year on year.

Total new gTLD domain name registrations were approximately 23.4m at the end of the third quarter of 2018, an increase of approximately 1.6m domain name registrations, or 7.5%, compared to the second quarter of 2018.

We are seeing growth across the board in a number of TLDs after a period of more limited progress. Some of this growth is still driven by cheap domain pricing strategies in territories such as China and some driven by speculation, as well as brands and businesses registering for general use. Of course, number of domains is not the only measure of success of a domain: levels of use, security of the namespace, etc. are other measures to consider, especially when you look at brands who have registered their own top level domains.

.luxe - Blockchain innovation in a new gTLD?

Registry operator Minds + Machines Group Limited (‘MMX’) have announced the launch of their latest new gTLD .LUXE. Initially intended to represent luxury goods and services, MMX have repurposed the TLD to support the blockchain platform Ethereum, using ‘LUXE’ to represent the phrase “Lets yoU eXchange Easily”.

While .luxe domains can be used in the normal way for websites and email addresses, registrants can also link their .luxe domain to their Ethereum account to replace their 40 character ID number to make it easier to remember and use. For example, payments using the Ethereum platform can be made to ‘johnsmith.luxe’, instead of to John Smith’s 40 character ‘wallet number’.

There has been much talk of innovation in the new gTLD space and this would appear to be one of those moves. Will it be a game-changer and take new TLDs to great heights? We’re not so sure, but this certainly feels like it’s the kind of development that has potential to start people thinking more widely about use of domains alongside emerging technology platforms.

Our only concern is an old one: what happens if an Etherium account holder “borrowed” the name of a brand when setting up his or her account? In a closed, private network, no-one could see but if the borrowed name transitions into the DNS as a domain name, there will be problems. We are advising our clients to check the availability of their core brands in the .LUXE Sunrise.

Nominet and Valideus offer end-to-end service for dot brand top-level domains

Valideus and Nominet are offering brands wishing to have their own space online an end-to-end consultancy, application and management service for new top-level domains.

With Round 2 applications expected to open from 2021, it is anticipated that thousands of brands will seek to secure their own domain. This follows steadily increasing activity from the brands that have already secured their TLD in order to enhance security, protect IP and create a platform for innovation. There are over 2,000 active websites using dot brand domains ranging from simple microsites and tailored content to full migrations of a brand’s entire web presence. Big brands from BMW to Sony are making use of their dot brands to signpost genuine content with memorable names.

The new partnership brings together Nominet’s respected registry capabilities (managing a portfolio including .uk, .london, .bbc and .blog) with the brand consultancy expertise of Valideus, responsible for 96% of the Round 1 applications achieving a 100% score.

Nick Wood, managing director of Valideus, said: ‘We are seeing more brands express an interest in having their own space online. But it’s a complicated process that requires delicate handling and attention to detail to ensure smooth passage. If you’re thinking of applying for your dot brand then the time for preparation is now.”

Oli Hope, Director of Registry Services, Nominet, said: “Brands that weren’t in the vanguard of round 1 are beginning to focus on how a dedicated registry will advance their digital strategy. If they don’t make their mark next time round, they risk waiting a decade to get up and running. Working with Valideus, we can offer an end-to-end service that is second to none.”

Update on the impact of Brexit on domains

The European Union has stated that it will not accept registrations of .eu domains from the UK post-Brexit – see here for full details:

https://ec.europa.eu/digital-single-market/en/news/notice-stakeholders-withdrawal-united-kingdom-and-eu-rules-eu-domain-names

However, it does note that there may be transition arrangements made. Eurid the registry operator responded to this saying that it has put a plan in place to deal with this and will review how it operates once the position is finally clear:

https://eurid.eu/en/register-a-eu-domain/brexit-notice/

It should also be noted that Eurid announced in early December 2018 that it will "expand the eligibility criteria surrounding the .eu TLD, as EU citizens will be able to register a .eu domain name regardless of where they reside."

https://eurid.eu/en/news/doteu-tld-new-regulation/

We continue to advocate on behalf of our brand clients as follows:
– A transition period for sunsetting names. 2 years would be a minimum, longer would be preferable;
– Permitting EURid to offer trade mark "blocks" in .eu, whereby a brand owner with a registered UK or European trade mark could pay to block the exact-match term from being registered in future at the second level by third parties in .eu (so, something akin to Donuts' DPML);
– Permitting EURid to offer a matching block as names lapse, i.e. a block on exact matches of existing UK-held .eu names when they terminate/lapse as a result of Brexit;
– Allowing proxies to hold names on behalf of UK registrants.

Verisign take a stance against "domain scalping"

In an interesting move for brand owners Verisign recently published a blog post that took a stronger position than they have taken previously regarding the secondary market for domains:

https://blog.verisign.com/domain-names/how-much-could-businesses-and-consumers-save-if-the-benefit-of-com-price-caps-were-passed-along-to-consumers/

Recently Verisign negotiated a new deal with the US government for the fee it pays for .com domains:

https://www.ntia.doc.gov/press-release/2018/ntia-statement-amendment-35-cooperative-agreement-verisign

The deal allows Verisign to increase its fees each year and this is not liked by many in the domaining community, a view they have expressed via social media platforms and forums.

Verisign has therefore taken this opportunity to talk up how much consumers could save if the secondary market were subject to price caps in a similar way that Verisign is. Commenting, Verisign's representative says: "Recently, some who profit most from the unregulated secondary domain market have been lobbying our government to freeze .com wholesale prices. They say their goal is to protect small businesses and consumers. But their business models and domain resale prices show that their real goal is to preserve the profits they earn from .com price caps. In fact, the real opportunity for consumer savings would come from reducing or eliminating the more than $1 billion per year in scalping fees that businesses and consumers pay today."

United Kingdom
28-30 Little Russell Street
London WC1A 2HN
United Kingdom
T: +44 (0) 20 7421 8250
E: info@comlaude.com

USA
1751 Pinnacle Drive, Suite 600
McLean, VA 22102
United States
T: +1 703 635 7514
E: usa@comlaude.com

1904 3rd Ave, Suite 332
Seattle, WA 98101
United States
T: +1 425 605 3531
E: usa@comlaude.com

Japan
Suite 319, 1-3-21 Shinkawa
Chuo-ku, Tokyo, 104-0033
Japan
T: +81 (0) 3 4578 9368
E: japan@comlaude.com

Spain
Edificio Epoca
Calle Barcas, 2, 2nd floor
46002 Valencia, Spain
T: +34 96 311 4251
E: spain@comlaude.com

www.comlaude.com

Com Laude