# Data compliance

## The conflict between a global internet and local privacy laws is leaving many advertisers confused. Engaging fully with users through a clear social strategy can be helpful

By Chris Swarbrick, ***MPG Media Contacts***

It doesn't really need saying that the internet is a global phenomenon. However, the internet is becoming more of a global phenomenon in many ways, including the growth of content delivery networks (CDNs), cloud computing, and mobile access.

Yet, set against this, is an increasingly intrusive legislative attitude that, by its very nature, is localised in scope.Whether it be the difference in opinion between EU and US on the right to privacy versus freedom of expression, or the variations in national implementation of a regional directive, governments are creating a patchwork of rules around privacy compliance.

Advertisers must be compliant with these rules but the inconsistencies and confusion arising from multiple initiatives leave advertisers uncertain how to proceed. Which laws apply to them? Who enforces these laws? It doesn't help that in many cases, governments themselves seem uncertain as to the answers, leaving advertisers in a limbo.

It's becoming increasingly impossible to compartmentalise the internet by national or regional boundaries.The theory of the internet is relatively simple: a network of machines that are connected and so able to pass data from one device to another.These connections could cross borders, but individual entities are still physically based in one geographic location.

However, the rapid growth of the internet has meant the nature of that network has significantly changed. Functionality has rapidly expanded beyond simple text pages, and by 2015, it is estimated that 20 households will generate the same volume of internet data transfer as the entire world in 1995. It's simply not possible for a single machine (or even group of machines) in one location to meet the demand for data transfer from the modern internet audience.

The result is the CDN (Content Delivery Network): a globally distributed network of servers. By replicating your content on to a CDN, you can allow a local device to meet demand for your data in a given region. Akamai, the largest CDN, handles 20% of the world's internet traffic.

At the same time as companies are using a more disparate internet infrastructure to deliver content, users are leveraging it to store their content in 'the cloud' – storing everything from Google spreadsheets to credit card information all over the world.

Cloud computing is also becoming a business resource, with services such as Amazon's EC2 allowing you to rent server space for just the time required.Across the course of several contracts the physical location you access for your business may jump all over the globe, even though it seems like a local computer to the end user.

Finally, mobile access allows users to take their internet connection with them, across national borders, and the volume of mobile access is growing. Morgan Stanley predicts that, by 2014, mobile internet users will outnumber fixed desk PC users.

These are all welcome developments, as they improve speed, redundancy, and relevancy, but make it almost impossible to relate the internet to national boundaries. Companies still have a legally registered address of course, but if a UK user uploads content to a US owned video hosting site (with servers in 50 different countries), it becomes less clear as to which local law most applies. Just as it is becoming a more difficult question to answer, many governments are passing or considering privacy legislation that will impact internet-based businesses.

Perhaps most controversially, since 26 May 2011,European Union member states require user consent to transfer data to or from a user's machine, but the definition of legal consent can be interpreted by local law. Some require full opt-in, which means that no cookies can be set before active consent is given. Others, such as the UK, only require that users are informed so that they can opt out if they wish (consent is assumed if users choose to ignore this option). As a result, what is legal in one country may not be enough for another and, at the time of writing, many EU governments have yet to confirm what their interpretation of the law will be.

Website operators can take a lowest common denominator approach, so that their site complies with the strictest interpretation of the law, but this may put them at a competitive disadvantage if it creates a negative user experience or means they can't monetise audience data.

It becomes even more of a challenge when legislative desire is in conflict from one region to another.The EU has expressed a desire for users to have the 'right to be forgotten', allowing individuals to remove digital content related to them. It views this as a global right and so non-EU based companies would also need to comply. In the US, however, the indications are that the focus is more on freedom of expression, which would protect the right of individuals to share content even if it included reference to somebody else.

So long as national or regional bodies

continue to consider privacy law within a localised context, not the broader implications for a geographically unrestrained technology network, such conflicts are likely to continue.

## IMPLICATIONS FOR ADVERTISERS

Unfortunately, such conflicts create a confusing framework in which digital advertisers have to operate. Compliance is required, but how to achieve it may be far from obvious.The UK Government has announced a desire to see the UK digital ad industry develop technical solutions to implement the new e-privacy requirements. In theory, this is a great opportunity for the industry to have more control over its destiny but, in practice, it means advertisers must be ready and willing to trial new solutions as they emerge, and accept the learning curve often associated with new technology.

This flexible attitude may also need to extend to definitions of responsibility. In early 2011, Spanish data protection authorities demanded that Google remove links to online articles on grounds that the articles contained out-of-date information, which infringed on the privacy of Spanish citizens. It was not Google-owned content, but Google has to take responsibility for it on the basis that Google provided the access route.

Ultimately, it may take similar legal challenges, and the resulting precedent that is set, to smooth out all the friction points between legal theory and business reality. This is likely to perpetuate uncertainty, as the trial results may force the industry to rethink new practices. Digital advertisers may need to accept procedural uncertainty as a cost of doing business.

## CONCLUSION

It's not all doom and gloom. While it could be viewed as using a sledgehammer to crack a nut, legislation relating to digital marketing has been created in response to some genuine user concerns.

Advertisers who engage with those concerns among their audience, rather than simply complying with the letter of the law, are likely to be rewarded by a more positive acceptance of their advertising.They will also placate governments who might otherwise

consider more extreme measures.A key example of this is the work of the trade bodies in the EU and US to create a self-regulatory framework around behavioural advertising.The European Commission has welcomed this development and the UK government accepts this as part of the solution to implementing the new e-privacy rules.This framework is a pan-European initiative and resembles a similar system in the US. In this way, the industry is creating uniform best practice around particular issues of concern to users.This is easier for businesses to accommodate on a global level, than inconsistent localised legislation.

Similarly, embracing avenues such as social media to monitor and respond to user concerns can help businesses stem such issues before they reach critical mass. Research from Dynamic Logic reveals educating users about marketing technology developments, such as lookalike targeting, and their benefits is likely to placate many of the Big Brother worries that currently exist.

To achieve the above, advertisers should:

- Actively participate in industry trade bodies, read trade news sources, or ensure they are kept up to date by their relevant agencies. Awareness of impending legal changes will allow maximum time for preparation and allow advertisers to roll out a consistent response to industry developments, rather than a rushed response to individual changes in the law.
- Understand how their marketing activities use data (from targeting of digital ads, through onsite data collection of user profiles, to personalising of CRM activities) and ensure this is transparently available, for example, via privacy policies, to site visitors who want to know more about how their data is captured and used.
- Have a clear social strategy in place or seek advice to develop one.This will allow proactive management of social sentiment and an ability to leverage this channel to respond to user concerns.

The conflict between a global internet and local legislation is likely to remain a problem for digital advertisers, creating headaches around implementation and responsibility. However, there is a chance for advertisers to seize the initiative and work towards a more open relationship with their audience.

more on data privacy at www.warc.com



**Fonte: Admap, Washington, v. 46, n. 9, p. 40-41, Nov. 2011.**