ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Border Crossings on the Digital Frontier

Compliance and Ethics

Cross-border compliance is an ongoing challenge for multinational companies. Jurisdictional laws can be as inconsistent as the policies meant to address them. Some companies have taken a “highest common denominator” approach, setting their policies and procedures to comply with the most restrictive set of laws of all the regions in which they operate. Other companies create a patchwork quilt of protocols that meet the standards of the individual jurisdictions in which they work. Still others take a middle ground, setting a standard that complies with the majority of jurisdictions for most of their global operations and then modifying those rules to comply with more restrictive regimes.

As long as we were dealing with just the physical world, we knew where we stood — literally. You were either in France or Germany, Russia or Ukraine, China or Nepal. There was never any question about which laws governed where.

But multinational compliance is much tougher when you are dealing with the virtual world. We obviously recognize when we send an email from Canada to China that the laws of both countries should be considered. But if the data packets that make up that email travel through France and Australia in transit, should the laws of those nations also apply? (Keeping in mind that the way the internet works, you may never know the path taken by the packets being routed.) And if you post a YouTube video in Italy that becomes instantly accessible worldwide, must you worry about the copyright or content laws of every nation in which that video may be accessed, even if people outside Italy weren’t your intended audience?

We are clearly in a period during which we are struggling to align many of our new technological capabilities with established paradigms. Take privacy, for example. Before the modern era, privacy was a relatively simple matter that boiled down to an agreement between obviously relevant parties.

A lender requested confidential information from a borrower in order to make a loan, and the two parties could agree that the borrower would not provide that information unless the lender adequately safeguarded it. Governments would get involved to protect the borrower's right to privacy only in circumstances in which the borrowers were not sophisticated enough, or did not have enough bargaining power, to insist that, for example, information would not be sold by the lender to third parties.

Or, when a consumer went to a pharmacy to purchase medicine to treat a sexually transmitted infection, or STI, only the pharmacist would know and keep any record of the transaction. Regulations only needed to address the narrow situation in which the pharmacist might have intended to share that information in a way the consumer might not have anticipated or wanted.

These kinds of situations gave rise to the traditional "notice-and-choice" model of privacy protections such as those embodied in the US Fair Information Practices from the 1970s. In general, the idea was that consumers would be adequately protected if they knew what information would be collected and why. This vision of informed, empowered, and decisive consumers was the bedrock of most traditional privacy policies.

Modern technology and our cultural attitudes to them now undermine that approach. First, it is difficult to mandate what constitutes effective disclosure in the complicated context of new online relationships such as social media platforms. Since most social media platforms make their money by selling user information to advertisers and others, their privacy policies try to reserve as much latitude as possible to use the information. This means not only taking a kitchen sink approach (everything including the kitchen sink) but also phrasing things ambiguously enough that they don't scare the users away. And, of course, they can and do rely on the fact that few users read through privacy policies or truly understand the complicated opt-out provisions.

Second, most consumers are not sophisticated enough to understand the implications of what they are agreeing to — even if it is clearly explained. Do most consumers really understand that researching STI symptoms online could result in directed advertising of pharmaceutical treatments and affect a pending workers' compensation claim?

Third, in the modern era of data analytics and tracking, it isn't even clear when a privacy notice should be required. If aggregators collect data from across a number of different sites that enable them to know that particular consumers are in the market for a car, or might need a loan, or have developed cancer, or are pregnant, or are facing financial hardship, should those aggregators (who most people don't even know exist) need the permission of the consumers involved? And how would they obtain it? ("Hi, you don't know me, but I would like to use tracking information you don't even know exists to sell your confidential information to others you don't know exist.")

And whereas the traditional model had obvious counterparts with straightforward obligations, the digital world leaves things much less clear. When a user receives an ad for skin treatment — not based on what they have posted on their own Facebook profile — but instead based on a photo posted by a friend (thanks to facial recognition software), who should be responsible for having "disclosed" that "confidential information"?

These problems suggest that we need to develop a new paradigm to address digital privacy issues. One interesting proposal relies on the idea that consumers trust that their privacy won't be abused. That trust should be considered a shared type of limited resource. Users and platforms would treat this pool of trust as a kind of digital "commons" similar to those for hunting and fishing, wherein the

users either agree, or are regulated, to prevent overusing the common resource and causing it to collapse. Similarly, a willingness to share private information is based on trust between the sharer and the recipient. If that trust is abused to the point of collapse, things like our current social media models would also collapse, similar to the overfishing model. Since both users and platforms have incentives to maintain a certain level of trust in the idea that privacy will not be abused, and since abuse could quickly cause that trust to collapse, treating it as a limited resource under the "commons" model may make sense.

In any event, these kinds of thorny complexities also pervade the application of traditional laws to other areas — such as IP protections and government censorship — in our brave new digital world.

Just look at the current controversy surrounding Article 13 of the EU Copyright Directive in the Digital Single Market. The directive is designed to limit how copyrighted content is shared online. In a time when copyright violators (who can hide their identities behind a pseudonym or inside a dark-web labyrinth) and hosting platforms both stand to make millions from casual infringement, it certainly makes some sense to hold the party who controls the platform liable. But many people have objected to Article 13 because that approach favors established platforms over smaller ones (since only the larger ones may have the wherewithal to pay for automated or human-enabled review systems). It may result in a form of censorship that limits appropriate creative expression.

Furthermore, what constituted copyright infringement used to be fairly clear. In the digital era, the copyright situation is murkier. Is hyperlinking infringement or attribution? What, in Article 11 terms, constitutes a permissible versus an impermissible "snippet"? When should an internet meme that references copyrighted material be considered an infringement? These and many more tough questions pervade digital infringement analysis. And what this shows, once again, is that traditional legal IP paradigms may have to be revised to extend to the virtual world. Traditional laws regarding governmental authority to police and protect is another area of complexity. In their attempts to ensure that their citizens do not access content that is illegal (or objectionable) in their own jurisdictions, China, Russia, and a number of other nations have attempted to prevent their own citizens from gaining full access to the standard version of the "World Wide Web." This has resulted not only in a worrisome fragmentation process but also in types of information discrimination that make many of us feel uncomfortable. As one scholar writes:

> The Internet is at a crossroads. Today it is generally open, interoperable and unified. Tomorrow, however, we may see an entirely different Internet, one not characterized by openness and global reach, but by restrictions, blockages and cleavages.
>
> Jonah Force Hill, Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers, John F. Kennedy School of Government, Harvard University Spring 2012.

As lawyers representing our companies on this digital frontier, we have an obligation to counsel our clients on how best to comply with the myriad complexities of their digital border crossings. We also have an obligation to help influence governments and trade partners to develop new legal paradigms that properly address the concerns that changes in technology are rapidly causing so that we can preserve the many benefits of the technologies, while still protecting the legal standards that matter to us.

Further Reading

Greg Stern

Former Global Integration Counsel

Chubb, Independent Consultant