Patents and the Internet

Guest Post by Professor Marketa Trimble (UNLV) (also posted at this blog).

Imagine that someone had a patent on the internet and only those who had a license from the patent holder could, for example, do business on the internet. This internet patent would not need to concern the internet protocol, the domain name system, or any other technical features of the network; the patent could, in fact, cover something else – a technology that everyone, or almost everyone, who wants to do business on the internet needs, a technology that is not, however, a technical standard. There might be one such patent application – the patent application discussed below – that could be approaching this scenario.

We must accept, however reluctantly, that activities on the internet will not be governed by a single internet-specific legal regime or by the legal regime of a single country. Although countries might agree on an internet-specific regime for the technical features of the internet, and might even adopt some uniform laws, countries want to maintain some of their country-specific national laws. People and nations around the world are different, and they will always have diverse views on a variety of matters – for example, online gambling. Online gambling might be completely acceptable in some countries, completely unacceptable in others, or somewhere in between; likewise, countries have different understandings of privacy and requirements for the protection of personal data. Therefore, countries now have and likely always will have different national laws on online gambling and different national laws on privacy and personal data protection. Compliance with multiple countries' laws regarding the internet is nonnegotiable, certainly for those private parties who wish to conduct their activities on the internet transnationally and legally. Nevertheless, in practice and for some matters, the number of countries whose laws are likely to be raised against an actor on the internet may be limited, as I discussed recently.

For some time the major excuse for noncompliance with the laws of multiple countries on the internet was the ubiquitousness of the network. The network's technical characteristics seemed to make it impossible for actors to both limit their activity on the internet territorially, and also to identify with a sufficient degree of reliability the location of parties and events on the internet, such as customers and their place of consumption. However, as geolocation and

geoblocking tools developed, location identification and territorial limitation of access became feasible. Of course the increase in the use of geolocation tools generated more interest in the evasion of geolocation, and increased evasion has prompted even further improvements of the tools. The argument that we cannot limit or target our activity territorially because we don't know where our content is accessed or consumed no longer seems valid. (Also – at least in some countries – courts and agencies have permitted internet actors to employ low-tech solutions as sufficient territorial barriers, for example, disclaimers and specific language versions.)

The multiplicity of applicable laws that originate in different countries and apply to activities on the internet is more troubling in some areas of law than in others. One area of law that permeates most internet activity is data privacy and personal data protection. Any internet actor who has customers and users (and therefore probably has user and traffic analytics) will likely encounter national data protection laws, which vary country-by-country (even in the EU countries, which have harmonized their personal data protection laws, national implementing regulations may impose country-specific obligations). Therefore, compliance with the varying national data protection laws will become one of the essential components of conducting business and other activities transnationally. If someone could patent a method for complying simultaneously with multiple countries' data privacy laws on the internet and claim the method broadly enough to cover all possible methods of achieving compliance with the national privacy laws, that patent owner might just as well own a patent on the internet, or at least on a very large percentage of internet activity.

A U.S. patent application that seeks a patent on simultaneous compliance with multiple countries' data privacy laws on the internet through broad method claims is application No. 14/266,525, which concerns "Systems and Methods of Automated Compliance with Data Privacy Laws," meaning "laws of varying jurisdictions" (the title and the "Abstract"). The invention is designed to facilitate an automatic method of complying with the data privacy laws of various jurisdictions, which are, as the "Introduction" notes, "complicated, diverse, and jurisdiction specific." The method envisions that once "person-related data" are requested from a data provider, a "filter is the [*sic*] automatically applied to the person-related data to restrict transfer of person-related data [that] does [*sic*] not meet the data privacy regulations applicable to the jurisdiction" (the

"Introduction"); the filter also checks for any consents by the data subject if the particular regulations require them. The method also foresees, for example, the possibility of "identif[ying] different origins of the person-related data sources" in terms of their geographical location ("Trust Object and Trust Data").

The patent application still must be prosecuted, and the – undeniably useful – invention will be subject to scrutiny as to its compliance with the requirements of statutory subject matter, novelty, and non-obviousness. A patent on the application may not issue at all, or the language of the application may be amended and the claims narrowed. Whatever the future might bring for the claimed invention, this patent application serves as a useful prompt for thinking about the components that have been or are becoming essential to conducting business and other activities on the internet.