THE IJLT FEED

A monthly law and technology newsletter with perspectives from India

JANUARY, 2013

Access to Knowledge

The Aaron Swartz Case and Indian law on hacking

Possibly the most talked about development in early 2013 was the suicide of 26 year old Aaron Swartz, a renowned activist in the areas of copyright policy and technology freedom. Swartz, founded the popular internet content aggregation website Reddit and was a Fellow at the Harvard Centre for Ethics. In 2012, he was charged with violations of the US Computer Fraud and Abuse Act, 1986 and faced criminal actions as a result. Swartz had accessed the computer network of Massachusetts Institute of Technology ("MIT") to download a large volume of files (4.8 million) from JSTOR, a non-profit research database of academic works. MIT allowed guests on its campus to access JSTOR using the University subscription. When JSTOR and MIT attempted to block the automated download, Swartz tried to circumvent these measures by changing the IP and MAC address on his computer. Crucially, JSTOR did *not* wish to press charges against Swartz, and was satisfied with the return of the downloaded files and Swartz' assurance that the files would not be distributed. Nevertheless, the US Attorney's Office arrested and charged Swartz with 13 felony counts, which could mean over 50 years in prison and a fine of $4 million. Swartz' controversial arrest met with immense criticism from public and scholars alike, including Tim Wu and Lawrence Lessig.

While Swartz' actions were presumably motivated by his involvement with the open-access movement, the charges for computer hacking have been termed as "excessive" and "disproportional", particularly since his actions constituted a mere breach of JSTOR's Terms of Service prohibiting automated downloads. Notably, one of the clauses in CFAA used against Swartz was the breach of this user agreement, commonly regarded as a *contractual* breach. Ironically, this statement by the US Attorney evinces the absurdity of this incident: "*Stealing is stealing whether you use a computer command or a crowbar and whether you take documents, data or dollars.*" The Aaron Swartz incident is yet another example of the catastrophic application of an age-old law (enacted prior to the invention of web) to technological innovations. In fact, the proposed amendments to CFAA ("Aaron's Law") exclude terms of service violations from its scope. Changing a computer's hardware address will also not be considered criminal hacking.

In contrast, Indian law against hacking is still in its nascent stages. Section 66, IT Act defines hacking as the *destruction/deletion/alteration of information on a computer; or diminishing the value/utility, or injuriously affecting a computer resource, with an intention to cause, or knowledge of the likelihood of wrongful loss or damage*. Under Sec. 66 read with Sec. 43A, hacking into an institute network is a bailable offence, punishable with a maximum of 3 years and fine of INR 5,00,000. While this may not be stringent enough to deter actual incidents of hacking. in the wake of Swartz' suicide being attributed to the intimidation and prosecutorial overreach in the US, it might be safe to assume that Indian law would not placed the prospect of indefinite jail time in the mind of an 'innocent offender' like Swartz, possibly pushing him to take his own life.

Intellectual Property

Patenting e-commerce Business Methods on the Sly in India and Abroad

Business methods are not patentable in India by virtue of Section 3(k) of the Patents Act, 1970 which excludes "*mathematical or business method or a computer programme per se or algorithms*" from the purview of the term 'inventions'. The Manual of Patent Procedures also states that business methods are not patentable subject matter, irrespective of the form in which the claims are described. This is particularly relevant in the age of the internet with burgeoning e-commerce platforms where patent applications are couched in language that identifies technological aspects of the claim, but are fundamentally a business method in nature. The Manual itself notes that 'claims are at times drafted not directly as business method but apparently with hitherto available technical features such as internet, networks, satellites, telecommunications, etc. The exclusions are carved out for all business methods and, therefore, if in substance the claims relate to business methods, even with the help of technology, they are not considered to be patentable." This position has been upheld in December 2011 by the Intellectual Property Appellate Board (IPAB) in the case of *Yahoo Inc.* v. *Controller of Patents and Rediff*, wherein the patent claim relating to a method for "operating a computer network search apparatus" was rejected.

However, despite this decision in addition to the express statutory prohibition, several patents have been granted in India to claims that clearly seek protection for business methods. For instance, Patent No. 252951 granted to Huawei Technologies protects "a method devised to monitor and manage economic arrears in the field of post-paid telephonic services". This business method solves the problem posed by charging mobile telephone customers for calls made after the call had been completed (post-paid), by devising a method wherein the creditworthiness of the customer can be assessed before the call is put through, thus securing risk assessment prior to the extension of credit by the service operator. Similarly, Patent No. 240258 was granted to Afton Chemical Corporation, partially for a method to enhance the fuel value of used lubricant oil in combination with an unpatentable business method (in this case, a method for the distribution and use of the used lubricant oils).

On the other hand, patent law in the United States of America have been more liberal in the grant of business patents. However, recent episodes of 'patent trolling' have brought this issue to the forefront, particularly from the point of view of innovation. The strategy employed generally involves a Non Practicing

Entity that acquires obscure patents from inventors and proceeds to sue corporations who use similar processes, which incidentally employs a particular business method that is covered by a patent. Unfortunately, the overwhelming majority of these suits never go to trial because defendants are petrified at the prospect of an injunction that will stultify their business for months or even years. As a result, defendants are forced to cave in to the demands of patent trolls and settle for ghastly sums of money to continue using processes that encompass a tiny proportion of the entire business operation.

A significant recent development in this arena is the appellate court decision arrived at on January 22 this year in the patent troll case filed by Soverain against Newegg. Although Soverain had successfully sued several big name companies in the past (for use of the 'online shopping cart' functionality e-commerce operations) Newegg was one of the only corporations to stand up to such claims in court. The US Court of Appeal for the Federal Circuit verdict invalidated three patents relating to the online shopping cart owned by Soverain on the reasoning that merely shifting the realm of operation of the business method to the internet would not make the method 'novel'.

The Newegg triumph has been hailed as a much needed check on the business of patent trolling, which has steadily grown to almost become an acceptable practice that corporations factor into their economic risk assessments. Their ability to hold a large section of the e-commerce industry to ransom by demanding huge settlement payouts in return for not filing infringement claims holds important warning signals for India. With a domestic patent regime that is, by many accounts, already plagued with inefficiency and corruption, the introduction of business methods patents (despite the express prohibition) and the consequent potential for the unchecked growth of patent trolling could seriously damage the Indian economy, especially in the sphere of e-commerce, in which India seeks to make massive strides.

Digital Privacy

Facebook Graph Search and Potentially Dangerous Revelations

Although wiretapping and warrantless user data requests have been in the news recently for the more serious threats they pose to privacy rights of users, a new feature recently announced by Facebook is set to replace these topics as the most controversial privacy rights issue in the near future. Facebook Graph Search is a search functionality being implemented by the social networking company to incorporate social aspects into its search engine. As such, it allows one to access information about a user based on search terms used within Facebook. So for example, a Graph Search by X for 'single females who work in New Delhi and frequent Big Chill restaurant' will return information from other users who've chosen to make this information publicly accessible on Facebook. One must keep in mind that most of this information (sex, occupation, current location and page 'likes') is public by default, unless the user chooses to change his or her privacy settings.

Woodrow Hartzog and Evan Selinger in an open-ed have emphasised the privacy concerns with such a feature by focussing on the many ways in which this feature would 'limit obscurity', thereby encroaching on the privacy of users. They argue that users employ several methods to remain obscure, including using

pseudonyms, changing privacy settings and making only some information publicly available. However, being invisible to search engines is what ensures the greatest sense of obscurity. As data miners begin to utilise this service, *aggregation* of publicly information data is certain to raise privacy concerns.

In the case of Facebook Graph Search, another compromising situation arises when certain information, intended to be accessible only to specific persons in a friend circle, is made retrievable by a stranger specifically seeking out this data. Advocates of internet privacy argue that the distinction between information 'discoverability' and 'accessibility' is a very real one, and is the fulcrum of their tirade against Graph Search.

Before examining the issue from an Indian perspective however, it is useful to theoretically examine the complexity associated with evaluating threats to privacy itself. Although Prosser, in 1960, attempted to categorise tortious privacy hams into a 4-pronged taxonomy, it has been found wanting by the likes of Daniel Solove who identifies new privacy harms in the digital age – a direct externality of the advancements in technology and communication media. Information processing, according to Solove's taxonomy, is a legitimate privacy threat, when there has been improper access to/aggregation of information. It is at this point of determination that the present legal structures in India reveal themselves to be woefully inadequate.

In this regard, it has been proposed by Sunil Abraham of the Centre for Internet and Society (India) that a Privacy Commission, along the lines of the one in the EU, be constituted in India to issue directives to websites such as Facebook. A more specific and intensive dialogue is required to be conducted with privacy stakeholders today, and a specific institution to spearhead this is definitely the need of the hour. It is imperative that this dialogue be dynamic, for privacy harms will only multiply henceforth - which further highlights the need for such a specialised body. Such a Commission will serve the interests of both sides of the market, and ensure that privacy (itself a fluid concept) is respected universally.

Freedom of Speech

Tracking User Data Requests from Around the World

Internet search giant Google's semi-annual Transparency Report reveals an alarming trend towards heightened government surveillance around the world. This includes requests for personal information of user accounts on Google-owned services, including YouTube and Gmail. This report is praiseworthy and particularly useful for privacy activists as it breaks downs the different *types* of requests it receives from the government instead of merely data on the number of requests categorised by country.

While previously, such Transparency Reports have included a section on 'government requests for removal of content from search results', this report does not include such data. On Google's official blog a clarification was issued: "That's because we've decided to release those numbers separately going forward. Stay tuned for that data."

In the latter half of 2012, the total number of requests for user data has increased by a whopping 70% since 2009. What is worse is that most of these requests are *without* the use of court-warrants. For instance, about 68% of the requests sought by the US government in the latter half of 2012 were made under the Electronic Communication Privacy Act. Contrary to what its title suggests, the Act raises serious privacy concerns for internet users, as information related to user data can be obtained by producing a mere subpoena, which circumvents the need for a judicial determination of the case. There is therefore no need for the government to demonstrate a 'probable cause' that the user information is related to a crime under investigation. Many believe that such a warrantless search violates the 4th Amendment guarantee under the US constitution.

The situation in India is equally alarming either as the Indian government ranks second in the list of the most prying governments in the world. Specifically, it has sent 2,431 data requests for 4,106 users in these 6 months. What is commendable though is that despite Google having no legal obligation to protect its users from these requests, it has chosen to act as a buffer and comply with only 66% of these requests.

Cyber Crimes

Getting Inside the Treasure Trove of Big Corporations

Sony Computer Entertainment has been asked to pay a fine totaling around £250,000 for a breach of the Data Protection Act, 1998 operative in the United Kingdom. Interestingly, Sony was held liable because of its failure to use software technology that is up to date and complies with industry standards as required under the Act. The infiltration into Sony's storage systems resulted in the disclosure of personal information of millions of customers, which was viewed by the Information Commissioner's office (recognized under the Act) to be a serious breach of mandated security procedures and systems. The Deputy Commissioner, David Smith emphasized the importance of effective data protection and said, "*If you are responsible for so many payment card details and log-in details then keeping that personal data secure has to be your priority. In this case that just didn't happen".* The penalty comes after the 2011 hack of Sony's PlayStation 3 experienced its biggest ever hack, wherein personal information of roughly 77 million users of Sony's PlayStation network had been compromised. However, the penalty amount is substantial and Sony plans to appeal the decision in court.

Sony's case is a glaring example of how seriously cases relating to data protection are considered in UK and the European Union at large. Unfortunately, such is not the case in India. Recently, a group of Chinese hackers called the 'Evil Shadow Team' hacked into Microsoft's India store stealing the login details (including passwords) of users who had previously shopped at Microsoft's online store. It is alarming to note that in the Microsoft incident, it was revealed that sensitive information such as login details and passwords were stored in unencrypted text files. This would imply that once someone has secured access to such information, he or she would have direct access to personally identifying or sensitive information

without an additional layer of security such as 16 or 32 bit encryption. The primary difficulty lies in the way Indian data protection laws find place in Indian legislation. While standards have been laid down under Section 43A along with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011 the regime is spread across a series of other legislations and regulations, creating a mash of obligations and standards that are sometimes contradictory.

Therefore, while the United Kingdom has dealt with such incidents in a stringent manner, it seems the lessons have still not been learnt in India. Hopefully a comprehensive legislation in the form of a Privacy Act will cover all aspects of data protection and specifically address the privacy concerns of users that have emerged in the cases mentioned above.