The Legislative& Judicial Pursuit of Technology Issues ‹The Areas of Intersection and Closeness›

By: Ameera AlTaan
LLM (Queen Mary, University of London)
Legal Counsel

Introduction:

The technology (Computer Devices, Internet, Smart-phones, music innovations..etc.) had solved many problems of our lives, and the internet now constitutes a transformative and powerful medium for social, commercial, political and cultural life. Nevertheless, it brought with it large-scale problems that had in most cases a dangerous impact when used in illegal ways, whether by willful conduct or by negligence. The illegal ways to use the technology brings negative impact in diminishing the drive and economic incentive.

Therefore, legislative and judicial efforts should be intensified to vitalize the existing laws or to improve and modernized the future implementation of intellectual property rights (IPR) system, commercial competition and monopoly system, confidentiality and freedom of expression and other areas of law.

It is of vital importance to focus on the speech of the American President Barak Obama, where he made it clear that [1] : «our single greatest asset is the innovation and the ingenuity and creativity of the American people.» An open Internet is vital to creativity, free expression, and innovation. A key part of preserving these qualities is ensuring that we have the right legal tools to counter criminal conduct that harms our creators and users (and our country's economic health) in the face of continuous technological advances. It is essential that in doing so, we preserve the openness, privacy, security, and creativity of the Internet and its users".

The current legal and judicial debate among the entrepreneurs reveals kind of frustration with regards to technological and purely technical matters, as they thought that the legal system couldn't protect their sides despite the innovative ideas and devices that they create or that the courts could not cope or adapt with the highly technical arena that needs an experts-dominated insights.

1. -http://www.whitehouse.gov/omb/intellectualproperty/quotes

Ultimately, I donot agree with the saying that the "Law cannot keep track of technology issues" [1] , as the law will be always approaching the technology advancement through the common legal senses that stem from the respected previously-entertained provisions, opinions and jurisprudence.

Even that the technology moves fast, the legal concepts move stably. And even that judges or "justices" -as called in some jurisdictions- themselves are not very technology-savvy; they may have loud and clear arguments.

I hereby would like to mention that, with all my respect to famous entrepreneurs in the current era who stand firmly to accuse the lawmakers of negativity of pursuing the technology matters, I have different opinion, even that I frowns the harsh behavior of law enforcement officers when they catch on alleged violators, and event that some regulatory gaps existed.

To understand the main areas of the subject matter, we hereby needs to go through the below mentioned topics.

Identifying and determining the scope of the problem:

1- Extremely rapid technological change and the slow legislative reform process:

Frankly speaking, it is not the legal arena alone that faces the reaction of the continued rapid advancement of technological change, other scientists, ethnic traditions, ideological viewpoints, and philosophical and religious beliefs are all having different reactions.

Citizens of the world are no longer isolated, as the "open source" movement has extended into the global networking community and broken through the haze of national boundaries [2] . We are all turning together as we face one of the most immediate issues that will affect the future of humanity—the technological advances in biotechnology, nanotechnology, and artificial intelligence.

This means that we need to understand that the innovation could not be initially imagined, predicted or anticipated, especially the emerging aspects and the challenges that may face not the current inhabitants of the earth, but rather may affect the future generations.

1. -http://www.technologyreview.com/view/526401/laws-and-ethics-cant-keep-pace-with-technology/
2. - http://www.natasha.cc/technologicalchange.htm

The developments in computer technology are occurring every day. With every new protocol, product or application that is developed, more doors are opened to computer intrusion and misuse. Most of the time it is not even known that a problem exists until vulnerability is found and exploited.

The other essential part of the problem is that we shall realized that some sort of law needs to be established to offer protection against misuse, and the process begins to develop a law. Laws take time to be formulated, finalized and approved before they go into effect. This however, is a necessary evil, as laws influence our public interest, our environment, economy, education, our families, our health and virtually every aspect of our daily lives, now and for generations to come. To make new laws or change those already on the books, lawmakers follow time-honored constitutional procedures 1 . The slow legislature reform process is sometimes long overdue, sometimes for reasons related to striking a balance between the long-term benefits to the people and protecting the public interest against dishonest or dangerous practices, or for saving the rights of the innocent and legal use that is different than the illegal use, or for reasons of maintaining the minimum safeguards and minimum public safety requirements. These are all justified reasons.

2- The rights that matter:

Most of the rights and freedoms that the technology may keep in danger are:

- Confidentiality and the right to privacy (Misuse of private information) which comes under it the fraudulent use and unauthorized access of devices and other cyber crimes.
- Intellectual Property Rights: (trademarks, copyrights and patent rights)
- Right of establishing businesses: in the negative form of illegal commercial competition and monopoly or engaging in other abusive practices.
- Freedom of expression.
- As we realize the rights that the illegal or defaulted use of technology could affect, it is very important to highlight the:

3- The harm thresholds:

- In case of confidentiality, privacy and other unauthorized access and cybercrimes, we can imagine a large-scale online piracy and hacking.

1. -http://www.sans.org/reading-room/whitepapers/legal/legal-system-ethics-information-security-54

We can also imagine the case of violating the privacy when the law enforcement officers seized and searched the smart phones of a suspect as will explained later on. It is very important to mention that the misuse of information in any manner could lead to wide-scale crimes such as the money laundering and/or for terrorism purposes.

- In case of IPR, we can imagine the illegal willful streaming-based infringement of copyrighted movies, music, and television on the Internet, in another way we can use the phrase of reproduction and distribution of infringing content.
- In case of commercial competition, we can imagine an electronic company that enters the market as a new non-stopping company to disrupt the local market to a large degree.
- In case of freedom of expression, we can imagine a libel case through social media, in which the society keeps asking how it can balance accountability with free speech. Or, as an example, a Facebook user in England for example sues another user in Australia for defamatory comments posted on the site. We can also take in mind the derogatory comments.
- Another important issue is to define the jurisdiction, let us take the above-mentioned brief example, which country has jurisdiction over the case, and which country's laws should be applied: England's, Australia's or those of the United States, where Facebook is based?

4- The Judicial role:

However, despite the legal procedures for enacting a law, the judicial and the Alternative Dispute Resolutions tools are the vital soil and the source that always convince the legislators to face the problems or to minimize the potential risks in a given subject matter.

Here we will shed lights on some examples of the judicial, especially "the courts findings" in USA and UK, with a glance mentioning of the situation in Bahrain.

First: The judicial situation in the United States of America:

A- The case of "Yahoo"[1] and the specification of jurisdiction:

Jurisdiction is a major stumbling block for the legal system when it comes to dealing with computers, networks and their security. In the US, the court must have jurisdiction over the person or the subject matter of a

1. - http://law.justia.com/cases/federal/appellate-courts/F3/433/1199/546158/

lawsuit in order to be able to try it. This works well with the current setup of law enforcement agencies that are very territorial and operate within distinct district, city, county, state or country lines. All of this however, gets thrown out the window when there are no physical boundaries to go by when determining jurisdiction, as is the case when it comes to computer networks and the Internet.

Perhaps no case highlights the confusing thicket of jurisdictional issues on the Web more than the Yahoo imbroglio. The saga began two years ago when two French human rights groups sued Yahoo, arguing that the posting of historical Nazi items on the company's U.S.-based site violated French law prohibiting the display of racist material. A French judge sided with the groups, ordering Yahoo to block French citizens from accessing the site or face steep fines. However, Yahoo turned to the U.S. courts and asked a judge to declare the French law unenforceable here.

Now, the company is facing another set of charges that it, along with former CEO Koogle, violated the country's war crime laws by displaying the items. In perhaps the most curious aspect of the case, the American Yahoo site at issue had no physical presence in France.

B- (Riley v. California) [1] and (United States v. Wurie) [2] and the case of seizing and searching the data and information of suspect's cell-phone:

The Supreme Court, on June 25th, 2014, ruled that it is illegal for cops to search a suspect's cell phone without a warrant. So, it is no longer acceptable for law enforcement to search a phone just because they seized it. The opinion was written by Chief Justice John Roberts, with all nine members of the court signing on. It's the result of two cases — a federal drug and gun case from Massachusetts, and a state gun case from California — where the defendants were charged and convicted based on evidence cops found while searching their phones. One case (Riley v. California) involved a smartphone; the other (United States v. Wurie) involved a search of a flip phone [3]. The Wurie case was based on an arrest in 2007. The first iPhone had just come out, and nearly all cellphone owners had flip phones. TheRiley case was based on a 2009 arrest, when smart phones were a lot more common. Because flip phones can store a lot less data than cellphones, and aren't as likely to interact with external cloud servers to get data, the Court wasn't sure that it should treat

1. - http://wings.buffalo.edu/law/bcls/2014/Team-23-Brief.pdf
2. - http://www.law.cornell.edu/supct/cert/13-212
3. - http://www.vox.com/2014/6/25/5841936/supreme-court-cell-phone-privacy-wurie-riley-roberts-decision-nsa

both cases as the same. So when it heard oral arguments in April (when both sides argued their cases in person), it looked at both cases independently. But in fact, the court decided, both phones had access to digital data that cops shouldn't have unrestricted access to. So today's decision covers both cases, because it uses the same reasoning. The importance of the Supreme Court's decision stems from that the Court itself has had other cases about privacy and technology, and in most cases, the government has said that new technologies aren't that different from old ones — so the old rules for searches and surveillance, which allow law enforcement to do a lot, should still apply. But Today's opinion is one of the first decisions that actually tackled the technology head on. The government argued that the old rules allowing cops to search physical objects applied to cellphones as well, so cops wouldn›t need a warrant. But they also suggested some «fallback options» in case the court wanted to require warrants in some cases but not others. Allowing warrantless searches if it is reasonable to believe it holds evidence relevant to the crime. This is the standard for car searches. But that standard, the court says, would «prove no practical limit at all when it comes to cell phone searches.» There's so much information in a cellphone that any cop could «come up with several reasons» to conduct a search, no matter the crime. Searching only the areas of the phone that could have information about the crime, who the suspect was, or officer safety. The court shot this down for the same reason: that's still a massive amount of data. Getting just information that police would be able to get through other means. The government argued that if, for example, it could just ask the phone company for a record of the suspect's calls, it might as well get them from the phone itself. But the court said, «No, no, it doesn't work that way. You went and got the information directly, and that's different.» That, he says, establishes an important distinction based on how the government can get information. Cops are allowed to search a person's body after they arrest him, and they are allowed to examine any physical items they find. That includes opening things up to see what's inside them: in one of the cases referenced in today's decision, police opened a cigarette pack they'd found in a suspect›s pocket and discovered heroin inside. And police are allowed to search arrestee›s cars under certain circumstances. In all of those cases, the court has decided that searches don't seriously threaten an individual's right to privacy — at least not once he is already been arrested. But today, they declared that the reasoning that makes it okay to open a pack of cigarettes doesn't make it okay to search a cellphone: ***"Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse".***

And because of that, they say, cops need to get a warrant to search a phone in nearly all cases — just like they would have to get a warrant to search a house. The implication is that the court recognizes that today's

technology requires new rules for what people can expect to keep private. The cell phones are different because they can store a lot of information. The court considers a phone with 16 gigabytes of storage space on it (like the iPhone 5c or Samsung Galaxy S4). That is equivalent to «millions of pages of text, thousands of pictures, or hundreds of videos.» And that means that it's possible to reconstruct someone›s entire life just based on data found on the phone: *"The sum of an individual›s private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet"*.

In the court's mind, that's a lot of privacy to give up for not a lot of law enforcement benefit. They often store very personal information. The court compares this to everyone walking around with a diary all the time: *"A decade ago officers might have occasionally stumbled across a highly personal item such as a diary, but today many of the more than 90% of American adults who own cell phones keep on their person a digital record of nearly every aspect of their lives"*.

The court even uses the catchphrase «there's an app for that» to point out how much extra information is on users' phones. They call all this information «the privacies of life.» In fact, the court's language to describe how personal cell-phone data is could be read as a reference: They have access to remote cloud servers that are nowhere near the person under arrest. Even the federal government, which argued in favor of cops being able to search phones, agreed that it wouldn't be okay for cops to access information from cloud servers. But the court points out that cops probably don't know where information is stored just by looking through the phone. When you take all of these together, the court concludes, it's ridiculous to say that cell phones aren't different from other things that could be in someone's pocket: *"The United States asserts that a search of all data stored on a cell phone is «materially indistinguishable» from searches of these sorts of physical items...That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together"*. In fact, the court says, searching a cell phone is even more intrusive than searching a house. And since cops definitely need a warrant before searching a suspect's house, they should have to get one for his phone, too. There was already a loophole that allowed cops to conduct warrantless searches of things that would otherwise require a warrant, if there were «exigent circumstances.» That exception applies to cell-phone searches too. But it has to be determined on a case-by-case basis. Justice Alito did not agree with the whole decision and he wrote a concurrence — he voted with the rest of the court for the criminal defendants over the government, but he wanted to make it clear that his reasoning was slightly different from Chief Justice Roberts›. Basically, Alito thought that the Chief Justice's opinion didn't give enough respect to police officers› need to get evidence about a crime

by searching the suspect. Roberts' opinion said that the reason for officers to search a suspect was to protect their safety and prevent evidence from getting destroyed; Alito thinks that it is also legitimate for the law to allow searches just because of the evidence they provide. But he still agreed that it wasn't reasonable to allow cell phone searches for this reason just because cops can search physical objects. Alito also explicitly called on Congress and state legislatures to make new laws that could guide warrantless cell phone searches. Alito's concurrence calls the Fourth Amendment a «blunt instrument» — he thinks that cell phone searches are too important to 21st-century crime-fighting for the question of regulating them to be left up to the courts.

The above court's ruling means a lot to (Smith v. Maryland) — the case the government uses to justify NSA surveillance. As, after the ruling today, government saying new technologies should be governed by the same Supreme Court decisions as old ones.

C- (American Broadcasting Companies v. Aereo [1]) and the case of violating the copyrights law:

Despite the above well-phrased ruling, it is not surprising me that at the same day the Supreme Court issued its judgment in ***(American Broadcasting Companies v. Aereo [2])*** where it ruled that : the service provided by Aereo, allowing subscribers to view live and time-shifted streams of over-the-air television on Internet-connected devices, violated copyright laws. The Court's decision describes Aereo as not being «simply an equipment provider,» with an «overwhelming likeness to cable companies» that «performs petitioners' works ‹publicly.›» Further, the Court adds that its decision should not discourage the emergence or use of different kinds of technologies.

However, I'm admired that Justices Scalia, Thomas and Alito dissented to the above ruling, writing for the dissenting minority, Scalia quoted from (Sony Corp. of America v. Universal City Studios, Inc.), noting that the broadcasters made similar predictions regarding the VCR. Like the final paragraph in that previous ruling, he stated that the Court should be in no position to make judgments on recently new technologies, and it is instead Congress's job to determine if the copyright laws should be modified to address these issues. It is important to mention that, Justices Antonin Scalia and Clarence Thomas are the most frequent ally, and deep orignalists of laws, despite that the analysts say that Scalia is taking the original public meaning approach and Thomas is taking the original intent approach [3] .

1. - http://www.supremecourt.gov/opinions/13pdf/13-461_l537.pdf
2. - http://www.supremecourt.gov/opinions/13pdf/13-461_l537.pdf
3. - Mark Walsh , The Quiet Man: Once again, experts sound off on Justice's Thomas' silence. ABA Journal, May 2014, Page 20 -21 (The Docket).

It worths mentioning that in August last year Google was fined £13.8m in the US after being found guilty of circumventing security settings on the iPad, iPhone, Mac and Safari browser in order to collect user data for advertising. This is not coming to hinder the technology, it is coming to foster and enhance the rights of the people that stand as threshold that cannot be overcome.

D- (Alice Corporation vs. CLS Bank [1]) : The Patent Trolls[2]:

It is very interesting to read the various views of the US Supreme Court regarding the "Patent Trolls" issues. In June 2014, the Supreme Court upheld the notion that an idea alone can't be patented; deciding unanimously that merely implementing an idea on a computer isn't enough to transform it into a patentable (Tangible) invention. The decision does leave room for patenting specific ways of implementing an idea, but it could prevent some of the most frivolous patent cases from moving forward.

Such cases have become an enormous problem in recent years, particularly in the tech industry. The industry is plagued by an increasing number of "patent trolls," companies that exist solely to force money out of others using patents, and many large companies now spend an enormous amount of time and money defending themselves from patents that should never have been granted in the first place. Legislators and activists have long pushed for new patent laws in an effort to solve this problem, but recent efforts have stalled, and today's court decision can help limit the problem while other bills are penned.

The case in question was *(Alice Corporation vs. CLS 3)*Bank. Alice Corporation, a financial company based in Australia, holds a number of patents for facilitating financial exchanges between two parties by using a computer as a third party. CLS Bank, a foreign currency exchange company, filed a claim that the patents were "invalid, unenforceable, or not infringed," and then Alice countered with a claim that CLS was infringing its patents. The court ruled in favor of CLS, reasoning that third party intermediation is

1. http://www.supremecourt.gov/opinions/13pdf/13-298_7lh8.pdf
2. http://www.wired.com/2014/06/supreme-court-deals-major-blow-to-patent-trolls/
3. JUSTICE THOMAS delivered the opinion of the Court: The patents at issue in this case disclose a computer implemented scheme for mitigating "settlement risk" (i.e., the risk that only one party to a financial transaction will pay what it owes) by using a third-party intermediary. The question presented is whether these claims are patent eligible under 35 U. S. C. §101, or are instead drawn to a patent-ineligible abstract idea. We hold that the claims at issue are drawn to the abstract idea of intermediated settlement, and that merely requiring generic computer implementation fails to transform that abstract idea into a patent-eligible invention. http://www.supremecourt.gov/opinions/13pdf/13-298_7lh8.pdf

a fundamental building block of the economy, and not a novel invention and that "merely requiring generic computer implementation fails to transform that abstract idea into a patent-eligible invention."

The decision is important because many software patent cases are based on ideas rather than implementations, says Julie Samuels, executive director at the public policy think tank and research outfit Engine. "Most of the troll cases involve software patents of dubious quality," she says. "What the Supreme Court did in the Alice vs CLS case is give parties dealing with those various patents a very important tool to fight back by invalidating those patents and, going forward, gives the patent office instruction about what it can and cannot issue patents on."

E- (Cohen V. Google 1): the case of anonymity and immunity in social media:

In August 2008, a user of Blogger.com, a Google subsidiary, created «Skanks in NYC.» The blog assailed Liskula Cohen, 37, a Canadian-born cover girl who has appeared in Vogue and other fashion magazines, by featuring photos of Cohen captioned with derogatory terms. Cohen sued Google to learn the name of the anonymous blogger on the grounds that the post was defamatory and libelous. A New York Supreme Court judge ordered Google to reveal the anonymous blogger's name, and Google complied.

The case provided insight into the debate between the competing values of privacy and free speech.

F- Hosted Web Videos and the Video Privacy Protection Act of 1998:

Websites are facing lawsuits alleging that the information collected and transmitted about viewers of their video content violates the Video Privacy Protection Act (VPPA), a 1988 law originally aimed at prohibiting video rental companies from disclosing the video tape rental records of consumer 2.

The VPPA prohibits a video tape service provider from knowingly disclosing, to any person, personally identifiable information concerning any consumer of the provider without the consumer's informed, written consent. VPPA provides for a private right of action, including statutory damages not less than $2,500 per consumer plus attorneys' fees.

1. http://www.nylslawreview.com/wp-content/uploads/sites/16/2013/11/55-1.Cheverud.pdf
2. http://www.natlawreview.com/article/you-better-watch-out-new-legal-risks-hosted-web-videos

Second: The situation in the Judicial system of the United Kingdom:

A- The "Google Case" "Safari users against Google's secret tracking", the issue of jurisdiction:

The High Court ruled on Thursday 16th Jan 2014 that Google can be sued by a group of Britons over an alleged breach of privacy, despite the company being based in the US and claiming that the case was not serious enough to fall under British jurisdiction. Google faced a group action by users of Apple's Safari browser who were angered by the way their online habits were apparently tracked against their wishes in order to provide targeted advertising, they claim that the company acted contrary to a 2009 amendment to an EU directive which requires consent before cookies are placed on a user's device for advertising purposes. A spokesperson for Google said: "A case almost identical to this one was dismissed in its entirety three months ago in the US. We still don't think that this case meets the standards required in the UK for it to go to trial, and we'll be appealing today's ruling." This case appears to stand to help the UK customers and UK users who used the services provided by European subsidiaries, but for me, the important lesson is to go in depth on the protection of technology and not merely allowing the case to be sued.

However, with regard to the mobile device «smartphone patent wars", Samsung applied to the High Court of Justice, Chancery Division, in Samsung Electronics (UK) Limited & Anr v. Apple Inc., for a declaration that its Galaxy tablets were not too similar to Apple's products. Apple counterclaimed, but Samsung prevailed after a British judge ruled Samsung's Galaxy tablets were not "cool" enough to be confused with Apple's iPad. In July 2012, British judge Birss denied Samsung's motion for an injunction blocking Apple from publicly stating that the Galaxy infringed Apple's design rights, but ordered Apple to publish a disclaimer on Apple's own website and in the media that Samsung did not copy the iPad. The judge stayed the publishing order, however, until Apple's appeal was heard in October 2012. When the case reached the court of appeal, the previous ruling was supported, meaning that Apple is required to publish a disclaimer on Apple's own website and in the media that Samsung did not copy the iPad.

B- The triumph of the TV-Links case and its relationship with the UK's Federation against Copyright Theft Organization (FACT[1])

1. http://torrentfreak.com/busted-tv-show-site-in-limbo-as-authorities-back-off-081121/

(TV-Links), a site which embedded videos from YouTube-like sites, was targeted by the police and the MPAA-funded FACT anti-piracy group.

When news broke that TV-Links.co.uk had been raided by police and admin David Rock arrested, it was met with a certain element of disbelief. TV-Links was not a warez (illegally copied software), but one which linked to videos hosted on sites like YouTube. It carried absolutely zero illicit content. This major detail was not of much concern to the UK's Federation against Copyright Theft (FACT), whose investigation along with Trading Standards later came to involve the police. FACT built a case against the operators of TV-Links, David Rock and site partner David Overton who was raided 5 months later.

David Rock later explained that it would have been an easy task for FACT to track him down, since he never made any attempts at secrecy. "To be honest I didn't really attempt to hide my ID, as under UK Law linking to another site isn't illegal, so I didn't see the need," he told TorrentFreak in a November 2008 interview.

There was confusion as to the basis for the initial raid, with FACT citing "offenses relating to the facilitation of copyright infringement on the Internet" – an offense that doesn't even exist under UK law – with Trading Standards and the police referring to "supplying property with a registered trade mark without permission." After a long wait, the official allegations became conspiracy to defraud and breaches of the Copyright Designs and Patents Act.

More than 2 years of waiting later, in January 2010 the TV-Links case went to court. On the 19th January 2010 the operators of TV-Links – represented by Morgan Rose Solicitors, counsel William Clegg QC and Alex Stein for David Rock, and Ian Bridge for David Overton – raised preliminary points of law and asked for the proceedings to be dismissed.

Judge Ticehurst gave his judgment, announcing that TV-Links had won their case. He ruled in detail for the first time in a Crown Court in relation to Section 17 of the European Commerce Directive 2000, stating that Section 17 indeed applied and afforded TV-Links a complete defense in criminal proceedings in England and Wales for their linking to other web sites. In a nutshell and to coin a familiar phrase, the site was deemed a mere conduit of information. The Judge also ruled that the allegations under the Copyright Designs and Patents Act failed because there was no evidence that TV-Links made available to the public the films and shows they linked to. There is no appeal available to FACT against this ruling. The Judge noted that FACT had not applied the Attorney General's guidelines when deciding to prosecute

the defendants with Conspiracy to Defraud.

C-The partial triumph of FileSoup [1]case and the OiNK[2]:

Two men who ran FileSoup, a site to help users find films to download via BitTorrent, have been found "not guilty".

Stephen Lanning, from Somerset and George Cartledge, from Glasgow reportedly faced charges of conspiracy to infringe copyright, but the Crown Prosecution Service decided not to proceed with a trial to nail the duo after following legal advice, which apparently said the alleged copyright infringements were a civil, not criminal matter.

The men were apparently arrested in August 2009 after police were tipped off by film industry body FACT. Their charges were reportedly for alleged unlawful sharing of a trio of films including X-Men Origins: Wolverine, which was leaked onto file sharing networks in April 2009 ahead of its official release, forcing the FBI to investigate.

Alan Ellis, the administrator of BitTorrent site OiNK was apparently acquitted of conspiracy to defraud by a jury around this time last year, after arguing he simply offered a service a bit like Google and was not responsible if users of his service chose to infringe copyright. Just like FileSoup, OiNK posted links to BitTorrent downloads, but did not directly share music and film files.

Cartledge is solicitor, David Cook, who also represented OiNK, told one newspaper that: *«This case is not a one-off. We have now seen two prosecutions for allegations such as these which were fundamentally flawed. We have persistently worked in exposing the flaws in these cases which have resulted in the absolute failure of both prosecutions.»*

Simon Morgan, managing partner of Morgan Rose Solicitors, of the firm that represented Lanning, reportedly said: *«We are pleased to see that a sensible and appropriate view was ultimately taken by the CPS to offer no evidence in the case. The Court of Appeal has found that cases involving complex issues of copyright law are much more appropriately heard in the civil courts rather than the criminal courts.»*

1. https://torrentfreak.com/court-drops-filesoup-bittorrent-case-administrators-walk-free-110224/
2. http://www.telegraph.co.uk/technology/news/8345801/Prosecutors-drop-piracy-case-against-film-sharing-website.html

D- The mind-boggling case of ACS:Law [1]:

ACS: Law was a United Kingdom law firm specializing in intellectual law.

In January 2011, ACS:Law, acting for its client MediaCAT, attempted to gain judgements against 26 suspected illegal file sharers. The case was heard in the Patents County Court in London by Judge Colin Birss. Shortly after proceedings started, ACS:Law attempted to drop the case. It was also reported that barristers for ACS:Law failed to provide vital documents due to them being «in storage». As the copyright holders were not present in court, Judge Birss was unable to end the case in a «simple» fashion. Judge Birss criticised ACS:Law, saying the case was «mind-boggling».

Through a statement read to court on 24 January 2011, Crossley announced that he was withdrawing from pursuing claims against alleged illegal file sharers, citing criminal attacks and bomb threats as reasons. In response, Judge Colin Birss said «I am not happy. I am getting the impression with every twist and turn since I started looking at these cases that there is a desire to avoid any judicial scrutiny» On 8 February 2011, Judge Birss told ACS:Law that the claims which had been brought to court could not be discontinued without the permission of the copyright holders, and a further hearing was set for 16 March. At this hearing the cases were officially closed. The judge deferred a decision on legal costs, saying: «If ever there was a case with conduct out of the norm it was this one».

Third: In Bahrain:

In the midst of diversity in the ways of perpetrating a crime, deterrent penalty in the law is needed to protect the community from risk. The law should evolve to address the technology-criminal phenomena in the society that pose a threat to stability and security, especially with the evolution of means of communication that facilitated difficulty with regard to the pattern of crime.

In Gulf region including Bahrain, there are some cases of stealing through credit cards or via internet banking account.

In October 2014 [2] , Bahrain issued a new law regarding the Cybercrimes "Information Technology's Crimes Law" (Cyber Crime Law no. 60 of 2014), in this Law, hackers could face up to 10 years behind bars. The new bill carries fines of up to BD100, 000. The penalties include a year imprisonment or BD30, 000 fine for those who gain unauthorized access to computer systems. People who deliberately hack into networks with the purpose of

1. - http://torrentfreak.com/file-sharing-lawyers-to-face-disciplinary-tribunal-100823/
2. - http://www.legalaffairs.gov.bh/AdvancedSearchDetails.aspx?id=71402#.VH64F9KsVZc

destroying them or damaging information will face imprisonment or a fine of BD50, 000, or both. Those who produce pornography or broadcast it using technology and telecommunications will be sentenced up to a year in jail or fined up to BD10, 000, or both depending on the pornographic material associated with the case. However, if the case is related to child pornography then the offender will face two years in jail or BD10,000, or both. The bill will also give the Public Prosecution the power to stop the broadcast of any information on the Internet, hide the information or enter computerized accounts if necessary for an investigation.

However, the Bahraini courts, has few cases regarding to technology issues. Still this area needs to be developed, but at the end, as long as the law has recently emerged, then it had benefited from the international best practices and had anticipated most of the areas of cybercrimes as only one side that relates to technology. It is very important to mention that other laws that maintain other areas such as the intellectual property rights law and the commercial completion law and other rights and freedoms are all maintained through the legislation and the constitution.

Conclusion:

It seems that the new inventions in any country are imposing their existence on the judicial and legislative fields to let the latter cope with this inventions' trend. It seems also that the judges should be malleable to study the changes and their consequences, whether from human rights laws point of view, common law perspectives and civic movements.

The legislatures also need to be not only active in tackling on the critical areas of technology; they should be 'proactive" so that to chase the needed forward-thinking economy. Moreover, the law should have pr-emptive impact with lots of imagination to the scenarios and tactics.

It is clear that some litigated cases, taking the example of IPRs infringements are time and cost-consuming, therefore I admired the European Commission Fifth Monitoring Report of Patent Settlements in the Pharmaceutical Sector [1] , as the patent settlements enable patent-related disputes to be resolved without having to litigate the infringement or the validity.

There is an essential need also to have an analytic legal review of whether the so called professional liability insurance or the all risks policy insurance may serve in reducing the cases of cyber security, competition or IPRs

1. http://www.natlawreview.com/article/eu-commission-publishes-fifth-report-patent-settlements-pharmaceutical-sector

infringements, and if so, to which extent?

I hereby call for the formation of a legislative committee in the parliament whose mission would be to consult with American and European trends as a face of object cooperation in the framework of adopting the best practices in legislation of IPRs, competition and privacy

It is appropriate to suggest that supporting the judiciary with an experts (Judicial experts) of cyber crimes and in helping to distinguish between the good faith use and the willful misconduct (i.e. the hackers and internet pirates), so that the technology and the eligibility or non eligibility of punishment through different penalties go hand in hand.

It is strongly recommended that strengthening the researches that pay attention to the development of criminality in the intellectual property issues through the computer and the Internet, is fundamental taking into account international experience.