International Research Programme : ISD
"Information Systems Dynamics"

The ISD program was launched by the CIGREF Foundation, with the central aim of sketching the potential outlines of "Enterprise 2020", by looking at how information systems have historically been used in business, as well as at emerging trends.

"The Essentials"

Intellectual Property Law and Freedom between the national and the International

With the "Essentials", the CIGREF Foundation offers an overview of each of the projects sponsored by the ISD programme
This project was coordinated by Ge Chen, from Cambridge University.

Ge Chen holds a Ph D. in law from the George-August Universität Göttingen. He is a Research Associate in Intellectual Property and Global Regulation at the Centre for Research in the Arts, Social Sciences and Humanities (CRASSH) and the Wolfson College of the University of Cambridge.
Executive Summary

This report summarizes the major results of this project based on the research of six major jurisdictions of the world (Canada, China, France, Hong Kong, the UK and the US).

Overall, this research reflects part of the current comprehensive efforts being made to establish a form of global Internet governance that addresses imminent issues presented by these new business models such as peer-to-peer (P2P) transmission, social network websites (SNWs), and cloud computing to corporate actors. The following paragraphs provide an executive summary that covers the major concerns, findings and proposals of this report.
**Major concerns**

Valuing, exploiting, and managing intellectual property rights (IPR) and privacy rights in different scenarios

The report addresses primarily the context of the new business models based on P2P, SNWs and cloud computing technologies. P2P is a distributed network architecture that allows individual users to share and trade files. Cloud computing furthers this technology and allows individual users to store data on remote servers and create and process their online resources. Examples of such business platforms are Google, YouTube, Yahoo, Ebay, Amazon etc. which rely on the “user-generated contents” (UGC) to attract advertisements and generate profits, or Google’s Apps, Wikipedia platforms, Facebook, LinkedIn and Twitter which operate a similar but extended business model.

In the model of knowledge-oriented economies and information-oriented societies, the exploitation, valuation and management of IPR and privacy rights plays a vital part in business performance and economic growth. Since multinational corporations shift to more dynamic models of providing creative products and services based on digital operation, external sourcing of knowledge, and transparency of personal information, they are exploiting and relying on the IP (for example, copyright) by transferring self-generated contents into their products, services and processes.

This is also the case with privacy rights, where companies require every user to submit their personal information before they can use their services. Moreover, companies license IP and personal data to other companies, governments or public entities, as their primary means of commercial negotiations, attracting external financial sources, or generating revenues.

As multinational corporations set foot in different countries and regions, they develop more important channels of knowledge transfer by providing products protected by copyright/privacy rights and delivering licensing services concerning materials protected by such rights. As such, companies use IP and privacy rights strategically to create corporate values, expand financial assets and maintain competitiveness.
The current models of P2P and cloud computing enhance the efficiency of this process by facilitating exchanges of protected information and putting protected materials in the hands of corporate actors who are able to commercialise them. Therefore, it becomes indispensable for managing staff of companies to learn how to exploit, value and manage those protected information in different scenarios.

**Scenario 1: Do companies need more protection of digital contents or more freedom?**

On the one hand, companies leverage their protected information to yield profits and attract investment. For instance, companies may use their IPR including copyright and patent as collateral for bank loans while relevant IP must be evaluated as a basis for investment decisions.

In this case, companies with high IP profiles would favour increasingly higher IP standards. On the other hand, companies such as YouTube (Google) often rely on unprotected contents in attracting huge advertisement revenues. Under such circumstances, it is more likely that loose enforcement of IP protection would benefit owners of such popular websites. In a word, corporate actors face the dilemma of demanding more protection of IP/privacy at times and more freedom from such protection at other times.

Managing staff of companies may often need to decide on issues such as: can they set up, on a website, framing of contents that have been worked out on another website or can a company engaged in media technologies and services of news provide its web users with contents that it works out on the basis of materials coming from other news agencies? Where Internet users are browsing and surfing websites or using the service of certain sites, can website operators collect, save, process or transfer the names, addresses, bank accounts, IP addresses, cookies, or other relevant personal information of their users?
Scenario 2: Should companies monitor websites or wage a laissez-faire policy?

In recent years, warnings of infringement have become the most frequent means of deterring mass IP violation and boosting the reputation of IP protection. The widespread use of cloud computing technology has reduced the costs and improved the ability of medium and small companies to extract values from their protected works and inventions. Companies also cooperate with right holders in strengthening the protection of their IP or personal information by adopting measures or imposing certain supervision in a timely manner. This is, however, also a two-edged instrument.

The closer a website operator monitors its system and watches its contents, the higher the risk of censorship may be and the less likely such websites would become popular. It seems that where a company intends to enhance accessibility to contents and, thus, the popularity of its website, it is almost inevitable to tolerate allegedly infringing activities to a certain degree. Moreover, concerns also arise where R&D can be impeded due to difficulties in acquiring sufficient information that are protected by copyright or privacy rights.

Scenario 3: Can companies launch cross-border litigations?

Internet-related business models assume a global nature, since both information products and a tort of information rights for the Internet would need to incorporate an international scope that disregards borders of physical territoriality. As long as the Internet is available, one can reach any digital contents from any corner of the world.

Thus, it is a crucial issue to which jurisdiction the online management of IPR and privacy rights will be subjected. Presumably, if a company establishes a website of musical programmes in China that allows users to download contents protected by European or US copyright law, can the copyright owner find remedies in the EU or the US? If, however, a company in the EU publishes on its website any contents relating to the private life of a celebrity in the US, can the latter seek justice in her/his hometown? While promoting knowledge transfer around the world, companies should try to avoid getting sued everywhere.
Indeed, sound strategies of targeting jurisdictions would assist companies in better safeguarding their intellectual assets and business interests.

**Major findings**

**Difficulties and uncertainties in balancing freedom of expression against IPR and privacy rights in different parts of the world**

The implications of digital information rights are, however, often inconsistent for corporate actors. In addressing the challenges posed by Internet-related business models, companies must develop strategies at different levels and in different dimensions.

**General strategies about copyright and privacy rights**

**Copyright**

Powerful countries and industrial actors are making use of available resources to establish electronic fences to block uncompensated access to copyright products, regardless of the extent to which basic public needs may have been integrated with the digital network. While countries around the world provide stronger protection of proprietary interests, it is a global practice to set limits on copyright protection.

This, however, contain a number of uncertainties that cast doubt on the flexibilities of uniform copyright standards, since copyright rules are invariably subject to the interpretation of national legislators and national courts.

In the EU, copyright protection must serve the “balance of rights and interests between the different categories of rightholders, as well as between the different categories of rightholders and users of protected subject-matter must be safeguarded.” While the sophisticated EU regulatory framework needs further specification, courts are expected to provide further interpretations on limitation/exception rules in its case law. In fact, national courts diverge on the border between copyright infringement and exceptions.
French courts, for instance, tend to focus on the extent of similarities between works to determine whether there is copyright infringement, whereas the most decisive criterion for an infringing act seems to be the “overall impression” that the work in question is similar to the original work.

In common law countries there are also no clear-cut doctrines. While English law is somewhat restrictive in allowing users to use protected works, English courts tend to interpret the “fairness” of making copies in a flexible manner in terms of the purpose or the nature and quantity of the work being copied. In Canada, the overall legislative and judicial trends embrace a large and liberal interpretation of permissible copying, leaving it more uncertain whether the scope of permissible acts is exhaustive.

The Hong Kong copyright law seems to be more specific in defining copyright infringements, as well as a wide range of permissible uses of copyright-protected works. The US copyright law embraces fair use doctrine, an open-ended rule that consists of four testing factors.

The most distinctive feature of this rule is that courts will decide any specific exception to copyright on a case-by-case basis rather than based on an abstract definition in statutory law. As such, US courts have been very flexible in deciding on the use of copyright-protected works in specific circumstances such as library, museum or other personal uses.

China also embraces a well-developed copyright legislation. It establishes copyright infringement rules on the basis of international standards, and has developed “free use”. It allows twelve circumstances of “free use” where materials protected by copyright can be accessed without authorization by, or remuneration to, copyright owners, as long as the name of the author of relevant works is indicated.

Chinese copyright law, however, serves to allow the government to exert better control of freedom of expression. The Chinese government often issues specific regulations that further define those statutory provisions. A recent regulation has adjusted the free use doctrine in the digital environment. Such practice, however, increases the legal uncertainties in practice for foreign companies.
Privacy

The prospects of the protection of privacy are, however, even more uncertain. Several uncertainties and difficulties in fitting Internet-related business into the privacy laws around the world may puzzle transnational companies.

First, there are two regulatory patterns in most countries: the traditional tort of personality/privacy-related rights which address the civil wrongs and the data protection (DP) regimes that regulate data privacy.

Secondly, privacy legislation is widely divided and the level of privacy protection remains largely different across different countries.

Finally, there is no consent on a viable set of exception rules that help determine the border between the protection of privacy and the right to freedom of expression/information.

Although many laws are not binding, they reflect largely similar principles in DP. In fact, to what extent these international and regional model laws can be put into practice depends on national legal systems. Nevertheless, national DP legislations are widely scattered, sporadic and different.

In the traditional model of protecting privacy rights, courts exercise more autonomy in determining the border between the protection of privacy and that of freedom of expression/information on a case-by-case basis. In several landmark cases, the European Court of Human Rights (ECtHR) establishes a balancing approach, affirming the fundamental protection of privacy unless the matter involves a public figure exercising official functions, or amounts to public concerns, contributes to a debate of general interests. In common law countries, privacy rights are not provided explicitly, but may be granted on the basis of case law. In the US, free speech including commercial speech enjoys such a strong protection under the First Amendment that there is generally no constitutional privacy right.

In the UK, defamation law plays a preeminent role in privacy protection, which may, however, create a chilling effect on freedom of speech, and is now subject to stricter conditions of bring a lawsuit. Canadian common law recognizes a limited right to personality, whereas Hong Kong privacy law has largely followed the UK style.
Finally, China has codified privacy protection in a patchwork of statutory laws. Nonetheless, since Chinese courts do not apply the constitutional provisions on freedom of expression, privacy protection is weighed against civil damages.

Due to these difficulties in the traditional approach of tort, DP laws are becoming significantly more relevant to Internet privacy, especially in the environment of SNWs/cloud computing.

The law itself focuses on the processing of data (e.g., collection, usage, dissemination) and aims to protect personal information/data from arbitrary collection, disclosure and misuse. DP laws are a self-contained regime that covers the need to balance privacy interests against expressive interests.

The EU has developed an advanced DP model for the rest of the world. The current EU law provides for a number of fundamental principles for the processing of personal data and prohibits data from being transferred to countries outside the EU where the domestic laws do not satisfy certain DP standards. It also justifies certain acts on the grounds of national security, protection of freedoms of others, research or private use, etc. In contrast, there is no generally applicable DP regime in the US, while one is often able to collect, store and use data without permission.

The US, however, has developed the EU-US Safe Harbour Principles which allow US companies to comply with EU DP principles voluntarily, thus removing certain obstacles and facilitating business freedom in cross-border business transactions. Canada follows a similar approach of looking to the DP standards of the EU, as there are many legislative similarities with the EU DP framework.

Since 2012 China has also issued laws and regulations that increasingly encompass international DP standards. Hong Kong enacted its DP law as early as 1995 and has imposed stricter conditions for privacy protection in the last two years.
Specific corporate strategies concerning copyright and privacy

The global context

With regard to intermediary liabilities of companies as ISPs, corporate practice follows the same rules for the protection of both copyright and privacy. Generally, international law allow courts to grant injunctive reliefs that prevent imminent infringements if right holders provide adequate evidence and notice to the allegedly infringing party. The latter may apply for revocation of such injunctions under certain circumstances. Finally, courts would hear the case where there is an irreconcilable dispute, but should maintain the balance between freedom of expression, copyright and privacy.

These rules are often referred to as “notice and takedown regime”, “graduated response” or “three-strikes” law. In the digital environment, these rules are of particular significance for corporate actors because they help determine whether companies will be held indirectly liable for illegal online acts or they may be exempt from such liabilities.

The US

The US law has developed two distinct principles for regulating indirect liabilities of corporate actors (or ISPs). Liabilities can be established when companies are entitled to supervise and capable of exerting control of online infringing activities, but fail to do so and benefit from an obvious and direct financial interest from the existence of such infringing materials, even without actual knowledge that the infringing activity is going on.

Alternatively, Liabilities can also be imposed where the ISP intentionally or negligently induces, causes, encourages or contributes to the act of direct infringement by another party. US courts have, however, also created a doctrine that exonerates companies of liabilities as long as their products or services are capable of “commercially significant non-infringing uses”.

These doctrines, now under the Digital Millennium Copyright Act serve to immunize companies in conduit, system caching, hosting information and providing location tools under certain conditions.
In practice, however, there are difficulties in defining those terms such as “direct financial benefit” and “actual/apparent knowledge”. The US law also contains rules that affect the liabilities of companies for violation of privacy, albeit in a different, pro-business manner, ie, Internet-related corporate actors could enjoy the freedom to conduct business more than individuals could claim the protection of their privacy.

This is because the First Amendment on the protection of free speech would usually prevail where commercial UGC may conflict with data privacy.

**The EU**

The EU law boasts of a uniform/horizontal regime regulating the ISP’s liability not only for copyright infringement but also for any online illegal conducts including violation of privacy. This EU law grants exemptions to companies provided that they do not collaborate with users in conducting illegal acts.

This does not, however, mean that companies are exempt from any monitoring obligations. The EU law imposes a general obligation that companies act “expeditiously to remove or to disable access” to any illegal information upon “obtaining actual knowledge or awareness of illegal activities”. If right holders of digital information rights require a company to filter illegal contents in the context of P2P or SNWs/cloud computing, their interests must be weighed against the general interests of freedom of expression/information.

Corporate actors may determine themselves what the best adapted measures are to curb and prevent illegal acts. It seems that European courts would uphold Internet freedom (freedom of expression/information and, thus, the companies’ freedom to conduct business) slightly more than other digital information rights.

**The UK**

The UK copyright law regulates infringement in a much similar way. Although there is no corresponding provision in its DP law, the UK does have a horizontal regime that provides for a safe harbour regime for “information society service” providers. The safe harbour regime can be applied to different legal branches to exonerate ISPs of both civil and criminal liabilities while ISPs provide information society services.
In other words, it is relevant to both copyright infringement and violations of privacy rights. English courts have also applied a similar interest balancing approach when determining the intermediary liabilities of corporate actors, upholding the protection of freedom of expression and data privacy.

Besides, the UK has also enacted its “Digital Economy Act” in 2010 to regulate the intermediary liabilities of companies in the digital context. This, however, has encountered great hurdles from the industries and civil society that claim the act might harm civil rights.

**France**

France follows the EU horizontal approach of addressing the intermediary liabilities in copyright and privacy cases and has developed its own regime of “graduated response”.

The rules in IP are, however, more specific and developed. France has issued a general safe harbour regime for Internet-related companies in its 2004 Law for Trust in Digital Economy, which applies to both copyright infringement and violation of privacy in the digital environment. Notably, the notice and takedown regime is a significant criterion, while companies are required to monitor or supervise online contents against future infringements. Moreover, France has successfully introduced the graduated response regime into its IP law through the HADOPI Act.

Nevertheless, the French Constitutional Council requires that the measures be proportionate and be integrated into an adversarial procedure. This shows that digital information rights would always have to be weighed against freedom of expression/information in the new digital context. In several recent cases, French courts have applied the safe harbour doctrines and affirmed the principle of technical neutrality of ISPs.

**Canada**

In a similar vein, Canadian copyright law regulates indirect tort and liabilities of ISPs but has not done so explicitly in its DP laws. Notably, the Canadian Supreme Court established the principle of neutrality for ISPs providing communication services by ruling that “knowledge that someone might be using content-neutral technology to violate copyright is not necessarily sufficient to constitute authorization, which requires a demonstration that the defendant did give approval to, sanction,
permit, favor, encourage the infringing conduct”. Internet-related companies would, however, cease to be “content neutral” if they received notice of the existence of infringing materials on their system and failed to take the necessary measures such as “take down” to prevent further infringements.

Otherwise, they may seek to shelter from intermediary liability for providing Internet services. In terms of general practice, such a principle may be applied in cases of violation of privacy as well, where Internet users may issue such notices to companies for removing materials that intrude into their privacy/personality rights.

**China**

Chinese civil law inherently provides for a horizontal regime for regulating tort of copyright and privacy including those in the digital context. Chinese law embraces the notice and takedown regime in an explicit manner, which serves as a criterion for determining intermediary liabilities of ISPs or exonerating them of such liabilities. In recent case law, Chinese courts have started to impose injunctive orders on ISPs to curb or prevent illegal acts on the basis of their knowledge.

As such, it becomes more meaningful for corporate actors to develop corporate strategies or policies in the context of P2P, SNWs and cloud computing that help defend their freedom to do business in terms of appropriate safe harbour regimes. An underlying reason for such difficulties in designing corporate policies for the protection of copyright and privacy lies in the fact that it is often hard for companies to have a strong incentive to monitor their services for illegal contents and make themselves responsible for protecting copyright and privacy.

If they do so, they may run the risk of incurring liabilities for failing to carry out such commitments. Where, however, they fail to protect the copyright and privacy rights of their customers properly, they may soon lose colossal shares of the market and get involved in marathonic legal disputes.
Defensive strategies regarding jurisdiction and choice of law

Jurisdiction relates to who has the power to decide on a dispute. Choice of law clarifies which national law(s) should be applicable in such cases. These two factors could ultimately affect the outcome of a dispute relating to digital information rights, including copyright and privacy rights. In global context, there is no uniform law governing these issues but for some general principles. Under the principle of territoriality, where a company resides or an act of infringement is committed in that country, the courts there may have jurisdiction.

Under the principle of effects, however, where a foreign national outside that country commits an online act that is targeted at and causes harm in that country, the courts there may assume jurisdiction over that foreign national. Concerning choice of law, national courts may govern a conduct that takes place elsewhere but has significant and intended effects in the forum. In such cases, the law where the courts are located would usually apply.

A problematic rule for determining jurisdiction lies in the difference between the place where an infringing act takes place and the place of damages. In the EU, different rules may apply in online privacy-related disputes and online copyright disputes. For example, French courts have shifted from the mere accessibility approach (one can sue where one has access to illegal contents) to the targeting approach (one can only sue where such content is targeted at). In common law countries, things stand differently. In the UK, English courts may usually decline to hear disputes involving foreign copyrights, but are increasingly embracing the targeting approach to hear foreign cases.

In contrast, Canada holds a low threshold for hearing online cases, since Canadian courts will hear such cases as long as they decide that there is a real and substantial connection between the dispute and the place where the courts are located. Hong Kong still follows the pre-EU English common law. In the US, the most relevant and controversial jurisdiction rule for online torts is to identify whether there are “minimum contacts”. Finally, China embraces international standards, but has developed more specific rules for hearing online IP infringement cases and privacy-related disputes.
Privacy-related rights are ultimately under constitutional protection in many countries. Therefore, courts would invariably apply national laws of the forum. In copyright-related disputes, however, more uncertainties would arise. In the EU, applicable law should be the law of the country for which protection is sought. Based on their jurisdiction rules, English courts would apply English common law in online privacy-related cases, while French courts could, theoretically, also apply the law of a foreign country.

US courts rely on the “most significant relationship” test, according to which the court should choose the law of whatever jurisdiction is most closely tied to the case. The practical result of applying such result, however, is that the US law will be applied. In Canada, the general applicable law in tort disputes is also the law of the place of wrong. In practice, Canadian courts would apply Canadian laws because of their low-threshold jurisdiction rules.

China has enacted explicit provisions on choice of law concerning online privacy-related and IP-related disputes. Hong Kong courts will generally apply the local laws when deciding on Internet-related disputes.
**Major proposals**

**Envisioning pro-civil-rights 2020 Enterprises**

In the environment of P2P, SNWs and cloud computing, the ISD Programme features several distinct cross-cutting topics addressing Internet-related business models. In particular, supporting “pro-civil-rights” societies is a prerequisite for a sustainable process of European integration and a compelling responsibility for European companies.

Managerial staffs of Internet-related businesses are challenged, above all, to address the daily tension between the proprietary model of knowledge production and dissemination relating to the traditional protection of IP and personal data on the one hand and freedom concerns of users on the other. In general, a pro-civil-rights approach derives from

1) the principle of interest balancing between freedom of expression/information, copyright and privacy;

2) the principle of neutrality encompassing safe harbour doctrines and the graduated response system;

3) the principle of territoriality complemented by the targeting approach in governing jurisdiction and choice of law.

Under these general principles, the report develops more specific corporate policies with managerial implications in the context of P2P, SNWs and cloud computing.

These policies cover the protection of freedom of expression, copyright and privacy, transparency, neutrality, legitimacy, necessity, proportionality and territoriality.
Half referee, half player

When assessing the future role of the global Internet governance, managerial staff of Internet-related enterprises would face the difficult task of carefully balancing the various fundamental rights that are engaged, in particular, the protection of copyright and personal data against freedom to conduct business. Multinational corporations should learn to assume the role of a “referee” more than that of a “player”.

Freedom of expression

Companies should make explicit commitments to the protection of Internet freedom. While managerial staff of Internet-related enterprises should also learn how to respect copyright and privacy, freedom of expression forms a fundamental principle for any Internet-related business conducts.

Copyright policies

Companies must refrain from copyright infringements, since copyright protection may be more important than most daily speeches online, as long as a speech or relevant information does not concern the political interests. Companies should identify copyright-protected materials and ensure remuneration while allowing for accessibility.
Privacy policies
Companies could choose not to play a complicit role in developing new surveillance technologies and facilitating States’ surveillance regimes which may not comply with the required human rights standards. Companies must process personal data in a transparent atmosphere and show respect for private life while having accessibility to personal data.

Neutrality
Companies should maintain a neutral status by helping Internet users address online infringing materials and activities efficiently without allowing them to misuse such instruments. Corporate actors participate in the regulatory process by overseeing the relationship between right holders and alleged infringers through the take down regime. Thus, managerial staff may need to learn to consider whether a required technical measure for the purpose of protecting copyright or privacy is appropriate, necessary and proportionate to curb and prevent online torts.

Territoriality
Since freedom of expression/information remains an uncertain issue under different jurisdictions, the freedom to conduct business for media corporations may come across different obstacles. Nevertheless, companies may choose to establish business branches in those countries and areas where they may expect to have fewer difficulties and uncertainties in practising their online business.

Executive summary authored by the research team and edited by the scientific coordination and the organizing committee of the ISD program. This work might be the subject of publication in ad hoc scientific series (e.g. The Springer Briefs in Digital Spaces Series).
The Scientific Committee of Foundation CIGREF

Pr. Ahmed Bounfour  
Université Paris Sud 11

Pr. M. Lynne Markus  
Bentley University

Pr. Pirjo Stahle  
Finland Futures Research Center

Jean-Eric Aubert  
World Bank Institute

Pr. Surinder K. Batra  
Institute of Management Technology Ghaziabad

Pr. M Beaudouin-Lafon  
Université Paris Sud 11

Pr. P-J Benghozi  
École Polytechnique

Pr. M. Cavalcanti  
Federal University of Rio de Janeiro

Pr. Leif Edvinsson  
University of Lund

Patrick Fridenson  
EHSS, Centre de Recherches Historiques

Dominique Guellec  
OCDE, Senior Economist

Pr. Tom Housel  
Naval postgraduate School of management

Pr. Juinichi Iijima  
Tokyo Institute of Technology

Pr. Moez Limayem  
University of Arkansas

Pr. Rik MAES  
University of Arkansas

Pr. P. Meusburger  
University of Heidelberg

Pr. Ian Miles  
University of Manchester

Pr. Yves Pigneur  
Université de Lausanne

Gérald Santucci  
Cion Européenne DG Société de l’Information

Pr. Frantz Rowe  
Université de Nantes

Pr. Eric Tsui  
Hong Kong Polytechnic University

"Essentials" of the International Research Programme ISD - CIGREF Foundation
Find the research program on the ISD website of Foundation CIGREF

Foundation CIGREF is supported by...

altran  Capgemini Consulting  Microsoft  Societe Generale