Chapter 23

CYBERSPACE AND CYBERCRIME

VAGELIS PAPAKONSTANTINOU
Attorney At Law, PK Partner, Athens

23.1. Cyberspace and Cybercrime

Ever since it escaped the pages of science-fiction books and entered the real world, cyberspace developed a strained relationship with security. This should have caused no surprise to those close to the new medium. First, a level of security compromise is to be expected in any field of human activity that is entirely new — things have to settle down for the regulator to take positive and long-lasting measures. Second, cyberspace per se was coined at the time as the last border of freedom, a space where humans may do as they please — this inevitably involves some tolerance when it comes to security. Whichever the reasons may be, the fact remains that cyberspace did and still does present a number of security issues that, nevertheless, are increasingly considered unacceptable in contemporary e-commerce-profiting societies.

Cyberspace, at least in a form relevant to the purposes of this analysis, is a relatively recent addition to our everyday lives. Widespread public use of the new medium does not date much before the 1990s. Of course, cyberspace was a term well-known and a space well-visited before that time, but its use was restricted to certain academic or other *avant-garde* circles much too scarcely populated to matter. In order for security to become a consideration, widespread use is necessary — and, such widespread use only happened more or less during the 1990s.

However, the lack of any substantial history does not mean that the new medium did not have enough time to complete its development cycles. On the contrary, cycles that would have taken years to complete were expedited at the astonishing speed that later came to characterise the new era (that is, the Information Society). Cyberspace was conceived and originally implemented as a borderless new space, transcending physical borders and formal legal rules, that would constitute the ultimate frontier for human freedom (and, discussions today

HANDBOOK OF ELECTRONIC SECURITY AND DIGITAL FORENSICS

on whether we should tax the Internet prove that this line of thinking still survives, *albeit* misguided). This afforded a certain level of freedom to its users at first. As more and more people were entering cyberspace, it was established that not all of them adhered to the same benevolent principles. In addition, cyberspace suddenly became commercially meaningful. Transcending its own original borders, that destined it to become a communications tool among individuals (preferably academics), cyberspace discovered e-commerce. From that point on, developments are known to everybody; within only a handful of years a previously unknown (if not, unheard of) tool was turned into an inseparable, self-evident part of doing business. Today, the commercial value of cyberspace simply cannot be measured. And, where there is money, crime inevitably follows.

Cybercrime thus emerged in cyberspace. Cybercrime comes in two forms: first, crime committed in cyberspace that was previously unknown to humanity (including regulators). Second, crime committed with the assistance of the Internet. Each case presents a number of particularities.

The self-evident cybercrime category refers to crime that was previously unknown, but only takes place in the Internet. All of the e-commerce-related crimes, as known today, may serve as examples: P2P (copyrighted) unauthorised file exchanges, libellous blogs and blogging and other Internet Service Provider-related crimes, e-commerce identity theft or fraud, all constitute new crimes that would have been impossible without the Internet. Some of these cases will be elaborated in this or in the following chapters in detail, a remark, however, of general application refers to their evolving character. Because such cybercrimes are connected with human creativity, as expressed mostly in ways of doing business on-line, they cannot be anticipated, but are only dealt with in retrospect. Web 2.0, that will be analysed later, constitutes an excellent example; once users had the opportunity of creating content and transmitting it to the millions, a new series of security risks emerged. The same is true with regard to social networks operating online. The law has no way of knowing from which direction the next flow of rights' infringements will come. In all these cases, it has to act in retrospect, sometimes only temporarily addressing the "loophole", until the conditions are mature enough for formal regulation. However, in all these cases, as is true with all new fields of human activity, an increased security risk is to be expected.

The second category of cybercrime is probably more widespread, and refers to new ways of committing crime, using the Internet. Exactly as the Internet has enabled new ways of doing business, it has also enriched the potential opening to criminals. In this case, older and well-known (and, dealt-with) crimes project themselves into cyberspace: pornography becomes on-line pornography, gambling becomes on-line gambling, credit-card fraud becomes on-line credit-card fraud. In all these cases, the law does have an answer; all said crimes (and any crime-making use of the Internet) are well-regulated in the real world. Difficulties arise, first, when the on-line circumstances gravely affect the conditions that the law required for a

crime to be committed until its on-line version emerged, and, second, due to the inherent international nature of cyberspace. An example of the first refers to on-line gambling: in countries of state gambling monopoly, is it a crime for their citizens to bet in on-line betting Internet sites whose servers are located abroad? The second source of difficulties is quite obvious: crimes committed through the Internet are hard to trace and fight in a world based on state-sovereignty and state-restricted crime prevention mechanisms. The Internet known no physical borders and this conflicts with any criminal law, as known so far.

This chapter will therefore attempt to throw some light into the relationship between cyberspace and cybercrime. In order to do this, first, a brief security-focused analysis of the Internet, and in particular its Web 2.0 form, will be attempted, before approaching specific cybercrime-prone on-line activities, in order to demonstrate how assessments of the first part of this analysis apply in practice (other activities may be found in the following chapters as well).

Two definitional clarifications first: For the purposes of this analysis, cyberspace and the Internet (the world wide web (WWW)) shall be hereinafter used as synonyms. Regardless of the (perhaps deplorable) arbitrary character of this decision, the fact remains that, being firmly in a Web 2.0 environment and perhaps planning for the immediate future, definitional clarity, as opposed to general public use, is of secondary importance. The second clarification pertains to the legal background: that will be unavoidably European- (and indeed, EU) centred. When possible, regulations and case law from other jurisdictions (mostly American) shall be provided, but the legal basis upon which the following analysis shall build is that provided by the European Commission.

23.1.1. *The Internet as a Living Space*

In order to assess the security implications of the Internet today, be they "cybercrimes" or not, we first need to examine what it encompasses, at least from a user perspective. Cyberspace, or the Internet, is an environment in constant development and human behaviour relating to it, that gives birth to such security issues, inevitably follows. Both the main characteristics and contemporary trends of the on-line world shape the "cybercriminology" background.

As regards the Internet's main characteristics, these relate to such common and well-known issues such as its "distributed" or its "borderless" nature. On their analysis, there is no need to over-expand. By now, it is common knowledge that the Internet is an uncentralised, borderless (virtual) space. Although some form of governance is sometimes necessary (for instance, ICANN), there is no such thing as a central authority (state or other) that monitors and regulates its use. This lack of centralised control creates a number of security issues: rules are applied selectively (if at all), individuals find no (easy way for) redress, organisations are constantly set up and dismantled in a virtual world. State regulations, as already

noted, are generally useless over the Internet. Unless Internet organisations refer to well-established real world (even listed in stock exchanges) enterprises, there is really no way of imposing penalties or regulating effectively Internet companies (see, for instance, the struggle of the music industry, even after Grokster, to being down Internet piracy organisations by blocking their IPs). The same is valid for individuals as well — once they decide to set their blog on an off-shore server, there is very little the criminal courts of their country may do against their potentially unlawful postings [8].

Both the "distributed" and the "borderless" nature of the Internet are issues known for quite some time. Nevertheless, their full potential has probably not been properly assessed yet, if placed under the "ubiquitous computing" or "intelligent environments" light: "*on the road to the realisation of the Ambient Intelligence (AmI) vision, physical space becomes augmented with computation, communication and digital content, thus transcending the limits of direct human perception. An Intelligent Environment consists of a set of technologies, infrastructures, applications and services operating seamlessly across physical environments (e.g. neighbourhood, home, car), thus spanning all the different spheres of everyday life. Their inhabitants, humans and agents, will carry out tasks, most of which will be very similar to those that we do today, only their activities will be very different. The introduction of ICT and its applications in order to support these activities (and improve the efficiency of tasks) will change many of their parameters and properties, especially those related to space and time*" [3]. In other words, the term "ubiquitous computing" describes living conditions whereby individuals will never really exit a computing environment — information about them will flow around them through invisible computing mechanisms (for instance, RFID), in order to facilitate mundane tasks. Obviously, such information shall not stay isolated; information must flow, and the only accommodating network is the Internet. Broadband connections and Wi-Fi technologies are already in commonplace. Eventually, once all this information is placed on-line, the security and regulatory issues shall be formidable; if today contemporary legal schemes find it hard to regulate cyberspace, although only a handful of human activities are projected on-line, we can imagine what the situation will be like once individuals project their digital personal on-line, into such "intelligent environments".

On the other hand, the new medium needs public trust in order to develop. E-commerce, by today, is a substantial part of the world economy; some of the most expensive companies around the world are but Internet search engines (Google, Yahoo, Baidu); others are on-line service or goods providers (Amazon). These evaluations evidently need public trust in order to be supported. However, cyberspace always aroused public suspicion, both by its ardent users and by those who are not at ease with new technologies. Again here Internet's "distributed" and "borderless" nature is to blame. Experienced users who are aware of the difficulties of controlling the new medium need increased security in order to entrust their

money in it. On the other hand, people with partial exposure to new technologies find it hard to comprehend a medium not connected to the physical world; this, together with public (justified or not) fears about on-line crime has called for a possibly secure and well-regulated environment.

E-commerce has thus imposed in practice the need for increased security standards in cyberspace. Equally, e-commerce has probably led to "cybercriminality", at least in its most serious forms, it could be maintained therefore that the same phenomenon gave birth to the problem and makes its solution imperative. At any event, the quest for "cybersecurity" shall be an endless one, given the basic characteristics of the Internet. This, coupled with the full-force-speeding-ahead trend towards ubiquitous computing (slowly making itself felt through Web 2.0 applications that shall be immediately discussed) only increases the level of efforts required, sometimes making obvious the shortcomings of contemporary legal schemes when put to the test.

23.1.2. *Web 2.0: Some Security Considerations*

Web 2.0 is the talk of the day (notoriously, Time's Man of the Year for 2007 was You — as seen through a mirror ingeniously published on its cover — due to the power Web 2.0 has awarded individual users). The term is used to describe what constitutes a, perhaps if seen from a distance self-evident, development of the new medium; in its original form, the Internet was used for one-way communication — each website communicated information to the public who, for the most cases, could only but read them passively. Web 2.0 has taken the next step, making the Internet a two-way communication tool; now users replied back, or even transmitted information themselves. The Internet's role changed (or was enhanced) from informative to communicative.

Web 2.0 is evidently based on wide public participation. User-generated content, blogs and blogging, social networks are all based on an as increased basis of Internet users as possible. Efforts have been undertaken to take the Internet out of the computer context and into TV sets, making it thus even more accessible to the last ones who refuse to acquaint themselves to it. The word, and the world's agenda, is "penetration": the level of countries or societies in more indexes than purely technology-connected ones is by now estimated according to its Internet connections.

The fact, however, remains that the Internet and cyberspace per se remained unchanged: the emergence of Web 2.0 applications and mentality did not necessarily mean that regulatory issues were resolved. Difficulties connected to their "borderless" and "distributed" nature continue to plague public trust, at a time when it is most needed.

In this context, Web 2.0 did nothing to appease public concerns (because after all it was not within its scope to do so). Quite on the contrary, its identifying characteristics (public participation, user-generated content and social networks),

its market importance (Web 2.0 — in effect only — Internet sites are being sold and bought for billions of dollars) as well as its business models (that keep pressing at the border of, the said, on-line projection of the human persona) have only exacerbated the "cybercriminality"-related issues.

As regards the identifying characteristics of Web 2.0 applications, as experienced after all by each one of us who has basic exposure to the Internet today, public participation is perhaps its most dominant trend. Practically, all Web 2.0 applications (as embodied into Internet sites) ask from users to participate into something (update their profile, upload their content, tell others what they are up to right now) in ever-increasing numbers — indeed, the more the merrier. Users necessarily interact among themselves. Not only do they "do something" but their actions interact with those of other users (for instance, while making friends in social networking sites, rating videos etc.). And, unavoidably this worldwide, wide interaction is not worry-free. Exactly because it relates to millions of humans, each with their own disposition, temperament and even agenda, conflicts are bound to exist while interacting; this can be very much true both in the real world (when real-life individual rights are infringed) or in cyber-world (when a new flow of "cybercriminality" that only takes place in cyberspace and does no harm to physical objects or persons is emerging).

User-generated content is a more than obvious source of conflicts. As it is by now known to everybody, there is a great commercial value in facilitating exchanges of users-created content (mostly pictures and videos). Such facilitators (in the form of Internet sites such as YouTube) are being traded for billions of dollars. Evidently, when millions of individual users create billions of separate pieces of content (videos, music, pictures etc.), conflicts are bound to appear. These conflicts may either concern interpersonal relationships (users infringing each other's rights) or mass, "institutional" infringements (see, for instance, the attack on the fundamentals of Intellectual Property (IP) Law launched by P2P networks or videos uploaded in YouTube).

Social networks constitute a more subtle source of security concerns. Social networks are intended to acquaint among themselves as many of their users as possible. A lot of effort, in the form of complicated algorithms, marketing and social science has been devoted in making this successfully; indeed, the most valuable networks are those that have created the most links among their millions of users. The standard way of accomplishing this is to become as intimate as possible: each user creates the so-called personal profile, in which his or her preferences, thoughts and realities are laid down with as much detail as possible (in order to attract as many compatible friends as possible). Security problems are plain for everyone to see, and can range to anything from sexual harassment of minors to fraud or even crime collaboration (suicidal tendencies included). From a security perspective, each Internet personal profile (and many users have more than one) is a source of risk, being effectively the equivalent of an individual being exposed to social, real-life

interaction. Never mind that all this takes place over the Internet: crimes, either Internet-assisted or Internet-enabled, usually tend to take a very real-life format at the end.

Risk sources shall probably not cease to emerge or even diminish in the near future, mostly due to Web 2.0 business models. In order to create a successful Web 2.0 application, that shall hopefully sell for billions, entrepreneurs need to assimilate or create as much as possible human-interaction situations. In other words, questions need to become as intimate as possible: in the, not so far, past it has been "tell us a bit about yourself", at the time these lines were written it is "tell us what exactly you are doing now". Virtual worlds also need to be as real-life as possible in order to become convincing (and, thus, attractive): a multitude of virtual worlds are made available to users, be they equipped with, virtual, swords and weapons or be they reality-like recreations (virtual money and contracting included). All these situations create security concerns that there is no practical way for regulators to address effectively. Because Web 2.0 is found at the avant guard of human (commercial) creativity, a level of security compromise is to be expected. On the other hand, because Web 2.0 is addressed to millions of users, an otherwise expected security glitch could affect individuals at an unprecedented scale. The main risk posed by Web 2.0 is that it has managed to bridge the unthinkable: living at unchartered waters in millions.

23.2. Certain (Contemporary) E-Commerce Security Highlights

Because e-commerce, be it in its Web 2.0 or in its more traditional format, is intricately connected with human ingenuity, a definitive analysis of its legal aspects is impossible. Apart from certain self-evident aspects (for instance, on-line contracting, that shall be elaborated in one of the following chapters), all other of its instances unavoidably have to be examined on a per-case basis. This is not only due to their unexpected form, reflecting some of the most ingenious human creations, but also due to their ever-changing content. E-commerce applications change along with their users at an unprecedented speed: a traditional book-selling website may record its users' preferences in order to enhance its book suggestions (adding thus privacy legislation to its list of relevant fields of law), protect its sales processes through patents and imposing them against competitors if necessary (adding also IP Law to the picture), and even try to artificially fragment cyberspace by creating country-specific shops and sell its wares only to residents of the same country (completing the mix of laws with some unfair competition or even EU, if in Europe, Law). E-commerce is a dynamic part of the market that shows no signs of settling down; as long as it re-invents itself every second or third year, adequate and comprehensive regulation of its many aspects is plainly impossible.

Security concerns and "cybercriminality" unavoidably follow this scene of continued developments. No one can regulate effectively risks whose full extent

has not unfolded (or will never unfold because their sources will have been replaced within a couple of years since they first appeared). Legislation may come in very broad terms (as are, for instance, the fundamental data protection principles). On the other hand, the need for public trust is as pressing as ever; the more Internet businesses trade in billions of real-life dollars, the more the public needs to trust and use as much as possible the Internet. The two trends are obviously conflicting: e-commerce develops and keeps creating new sources of risk, while millions of individuals have to use them in order to keep the world economy going. Security balances and checkpoints, industry self-regulation and watchful regulators are all necessary, but there is only so much they can do by definition.

It is under this light that the following analysis should be read. What is effectively attempted is to address, from a security perspective, certain e-commerce-related issues in their contemporary form. Risks, "crimes" and their regulatory responses for each one of them tend to change constantly; while the analysis shall focus on certain basic e-commerce aspects that are thought to be as fixed as possible in the on-line context, readers should be aware that on-line notions, issues and solutions tend to outrun traditional, off-line publishing.

23.2.1. *Cyber-Enterprising*

Cyber-enterprising lies at the heart of the "cybercriminality" issue. As already said, e-commerce is inseparably connected to the most innovative and creative ways of doing business. Practically, millions of people around the world are thinking up of new ways to make money out of cyberspace; once they have identified an opening they storm in, in order to capitalise on their findings as quickly as possible before the next on-line trend makes their own obsolete. E-commerce, particularly Web 2.0 business models only have a life span of a few years. Within this time, their owners either make it big (whereby a major sale is in order) or they quit for the next wave. Even the same applications have to change constantly in order to keep relevant: on-line social networks a couple of years ago afforded different functionalities to their users as compared to today (and only the future knows how they develop in their effort to create real-life income).

Another point to be taken into consideration (that was too analysed above, under Section 23.1.2) is mass participation. By now virtual enterprising is not addressed to a handful of people in a few technologically advanced societies; rather than that it is addressed to the whole wide world. The only measurement of success today for any e-commerce application (essentially, website) is the number of individual visits ("hits") to its webpages — mass participation is thus pursued at any cost. This only exacerbates the security problem. Infringements to individuals' rights now come in waves and indeed may originate from anywhere in the world.

The above two factors were indeed analysed above (under Section 23.1.2). What could perhaps constitute a useful perspective while analysing virtual enterprising

refers to highlighting the, typical by now, "cyber-enterprising legal process". This process has become time after time and Internet "phenomenon" after Internet "phenomenon" typical when it comes to e-commerce. It certainly builds upon the above two factors (need to innovate and mass participation) and it also takes into consideration certain financial factors as well: the short life-span of most e-commerce applications and the need to sell. In this context, the typical "cyber-enterprising legal process" is comprised of three stages: first comes a certain disregard for contemporary laws, second an exacerbation of the problem while the (successful) Internet application explodes through mass participation, and, finally, an arbitrary *ex post* solution not always in the best interest of either themselves or individuals.

The disregard for contemporary laws is inherent to virtual enterprising, at least during its conception stage. Innovators usually do not bother to ask their lawyers, and, even if they do, they tend to ignore their opinions. Indeed, there is no other way to explain P2P networks or users' video exchanging sites like YouTube or even the original iTunes deal offered to users. There is no way that any competent attorney would have counselled the first P2P network facilitator that basing its marketing strategy on affording users to exchange copyrighted material in millions would constitute a legitimate enterprise. There is no way that the owner of YouTube was not aware ever since its launching date that users, when creating their videos, invariably step into well-established and protected IP rights and his website made profit out of this. And, there is no way that no one told Apple that binding users through its iTunes to its iPod would not ultimately stand a chance (well, in Europe at least). And, nowadays, it is highly improbable that no one is advising on-line social networks on the privacy implications of certain policies they implement. Nevertheless, all of these projects got at the time the green light to be implemented at a mass scale. It could be because innovators feel that they need to risk in order to reap profit. Or because they feel that cyberspace affords them different rules than traditional real-life distribution channels. Or because they simply feel that contemporary laws need to change. Whichever the case may be the fact remains that practically all ground-breaking on-line projects present serious legal issues, at least when examined under the law then in effect: it seems that after all cyber-enterprising includes a certain level of cybercriminality by definition.

Successful on-line projects evidently exacerbate the problem. A lot of e-commerce applications do not meet public acceptance and eventually die out — their legal shortcomings never thus come to affect us. Those of them, however, who do appeal to the public, increase the problem into unexpected dimensions. Once P2P networks became successful, millions of users were logged in at any time exchanging millions of songs. When YouTube was sold, it came packed with millions of videos all including some form of IP infringement (be it in background music or using extracts from copyrights videos). When iTunes had to withdraw, its lock on iPod millions of users had already paid it under the previous terms and conditions

(indeed, Apple is into a First World War barracks-type pitch fight to protect other equally obvious shortcomings, such as its country-specific sale of content through its local "stores", clearly infringing EU law). At any event, during this second stage of the "cyber-enterprising legal process", the problem is blown up but not resolved or even acknowledged. Millions of users see their rights infringed, various watchdogs complain, regulators start thinking that something should be perhaps done, but on-line enterprises seem to just wait for the problem to simply go away.

What on-line enterprises and entrepreneurs patiently wait is for the third stage of the "cyber-enterprising legal process" to take place, that is, for the final, big settlement. Once it is firmly established that mass infringement of rights does take place and that something must be done about it the same enterprises that caused the problem are ready to discuss. However, by now, they are big enough to negotiate favourable terms. Regulators generally show understanding while imposing fines for past sins to major players (and taxpayers) in their economies (with the exception perhaps of Microsoft). A settlement is thus reached that may include payment of some amount but is rather addressed to the future, adjusting the situation to legal requirements (P2P networks had to shut down but P2P television of telephony thrives; YouTube had to settle through payment of an arbitrary amount to content providers; Apple has to change its Sale Terms and Conditions from time to time). This settlement not always serves the best interests of the public, or even of the business itself, but is seen as a remedy than a solution.

The above typical "cyber-enterprising legal process" is necessarily cyber-criminality-prone. The disregard for legal requirements in its first stage means that the possibility of crimes being committed through the new applications is assessed and, ultimately, accepted. If crimes or security loopholes do make themselves evident during the second phase they are neglected, with the hope of acquiring in the meantime a base from which to favourably negotiate. The final settlement is the, winning, exit for the original perpetrators, leaving society to face with the problem. Although it could be supported that these stages are met in other dynamic fields as well (for instance, finance), they tend to constitute the rule when it comes to cyber-enterprising.

23.2.2. *Blogs, Blogging and Cyber-Opinioning*

The issues relating to blogs and blogging are well known by now: blogging has become such a popular trend that very few of us do not own or do not have sometimes owned or even regularly contributed to a blog. Using the Internet as a two-way communication tool has not been a recent idea (certainly not a Web 2.0 contribution), but its widespread, almost unanimous use has only been a recent addition. Before the time of blogs on-line *fora* or bulleting boards served the purposes of user interaction. These options were available since the early days of the Internet; what is new, is the unprecedented scale of today's opinion expressing over the Internet.

Mass participation means mass influence as well. By now millions of people visit and learn or entertain themselves from blogs. Blogs have thus developed towards two, interesting from a security point of view, directions: First, mostly news-related, blogs have become small news agencies of their own, employing several people and creating substantial income. Second, blogs are the preferred way to bring to the public unpopular or shocking news or even to organise acts of opposition. Each of these categories presents different crime-related issues.

The first category was perhaps a foreseeable development. The most successful blogs, that indeed started out by individuals, had to develop in order to survive. Particularly, those blogs that offered information on niche fields (see, the discussion on the long tail of the Internet) had to keep gaining in depth in order to keep users connected. They thus developed into small news agencies, employing several people or expanding overseas. Nevertheless, news blogs never lost their character, meaning that they never intended to be possibly impartial news agencies, but rather ways to express conceptions and ideas of their, individual, creators. These same creators also participated in the market or field they covered through their blog. When money also came into the picture, conflicts became inevitable. Blogs and bloggers may infringe rights of third parties mentioned in their blogs (indeed, several blogs have as central purpose to identify "bad" participants in the market they cover); they also may misguide public opinion (and perhaps, shares' value) to their own benefit. Bloggers are also frequently operating through nicknames, and are hard to find (and sue, if applicable). Given the "borderless" nature of the Internet, users are rather advised to exercise caution, than to file later for damages. Regardless of the latter recommendation, however, the fact remains that the development of blogs as known today constitutes a continued source of risk both for users and unsuspecting third parties who may find themselves mentioned in them.

Blogs are also the preferred way of self-organisation when it comes to acts of public opposition. This may be in the form of publishing shocking news (for instance, photos), or organising events or posting breaking news from sites of upheaval or repression. All of the above have been used in more than one instances until today all around the world. Bloggers are sometimes identified and prosecuted; most of their actions, however, are successful, at least from a raising public awareness perspective. The immediate nature and the, at first, anonymity that the new medium affords have made it indispensable to similar causes. Nevertheless the security risks potential is obvious for everyone to see — whether we should live with it or take positive measures to abolish it is a totally different discussion.

Cyber-opinioning came at the time the Internet was invented and has accompanied it ever since. It has developed, taking advantage of enhancements afforded by new technologies, but it has remained in essence the same, affording the option to individuals to express themselves and interact, sometimes anonymously. Misunderstandings, and "crimes" therefrom stem from a misguided perception by authors that expressing themselves over the Internet differs from expressing

themselves in the streets or in the traditional press, as well as, by a reader's award to their readings of more value than they are really worth. Although this situation has often led to serious difficulties, abolishing or even policing it more effectively hardly appears the best (if at all possible) way forward.

23.2.3. *Framing and Deep-Linking (and Associated Practices, Including GoogleNews)*

Practices such as "framing" or "deep-linking" may be categorised, according to the distinction above (under Section 23.1), as infringements of rights that take place in cyberspace and were previously unknown both to humanity and regulators. They both relate to e-commerce and in particular to the so-called cyber-enterprising. In order to properly explain their function, certain clarifications need to be made with regard to the commercial use of the Internet. Because since the first days of the Internet until today no effective business model has been devised to make users pay money (and e-commerce companies incur income) from service provided on-line (indeed, the trend of "free" has gained exponentially in strength [14]) advertisers' money is the obvious alternative. In fact, today the biggest companies over the Internet (and some of the biggest, as least according to their Stock Exchange evaluation, in the world) are solely based on advertising income. However, in order for advertisers to spend their money on Internet sites, they need proof that their clients' webpages are indeed visited by individual users. Individual visits per webpages (or, "hits") have become thus the Holy Grail of the Internet, at least from its business perspective, these days. In fact, "hits" (a term that shall be used here invariably, regardless whether it refers to individual visits or repeated downloads of the same page by one user or in any of its other, technical, distinctions) are the standard measurement of a websites' success. It is according to its number of daily, weekly or monthly hits that its owners ask for advertising spending, mostly in the form of banners affixed onto one or more of the same website's pages. It is according to their number of hits that bloggers count their readership, product- or service-selling websites their potential clientele, search engines their use (and penetration) to the public.

It becomes therefore evident that whoever wants to make money (or even a difference) out of the Internet needs to generate as much as possible traffic to his website, in order to then ask for adequate advertisement spending. The more the hits, the merrier.

In this continued struggle for hit-dominance, it would have been quite extraordinary if a number of deviant practices did not arise, aimed at directing hits towards webpages that do not deserve it. Under this category fall the various offsprings of cyber-squatting (most common today in its form of typo-squatting), that shall however not be analysed in this chapter because of the relatively stable environment accomplished by ICANN to-date, as well as, such tricks as "framing" or "deep-linking".

"Framing" broadly refers to the practice whereby specific webpages are "boxed" or "incorporated" into the websites of third parties other than their owners'. For instance, a newspaper article is included as a whole into a blogger's website; or, real-estate classified ads of a certain website are copied-pasted into another Internet site even under a different or even better presentation method; or, government information webpages are "boxed" into a search engine's results to a query relevant to their content. Evidently, around such "boxes", the advertisements and the Internet site of the perpetrator appear to Internet users.

The obvious result of "framing" is the loss of hits for the original owner of the webpage and the, unworthy, increase of hits for the "framer" 's website. Evidently, in the above example, the blogger will have diverted to his/her Internet site people who want to read that same article but who would have otherwise visited the newspaper's Internet site. The site that copied the classified ads will have increased its number of hits based however on content provided by the original, even cruder, Internet site. And, the search engine will have found a new way for generating hits, diverting them from the official government site from where the relevant webpages were taken. In all these cases, the conflict of interests and rights is plain for everyone to see: the "framing" site increases its income with content that does not really belong to it, while the content-owner loses Internet traffic (in equal or other numbers).

On the other hand, "deep-linking" refers to the practice whereby that internet traffic for the "victim" website is diverted to its internal webpages, where it does not matter that much. In e-commerce websites, mostly their homepage has come to matter; it is this page that attracts the most hits, and it is the hits of this page that receive attention; for instance, a newspaper will count hits on its first page and not necessarily on each webpage containing a single article. By deep-linking to its internal webpages, even without copying-pasting them and framing them into another website, still damage is caused to their owner, because users avoid the homepage (and thus their hit is missed) and visit directly the webpage that interests them.

Websites that engage into "framing" or "deep-linking" customarily claim that they do offer an added-value service to the public, organising information better. People have too little time, and by sorting out huge Internet sites (such as those of newspapers) and guiding them to the exact webpage that interest users is a worthy cause. Additionally, deep-linking at least does not cause much harm, because after all it is normal, and lawful, "linking" (the equivalent of referencing to the academic world), only to the exact webpage and not the homepage (again, the equivalent in the real world is referencing to a page rather than the cover page).

Regardless of the merits of such reasoning, the fact is that by now both "framing" and "deep-linking" have been found unlawful around the world. In more than one jurisdiction, it has been established by courts that these practices constitute unlawful infringements of the IP rights of the original webpages' rightsholders. The legal grounds may vary, ranging from traditional IP (copyright)

law to (EU-specific) database protection legislation (the *sui generis* database right). There is thus not much meaning in continuing the above discussion.

What does however merit discussion is the contemporary forms (or not) of similar practices, the most well-known of which today is GoogleNews (http://news.google.com). As by now everybody knows, Google has established a service free to its users, whereby more than 4,000 news websites are scanned daily, and the news appearing thereon are indexed with a 3-line summary to Google's website. Users may visit Google's site, read the news and the summaries and click on the article, if they wish to, in which event they are guided to the actual webpage (not the homepage). Additionally, users may store keywords in their personal profile, and Google shall alert them whenever a relevant article appears in one of its indexed sources (again guiding them to the actual webpage). From this point of view, the practice is nothing more than a typical deep-linking example, with an information aggregator oranising information and guiding traffic first on his/her own Internet site and then to the internal webpages of its sources. Newspapers that participate in the GoogleNews "programme" evidently lose on hits from their webpages. Nevertheless, such is the power of Google today (or the amount of hits created to its featured articles anyway) that from all around the world, including some of the biggest and best news agencies, only the press from Belgium objected (and, evidently, succeeded). The rest have not reacted; the situation is obviously found at its second stage of the "cyber-enterprising legal process" described above, under Section 23.2.1 — the outcome shall probably depend on the popularity of this new service.

23.2.4. *On-Line Auctioning*

Although auctioning is by no means an activity previously unknown to humanity, the Internet has taken it at a whole different level. What was restricted in the past to expensive assets (real estate or machinery) or art and was fragmented and difficult to participate, which is still the case in the real-world, has nowadays become available to the millions who are now bidding for anything from the most mundane and trivial to the most exclusive and expensive. On-line facilitators have afforded Internet users this possibility. Internet e-commerce sites are offering to sellers the opportunity to upload their goods and the respective asking prices and to bidders the opportunity to participate in a simple but secure on-line auction. Money again is made through advertisement. Facilitators normally do not accept any responsibility for the professionalism of their users — most of the times they are not even aware what is being auctioned through their Internet sites.

It is exactly these unique characteristics of on-line auctioning that have caused various cyber-criminality issues. Sales by individuals to individuals around the world have frequently led to fraud. Unmonitored auctioning has led to crimes being committed whenever yet another vulgar auction (for instance, human-body parts, nazi memorabilia) takes place unnoticed (or, noticed too late).

And, whenever there is profit to be made, various schemes are put to work (for instance, automated-bidding web-bots) that thrive at the borders of either the law or contract. It is these three sources of risk (seller-bidder relationship, subject-matter auctioned and system operation) that taunt contemporary on-line auctioning providers.

Seller-bidder relationships are bound to include some fraud when the numbers rise to the millions; fraud is, expectedly, the greatest security concern when it comes to on-line auctioning. It may come in many forms: sellers may dispatch to successful bidders goods that are far from what was promised on-line. Credit card details that are used for payment by bidders may be put to other, unauthorised, uses as well. The anonymity frequently afforded to both sellers and bidders by on-line facilitators only aggravates the problem. The international element, when combined with the insubstantial value of most transactions, means that any attempt to legal recourse makes no sense, at least from a financial perspective. What we are effectively left with is with millions of individuals being helplessly engaged into international transactions whose proper execution they are in no condition to secure.

This fundamental problem of lack of trust has been addressed in the best way possible by on-line auctions facilitators. Websites making their money out of the number of auctions that take place through them (and the hits and advertising income realised therefrom) are absolutely interested in providing their users with a possibly secure, worry-free environment. Various systems have been put to this end: on one side of the auctioning system secure electronic-payment systems (such as PayPal) are offered to users in order to avoid credit card fraud. At the other, more difficult to regulate, side, scoring systems have been devised in order to generate public trust. According to these systems, sellers are graded each time they successfully complete a sale through an on-line auction. Users are to trust those sellers with the highest scoring. Public trust is thus gained upon a trial-based, past-experience system that is said to resemble as much as possible as the real world, whereby the most experienced and well-known merchants make the most sales.

The subject-matter auctioned in on-line auctioning systems is the second source of risk. With millions of auctions taking place simultaneously some unlawfulness is unavoidable. This may be in the, relatively harmless, form of auctioning prohibited goods (for instance, medicine) to the vulgar (and perhaps hard to believe) recorded cases of human-body parts or nazi memorabilia auctioning. Website facilitators defend themselves on the basis of the fundamental e-commerce legal principle, that providers are not held liable for their users' actions unless they known them (or are notified accordingly). Whenever therefore a prohibited auction takes place, the facilitator shall invariably claim no knowledge of it; if he/she is notified in time, he/she must disrupt it. This legal treatment, unavoidable and ultimately fair as it may be, may save on-line auctioning entrepreneurs from their responsibility for what is actually being auctioned on their webpages but does, however, little good to the credibility of the system altogether.

Finally, the system itself may be bent: auctioning facilitators are, as seen, equipped with secure electronic-payment systems and scoring systems and the law on their actual liability and are hoping for the best, but security concerns are far from resolved. Whenever there is money to be made, various schemes are put to work. Scoring systems may be cheated; in fact, sellers knowing that unless they are able to show some history and positive scoring they will not make any sales will most probably make their first sales to themselves, thus adding up to their profile. Accordingly, any elaborate bidding system can be cheated; because users are expected to bid until the last minute but technical (on-line) restrictions do apply when submitting, web-bots and other applications have been developed that will perform this task for them according to their instructions (for instance, "make my best offer one minute before the auction's ending time). In fact what on-line auctioning is sometimes is a fight between web-bots for last-minute bid submission. Naturally, this "bends" or even blatantly breaks the terms of service of the Internet site hosting the auction, but it is hard to prove (and the site's owner will ultimately prefer not to disturb his/her clients).

On-line auctioning systems are ultimately connected to the issue of trust over the Internet. Cyber-enterprising, in this case, simply refers to facilitating simple transactions between individuals around the world. Some cyber-criminality is bound to emerge somewhere in cyberspace and, because cyber-entrepreneurs are not (could not, as well) be held liable for it, it ultimately is up to individuals to protect themselves. However, public trust needs to be vested in the new medium in order for it to develop; whether by scoring systems or secure payment systems or any other idea that may come up in the future on-line auctioning systems' continued well-being actually depends on it.

23.2.5. *On-Line Gambling*

On-line gambling belongs to the type of cyber-criminality that, as discussed above under Section 23.1, is committed with the assistance of the Internet. In fact, the Internet is ideal for on-line gambling. Its "borderless" and "distributed" character means that gambling sites may be set up anywhere in the world, where they are lawfully allowed to operate, and still make sales to individuals in countries that may have a legislative gambling prohibition. On the other hand, individual users find that they no longer need to travel to casinos or have access to betting shops (or be adults, for the same purposes) in order to gamble; with the assistance of a multitude of gambling Internet sites, they can do so as the comfort of their living rooms. From this point of view, it is a win–win relationship.

Those who do lose out of this are legislative prohibitions and society ethics. A state ban on gambling may easily be circumvented; servers (and their sponsoring companies) may be setup off-shore, individuals who gamble on them are hard to trace. The situation is even worse for those countries that have a state monopoly

(such as the case in may EU Member States): in this case, the Internet has enabled gambling outside state-sponsored channels and governments find it increasingly difficult to explain why these sites should be banned, at least based on reasonable argumentation (if state-sponsored gambling is allowed after all, accepting thus gambling risks to individuals, why is it wrong for private parties to engage in a profitable activity?). Society ethics also suffer: those societies that have chosen not to afford the option of gambling to their members, out of fear for what gambling can do to them, find it impossible to apply their decision to those of their members with Internet access.

Naturally, legislative and other solutions do exist: on-line gambling facilitators may be held liable for breaking the laws of one country although their servers are off-shore and their sites are addressed to the whole wide world, when, according to what has become a basic Internet principle, out of the content of their webpages it can easily be concluded that all or part of them is addressed to residents of that particular country. This, for instance, can be established through flag-enabled special webpages for these users, the languages an Internet site is offered into, its terms of service and other similar case-specific circumstances. At any event, the fact remains that infringement by a website of the laws of a particular country may be established in courts regardless whether it has a domain in .com or country-specific; acquiring thus court protection is possible after all — applying it is a totally different issue.

When application of the law or a court decision is the issue at hand, more radical measures are needed. Because gambling sites will normally operate behind off-shore companies, located in jurisdictions, that is, that are broadly negative to the option of losing valuable tax income, usually international judicial co-operation agreements for the enforcement of court decisions are of no use. This is why countries, such as the United States, have recently launched a two-front, practical thought-of attack on on-line gambling. First, they attacked their payment systems; then, they attacked the big players, those of on-line gambling sites that were audacious enough to become big enough to be listed in Stock Exchanges and behave like multinational enterprises.

The first attack was easy enough: all on-line gambling is obviously based on credit card payments. And, credit card payments are easy to trace and are also carried out by well-established companies that want no trouble with the law. What America, therefore, did what to make all on-line gambling-related credit card payments illegal. Credit card companies had to comply — on-line gambling sites were suddenly deprived of their source of income (at least from Americans).

The second offensive included the arrest of certain high-profile CEOs or (on-line gambling) company owners on American soil, demonstrating thus that no one is safe, no matter how big his/her company is (regardless whether it has been until recently lawfully operating in America too, and whether it continues to do so in others, equally sophisticated, jurisdictions across the Atlantic).

Reactions in Europe towards on-line gambling greatly vary. Many Member-States sponsor a state monopoly on all gambling activities, a practice that may conflict with more than one field of basic EU Law. Those Member-States profiting from a very strong gambling industry that has fully taken advantage of cyberspace (for instance, the United Kingdom) are obviously positive and would like the markets of other Member-States, profiting from a state monopoly, to open. The latter have reacted in various ways in order to protect their internal markets: sometimes, in the cases for instance of Greece and Italy, it has gone as far as prohibiting or attacking Internet cafes (being popular points of access to individuals). A number of court decisions both at Member-State level and even of the European Court of Justice have thrown some light into the matter. However, until the time this analysis was written, no final decision had been reached for opening up the markets; in principle, however, it is evident that the existence of a state monopoly per se deprives governments from any argumentation on whether gambling (in its on-line or off-line format) is good for their citizens — discussions have shifted by now on how to preserve tax income and Stock Exchange (government-owned) corporations' evaluations.

At any event, the fact remains that countries are broadly at war with on-line gambling, sometimes winning and sometimes losing battles. Regardless whether opposed to the idea itself, as is the case in America, or fighting to preserve profitable state monopolies, as is the case in the EU, the issue of on-line gambling raises eyebrows among legislators and security officials in both sides of the Atlantic. Users, on the other hand, are not as negative: on-line gambling sales are peaking. Users also enjoy an unprecedented freedom to gamble (never before was it so easy to any European to gamble on American sports) and to compete — once poker went on-line its international champions came in the unlikely forms of 19-year-olds who, instead of having to spend their whole life in bars, spent a lot of time on the Internet playing with other players around the world and improving their technique. Choice is ultimately good for them.

The internet has therefore enabled a question of ethics to be repeated: is gambling to be allowed or not? Societies that thought they had already answered that had better think again — the Internet has changed all their data. If the society's answer to the above question was an unequivocal "yes", then its member may only rejoice at the limitless options that are opened to them by the Internet. If the answer to the same question has been a (hypocrite's) "no, as a general rule, but yes when made by the government", then the Internet has emptied this society of its arguments: no more is gambling unsafe, connected to crime in shabby-looking places — the on-line Internet sites are a polished and secure way of doing business. This society had therefore better think again whether tax income has not blurred its judgement criteria. Ultimately, it is only those societies that prohibit gambling altogether that face the greatest threat by the on-line environment; because controlling it in cyberspace is more or less impossible that they might need to re-evaluate their original decision. The Internet has in fact been a catalyst in the

case of on-line gambling, depriving hypocrites of their arguments and confronting general bans against an individual choice.

23.2.6. *On-Line Advertisement*

On-line advertisement has of course nothing to do with crime. Quite the contrary: it is in effect because of on-line advertisement that the internet developed in the way we know it. As already explained (under Sections 23.2.1 and 23.2.3), practically all e-commerce models have failed to identify until today any serious source of income other than advertising revenue. Based on the number of individual visits per webpage, advertisers are willing to pay its owner in order to place advertisements (in the form of banners) on them. Search engines (most notably, today Google, but others too) have devised similar methods to commercialise on users' searches: each time a term is searched, users are served apart from the results with, sponsored, links to goods or services that might be of interest to them. Software industries are trying to make models of on-line advertisement as effective as possible. As long as advertisement income continues to flow into the Internet, its existence (and even its development into Web 2.0 or Web 3.0) is secure.

On-line advertisement, in itself, has therefore nothing to do with cyber-criminality. Those few legal issues that were posed by it (for instance, potential infringements by AdWords to trademarks) have been resolved by now. The reason why it shall be briefly elaborated here pertains to the technical means it uses or the business decisions it makes from time to time in order to increase its effectiveness, and the effect the latter have on the law.

Banners constitute intrusive technology. As all of us know by now they tend to pop-up anywhere on webpages, sometimes obstructing our view or even refusing to go away until they have displayed their message in full. What is perhaps unclear to most of us is that banners are elaborate computer programs. Apart from their impressive graphics, they have code behind them that carries out a series of functions, from displaying properly depending on our system configuration to transmitting information back to their owners. Banners are seldom one-way communication tools that, once incorporated onto webpages, their job is to simply stay there and make themselves visible. Under normal circumstances, they are expected to keep communicating with their owners long after they have been attached onto webpages. The type of communication and the depth of information transmitted is the object of some, security and legal, controversy.

To begin with, banners and other on-line advertising methods are invariably security loopholes. Because of their need to communicate information back to their owners, they need an open communication channel from each computer they play on. An open communication channel is, understandably, very bad for security network. This is the reason why most contemporary Internet browsers come equipped with security settings that by default prohibit pop-ups from showing; users may disable them at their peril. On the other hand, on-line advertising in fields such as porn

may have even worst implications for those unlucky users who visit relevant Internet sites: apart from all the above, it may come bundled with malicious software (for instance, dialers) that will attempt to defraud unsuspecting visitors and non-experts of their money.

Evidently, any malicious actions by banner-covered software onto individual computers are crimes committed by their owners (or even the site owners, if they were aware of it). Most countries have by now implemented computer crime legislation that normally covers any unauthorised actions taking place on computers. The problem in this case is not that much identifying the crime but rather applying the sentence; the "distributed" nature of the Internet means that perpetrators may reside off-shore, while users will normally prefer to format their hard drive than take the expenses and time to pursue them.

Even if users are not bothered by two-way communication happening on their computers, in return of watching these fancy videos, they would probably be interested to find out that on-line advertisement schemes in their more aggressive forms systematically make profiles on them. This is a business choice by on-line advertisers: in order to improve the effectiveness of their practices, they try to profile users. In fact, the Internet advertises exactly on this added-value functionality, as opposed, for instance, to television. While on television, broadcasting of commercials is random and advertisers have no way of knowing if they were broadcasted to interested parties or if individuals really saw them, the Internet is more accommodating. Mechanisms do exist to ensure that ads showing on users' computers are relevant to their taste and preferences; the same mechanisms let advertisers know whether users have viewed their ads (by clicking on them) or not. All these are accomplished by more or less making profiles on users. User preferences, IPs, sites visited etc. are all meticulously recorded, by way of installing relevant software onto a computer (through, for instance, banners or cookies), and are then transmitted back for further processing. Once profiles have been prepared, users are only shown those banners that are thought to be more relevant to them. Although this practically breaches every known data protection notion and principle, at least in the EU, perpetrators are hard to track because they tend to operate from friendlier jurisdictions. Here again, the costs required to do this are prohibiting.

On-line advertising is thus interesting from a security point of view when it comes to its business models and the decisions behind them. Because of the struggle for (on-line) survival, aggressive decisions are frequently taken that disregard both the law and fundamental security requests by users. The situation is aggravated by contemporary e-commerce trends. Once it has been established that advertisement income is the only sustainable solution for Internet services that users want to be given out to them for free [14], the only way forward is for on-line implementations to increase in number and improve in quality. This will unavoidably lead to increased attacks on individual privacy, and may even create some additional loopholes in

computer security. Although each one of us should be grateful to on-line advertising and the money it has spent in order to make the Internet what it is today, we should all at the same time be watchful when it asks for more privacy and security compromises in order for it to thrive.

References

1. L. Edwards, *The New Legal Framework for E-Commerce in Europe* (Hart Publishing, 2005).
2. T. Hingston and S. Adam, Click-through banner advertising: A technical review, available at http://ausweb.scu.edu.au/aw2k/papers/hingston/paper.html.
3. http://conferences.theiet.org/ie06/index.htm.
4. I. Lloyd, *Information Technology Law*, 4th Edition (Lexis Nexis UK, October 2004).
5. M. I. Melnik and J. Alm, Reputation, information signals, and willingness to pay for heterogeneous goods in online auctions, February 2003, Available at SSRN: http://ssrn.com/abstract=452820.
6. OUT-LAW News, Google proposes 'crumbled cookies' in privacy pledge, 1 October 2007, http://www.out-law.com/page-8511.
7. C. Reed and J. Angel, *Computer Law*, 5th Edition (Oxford University Press, 2003).
8. *The Economist*, Leaks and lawsuits, 6 March 2008.
9. *The New York Times*, Italian case may open up crossborder gambling, 07 March 2007.
10. The Register, Google news faces 1m fine in Brussels, 18 September 2006.
11. The Register, Google loses Belgian news appeal, 22 September 2006.
12. The Register, US restricts online gambling, 12 July 2006.
13. P. Todd, *E-Commerce Law* (Routledge Cavendish, 2005).
14. WIRED, Free, 16 March 2008.
15. WIRED, Online poker: Is it legal?, 5 August 2006, http://www.wired.com/techbiz/media/news/2006/08/71547.
16. WIRED, Refusing to fold, Online poker players bet on prohibition repeal, 21 May 2007, http://www.wired.com/politics/law/news/2007/05/gambling_laws.