Harvard: Changing Legal Systems Governing the Internet

From July 1-5, 2002 the third Internet Law Program took place at the Harvard Law School, Cambridge, Massachusetts (USA). Organized by the Berkman Center for Internet and Society, the purpose of this program was to provide more than 100 participants from 23 countries with a comprehensive survey of the changing legal systems that govern the Internet. There was also the opportunity to discuss recent legal developments with leading scholars in the field.[1]

Professor Lawrence Lessig (Stanford University) started the first of twenty 90-minute lectures during this intensive five-day program with some thoughts on how cyberspace could be governed. In his view, there are four elements that influence our behaviour and freedom in cyberspace: law, social norms, the market and – crucially – architecture. By architecture, *Lessig* meant the software and hardware running the Internet. While the early architecture of cyberspace made it difficult to regulate, emerging changes in the architecture of the Internet make regulation now possible. Examples of such changes include the introduction of "cookies" that track Internet surfing, packet "sniffers" that can read e-mail, and technologies that map Internet protocol addresses to identify the geographic locations of websites. At the end of the session, *Lessig* drew a pessimistic conclusion: "The interaction between commercial and government interests transforms the Internet from something that is unregulable to an architecture that is more perfectly regulable than life in real space."

Professor William Fisher III (Harvard University and faculty chairman of the Internet Law Program) talked on new developments in the field of domain names. According to *Fisher*, there are at least six ways in which domain names on the one hand and trademarks on the other hand clash:

- Cybersquatting: the practice of registering domains similar or confusingly similar to names held by trademark owners.
- Typosquatting: the practice of registering names with a common typographical error for popular domain names.
- Competing use: the practice of registering a website to criticize a competitor.
- Non-competing use: the practice of registering a private name that happens to be the same as the name of a company.
- Reverse domain name hijacking: a tactic used in bad faith by a complainant to attempt to deprive a registered domain-name holder of a domain name.
- Parody and commentary: the practice of registering a website for the purpose of a creating a critical parody.

According to *Fisher*, the primary legal system for resolving conflicts of this nature is the Uniform Dispute Resolution Policy (UDRP), of the Internet Corporation for Assigned Names and Numbers (ICANN). The UDRP is a streamlined arbitration process that allows people to challenge domain name registrations in an ICANN-accredited forum of their choice. Another source of protection for trademark holders is the US Anticybersquatting Consumer Protection Act (ACPA) which goes further than the UDRP in some respects. The ACPA permits heavy penalties and gives litigants the opportunity to go after the alleged "property" itself. In addition to the UDRP and ACPA, US common law, traditional trademark law and a variety of other conventions and treaties could provide a structure to harmonize domain name disputes. Each type of conflict has produced an array of case law, with nearly 80 percent of the decisions ending in victory for the trademark holders. Due to variety of case law and overlapping rules, the situation is quite confusing at the moment, *Fisher* said. Possible reforms of the UDRP process, according to *Fisher*, include randomly assigning the forum for resolving disputes rather than allowing complainants to choose it, establishing an appeals process, and requiring complainants to post a $ 1,000 bond in order to discourage baseless complaints. Other solutions *Fisher* suggested are creating more top level domains, increasing the latitude for criticism and parody and a return to the first-come, first-served doctrine.

Guest Lecturer *Professor Julie Cohen* (Georgetown University) spoke about the core legal cases affecting the field of intellectual property law. She focused her lecture on section 1201 of the Digital Millennium Copyright Act (DMCA), which prohibits circumventing -access controls. *Cohen* reviewed three key-cases concerning the circumvention of digital protection systems:

- In *Universal v. Reimerdes* (DeCSS case), a Norwegian teenager cracked the DVD decrypting system. The hacker magazine 2600 published a Link to the software and was consequently served an injunction against the linking. Citing section 1201, the judge decided that the activity of the magazine constituted "trafficking" in a circumvention-technology.
- In *Felten v. RIAA* (SDMI case), a computer science professor from Princeton cracked a system for protecting the playing, storing, and distribution of digital music. The Recording Industry Association of America (RIAA) warned *Professor Felten* that he would be sued if he published the results of his research. In response, *Felten* sought for a declaratory judgement challenging lawfulness of a civil suit or prosecution. The court dismissed the case, accepting RIAA's assertion that it had never intended to sue *Professor Felten*.
- In *US v. Elcom* (Adobe eBook case), a Moscow-based company disabled the copy protection on the Adobe eBook reader. The programmer of this circumvention was arrested when he came to the US to attend a conference. The charges against him were eventually dropped on the condition he to cooperate in the prosecution of his company.

All the three cases address the question of what section 1201 means by "a technological measure that effectively controls access", *Cohen* explained. Obviously, "effectively" does not mean hack-proof. According to the court there is no requirement that the technology has to satisfy some standard of effectiveness. The threshold that determines if a technological measure is effective enough is unclear at the moment, *Cohen* said. The legal landscape is clearer regarding linking to software that circumvents a copy-protection. If done knowingly, linking is equivalent to distribution. In the future, *Cohen* fears that the development of stan-

1) Find more information about the program at *http://cyber.law.harvard.edu/ilaw*.

dards and technologies will become more difficult unless section 1201 is changed. At the least, a "zone of safety" where researchers can operate without fear of prosecution is needed.

Following *Professor Cohen's* presentation, *Lawrence Lessig* discussed *Eldred v. Ashcroft* (*cert. granted* 122 S. Ct. 1062 (2002)). *Eric Eldred* publishes works that are already in the public domain, making them widely and freely available on the Internet (similar to the more known Gutenberg Project). He was especially eager to post certain materials that were due to pass into the public domain following the expiration of their copyright. But Congress disrupted Eldred's plans when it passed the Copyright Term Extension Act (CTEA) in 1998. *Lessig* and Eldred got together and filed a suit, arguing that the CTEA violates the "limited time" provision of the US Constitution's Copyright Clause by granting retroactive copyright expansions. The law, which was strongly favoured by copyright interests, added 20 years to both existing and future copyright terms, extending protection to 70 years beyond the life of the creator and 95 years for a work copyrighted by a corporation. *Eldered* will be argued before the Supreme Court this fall.

Lessig suggested a system in which copyrights would expire after five years unless their owners re-register them. Under this proposal, a copyright would expire after the end of the term set by Congress. *Lessig* said that, after Congress' efforts to extend retroactive copyrights is checked, the next stage in the battle for the public domain is to institute a system of taxation for intellectual property. He proposed a $ 10 annual tax on each copyrighted work. If the owner failed to pay it for three successive years, the copyright would revert to the public domain.

Conclusion

In conclusion, the program at Harvard Law School raised nearly all the important issues in the field of Internet Law. Clearly, only the most interesting lectures could be mentioned here. Other renowned speakers included Professors *Charles Nesson* and *Jonathan Zittrain* of Harvard Law School as well as *Professor Jerry Kang* from the University of California Los Angeles. The next Internet Law Program will take place in early 2003 in South America. It will be worth attending.

Christian Solmecke, Cologne.

(Further information about the author on p. 160.)