UNITED KINGDOM

The UK Electronic Communications Bill: The Law of the Future

By Phil Auld of Birmingham Solicitors Wragge & Co.,
tel.+44 121 233 100, fax+44 121 214 1099.

Introduction

What will harm industry, hold back the growth of e-commerce, undermine consumer protection and violate the European Convention on Human Rights? The newly released UK Electronic Communications Bill will, according to the think tank of the Foundation for Information Policy Research. In contrast, Intel and Microsoft have both welcomed the Bill as defining the ground rules for the growth of electronic commerce, which is vital to the UK's competitiveness.

As these examples suggest, overall reaction to the draft Bill produced at the end of July has been mixed.

Background

The Electronic Communications Bill has changed dramatically since it was first created as the E-Commerce Bill. It was the fundamental element of the Government's White Paper which was unveiled last December, but due to heavy criticism from industry and lobbyist alike, it has since been amended so that it has lost most of its bite.

Despite the length of time that has already elapsed since it was first proposed, the Bill has only been produced in a draft form and will not be debated in Parliament until the autumn. It is intended to create an appropriate legal and regulatory environment for secure e-commerce and to provide legal certainty for transactions created in a digital environment.

Content

The Bill has three main parts: cryptography service providers, facilitation of e-commerce and investigation of protected electronic data.

Part I deals with cryptography service providers, and proposes a register of approved providers. Cryptography is the key to successful e-commerce. Without a secure digital environment in which to send financial information to complete transactions, e-commerce will not develop into the trading environment for cryptography service providers. These service providers will provide users with the means to utilize digital signatures and to ensure secure transmission of data.

Part II is concerned with the facilitation of e-commerce, data storage, etc. and in particular with the facilitation of electronic signatures and related signatures. This part gives digital signatures the legal recognition they require. It means that contracts concluded digitally would be legally binding, a point that would avoid any doubt in litigation.

Part III deals with the investigation of protected electronic data, and the forced disclosure of encryption codes to law enforcement agencies. It is well-known that the criminal world is utilizing the web to its own advantage. It is not surprising, therefore, that the Government has made provision for decoding encrypted electronic data. Under the Bill the police will have the power to demand decoding keys, and failure to produce them can result in a two-year prison sentence.

Conclusion

After much internal and external debate, the Bill has created a much more watered-down regulatory frame-work for the future of e-commerce. The Government's vision of e-commerce is one of a relaxed legal framework in which to allow the technology to develop. The Bill contains some worrying features that give both law enforcement bodies and the Government the ability to invade privacy in the hope of preventing crime. At the very least, however, anyone trading on the Internet now has a much clearer idea of how to shape their website and e-commerce vision.