Theories of government control of the internet

ASSIGN BUSTER

Critically analyse Lawrence Lessig's argument that the ability of governments to control activities within cyberspace is determined by the codes of cyberspace.

The Internet enables individuals to access a ' new realm of human activity' [1] and has affected the lives of billions of people. Due to the effect that the Internet has on citizens of all states, many called for legal involvement. The increasing use of the Internet for commercial purposes sparked initiatives to attempt to legally regulate the system [2] . Internet traffic is carried over vast communications networks which are owned and controlled by public and private sector providers. The European Commission has had to step in on a number of occasions were a merger of providers would be a breach of competition laws, due to the stake of the market each provider has. [3] Ian Lloyd states that the internet is similar to other forms of communication as it is heavily regulated but it lacks specific legal provisions [4] . The Communications Act 2003 is said to have few provisions regarding internet regulation. At a national level, communication regulation has operated for years and international agencies like the International Telecommunications Union adopts a more functional role towards regulating. As the Internet is a global tool, policing and regulating it seems a considerable legal and political question.

Some argue that the internet is governed by internet users as they reach a consensus. Regulatory structures are seen to evolve on their own rather than develop in an organised way. Lawrence Lessig believes that governments' attempts to regulate the internet will fail. He concedes however, that

governments may be able to regulate the architecture of the Internet and in turn it could develop into a form of regulation across all areas [5] . Lessig proposes that internet sites should have greater power to identify customers so as to recognise individuals' credentials [6] . This form of indirect regulation would form a basis of self-regulation within cyberspace. He states that the state may affect Internet service providers (ISPs) from regulating an aspect which will make it more difficult for it to do business. [7] Further e-commerce will lead to greater involvement of the state due to the commercial nature of these transactions thus making identification of parties easy. Lessig continues by warning that if the Internet is regulated by a ' closed code' then the state's effectiveness to regulate remains unchanged. If however, the Internet adopts an ' open code' then it will act as a check on the governments' power. [8] The internet is defined by a set of protocols (TCP/IP) which are rules for how your computer will interact with a server and vice versa. These protocols make interaction possible as users agree on simple protocol of data exchange. A ' closed code' has bothered many which believe that an ' open code' fits in with the values of the internet of free and easy file sharing. This code is a public code, which people may view without gaining permission of others and so facilitates transparency.

Alternative views state that the rise in e-commerce will result in greater input of the state, but there are problems connected to regulating e-commerce. Rowland & Macdonald point out there are inherent difficulties when regulating e-commerce as it is not geographically or jurisdictionally restricted and there are also competing pressures whether to regulate or not to regulate as seen in Lessig's argument [9] . Lars Davis states that two

dangers must be avoided [10] . The first danger is under-regulation, as this would lead to the perception that e-commerce is an activity that contains an unacceptable high element of risk and so it will prevent parties from people participating in commercial activity on the Internet. This decrease in commercial activity will be regardless whether they are commercial entities or they are consumers. The second danger is over-regulation. The market would become rigid and inflexible which can be said to be the Internet's most appealing feature. This in turn would lead to a stifling in development and perhaps in commercial entities setting up in jurisdictions which have less rigid regulations. Davis states that these ' regulation havens' which have a reduced or minimal control is a distinct possibility. The overly strong control could be detrimental to the attractiveness of parties conducting e-commerce. The benefits offered by e-commerce would be lost to markets with less rigid regulations and so economic development would suffer in those countries which have rigid regulations.

Rowland & Madonald note a further difficulty in deciding where the scope of a particular state's regulation should extend [11] . They ask the question whether it should extend to ' businesses that are based in another state but which conduct business with consumers or businesses in the particular state?' The geographical factors which usually make the scope of a jurisdiction easy to see are blurred when relating to internet commerce. They use the example of the EC Directive on Certain Aspects of Electronic Commerce in the Internal Market [12] to show an attempt to create a ' balance point' between member states and regulating e-commerce. The Directive recognises the difficulties which commercial entities face when

having to take into account different legal regimes. The ‘ country of origin’ principle which EC member states adhere to, allow the regulations of one state the right not to be discriminated against the regulations of another. In other words, once marketed in the home state, it can be marketed in all member states. However, these regulations which provide a balance for e-commerce provide little help when dealing with commercial entities that are not based in the EU. By using the Directive as an example, we see that incompatibility with its clauses regarding e-commerce could result in an action being taken and a case being brought in the European Court of Justice (ECJ) and a judgment against a party. If the commercial entities are not EC member states then there is no authoritative organ which can force a party to comply with the regulations.

Amit Sachdeva proposes that rules governing private international law are inadequate to deal with e-commerce [13] . Sachdeva states there are four solutions to the problem of regulating cyberspace and its jurisdiction. First, the laws could be expanded to include the Internet. This suggestion is taken by Davies but as noted, the problem of an over-regulated system would be detrimental to many economies. Secondly, the establishment of a new international organisation to propose a set of rules appropriate for cyberspace jurisdiction would be beneficial to governments when attempting to legislate. Thirdly, these decisions need to take into account commercial entities acting as a decentralised body of various actors and stakeholder. Lastly, he proposes a treaty based international harmonisation model where rules are certain and predictable and at the same time flexible in order to ensure that the potential benefits of this technology are meaningfully

consumed by individuals [14] . However, Sachdeva warns that a comprehensive treaty based solution on all possible issues is an unrealistic target as the apparent youth of the Internet suggests that a number of complex issues are yet to be seen [15] .

Georgios Zekos believes that new terminology, which recognizes the complexity of the Internet relationship and state, is necessary [16] . He suggests that a cyberspace jurisdiction should be used for cyberspace actions as their actions are only felt in cyberspace. Zekos proposes that cyber courts and cyber arbitral tribunals could have jurisdiction to solve all actions taking place on the net and the enforcement of their awards and decisions will be made according to international conventions on internet enforcement and e-awards [17] . Therefore, cyberspace does not owe sovereignty to any state but only to cyberspace itself.

Conclusion

Before adopting any model or any combination of different models, it must be remembered that the internet is here to stay, and so is the potential to commit and facilitate unlawful acts, and the resultant litigation by commercial entities or individuals. We have heard of Lessig’s argument, but have also seen acts made by the EC in order to regulate internet use. Certainly, with growing numbers of Internet users and the growth of e-commerce, more breaches of law will arise and it is for the states to find an appropriate balance between over-regulating and under-regulating the Internet.

Bibliography

Johnson, D. R. and Post, D. ‘ Law & Borders–The Rise of Law in Cyberspace” (1996) 48 Stanford Law Review

Lessig, L. *The Code and other laws of cyberspace* 1999. New York, Basic Books.

Lloyd, Ian J. *Information Technology Law 5 th ed.* 2008. New York, Oxford University Press

Reed, C. & Angel, J. *Computer Law: The Law and Regulation of Information Technology 6 th ed.* 2008. New York, Oxford Universtiy Press.

Rowland, D. & Macdonald, E. *Information Technology Law* 2008. London, Cavendish.

Sachdeva, A. M. ‘ International jurisdiction in cyberspace: a comparative perspective’. *Computer and Telecommunications Law Review* 13(8), 2007; 245-258.

Zekos, G. I. ‘ State cyberspace jurisdiction and personal cyberspace jurisdiction’. *International Journal of Law & Information Technology* 15 (1) 2007. pp 1-37.

Footnotes

[1] David R. Johnson and David G. Post, (1996)p. 1367

[2] Liability for breach of the statutorily implied terms as to the quality of goods in s. 14 of the Sales of Goods Act 1979.

[3] Proposed merger of MCI/Sprint and Worldcom. Case No. COMP/M. 1741-MCI.

[4] Lloyd (2008) p. 457

[5] Lessig (1999) p. 49

[6] Lessig p. 50.

[7] P51. He uses an example of a mandatory ‘ traceability regulation’ where software could trace the user when he provides minimal level of identification. The state could then legislate, making it mandatory for banks to do business with ISPs which have traceability software.

[8] Lessig p 100

[9] Rowland & Macdonald (2008) p. 243.

[10] Lars Davies-www. scl. org/content/ecommerce, s1. 3. 2. Report funded by the Society for Computer and Law.

[11] Rowland & Macdonald (2008) p. 244.

[12] 2000/31/EC

[13] Sachdeva (2007) p. 245.

[14] Ibid p. 255.

[15] Ibid p. 256.

[16] Georgios Zekos (2007) p. 2

[17] Ibid p. 36.