Robin Mansell

Introduction - human rights and equity in cyberspace

Book section

Original citation:
Originally published in Murray, Andrew D. and Klang, Matthias (eds), *Human rights in the digital age*. London, UK : Glasshouse Books, 2004, pp. 1-10.

Introduction – Human Rights and Equity in Cyberspace

By Robin Mansell

Introduction

Summit meetings and world conferences have been convened on issues ranging from sustainable development to social development, and women and children. In December 2003, the World Summit on the Information Society (WSIS) was convened under the auspices of the United Nations. This meeting aimed to stimulate action to ensure that the information societies that are emerging today are more, rather than less, equitable than the societies that have preceded them. Summit meetings generally lead to declarations of principles and intended actions. These are the result of lengthy negotiations that seek to find common ground between the disparate interests of government, business and, in the case of the WSIS, civil society, representatives from around the world. One important area that engendered considerable debate in the case of this Summit and the necessity for compromise was a core issue that is addressed in this volume – human rights and their legal protection.

Human rights in the digital age are being contested very openly today. The text of the WSIS Declaration of Principles espouses a common vision of the information society, particularly with respect to human rights. For example:

> ‘*We reaffirm* the universality, indivisibility, interdependence and interrelation of all human rights and fundamental freedoms, including the right to development, as enshrined in the Vienna Declaration. We also reaffirm that democracy, sustainable development, and respect for human rights and fundamental freedoms as well as good governance at all levels are interdependent and mutually reinforcing. We further resolve to strengthen respect for the rule of law in international as in national affairs. …
>
> *We reaffirm*, as an essential foundation of the Information Society, and as outlined in Article 19 of the Universal Declaration of Human Rights, that everyone has the right to freedom of opinion and expression; that this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. Communication is a fundamental social process, a basic human need and the foundation of all social organisation. It is central to the information society. Everyone, everywhere should have the opportunity to participate and no one should be excluded from the benefits the Information Society offers
>
> Nothing in this Declaration shall be construed as impairing, contradicting, restricting or derogating from the provisions of the Charter of the United Nations and the Universal Declaration of Human Rights, any other international instrument or national laws adopted in furtherance of these instruments.’[1]

[1] World Summit on the Information Society (2003) ‘Declaration of Principles’, WSIS-03/GENEVA/DOC/4-E, 12 December at http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!MSW-E.doc accessed 29 Feb 04, paras. A.3, 4, 18.

The Declaration goes on to emphasise the need to foster an inclusive information society and to ensure the ability, not just to access information and to communicate, but also to contribute. Observations are made about the need for capacity building and for an enabling institutional and legal environment. On issues of building confidence and security in the use of information and communication technologies, the Declaration has this to say:

> 'Strengthening the trust framework, including information and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society. …
>
> It is necessary to prevent the use of information resources and technologies for criminal and terrorist purposes, while respecting human rights….
>
> All actors in the information society should take appropriate actions and preventative measures, as determined by law, against abusive uses of ICTs, such as illegal and other acts motivated by racism, racial discrimination, xenophobia, and related intolerance, hatred, violence, all forms of child abuse, including paedophilia and child pornography, and trafficking in, and exploitation of, human beings'.[2]

Issues of trust, protection from criminal behaviour, and the applicability of international and national legal frameworks are clearly signposted in the WSIS Declaration. The declaration is accompanied by a Plan of Action.[3] The actions envisaged are numerous and are aimed at reducing 'digital divides of many different kinds. However, the documents are silent with respect to how existing and new interpretations of the law should apply nationally or internationally and on whether variations between countries mean that the Internet makes law enforcement virtually impossible.

Following the WSIS there has been much discussion about whether the Summit simply provided a costly opportunity to foster a hollow rhetoric about the need for 'digital solidarity' or whether it succeeded in mobilising a major step-shift in the priority that will now be given to finding the resources to implement the high ambitions of the authors of the Declaration and Plan of Action. A clear call is made for research to unveil the causes and consequences of developments in all of the facets of the digital age.

An essential prerequisite if the respect for human rights that is embedded in the WSIS Declaration is to be upheld is investigation of the way legal institutions, practices and interpretations are influencing today's information societies. An important aspect of this field of inquiry is research on the way cyberspace is being experienced by people in the very disparate contexts of their everyday lives. The contributors to the present volume tackle these issues from a variety of vantage points. Central to this volume is an inquiry into human action and human rights in those instances where it is mediated

[2] Ibid, paras. 35, 36.

[3] World Summit on the Information Society (2003) 'Plan of Action', WSIS-03/GENEVA/DOC/5-E, 12 December at http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!MSW-E.doc accessed 29 Feb 04.

by the technologies of the digital age. The chapters encompass a wide range of issues including the production and consumption of digital content, the means of control over unwanted intrusions to individual's privacy, and emerging means of governing in cyberspace.

Globally and locally today's information societies are underpinned by digital technologies. These technologies enable applications that may be empowering for some people, enabling them to develop new ways of seeing the world around them. Ubiquitous networks are at the heart of the digital age. They are becoming familiar to people in all parts of the world, albeit, unevenly so. The Internet allows for use of chatrooms, email, and voice communication by people representing numerous interests, values, and aspirations. Together with the World Wide Web's enormous repository of information, the Internet is limited in its application only by the limits of human imagination. Within the digital spaces – or cyberspaces – of this century, there are many opportunities for new forms of business and governance as well as for new forms of criminal or unwanted behaviour. Many of these also create the potential for changes in behaviour and perceptions of the non-virtual world.

One of the key findings of recent research on the way digital technologies and the Internet are mediating our lives is that off-line conventions and practices do not diminish in importance in the face of new cyberspace developments. In some cases, cyberspace simply offers a complimentary space to conduct familiar activities, while in others, the new virtual spaces amplify existing activities or create opportunities for completely new activities and behaviours.[4] While many efforts are underway to foster e-strategies for the development of new forms of electronic commerce and electronic government as well as host of other applications, the darker side of cyberspace is often shrouded in mystery or revealed only by the media as 'moral panics' over signs that the Internet is untrustworthiness or that the riskiness of cyberspace is substantial.[5] This collection of papers offers a research-based assessment of the implications of the law and its evolving institutions for the protection of human rights and greater equity in cyberspace developments.

Consent and Possession in Cyberspace

The volume opens with Bela Chatterjee's (ch. 2) examination of the cyber sex phenomenon. This involves the use of digital technologies including the World Wide Web to provide and exchange information about prostitutes or pornographic materials. She notes that, while cyberspace may enable women to engage in the sex trade on more favourable terms to themselves, there are also new opportunities for cyber stalking, 'virtual' pimps and an intensification of harm and exploitation. She reviews UK, European and international legislation and protocols that are intended to deal with these issues. While human rights are being recognised and legal and socio-economic solutions to protect women from sexual exploitation are being devised, she

[4] See Mansell, R. and Steinmueller, W. E. (2000) *Mobilising the Information Society: Strategies for Growth and Opportunity*. Oxford: Oxford University Press; Silverstone, R. (1999) *Why Study the Media?* London: Sage Publications.

[5] See O'Hara, K. (2004). *Trust: From Socrates to Spin*. Cambridge: Icon Books; Thomas, D. and Loader, B. D. (Eds) (2000) *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. London: Routledge; Wall, D. S. (Ed) (2001) *Crime and the Internet*. London: Routledge.

suggests that there is little recognition that civil and political rights are ‘gendered’. The cyber sex trade no longer necessarily involves movement and travel, creating new challenges for legislators and it continues to be unclear as to the circumstances under which consent may be deemed to have been given or not given in cyberspace.

The infringement of children’s rights is central to Marie Eneman’s chapter (ch. 3) which tackles the difficult issues of child pornography involving the abuse and harm of children. She warns that digital technologies not only make it easier and less costly to produce pornographic content, but software can also be used to produce ‘morphed’ images which fall uncertainly within the ambit of existing law. Anonymity and closed Internet-based membership communities also protect paedophiles, make content production a potentially lucrative activity, and enable contacts to be made with children on- and offline. Although there is a Council of Europe Convention on Cybercrime which deals with child pornography, Eneman highlights gaps in existing legislation such that the meaning of ‘possession’ of child pornography is open to question because of the immaterial nature of this form of digital content.

Governance, Liability and Balance

Douglas Vick’s (ch. 4) discussion of the implications of cyberspace for the control of hate speech, begins with the observation that ‘no society in the world has concluded that free speech is an absolute barrier to state regulation of harmful expression’. The governance of cyberspace is often said to be beyond the capabilities of the nation-state, yet this chapter shows how differences in national law have implications that make it very difficult to achieve a universally applicable definition of how to protect human rights in the face of the propogation of hate speech over the Internet. Vick stresses that in the US, the prevailing view is that the best way to counter hate speech is rebuttal by others, rather than by sanctions imposed by the state. It is also the case that hate speech laws may be enforced against marginalized members of society, succeeding only in amplifying resentments. Neither hate speech laws nor a laissez faire approach address the underlying problems of poverty, social isolation and ignorance that give rise to group hatred. In this chapter, the difficulties of governing the Internet are posed as matters for social policy as well as for legislators.

Closely related to this issue is the appropriate balance between the protection of reputation from defamatory speech and the right to freedom of expression. In her analysis of this issue, Diane Rowland (ch. 5) defines defamation as statements that are ‘injurious to the reputation or dignity of the person allegedly defamed, it must be published or communicated to another who must understand its connection with the person allegedly defamed’. She shows that, in practice, there is a ‘hierarchy of speech’ protection. Internet mediated speech raises issues including the standard to be applied, where publication is deemed to occur and the jurisdiction within action can be taken. Should liability fall only on the originator of an allegedly defamatory statement or on an Internet Service Provider (ISPs)? This chapter draws attention to the potentially ‘chilling’ effects of imposing liability on the latter, such that ISPs may remove information even before there is judicial verification that it is defamatory. Despite the potential of the Internet to amplify defamatory speech, Rowland insists that ‘the application of existing legal rules and pre-existing tension between rights of reputation and those of free speech’ should pertain, not withstanding the fact that the stability of the law and its enforcement are challenged by the global reach of the Internet and many different local legal and cultural norms.

The problem of ISP liability is taken up again in Chapter 6 by Gavin Sutter, this time specifically with respect to the European Union and UK legislative context of liability for failing to provide contracted services, failure to remove potentially harmful content, or failure to offer the required consumer protection. Existing legislation envisages 'a form of notice and take-down procedure', but it remains unclear what constitutes 'knowledge' and what time frame is applicable for judgements about an ISPs liability or immunity. Sutter asks whether ISPs will take it upon themselves to function as the moral guardians of cyberspace. Again there are issues of balancing rights and obligations. If over-zealous ISPs refuse to host certain types of Internet sites, they may jeopardise free speech rights. Alternatively, ambiguity about ISP liability could mean that ISPs permit the provision of content without regard to its potentially harmful effects.

Digital Divides in Cyberspace

There is ongoing debate about the unevenness of access to the means of communicating using digital technologies and about whether, and the extent to which, measures should be taken to reduce the effects of various types of digital divides. [6] After all, there are many other major claims on the scarce resources of time and finance to support health care, education, economic development, or democratic governance. In chapter 7, Daniel Paré provides an empirically grounded account of why a binary distinction between those with and those without access to the Internet is unhelpful in thinking about what steps should be taken by legislators to address the numerous and differentiated uses of the Internet. Summarising recent research which has examined Internet use to support commercial activity, he finds that for small and medium-sized enterprises in developing countries, particularly, efforts to introduce uniformity in the law governing electronic transactions often embody a 'techno-centric' logic which runs counter to people's experiences and preferences for how and with whom they choose to trade. As all the chapters in this volume demonstrate, user and use-centred approaches to analysing behaviour associated with the spread of the Internet, have a much greater potential to shed light on the complex and multi-faceted issues that legislators and legal experts face in the digital age.

The Technologies of Governing

The foregoing chapters are concerned mainly with choices and actions on the part of human beings who interact with digital technologies. However, the spread of the Internet is encouraging the development of technologies that can be used by individuals, or programmed as software agents, to filter, block and rate content that is

[6] See Couldry, N. (2003) 'Digital Divide or Discursive Design? On the Emerging Ethics of Information Space', *Ethics and Information Technology, 5,* pp. 89-97; DiMaggio, P. and Hargittai, E. (2001) 'From the "Digital Divide" to "Digital Inequality": Studying Internet Use as Penetration Increases', Princeton: Working Paper No. 15, Center for Arts and Cultural Policy Studies, Princeton University; Gunkel, D. J. (2003) 'Second Thoughts: Toward a Critique of the Digital Divide', *New Media & Society, 5*(4), pp. 499-522; Hargittai, E. (2002) 'Second-level Digital Divide', *First Monday, 7*(4), http://www.firstmonday.org/issues/issue7_4/hargittai/ accessed 29 Feb 04; Mansell, R. (2001) 'Digital Opportunities and the Missing Link for Developing Countries', *Oxford Review of Economic Policy, 17*(2), 282-295; Norris, P. (2001). *Digital Divide?* Cambridge: Cambridge University Press.

available to end-users. While the market for these technologies has not grown nearly as rapidly as initially expected and there is little harmonisation or interoperability of approaches, these technologies raise crucial issues about the nature of the 'public sphere' and about censorship.[7] Brian Esler (ch. 8) asks 'whether free speech has any value if it cannot be heard?' He reviews experience with filtering technologies and content rating initiatives in the US and Europe. Aimed at limiting access to illegal, harmful and racist content on the Internet, he shows that new technologies can be institutionally mandated for use, for example, in libraries to prevent children's access. As Esler graphically puts it: 'will the Internet remain a true "marketplace of ideas", a blowsy bazaar of the bizarre to the banal, or will filtering technology transform the experience of many users into something akin to a Communist-era department store, where choice is limited by central governance?' These technologies also make it feasible for end-users' prejudices to become embedded in the technology, making their use and effects anything but transparent over time.

Ronald Deibert and Nart Villeneuve (ch 9) take up the theme of state intervention as a form of Internet governance. In this case the discussion of filtering, self-censorship and the practices of states focuses on efforts to limit access to content for political reasons.[8] Quite apart from the fact that filtering can lead to errors and mistaken or unintended blockages, the notion that the Internet is inherently open because of the nature of its architecture is not one that can be sustained in the light of current technological developments and various methods of fostering self-censorship. These authors consider the experience of China where citizens are encouraged to make 'public pledges' not to publish information of certain kinds. Elsewhere, Internet Café owners are often required to block certain kinds of content. In the US (and as also indicated in by Esler (ch. 8)), legislation requires libraries and schools to block content to protect children. Deibert and Villeneuve raise the spectre of the 'strangulation' of the open Internet and point to various ways in which Internet filtering software is being used in ways that elude public scrutiny of the types of content and web sites that are excluded. This suggests that the new technologies of governance do not always support the empowerment of civil society movements.[9]

The variety of means by which virtual community actors who use the Internet can be controlled with respect to their use of content that is subject to intellectual property protection is examined by James Couser (ch. 10). In the case of Napster and subsequent efforts by the music industry to prosecute individuals who download music which is subject to copyright protection, Couser argues that current copyright protection of digital content and software provides a completely inappropriate 'blanket, one-size-fits-all solution'. When software is so protected, creative efforts to develop new applications are suppressed since any effort to re-use or build upon the software code becomes an infringement of the law. Couser suggests that the practice

[7] See Habermas, J. (1989 [1962]). *The Structural Transformation of the Public Sphere*. Cambridge: Polity.

[8] The broader issues in this area are discussed in Kalathil, S. and Boas, T. C. (2003) *Open Networks: Closed Regimes: The Impact of the Internet on Authoritarian Rule,* Washington DC: Carnegie Endowment for International Peace.

[9] See Surman, M. and Reilly, K. (2003) 'Appropriating the Internet for Social Change: Towards the Strategic Use of Networked Technologies by Transnational Civil Society Organizations', New York: prepared for the Social Science Research Council.

of registration of copyrights before they take effect offers a means of providing appropriate and differentiated levels of protection.[10]

One of the reasons that states seek legal means of intervening in cyberspace is to counter Denial of Service (DoS) attacks on Internet servers. In chapter 11, Mathias Klang distinguishes between civil disobedience, criminal activity and terrorism, suggesting that each of these has different legal implications. The meaning of the term terrorism is changing such that emphasis is being given to whether fear is engendered rather than to the extent of violence or devastation. Whether they are the result of coordinated action or the actions of a single individual, DoS attacks can completely overwhelm Internet servers. In consequence, legislative measures are being put in place. These include the European Union's Cybercrime Convention, European Council Framework Decision on Attacks against Information Systems and the UK Terrorism Act. Although these measures aim to reduce the likelihood of such attacks, Klang suggests that when such attacks represent a form of civil disobedience and democratic protest, they should not be criminalized. The right to free expression should not be limited without evidence of a clear threat to society. Klang argues that current measures are likely to jeopardise human rights.

Privacy and Surveillance

Cyberspace raises many issues for privacy protection.[11] Rebecca Wong (ch. 12) reviews definitions of privacy focusing particularly on control-based definitions emphasising the individual's autonomy to determine what is kept in the private sphere in contrast to those who regard the social importance of transparency as a collective value that should be considered. She raises the issue of whether privacy should be regarded as a unique or a derivative right. Wong's examination of the European Convention of Human Rights, data protection legislation in the UK, and laws on confidentiality, highlights the ambiguity of the law. For instance, it is unclear whether the Human Rights Act 1998 in the UK created a right to the protection of privacy via an extension of the law of confidentiality. Similarly, in the case of the UK Data Protection Act 1998, there are answered questions about how privacy infringement should be valued and about the meaning of informed consent with respect to the use of information on the web.

The digital age has spawned many new techniques of surveillance and these have been applied increasingly extensively within the workplace. David Christie (ch. 13) discusses how the law in the UK attempts to reconcile employee's perceptions of the right to privacy with employers' interpretations of employment relationships. Common law does not provide employees with a general right to privacy in the workplace, but Christie suggests that the Human Rights Act 1998 together with the European Convention on Human Rights, may have conferred new rights. However, the new legislation on curtailing employee surveillance (monitoring telephone calls and email communications) is likely to be slow to take effect. On balance, Christie concludes that despite numerous legislative measures, UK legislation is neither

[10] See also Steinmueller, W. E. (2003) 'Information Society Consequences of Expanding the Intellectual Property Domain', Brighton: STAR Issue Report No. 38, SPRU, University of Sussex, October.

[11] See Bennett, C. J. and Raab, C. D. (2003) *The Governance of Privacy: Policy Instruments in Global Perspective*. Aldershot: Ashgate.

coherent nor straightforward in protecting employees' privacy in the workplace. In the absence of clarity about how much privacy can be expected, Christie suggests that the balance favours the employer's right to monitor, rather than the employees' right to privacy.

Mathias Klang takes up broader issues of surveillance and privacy in chapter 14, by considering the 'camera as the unblinking, unforgiving eye in our urban environment'. Facial, pattern and number recognition using digital technology is being deployed increasingly to detect socially undesirable behaviour. Public surveillance using Closed Circuit Television (CCTV) is becoming pervasive despite the absence of empirical evidence on the effectiveness of its use as a means of crime prevention. Klang argues that it is a matter of human choice as to which individuals or groups receive the greatest attention because of the need to select from the huge quantities of data that are being gathered. In the UK, the Data Protection Act 1998 enables the Information Commissioner to set out a CCTV Code of Practice which is intended to provide acceptable levels of privacy protection. The extent of protection is considered in this chapter in the light of the provisions of the European Convention on Human Rights, Article 8, which implies that surveillance can be intrusive because of its potential for error, function creep, privacy invasion. Klang concludes that resources would be better devoted to combating crime in ways that are not so reliant on technology.

Individual privacy protection is an important issue in the digital age, but questions also need to be asked about whether states should have a right to privacy. As the Internet spreads, there are increasing calls for informational transparency on the part of the state,[12] but as government services go online, Andrew Murray (ch. 15) suggests that there are strong arguments in favour of more, rather than, less state secrecy. The convergence of digital technology is providing numerous outlets for digital media. Murray suggests that the growing capacity for information gathering and transmission means that the 'State is paralysed by fear' and its response is 'spin'. Arguing from Edward Shils' contention that modern democracy depends upon a 'state of political civility',[13] he indicates that it is becoming more and more difficult for the State to manage its relationship with the media. Individuals who embody the precepts of the State may benefit from a greater emphasis on personal autonomy, emotional release, self-evaluation, and protected communication. In the UK much emphasis is given to media management and the co-ordination of information as a result of unrelenting media coverage of the government's actions. Murray argues in favour of an open debate about the feasibility of providing privacy protection for the State as an antidote to the politics of 'spin'.

Cyberspace Futures

The contributors to this volume highlight many of the ambiguities with respect to human rights, available legal protections, and the difficulties of their enforcement due to technological inadequacies and human frailties. The future of digital rights management, for instance, depends on choices with respect to the evolution of the law

[12] See Miller, P. (2003) 'The See-through Society: Openness and the Future of the Internet', London: DEMOS, note prepared for the Foresight Cyber Trust and Crime Prevention Project.

[13] Shills, E. A. (1966) 'Privacy: Its Constitution and Vicissitudes', *Law and Contemporary Problems, 31*, 281.

and its interpretation. Jon Bing (ch. 16) emphasises the interdependence of the evolution of digital technologies, the law as a means of regulation and control, and the potential for inconsistencies between the interpretation of the law and its implementation in computerised code. Once regulations and rules are automated, they are extremely difficult to subject to judicial review. Following Lawrence Lessig's argument that the code of cyberspace becomes the 'regulator', Bing warns that we face a situation in which 'technology [is] implementing the law'. As 'click wrap licensing' for access to intellectual property on the web becomes more pervasive, Bing suggests that technology could be used by rights holders to restrict the buyer's legal position. Increasing diversity in the bundles of rights offered to users of protected information is likely and differences in the negotiating power of the rights holders and users may lead to the need for new forms of consumer protection. Bing emphasises that the buyer is, in effect, purchasing a legal position, rather than an immaterial service. Software agents will become negotiators of legal positions and be guided by formalisms in the software code that may not be consistent with the offline position. In the future, 'rights themselves are defined in the terms of programming language', raising many challenges for legal policy and practice.

Chapter 17 by Roger Brownsword considers issues associated with developments in biotechnology and human rights alongside those raised by digital technologies. He suggests that there are three main ethical positions on these issues: a utilitarian pragmatic stance based on assessments of risk and cost, a defence of human rights based on respect for human dignity, and a 'dignitarian alliance' that permits no compromise of human dignity. Brownsword argues that the first position is problematic because it is subject to the erosion of rights. The second rights-based position puts respect for human dignity at the centre of ethical choices about the development of technology, indicating that individuals must have the capacity to make free and informed choices. In the case of the 'dignitarian alliance', which is informed by a Kantian claim that human dignity has no price, developments in biotechnology are ruled out if they do not uphold a duty of self-esteem. Of the three positions, Brownsword indicates that the first two are gaining ground in the UK. He suggests that 'techno-regulation' is eroding the contexts in which the dignity of individual choice, responsibility and achievement are respected, with the result that technologies are being developed that treat human subjects as if they lack the capacity to choose.

Conclusion

This book demonstrates the value of considering the evolution of cyberspace law and the interpretative flexibility of that law from one jurisdiction to another. It is increasingly difficult to unambiguously define human rights and responsibilities in cyberspace. The contributors to this volume take the question of human rights, not as an absolute, but as a social construct that is subject to interpretation in the light of changing values. They highlight the way many of the judgements and social values that appear to have achieved a consensus are subject to misapplication as we come to rely on technology to implement the law.

There is clearly a growing need for critical assessments of the 'less glamorous' aspects of cyberspace. The chapters in this volume demonstrate why the issues of consent, governance, privacy and surveillance and technology need to be coupled with analysis of ethical positions and legal positions and practices. Only in this way will there be a chance of protecting basic human rights and of fostering responsibility in the digital age.