Case Western Reserve Journal of International Law

Volume 42 | Issue 3

2010

Digital Multi-Media and the Limits of Privacy Law

Jacqueline D. Lipton

DIGITAL MULTI-MEDIA AND THE LIMITS OF PRIVACY LAW

Jacqueline D. Lipton[*]

While digital video and multi-media technologies are becoming increasingly prevalent, existing privacy laws tend to focus on text-based personal records. Individuals have little recourse when concerned about infringements of their privacy interests in audio, video, and multi-media files. Often people are simply unaware that video or audio records have been made. Even if they are aware of the existence of the records, they may be unaware of potential legal remedies or unable to afford legal recourse. This paper concentrates on the ability of individuals to obtain legal redress for unauthorized use of audio, video, and multi-media content that infringes their privacy. It focuses on an analysis of the European Union Data Protection Directive. The Directive is one of the most comprehensive digital age legal reforms to address information privacy. Yet even the Directive suffers from shortcomings when applied to audio, video, and multi-media records. The author argues that global law reform is needed to bring privacy law into the age of digital video and multi-media.

I. INTRODUCTION

This paper focuses on difficulties of applying existing privacy laws to digital multi-media files. There are a number of digital file formats, including still images, audio recordings, video recordings, and combinations

[*] Professor of Law and Associate Dean for Faculty Development and Research, Case Western Reserve University School of Law, 11075 East Boulevard, Cleveland, OH, 44106. Email: JDL14@case.edu. The author would like to thank Professor Robert Strassfeld for the invitation to present this work at *Somebody's Watching Me*, Case Western Reserve University School of Law, October 23, 2009. All mistakes and omissions are my own.

of these formats in the form of digital multi-media files. Some of the controversial issues surrounding digital multi-media files include the unauthorized *gathering* of data, as well as the unauthorized *use* of data, say, in the context of dissemination, analysis, or profiling activities. Historically, laws in many jurisdictions have treated unauthorized gathering and usage differently. Laws have tended to focus either on *information gathering* or on *information dissemination or use*.[1] Many legislatures have historically been concerned with intrusive information gathering practices rather than with subsequent uses of the information gathered.[2] Nevertheless, recent laws in some jurisdictions have treated the two kinds of conduct as occurring on a continuum.[3] Conceiving of these activities on a continuum makes sense given that much new digital technology enables gathering and dissemination to occur almost simultaneously at the push of a button.

The ability of new digital devices such as cell phone cameras to transmit information wirelessly and globally raises important new challenges for privacy laws. Even laws such as the European Union Data Protection Directive (Directive), drafted in the mid-1990s, now seem dated. When the Directive was drafted, policy makers were predominantly concerned with regulating text-based information rather than other formats of information, although they did contemplate the likely future rise in uses of "sound and image" data.[4] In the 1990s, the Internet and associated technol-

---

[1] For example, anti-stalking legislation tends to focus specifically on information *gathering*. For a comprehensive survey of state anti-stalking legislation, *see* NAT'L INST. OF JUSTICE, U.S. DEP'T OF JUSTICE, DOMESTIC VIOLENCE, STALKING, AND ANTISTALKING LEGISLATION A1 (1996), *available at* http://www.ncjrs.gov/pdffiles/stlkbook.pdf. Laws referred to often as "anti-paparazzi" legislation likewise focus on information gathering practices rather than information dissemination practices subsequent to the information gathering. *See, e.g.*, CAL. CIV. CODE § 1708.8 (2009). Defamation law, on the other hand, traditionally focuses on information dissemination, as opposed to information gathering. *See, e.g.*, PERSONAL INJURY: ACTIONS, DEFENSES, DAMAGES 11–46, § 1.01[1] (2010) ("Defamation . . . [is] the unprivileged *publication* of false *communications*, which naturally and proximately result in injury to another.") (emphasis added).

[2] Regarding anti-stalking and anti-paparazzi legislation, *see* NAT'L INST. OF JUSTICE, *supra* note 1; CAL. CIV. CODE § 1708.8 (2009).

[3] *See, e.g.*, Council Directive 95/46, 1995 O.J. (L281) 31 [hereinafter Directive], *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

[4] *Id.* at recital 14 ("Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data."); recital 17 ("Whereas, as far as the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to apply in a restricted manner according to the provisions laid down in Article 9."); art. 9. Article 9 reads:

> Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried

ogy were in their relative infancy. System constraints—such as limited bandwidth—effectively restricted the amount and type of information that could be easily gathered, stored, and disseminated. As the technology developed, and bandwidth increased, so did the possibility of much more sophisticated transactions and transmissions of digital information in a variety of formats. This variety of formats raises new challenges for laws such as the Directive, and even for the privacy protections in the European Convention on Human Rights (ECHR).[5]

This paper takes as a case study the limitations of the Directive in protecting privacy interests in audio, video, and multi-media content. Part II examines the key provisions of the Directive that define and describe prohibited activities with respect to personal information. These provisions include the Directive's definitions of personal data and data processing, as well as the available defenses under the Directive. Part III identifies lessons that may be drawn from the European Union's experience with the Directive for future global developments in privacy law. The rationale for taking the Directive as a case study is twofold. First, the Directive was aimed specifically at new developments in digital technology in the 1990s that affected personal data and data processing capabilities with respect to that data. Secondly, the Directive is one of the more comprehensive examples of data protection legislation in the modern world. Thus, any perceived shortcomings in the Directive will be instructive for future developments in privacy law in other countries.

II. FRAMEWORK OF THE DATA PROTECTION DIRECTIVE

A. Personal Data

The Directive was implemented in 1995 to address perceived threats to individual privacy and autonomy as a result of disharmonized laws protecting individual privacy throughout the European Union. Member States' laws in the 1990s varied on the amount of protection provided to individuals, particularly as digital technologies became increasingly widespread.[6] The Directive aimed to ensure fair information gathering practices

> out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

Id.

[5] Convention for the Protection of Human Rights and Fundamental Freedoms art. 8(1), Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter Convention] ("Everyone has the right to respect for his private and family life, his home and his correspondence.").

[6] *See* Directive, *supra* note 3, at recital 4 ("Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of

pertaining to individuals.[7] It also sought to ensure that individuals were able to access data gathered about them.[8] Some protected classes of information—such as information relating to race, health, sex life, and political opinions—were given greater protections than others.[9] In other words, a more stringent set of standards relating to the access and use of protected classes of information was put in place under the Directive.[10]

Article 1(1) of the Directive sets out its key objective: "Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[11] The Directive is addressed to Member States, rather than citizens, because European Union directives operate as mandates to Member States to ensure that domestic laws comply with the requirements of the directive. The key terms in Article 1(1) for the purposes of this discussion

---

economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier.") Recital 5 reads:

> Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market.

Id. at recital 5. Recital 7 reads:

> Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions.

Id. at recital 7.

[7] *See id.* art. 6(1)(b) (requiring Member States to ensure that personal data is only collected for "specified, explicit and legitimate purposes.").

[8] *Id*. art. 12 (discussing data subjects' rights to access personal data).

[9] *See id.* art. 8(1) (providing special protections for personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life).

[10] *Id.* (providing that Member States shall prohibit the processing of special categories of data unless an exception in Article 8(2) applies).

[11] *Id.* art. 1(1).

are *processing* and *personal data*. If information is not personal data or is not being processed as contemplated by the Directive, the Directive will not apply. The question for the age of digital multi-media files is whether the concept of personal data processing contemplates now-common activities involving the gathering and dissemination of audio, image, video, and multi-media content in readily accessible and transmittable digital file formats.

While personal data is defined broadly in the Directive as "any information relating to an identified or identifiable natural person,"[12] the extent to which this definition extends beyond text-based records is open to question.[13] The recitals to the Directive illustrate that the question of the Directive's application to *sound and image* files, for example, was contemplated by the drafters, but that they were not necessarily sure how practices would develop with respect to these kinds of files. Recital 14 states that: "[G]iven the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data."[14] The recital suggests that at least audio files and still images were intended to be subject to the provisions of the Directive. However, the recital does not specifically contemplate multi-media files or video files in the sense of moving images—although the reference to *image data* may be intended to encapsulate both still and moving images. Likewise, the phrase *sound and image data* may have been intended to encapsulate multi-media file formats—that is, formats where sound and image data are combined.

Recital 14 should be read in conjunction with Recital 17. The latter recital contemplates some limitations on the Directive's application to sound and image files in certain contexts. It states that:

> [A]s far as the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to

---

12 *Id*. art. 2(a).

13 *See First Report on the Implementation of the Data Protection Directive (95/46/EC)*, at 20, COM (2003) 265 final (May. 15, 2003) [hereinafter *First Report*], *available at* http://www.statewatch.org/news/2006/oct/com-implentation-1995-dir.pdf. This report read:

> During the Directive's preparation, some people were concerned that it might not be able to cope with future technological developments. The extent of such technological developments was uncertain, but there was concern that a text drafted mainly with text processing in mind could encounter difficulties when applied to the processing of sound and image data. For this reason, Article 33 contains a specific reference to sound and image data.

Id.

14 Directive, *supra* note 3, at recital 14.

> apply in a restricted manner according to the provisions laid down in Article 9.[15]

Article 9 deals with freedom of expression. It states that:

> Member States shall provide for exemptions or derogations from the provisions of [the Directive] for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.[16]

While Article 9 relates to personal data generally in the contexts of journalism and intellectual property, it is interesting that Recital 17 contemplates that *audiovisual data* should be given particular deference in this context. This makes sense given the need for print and broadcast media to rely on audio recordings and visual images in collecting information and for disseminating news stories in the digital age. There is also a reference to artistic and literary expression—clearly contemplating that audio and visual works are often the most important subjects of intellectual property protection, notably under copyright law. Nevertheless, it is interesting that the drafters of the Directive perceived a higher likelihood of a future clash between privacy and free speech in the audiovisual context than in the context of text records. It suggests an implicit focus of the Directive on commercial and governmental aggregations of *text* records which are less likely to be the direct subject of news reporting or copyright claims.

The words of Recital 17 are prescient given the modern rise of claims involving video privacy and free speech in the media reporting context.[17] Many of the claims involve the balance between privacy rights and free expression as fundamental human rights under the ECHR. While the balance between privacy and free expression has historically been difficult in many jurisdictions, it is particularly noteworthy that modern cases involving digital age journalism increasingly involve video rather than text.[18] Brit-

---

15 *Id.* at recital 17.

16 *Id.* art. 9.

17 *See, e.g.*, Campbell v. MGN Limited, [2004] UKHL 22 (2002), *available at* http://www.parliament.the-stationery-office.co.uk/pa/ld200304/ldjudgmt/jd040506/campbe-1.htm (claim by supermodel Naomi Campbell for breach of confidence and infringement of privacy rights in respect of text data and photographs relating to her treatment for narcotics addiction); Mosley v. News Group Newspapers Limited, [2008] EWHC 1777 (Q.B.), *available at* http://www.bailii.org/ew/cases/EWHC/QB/2008/1777.html (claim for infringement of privacy rights of public figure in respect of both text and video files relating to a sex scandal).

18 *See* cases cited *supra* note 17.

ish judges in recent years have noted important qualitative differences between video and text records in the context of privacy claims.[19]

Even though Recital 14 contemplates the Directive's application to audio and video files, and there is nothing in the Directive's definition of personal data that explicitly suggests a limitation to text records, it is useful to consider Article 33 in the privacy context. This article states that:

> The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society.[20]

Even though the Directive apparently applied to sound and image data from day one, the European Parliament appears to have had some concerns about how the operation of the Directive to non-text data might play out in future practice. The Parliament assumed that further examinations of the applicability of the Directive to non-text data would likely be necessary. A detailed mechanism is set out in Articles 29 and 30 of the Directive to enable such examinations to take place periodically.

To date, there is little evidence that the European Commission's subsequent reviews of the Directive will lead to a major reworking of its provisions, particularly those relating to sound and image files. In the 2003 review of the Directive, the European Commission commented about sound and image files containing personal data. Its findings were inconclusive, suggesting in the final analysis that:

> Despite the doubts raised during the negotiation of the Directive, Member States have . . . reached the conclusion that the Directive's ambition to be technology-neutral is achieved, at least as regards the processing of sound and image data.
>
> No Member State or other contributor has proposed modifications to the Directive in this regard.[21]

The 2003 review also noted that some issues had been handed to a Working Party for further discussion,[22] notably issues of video surveillance.[23] The Working Party, in fact, released both a Working Document in November of

---

[19] *See Mosley*, [2008] EWHC 1777 (QB), ¶¶ 16–23 (noting qualitative differences between video and text files in the context of privacy claims).

[20] Directive, *supra* note 3, art. 33.

[21] *First Report*, *supra* note 13, at 20.

[22] *See* Directive, *supra* note 3, art. 29(1) (establishing the Working Party to review the operation of the Directive).

[23] *First Report*, *supra* note 13, at 20.

2002,[24] and an Opinion in February of 2004[25] canvassing the operation of the Directive to various kinds of video surveillance.[26] In principle, the Working Party accepted the importance of the application of the Directive to video surveillance activities.[27]

The 2009 review of the Directive was more aggressive in its recommendations on the future of the Directive. However, these recommendations were not focused on concerns about sound and image files. The Commission more generally suggested that the Directive is "outdated, in terms of technology and regulatory approach,"[28] and that "[i]ts scope is becoming increasingly unclear, for example in on-line and surveillance contexts."[29] The Commission concluded:

> Overall, we found that as we move toward an increasingly global, networked environment, the Directive as it stands will not suffice in the long term. The widely applauded principles of the Directive will remain as a useful front-end, yet will need to be supported with a harms-based back-end in due course, in order to be able to cope with the challenges of globalisation [sic] and flows of personal data.
>
> However, it was also widely recognised [sic] that value can still be extracted from current arrangements and that a lot can still be achieved very quickly by better implementation of the Directive, for instance by establishing common interpretations of several key concepts and a possible shift in emphasis in the interpretation of other concepts.[30]

In the 2009 review, the emphasis was on developing a new, more global, and more participatory approach to the protection of individual privacy generally, and to the identification of individual privacy harms that

---

[24] *Working Document on the Processing of Personal Data by Means of Video Surveillance*, 11750/02/EN WP 89 (Nov. 25, 2002) [hereinafter *Working Document: Video Surveillance*], *available at* http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2002_en.htm.

[25] *Opinion 4/2004 on the Processing of Personal Data by Means of Video Surveillance*, 11750/02/EN WP 89 (Feb. 11, 2004) [hereinafter *Opinion: Video Surveillance*], *available at* http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2004_en.htm.

[26] *Working Document: Video Surveillance*, *supra* note 24, at 2–3 (listing different categories of video surveillance).

[27] *Id.* at 5–7.

[28] Richard Thomas, *Foreword* to NEIL ROBINSON ET AL., REVIEW OF EU DATA PROTECTION DIRECTIVE: SUMMARY 2 (May 2009) [hereinafter 2009 REVIEW], *available at* http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive_summary.pdf.

[29] *Id.*

[30] NEIL ROBINSON ET AL., REVIEW OF THE EUROPEAN DATA PROTECTION DIRECTIVE 41 (2009), *available at* http://www.rand.org/pubs/technical_reports/2009/RAND_TR710.pdf.

should be appropriately protected by laws and best practices.[31] Such an approach would by its nature encompass privacy threats involving audio, video, and multi-media files. The importance of this issue has been recognized further by an Opinion on online social networking released in June of 2009 by a Working Group on the Directive.[32]

The 2009 Working Group report recognized the importance of online social network providers understanding their rights and responsibilities with respect to the "processing of sensitive data and images."[33] Prior to that, the Working Group had released an Opinion on the concept of personal data in 2007.[34] In this Opinion, the Working Group clarified its position on sound and image data and, in particular, the extent to which such data was intended to be included within the definition of personal data in the Directive. Attempting to clarify any lingering doubts under Article 33, the Working Group noted:

> Considering the format of the medium on which . . . information is contained, the concept of personal data includes information available in whatever form, be it alphabetical, numerical, *graphical*, *photographical* or *acoustic*, for example. It includes information kept on paper, as well as information stored in a computer memory by means of binary code, or on a videotape, for instance. This is a logical consequence of covering automatic processing of personal data within its scope. In particular, *sound and image data qualify as personal data from this point of view, insofar as they may represent information on an individual*. In this regard, the particular reference to sound and image data in Article 33 of the Directive has to be understood as a confirmation and clarification that this sort of data is indeed included within its scope (provided all other conditions are fulfilled), and that the Directive applies to them.[35]

The Working Group goes on to cite Recital 14 of the Directive[36] as further evidence that the Directive is intended to apply to sound and image

---

[31] *Id.* at 2–3 (identifying four distinct classes of privacy harms—information based harm, information inequality, information injustice, and restriction of moral autonomy).

[32] *Opinion 5/2009 on Online Social Networking*, 01189/09/EN WP 163 (June 12, 2009) [hereinafter *Opinion: Online Social Networking*], *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf.

[33] *Id*. at 3.

[34] *Opinion 4/2007 on the Concept of Personal Data*, 01248/07/EN WP 136 (June 20, 2007) [hereinafter *Opinion: Personal Data*], *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

[35] *Id*. at 7–8 (first emphasis in original, second and third emphasis added).

[36] Directive, *supra* note 3, at recital 14 ("Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data.").

files.[37] The Working Group makes special reference to video surveillance, stating that "[i]mages of individuals captured by a video surveillance system can be personal data to the extent that the individuals are recognizable."[38] Despite the assurances that the Directive applies to audio and video data, and that generally European Union countries' laws have been found adequate to encompass such data,[39] commentators over the years have raised concerns about the lack of privacy in some European Union countries as a result of video surveillance technologies.[40]

B. Information Processing

As noted in the previous section, Article 1(1) of the Directive explains the Directive's aims in terms of protecting privacy "with respect to the processing of personal data."[41] The term processing is defined broadly to encapsulate "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."[42] While potentially not so obvious to the drafters of the Directive, modern technology increasingly allows many of these operations to be carried out with respect to data in audio, video, and multi-media formats. Consider, for example, the case of an online social network such as Facebook.

Facebook obviously collects, records, organizes, and stores data about its users in multiple formats—including text, audio, and video formats. This is made clear in an Opinion of the Article 29 Data Protection Working Party on online social networking released in June of 2009.[43] The Opinion notes:

> SNS [Social Network Service] providers are data controllers under the Data Protection Directive. They provide the means for the processing of user data and provide all the "basic" services related to user management (e.g. registration and deletion of accounts). SNS providers also determine the

---

37 *Opinion: Personal Data*, *supra* note 34, at 8.

38 *Id.*

39 *See First Report*, *supra* note 13, at 5.

40 *See, e.g.*, David Rowan, *Britain 'Leads Way' in Eroding Privacy*, LONDON TIMES, Sept. 5, 2002, at 16 (raising concerns about intrusive video surveillance in Britain); Adam Sage, *French Unease Grows over Spread of Secret Surveillance*, LONDON TIMES, August 11, 1994 (raising concerns about use of video surveillance in France); Veronica Cowan, *If You Feel That You Are Being Watched*, LONDON TIMES, Sept. 19, 2000 (describing rise of video surveillance activities in the U.K.).

41 Directive, *supra* note 3, art. 1(1).

42 *Id.* art. 2(b).

43 *Opinion: Online Social Networking*, *supra* note 32.

> use that may be made of user data for advertising and marketing purposes—including advertising provided by third parties.[44]

What about video surveillance, such as that used by many governments and private entities in the U.K. with Closed Circuit Television (CCTV) cameras?[45] Capturing images by means of CCTV cameras certainly appears to amount to collection or recording of data as contemplated by the Directive's notion of processing. When the data is stored in systems connected to CCTV cameras, this would likely amount to storage of data under the Directive. When information is accessed by the owners of the cameras, this would likely be "retrieval," "consultation," or "use" as contemplated by the Directive's definition of processing.

C. Exceptions to the Operation of the Directive

1. Copyright and freedom of expression

Not all activities relating to the processing of personal data will fall within the ambit of the Directive. There are some express carve-outs that may apply to information in audio, video, and multi-media formats. The exceptions in Article 9 have been mentioned in a previous section.[46] This is the Article that requires Member States to provide exemptions for the "processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression."[47] However, these exemptions should only be created "if they are necessary to reconcile the right to privacy with the rules governing freedom of expression."[48] Recital 17 contemplates that this Article may have particular resonance in the audiovisual field.[49]

Questions involving the balance between free expression and privacy are always difficult to resolve. They must be addressed in the context of any constitutional protections for speech and privacy as basic human rights. Different jurisdictions vary with respect to constitutional protections for speech and privacy. The U.S., for example, has strong express protections for free speech and for a free press under the First Amendment to the Con-

---

44 *Id*. at 5.

45 *See* Patrick Foster, *Big Brother Surveillance Means No One Is Safe, Experts Warn*, LONDON TIMES, March 27, 2007, at 25 (discussing risks inherent in use of CCTV cameras in Britain).

46 *See supra* Part II.A.

47 Directive, *supra* note 3, art. 9.

48 *Id.*

49 *See supra* Part II.A.

stitution.[50] However, there is no express constitutional right to privacy.[51] While the ECHR contains express protections for both speech and privacy as fundamental human rights,[52] relevant articles have been implemented in national laws in a piecemeal fashion. For example, the U.K. did not acknowledge express guarantees of free speech and privacy until the enactment of the Human Rights Act of 1998.[53]

Because of the relatively recent adoption of speech and privacy as legal rights in the U.K., British courts have struggled with the best way to achieve a balance of those interests as required under the Human Rights Act.[54] Additionally, whilst dealing with that basic problem they are faced with the need to differentiate the application of these rights in cases involving different digital file formats. British courts have acknowledged that video images, for example, raise different privacy concerns to textual descriptions of an event in the context of journalism.[55] Thus, when balancing the right to free speech against the right to privacy, a court will consider the format of the personal information as a relevant factor in making its determination.[56]

The important point here for the application of Article 9 of the Directive is that this article cannot be applied in a vacuum. It cannot be assumed in any given case that if a speech interest or a copyright interest is implicated, the protections of the Directive will not apply. The Directive itself makes this clear by contemplating a balance between expression and privacy in the wording of Article 9—the words themselves require a balance between expression and privacy.[57] However, in cases where, say, a journal-

---

50 U.S. CONST. amend. I ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.").

51 DANIEL J. SOLOVE ET AL., INFORMATION PRIVACY LAW 33 (2d ed. 2006) ("Although the United States Constitution does not specifically mention privacy, it has a number of provisions that protect privacy, and has been interpreted as providing a right to privacy.").

52 Convention, *supra* note 5, art. 8(1) ("Everyone has the right to respect for his private and family life, his home and his correspondence."); art. 10(1) ("Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.").

53 Human Rights Act, 1998, c. 42 (U.K.).

54 *See, e.g.*, Mosley v. News Group Newspapers Limited, [2008] EWHC 1777 ¶¶ 7–15 (Q.B.), *available at* http://www.bailii.org/ew/cases/EWHC/QB/2008/1777.html (describing the need for a new approach to balancing privacy and expression under the Human Rights Act of 1998).

55 *Id.* ¶¶ 16–23.

56 *See id.*

57 Directive, *supra* note 3, art. 9. Article 9 reads:

ist has received a potentially damaging video of an individual and has a valid argument about publishing it in the public interest, it may be that the speech interest will take precedence over a privacy claim. Article 9 of the Directive seems implicitly to contemplate such a result.

The case of a journalist obtaining a damaging video of an individual is a good example of the way in which today's digital technologies push the boundaries of privacy law. Today, many systems are open rather than closed. It is easy to disseminate damaging images and other information globally at the push of a button. Once an image or other information is "out of the box"—say, because a journalist obtained it from a private company's CCTV system or from a paid photographer—further global dissemination of that information could be extremely damaging to the individual. Yet, if the dissemination has public interest merit, the disclosure may be excused, despite the provisions of the Directive.

2. Personal or household use

Article 3(2) provides that the Directive does not apply to the processing of data "by a natural person in the course of a purely personal or household activity."[58] This exception provides interesting challenges in the context of a global information society, particularly in the age of Web 2.0 where the Internet is more interactive and contains more user-generated content.[59] Interestingly, the European Court of Justice (ECJ) in the 2003 *Lindqvist* decision interpreted Article 3(2) as not excusing the posting on a publicly available website of gossipy text relating to private individuals by a peer who worked in a church with the data subjects.[60] In this case, and in the subsequent European Commission Working Party Opinion on online social networking, the court—and the Working Party—found decisive the public character of the disclosure of personal information.[61] The argument here seems to be that once a user makes a conscious decision to disseminate per-

> Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

Id.

58 *Id.* art. 3(2).

59 JANET LOWE, GOOGLE SPEAKS: SECRETS OF THE WORLD'S GREATEST BILLIONAIRE ENTREPRENEURS, SERGEY BRIN AND LARRY PAGE 294 (2009) (defining Web 2.0 as "[a] term used to describe an evolving generation of a participatory Web. Web 2.0 describes the proliferation of interconnectivity and social interaction on the World Wide Web.").

60 Case C-101/01, *In re* Bodil Lindqvist, ¶¶ 46–48 (E.C.J. Nov. 6, 2003), *available at* http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.

61 *Id.* ¶ 47; *Opinion: Online Social Networking*, *supra* note 32, at 6.

sonal information beyond a group of friends or close contacts, the user becomes a "data controller"[62] for the purposes of the Directive and is subject to its restrictions on processing of personal data.[63]

While the *Lindqvist* case contemplated text based data, it seems likely that similar reasoning would apply to audio, video, and multi-media content disclosed publicly on the Internet. The Working Party Opinion contemplates both "data and images."[64] Thus, it is likely that non-text information disclosed publicly on digital services would potentially be covered by the Directive provided that the information fell within the broad definition of personal data.[65] Of course, difficulties in distinguishing closed disseminations from open disseminations of information are likely to arise with respect to some of today's technologies. If the concern of the ECJ and the Working Party was with public disclosures of information outside a specific social sphere, how should we, for example, characterize disclosures over online social networks? Would posting information on a closed site such as Facebook contravene the Directive, provided that only Facebook "friends" could access the material? Bear in mind that individuals can have large numbers of friends on Facebook, many of whom they have never actually met in the "real world."[66]

In the *Lindqvist* case, the ECJ raised an additional concern about personal information. The disclosure in question concerned particularly sensitive information relating to a health condition—a foot injury.[67] Health information is one of the categories of sensitive information that receives special protection under the Directive.[68] Such information cannot be processed without the explicit consent of the data subject.[69] While the in-

---

62 Directive, *supra* note 3, art. 2(d) (defining "controller" in the context of data as meaning "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.").

63 *See Opinion: Online Social Networking*, *supra* note 32, at 6.

64 *Id*. at 3 (Executive Summary).

65 Directive, *supra* note 3, art.2 (a) (defining "personal data" as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.").

66 *See* James Grimmelman, *Saving Facebook*, 94 IOWA L. REV. 1137, 1154 (2009) (noting that online social networking services can be used both to maintain contact with real world friends or to make new friends who you have never met in the real world).

67 Case C-101/01, *In re* Bodil Lindqvist, ¶ 13 (E.C.J. Nov. 6, 2003), *available at* http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.

68 Directive, *supra* note 3, art. 8(1) ("Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning *health* or sex life.") (emphasis added).

69 *Id*.; *Opinion: Online Social Networking*, *supra* note 32, at 8.

formation in *Lindqvist* was a textual description of the injury, the question has arisen subsequently as to whether video data in particular should be regarded as sensitive information per se because of its ability to disclose or encapsulate race, sex, ethnic origins, or potentially religious beliefs.[70] Some European Union Member States automatically regard video images of data subjects as sensitive information for this reason.[71] However, that view was not endorsed by the Data Protection Working Party in its 2007 Opinion on online social networks.[72] The Working Party expressed the view that images are not necessarily sensitive data unless they "are clearly used to reveal sensitive data about individuals."[73]

In its Opinion on online social networks, the Working Party took some pains to describe the extent to which the "personal or household use" exception might apply to online social networks like Facebook and MySpace. In particular, the Working Party took the view that users of these services are generally not "data controllers" for the purposes of the Directive and will generally not be subject to its provisions provided that they are engaging in purely personal activities contained within a network of friends.[74] However, the Working Party suggested that there will be some circumstances in which activities on an online social network may go beyond the personal or household use exception. Examples include (1) situations where a social network is used as a collaboration platform for an association or company to advance commercial, political, or charitable goals;[75] (2) situations where a user has acquired a high number of contacts

---

70 *See Opinion: Online Social Networking*, *supra* note 32, at 8.

71 *Id.*

> In some EU Member States, images of data subjects are considered a special category of personal data since they may be used to distinguish between racial/ethnic origins or may be used to deduce religious beliefs or health data. The Working Party in general does not consider images on the Internet to be sensitive data, unless the images are clearly used to reveal sensitive data about individuals.

Id. (footnote omitted).

72 *Id.*

73 *Id.*

74 *Id.* at 5 ("In most cases, users [of online social networks] are considered to be data subjects. The Directive does not impose the duties of a data controller on an individual who processes data '*in the course of a purely personal or household activity*' . . . .") (emphasis in original).

75 *Id.* at 6. Section 3.1.1 reads:

> If an SNS user acts on behalf of a company or association, or uses the SNS mainly as a platform to advance commercial, political or charitable goals, the [household use] exception does not apply. Here, the user assumes the full responsibilities of a data controller who is disclosing personal data to another data controller (SNS) and to third parties (other SNS users or potentially even other data controllers with access to the data). In these circumstances, the user needs the consent of the per-

or "friends" including a high number of contacts that she does not actually know in person;[76] and (3) situations where the rights of third parties in relation to their personal data are implicated by an individual's use of an online social network.[77]

The third situation contemplated above is relevant to surveillance issues. Surveillance activities involve the gathering of information about third parties without their knowledge and potentially also involve the unauthorized use or dissemination of that information without their consent. If an online social network user—or any other Internet user for that matter—obtains audio, video, or multi-media content pertaining to a data subject and utilizes it online without that person's consent, she may have contravened the provisions of the Directive. In a closed network like Facebook, the dissemination of information about a third party might contravene the Directive if the dissemination goes beyond a group of friends of the third party, particularly given that the third party has effectively lost control of the information. However, the Directive's provisions here are unclear, and the Working Group on online social networks hedges its bets on this point by noting that "even if the household exemption applies, a user might be liable according to general provisions of national civil or criminal laws in question (e.g., defamation, liability in tort for violation of personality, penal liability)."[78]

3. National security

Along with the personal and household use exemption, Article 3(2) of the Directive also exempts from the operation of the Directive "processing operations concerning public security, defence [sic], State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in

---

sons concerned or some other legitimate basis provided by the Data Protection Directive.

Id.

[76] *Id.* Section 3.1.3 reads further:

> Typically, access to data . . . contributed by a user is limited to self-selected contacts. In some cases however, users may acquire a high number of third party contacts, some of whom he may not actually know. A high number of contacts could be an indication that the household exception does not apply and therefore that the user would be considered a data controller.

Id.

[77] *Id.* ("The application of the household exemption is also constrained by the need to guarantee the rights of third parties, particularly with regard to sensitive data.").

[78] *Id.* at 6–7 ("[I]t must be noted that even if the household exemption applies, a user might be liable according to general provisions of national civil or criminal laws in question (e.g. defamation, liability in tort for violation of personality, penal liability).").

areas of criminal law."[79] While this exemption would clearly cover fairly broadly conceived surveillance activities undertaken for the purposes of public security or defense, it would not capture all forms of surveillance.

The U.K. is an interesting case study on video surveillance because of the large scope of CCTV monitoring throughout the country and the lack of apparent controls on this monitoring despite the privacy protections in the Directive and the ECHR. It has been reported that nobody currently knows how many CCTV cameras are in operation in the U.K., although a rough study suggested that there are currently around five-million cameras operating in Britain.[80] Surveillance cameras can be used for a variety of purposes as recognized by the European Commission Working Group in its 2004 Opinion on video surveillance.[81] Purposes for using video surveillance include: protection of property; protection of individuals; public interest; detection, prevention, and control of offences; and making available of evidence.[82]

Some of these purposes would fall within the ambit of the public security exemption in Article 3(2) of the Directive, but probably not all. Where a CCTV system is used to protect private property, and is used by a private company, the company is probably a "data controller" under the Directive and subject to the restrictions on the processing of personal video data. The protection of property is probably not a matter of public security, defense, or State security. As there are no definitions in the Directive of the terms "public security," "defence [sic]," and "State security," the scope of the exemption for these activities is unclear. Some surveillance activities clearly aimed at protecting the public from, say, violent crime or terrorist attacks will likely meet the criterion for the exemption.[83] Nevertheless, many more common uses of video surveillance will be questionable. Thus, the Directive will apply in a piecemeal fashion to video surveillance activities depending on who is doing the data gathering and for what purposes.

---

79 Directive, *supra* note 3, art. 3(2).

80 Foster, *supra* note 45 ("Britain has about five million CCTV cameras, one for every 12 people.") (quoting Ian Forbes, co-author of a report by the Royal Academy of Engineering, Dilemmas of Privacy and Surveillance—Challenges of Technological Change).

81 *Opinion: Video Surveillance*, *supra* note 25, at 1–5 (listing different motivations for video surveillance).

82 *Id.*

83 However, note the balanced tone taken on protecting privacy in the face of concerns about terrorism after the 9/11 attacks. *See Opinion 10/2001 on the Need for a Balanced Approach in the Fight Against Terrorism*, 5403/01/EN/Final WP 53 (Dec. 14, 2001), *available at* http://www.statewatch.org/news/2002/jan/wp53en.pdf.

III. CONCLUSIONS: LESSONS LEARNED FROM THE DIRECTIVE

While the discussion in Part II highlighted shortcomings of the Directive with respect to modern technologies involving digital audio, video, and multi-media file formats, the 2009 review of the Directive's operation raised more general concerns about the continued operation of the Directive.[84] In reviewing the Directive, the Information Commissioner's Office acknowledged new challenges for privacy law, including, in particular, the difficult balance between personal privacy and other social imperatives.[85] In many ways, the ongoing analysis of laws in the European Union with respect to protecting privacy, and to balancing privacy against other social needs, outstrip efforts to protect privacy in other jurisdictions. Thus, if there is a glaring need for change and a call for new approaches to privacy law in the European Union, those calls should be amplified in other jurisdictions that currently have lesser privacy protections.

In the U.S., for example, where attempts have been made to balance privacy and free speech values, or privacy and national security interests, privacy tends more often than not to be the loser.[86] The U.S. has a piecemeal and outdated approach to privacy law which has stood up less well to the challenges of new digital technologies than its counterpart in the European Union Directive.[87] American privacy law is predominantly premised on the four privacy torts developed prior to the digital age. As set out in the Restatement, the privacy torts encompass: (a) intrusion into seclusion; (b) public disclosure of private facts; (c) false light publicity; and (d) commercial misappropriation of personal information.[88] The only one of these torts that potentially impacts surveillance activities is intrusion into seclusion, and even the application of that tort is problematic as it is premised on the shifting notion of reasonable expectations of privacy.[89] Additionally, to the

---

84 2009 REVIEW, *supra* note 28, at xi (advocating recasting the Directive to become a more globally consistent set of general principles concerning privacy protection).

85 *Id*. at viii ("Within the contexts of rapid technological change and globalization, a set of distinct challenges were identified . . . . [U]nder what circumstances can personal privacy become secondary to the needs of society, considering the fundamental importance of privacy protection for the development of a democratic society as a whole?").

86 *See* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 126–7 (2007) (describing historical difficulty in the U.S. of preserving privacy interests in the face of strong First Amendment guarantees of freedom of speech).

87 *See* Patricia Sanchez Abril, *A (My)Space of One's Own: On Privacy and Online Social Networks*, 6 NW. J. TECH. & INTELL. PROP. 73, 78–81 (2007) (surveying the patchwork nature of American tort law as applied to online privacy incursions).

88 *Id*. at 79.

89 *Id*. at 79–80 (describing uncertainty inherent in the concept of applying a test of reasonable expectation of privacy to the intrusion upon seclusion tort).

extent that the tort is applicable, it will not capture the kinds of harms that might result from dissemination of recorded surveillance information.[90]

Related to the privacy torts is the tort of intentional infliction of emotional distress.[91] Like the privacy torts, this tort is likely to be of limited use in the situations under consideration in this paper because the tort generally requires a showing of extreme distress on the part of the complainant resulting in physical manifestations of the distress.[92] A person unaware of surveillance activities may not be able to show any distress, and, even where she becomes aware of the surveillance, her discomfort may not rise to the levels of damage historically required by American courts. However, that might change if courts reassess the contours of the tort in light of activities involving intrusive modern digital technologies.[93]

Likewise, the tort of defamation is unlikely to be particularly relevant for the kinds of situations under consideration in this paper. A defamation action requires proof that an audio, video, or multi-media file is both false and harmful to the complainant's reputation.[94] This is likely an insurmountable hurdle in many cases involving unauthorized dissemination of such information online. Images and audio files are unlikely to be false for defamation purposes unless they have been doctored. Further, defamation law can do little about viral distributions of personal images or about the permanence problem of information when released online. Enforcement of a defamation order[95] online can be problematic if the information in question

---

90 *Id.*

> The tort of intrusion upon seclusion addresses harmful information-gathering, but not the subsequent disclosure of its fruits. It would only apply if the information was uncovered in a furtive way from a place within which the plaintiff had a reasonable expectation of privacy, such as a home, hotel room, a tanning booth, or a shopping bag.

Id. (footnotes and citations omitted).

91 RESTATEMENT (SECOND) OF TORTS, § 46 (1977); Sanchez Abril, *supra* note 87, at 81 (noting limitations of the intentional infliction of emotional distress tort in the online social networking context).

92 Sanchez Abril, *supra* note 87, at 81 (noting that the tort is ineffectual in the online social networking context because conduct in question is usually not sufficiently "extreme and outrageous" and because many courts require physical manifestations of the claimed emotional distress) (quoting RESTATEMENT (SECOND) OF TORTS, § 46(1) (1965)).

93 JON MILLS, PRIVACY: THE LOST RIGHT 195 (2008) ("The law [on intentional infliction of emotional distress] is still in a stage of development, and the ultimate limits of this tort have not yet been determined.") (citing RESTATEMENT (SECOND) OF TORTS, § 46, cmt. c (1977)).

94 Sanchez Abril, *supra* note 87, at 79 (noting that although the plaintiff in an online social network, for example, may well have suffered indelible harm to her reputation, it is difficult to establish a defamation claim with respect to true information).

95 Jennifer Meredith Liebman, *Defamed by a Blogger: Legal Protections, Self Regulation and Other Failures*, 2006 U. ILL. J.L. TECH. & POL'Y 343, 368–72 (2006) (describing differ-

exists on multiple websites and in multiple jurisdictions by the time the order is made.[96] Additionally, online intermediaries such as Internet service providers, who serve as conduits for potentially defamatory content—and are often the easiest potential defendants to identify—, are generally immune from liability.[97] Further, the defamation action does little to chill the actual *gathering* of information if that is the complainant's basic concern. It only potentially comes into play at the dissemination stage when the genie may well be so far out of the bottle that it is difficult to achieve any form of redress for the complainant.

While American criminal procedure incorporates some notions of privacy as implicit requisites of the due process clause in the Constitution, these notions of privacy also rely on an often-shifting concept of the "reasonable expectations of privacy."[98] As intrusive surveillance technologies become more advanced, courts have struggled with establishing an appropriate bar for the reasonable expectation of privacy test,[99] and, of course, criminal procedure notions of privacy are only applicable to criminal proceedings, while much surveillance does not result in criminal cases.

The position on privacy in the U.S. is much more disharmonized and piecemeal than that in the European Union. Even so, the European Union is likely to move towards a newer and more comprehensive approach to privacy to meet the needs of the Web 2.0 society. The fact that the European Union Member States have so much experience with a comprehensive privacy law and are now in a position to evaluate it and improve upon it could in fact serve as a useful guide for law and policy makers in the U.S. Rather than reinventing the wheel and starting from scratch, if there is sufficient

---

ent kinds of defamation remedies that may be sought online including a retraction, an injunction, and damages).

96 *Id*. at 375 (noting that even if the complainant obtains a retraction by the original poster of defamatory context, the information is likely available in many other places online, including places like the Internet Archive Project that preserves information that has already been retracted from websites).

97 47 U.S.C. § 230(c)(1) (2006) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

98 DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 2–3 (2008).

> Although the U.S. Constitution does not explicitly mention the word "privacy," it safeguards the sanctity of the home and the confidentiality of communications from government intrusion. The Supreme Court has concluded that the Fourth Amendment protects against government searches whenever a person has a "reasonable expectation of privacy.

Id. (citation omitted). *See also* Sanchez Abril, *supra* note 87, at 79–80 (discussing the notion of "reasonable expectations of privacy" in the context of American tort law).

99 SOLOVE, *supra* note 98, at 71–74 (describing practical problems inherent in applying the reasonable expectation of privacy test in both criminal and tort law contexts in the U.S.).

political will in the U.S. to change the position on global privacy, legislators here can take up where the European Union has ended up after fifteen years of experience with the Directive. The U.S. could potentially work with the European Union to implement a global and participatory approach to information privacy that resolves problems posed to privacy from audio, video, and multi-media technologies, as well as resolving more complex problems about information privacy. The next decade may provide a good opportunity to strike a much-improved global balance between privacy and other important social needs such as freedom of expression and public security.