The European Law Students' Association

UNITED KINGDOM

The Protection of Human Rights on the Internet

ELSA Day UK Magazine

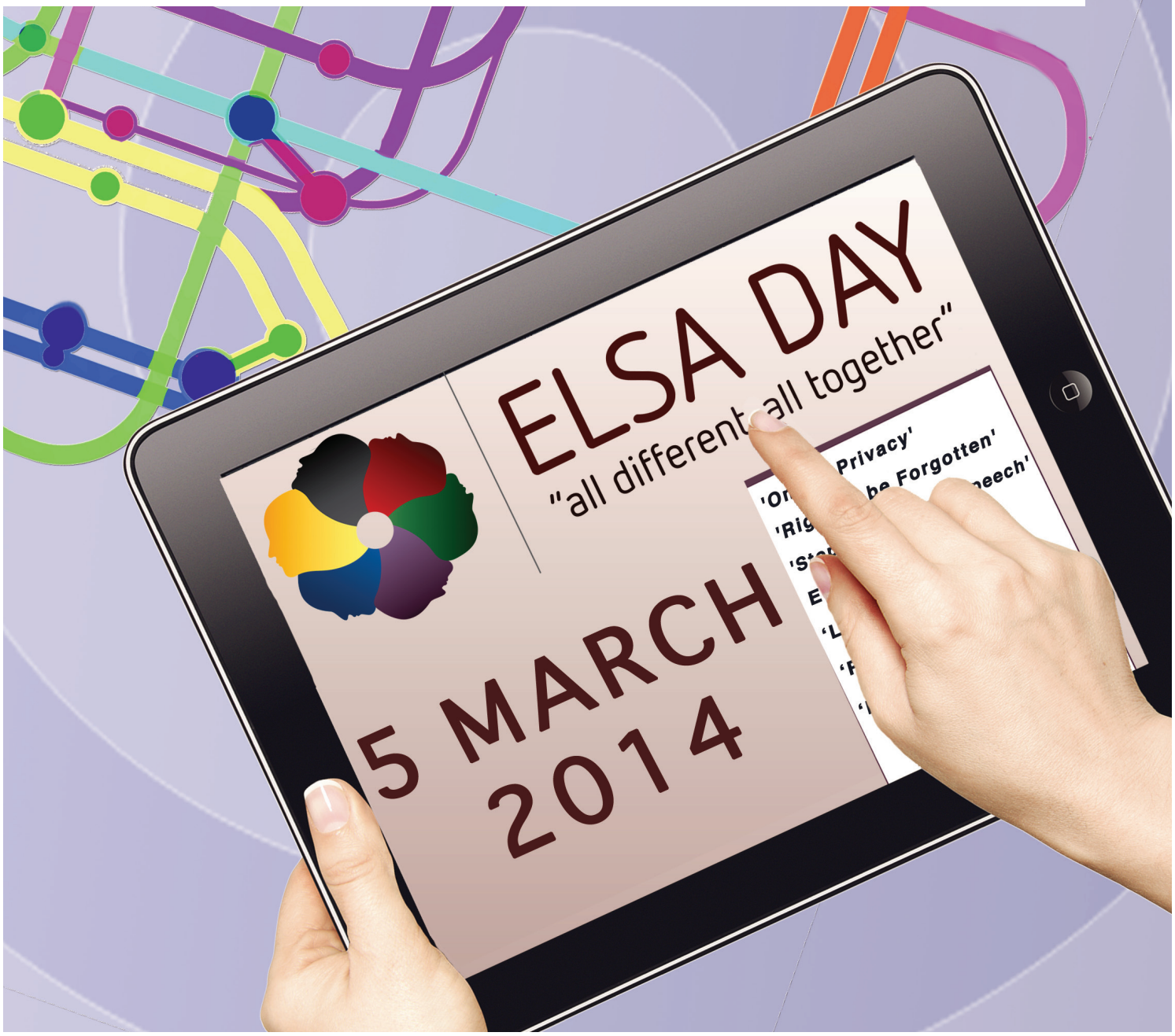


Table of contents

About ELSA

The Association

The European Law Students' Association, ELSA, is an international, independent, non-political and non-profit-making organisation comprised and run by and for law students and young lawyers. Founded in 1981 by law students from Austria, Hungary, Poland and West Germany, ELSA is today the world's largest independent law students' association.

ELSA's members

ELSA's members are internationally-minded individuals who have an interest for foreign legal systems and practices. Through our activities such as seminars, conferences, lawschools, moot court competitions, legal writing, legal research and the Student Trainee Exchange Programme, our members acquire a broader cultural understanding and legal expertise.

Our Special Status

ELSA has gained a special status with several international institutions. In 2000, ELSA was granted Participatory Status with the Council of Europe. ELSA also has Consultative Status with several United Nations bodies; UN ECOSOC, UNCIT-RAL, UNESCO & WIPO.

ELSA is present in 41 countries

Albania, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Kazakhstan, Latvia, Lithuania, Luxembourg, Malta, Montenegro, The Netherlands, Norway, Poland, Portugal, Republic of Macedonia, Romania, Serbia, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine and The United Kingdom.

Our partners

KAPLAN LAW SCHOOL

BPP LAW SCHOOL

ELSA International

41
ELSA National Groups

240
ELSA Local Groups

38,0000
ELSA Members

elsa
The European Law Students' Association
UNITED KINGDOM

NSLS
THE NATIONAL STUDENT LAW SOCIETY

Letter from the Editor

Dear ELSA friends,

ELSA The United Kingdom is continuously striving to strengthen our interactions with our Local Groups, the academic community, and other networks and organisations – both on a national and an international scale. This is achieved through arrangements that are focused on promoting dialogue and knowledge-sharing, including seminars, workshops, debates, publishing, and various other events and resources. This enables us to promote collaborative learning and working, and fosters relationships with the academic environment and professional sector. One of our biggest challenges lies in creating a platform for students and young professionals to express their thoughts and ideas, and expose them to the world – thus empowering them to contribute, discuss and share these with academics and professionals in the field.

With that in mind, on behalf of the National Board of ELSA The United Kingdom, I would like to welcome you to the first issue of the ELSA Day UK Magazine! Here, we encourage students and young professionals of all cultures and of all levels to use their multidisciplinary skills and experience to convey their understanding of the law as it exists now.

In this issue, we would like to draw attention to The Protection of Human Rights on the Internet, and allow our readers to become better communicators of their understanding of the topic, facilitate peer-to-peer learning, and provide opportunities for dialogue and encouraging information- and knowledge-sharing through ELSA Day events.

Nadia Tjahja
Vice President for Marketing
ELSA The United Kingdom 2013-2014

The European Law Students' Association
UNITED KINGDOM

The National Board of ELSA The United Kingdom on ELSA Day

Introduced by Federica Toscano – Initiator of ELSA Day

ELSA Day is an international human rights forum where students from all over Europe organise a large variety of coordinated events to discuss the International and European standards of protection and implementation of human rights. The events are not only targeted to law students, but the civil society in general. Some groups propose a scientific approach, where they are analysing challenging issues through panel discussions, moot court competitions, legal debates and public lectures; whereas others organise social activities like photo competitions, marathons and visits to institutions. The common aim of ELSA Day is to raise awareness on the aforementioned crucial topics and, at the same time, to challenge the status quo of legal education, which is the final objective of all ELSA activities. Being part of the organisation of ELSA Day with students from different countries is another opportunity for law students to become open-minded, internationally oriented and, at the same time, allows them to acquire a broader cultural understanding.

On the 20th of March 2013, the first edition of ELSA Day, the ELSA Network demonstrated that students can participate in and influence the international discussion, obligations and integration of Human Rights with high quality events and with the energy and creativity that characterize youth activities. At the same time, they demonstrated the impressive result that can only be achieved when people are cooperatively working together, uniting different ideas, coordinating actions and inspiring each other. ELSA demonstrated that there is a generation of young Europeans that thinks that a culture of sharing and understanding shall not halt at political borders and human dignity shall be promoted without frontiers. ELSA also demonstrated that these values are not only nice words on a piece of paper, but that we can and that we want to work concretely for it, "All different, all together", as the ELSA motto says. Future lawyers and decision-makers are already taking concrete steps to spread these values among the European society with high quality events, which are organised with professionalism and enthusiasm.

In my opinion it is not fortuity that the first ELSA Day and the first International Day of Happiness happened on the same date – the 20th of March 2013. I feel once more, and much stronger, the joy of being a member of ELSA and the joy of sharing with my board and thousands of other students the satisfaction of this impressive result. This year, let´s make it even better. All different, all together.

What does ELSA Day mean to you?

Josie Beal
President of ELSA The United Kingdom
To me, ELSA Day is primarily two things. Firstly, it is raising awareness and supporting a core value of ELSA; human rights. This year the focus on the protection of human rights on the Internet is extremely relevant in today's social media generation. Secondly, ELSA Day is a chance for the entire ELSA network to join together on one day in support of a common cause. Students from ELSA's forty-one National Groups with thousands of miles separating their countries – who may never even meet each other – will, in effect, be working together on 5 March 2014. This is ELSA. We are all different, all together.

Harry Mach
Treasurer
ELSA is an opportunity to network, an opportunity to talk and an opportunity to work across borders. A vast network of lawyers stretching from Kazakhstan to the Atlantic coast. When it comes to defending human rights, lawyers are often an overlooked first line of defence. However, when that fails, when governments ignore the courts, the next line is to shout about what is happening. And who is better placed to do that than a pan-European network of Law students with their understanding of human rights and an unrivalled ability to share that knowledge across borders? That is what we intend to do with this Magazine and what we are trying to do with ELSA Day.

Nadia Tjahja
Vice President for Marketing
ELSA Day reminds me that we are a network. We are groups of individuals that are geographically dispersed who share common interests, linked together on a voluntary basis. We want to share knowledge and information, sharing a common sense of purpose, collaborating directly, and wanting to learn from each other. We are raising awareness by being aware of how we use the Internet and how we conduct ourselves on the Internet. We are exploring the boundaries of the Internet and we have to make sure that we are protecting ideas and values that we have in real life with real people – online, because it is now part of our real life and still affects real people. We are more than communities of learners. We are ELSA.

Alexander Adamou
Director for Academic Activities
To me, ELSA day means an opportunity to provide and promote a deeper understanding for people as to what their rights are and how they can enforce them. Thus, it is an opportunity to help others through the network we have available, and make the world in some small part a more educated and understanding place. To me, these are rights that are not given enough media attention – and thus there is a fundamental lack of public understanding on Internet security and how this affects their rights. This needs to be addressed and one way to do this is through greater exposure and publicity. ELSA day provides a memorable and unique experience to help resolve these problems on a grand scale.

Sorin Popescu
Director for Seminars and Conferences
Since I joined the European Law Students Association back in November, I was presented with ELSA Day. I quickly realised that this sort of activity is a great opportunity for students, and as a Local Group president I can say that I was very excited about the possibility of organising ELSA Day events at my University. This year's topic, The Protection of Human rights on the Internet, is particularly interesting as it is a topic in which I am personally interested. ELSA Day, for me, represents a good opportunity to get involved and take part in an international event where students organise and participate actively, discussing and expressing their opinions on the topic that was set out. I can say that to me, ELSA Day seems one of the best things that ELSA has to offer, and I encourage all members to get involved.

Ashley Robertson
Vice President for the Student Trainee Exchange Programme
As a STEPer, the key aspect of ELSA Day for me is the international element of integration. The integration of a cornucopia of values and ideals lies at the heart of European human rights legislation – and it is that same integration of values which is embodied by the united effort of tens of thousands of ELSA members on ELSA Day. Personally, I find it particularly fascinating to note the change in society's focus from the lingua franca of 'equality' - a cornerstone in our society with the rule of law - to such challenges as integrating legislative efforts for a virtual environment.

Privacy in the EU:

The distinctive treatment of photographs compared to the written word

by Oliver Marriage | ELSA Aberdeen

elsa
The European Law Students' Association
ABERDEEN

The privacy of an individual is a fundamental aspect of our right to self-determination; however it is not an absolute right and is frequently infringed whether objectively justifiable or not. Recently the media has brought to light the actions of the NSA – I do not for a minute believe that they are the only institution engaging in this behaviour; however, it demonstrates a general culture of infringement justified on broad public protection grounds. Privacy is a hot topic, and this level of attention will undoubtedly affect the way in which privacy claims are treated as the law develops. In this paper I will attempt to demonstrate the evolution of this area of the law. Then to critically analyse the difference – in the judicial treatment between photographic images and verbal expressions in privacy cases – and determine on what basis this differing treatment is justified in the EU.

Privacy is known to be an integral part of many institutions, without this protection of privacy, in the form of confidentiality in a lawyer client relationship for example, it is thought that the level of service would be diminished, and it is settled that there is a right to confidentiality when engaging in either medical treatment or legal services. The current debate in the UK regards the protection of private information that is not protected by a confidentiality contract; the law is being developed through an extension of breach of confidence. Through this, the law is being developed by high profile celebrity cases in an attempt to protect their personal information from the press. The debate rests on the balance of ECHR Article 8, the right to respect private life, and ECHR Article 10, freedom of expression.

The law relating to invasion of privacy as stated earlier evolved from breach of confidence. Lord Nicholas in *Campbell v MGN* stated that: "The continuing use of the phrase 'duty of confidence' and the description of the information as 'confidential' is not altogether comfortable. Information about an individual's private life would not, in ordinary usage, be called 'confidential'. The more natural description today is that such information is private. The essence of the tort is better encapsulated now as misuse of private information."[1] This move marks a change from the traditional action of breach of confidence when it was a remedy for unjustified publication of personal information. Lord Hoffmann acknowledged that: "the questions at issue in modern privacy cases have little to do with the relationship of trust and confidence at the heart of the traditional breach of confidence action and there is much to be said for acknowledging openly that it is "privacy" rather than confidence which is being protected in these cases"[2]. There is now a distinct branch of breach of confidence actions, not related to violations of unauthorized disclosure in a confidential relationship, but related to the nature of the information disclosed to protect the self-esteem, dignity and personal autonomy of the individual. As Lord Mustill said in *R v Broadcasting Standards Commission*: "An infringement of privacy is an affront to the personality, which is damaged both by the violation and by the demonstration that the personal space is not inviolate."[3] It is this affront to the personality that the law seeks to protect.

The courts must, when determining the development of the law of privacy, consider the balance of the privacy interests of the individual and the freedom of expression interests laid down by the ECHR. This is a tenuous balance that has led to different aspects in the law of privacy to be distinguishable. Through the development of case law, the courts have drawn a distinction between photographic images and verbal expressions in relation to their treatment in privacy cases. As the courts have made a distinction between these two, they have been notably separated in their treatment by the courts.

The case Campbell v MGN Ltd[4] is the leading authority for the treatment of privacy actions under UK law. This case concerned the model Naomi Campbell, who sought damages for the publication of an article, which showed the time, the location (Narcotics anonymous) and how often she received treatment for her drug addiction. In addition to the article, a picture of her outside the treatment centre was published; on its own it was an ordinary street scene. The court of appeal held that the press was entitled to correct false public statements made by Ms Campbell in which she claimed that she was not addicted to drugs and projected a squeaky clean public image; the additional details were allowed to add credulity to the story. The case went to the House of Lords where they marginally overturned the previous judgement, ruling that the additional details like the photograph and information regarding when and where she received treatment were in breach of confidence. In determining whether information is private the House of Lords created a two-stage test. Firstly, they ask whether the information is obviously private and secondly, where it is not, is the information of a nature where its disclosure would be likely to give substantial offence to the subject of the information? However, a positive answer to either of these questions will trigger the balancing exercise of the competing ECHR rights.

[1] Campbell v MGN Ltd [2004] 2 AC 457
[2] Campbell v MGN Ltd [2004] 2 AC 457
[3] R v Broadcasting Standards Commission, Ex p BBC [2001] QB 885, 900,
[4] Campbell v MGN Ltd [2004] 2 AC 457

The photographs were of Ms Campbell in the street so they were not obviously private, but the disclosure would have caused substantial offence to Ms Campbell. It was on the following grounds that the court ruled that the photographs should not be published: the courts distinguished photographic treatment from the written word; it was also distinguished when publishing a photograph would lead to breach of privacy.

In *Theakston v MGN*[5], a presenter of the children's television show 'top of the pops', Jamie Theakston, sought to restrain the publication of both the fact that he had been to a brothel and that photographs were taken of him there. The information about his visit was permitted to be published by the court, but they granted an injunction over the publishing of the photographs on the grounds that they were more intrusive into his private life than was justifiable.

Per Ouseley J: "The courts have consistently recognised that photographs can be particularly intrusive and have shown a high degree of willingness to prevent the publication of photographs taken without the consent of the person photographed but which the photographer or someone else sought to exploit or publish."[6]

This distinction between the treatment of photographs and the written word can be seen further in the rulings of the European Court in the case *Von Hannover v Germany*[7]. Princess Caroline of Monaco brought a claim suit after pictures were taken covertly and published of her engaging in public and private activities on holiday. The court held in this case that the concept of personal life extends to aspects of individual identity such as a person's name or picture as they contain aspects of the individuals physical or psychological integrity. "There is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life"[8].

Caroline clearly stands as a decision emphasising the importance of photographs, and it seems to have been the photographs, which tipped the balance in Campbell. Photographs are simply different from and have more impact than verbal information, as everyone knows. So the quality of what is "taken" from an individual and displayed to the public is different, and more intrusive, when the information is photographic[9]. It seems, however, to have been a different reason, which played a powerful role in these two decisions: the surreptitious taking of the photographs, the expectation of privacy. The judges drew a distinction between occasions where the Princess was pursuing private activities and when she was acting in an official capacity, and stated that just by the mere fact that photographs are taken in a public place does not mean in itself that there can be no reasonable expectation of privacy.

A case following was *Murray v Express Newspapers*[10], in which it was hoped that it would resolve disputes over whether the publication of photographs of individuals involved in ordinary activities should be off limits. Although the law has not been clarified, the court of appeal highlighted the factors that would be taken into consideration when determining whether or not there is a reasonable expectation of privacy.

"The question of whether there is a reasonable expectation of privacy is a broad one, which takes account of all the circumstances of the case. They include the attributes of the claimant, the nature of the activity to which they were engaged, the place at which it was happening, the nature and purpose of the intrusion, the absence of consent and whether or not it was known or could be inferred, the effect on the claimant and the circumstances in which and the purposes for which the information came to the publisher."

Unfortunately the case was settled before trial, despite the fact that the Court of Appeal felt it should proceed, therefore the law still has an air of uncertainty, as it is not possible to access the detailed judicial deliberation of the facts. The reasonable expectation test was created in *Campbell v MGN*, two other tests were also suggested, but legal systems have continued to use the reasonable expectation test, suggesting that this is the method for determining whether publishing a photograph will be deemed too intrusive.

Peck v UK[11] played a role in the development of the law of privacy in regards to photographs. It concerned a man, Peck, who attempted suicide on a street covered by CCTV. A still was taken from the CCTV image for a Local Government publication to demonstrate the value of CCTV in preventing crime and harm. The still showed Peck with a knife in his hand. Local newspapers and Anglia Television used the tape without masking the applicant's identity; and Peck thought this amounted to a breach of his privacy.

To determine if the disclosure of the record of the applicant's movements to the public in a manner in which he could never have foreseen gave rise to an interference with his private life, it was necessary to consider whether the images related to a private or public matter and whether the material obtained was envisioned for a limited use or was likely to be made available to the general public. In this case, the applicant was on a public street, but he was not there for the purposes of participating in any public event nor was he a public figure. Moreover, when the material was broadcasted, the applicant's identity was not adequately masked. As a result, the relevant moment was viewed to an extent, which far exceeded any exposure to a passer-by or to security observation and to a degree surpassing that which the applicant could possibly have foreseen when he walked along the High Street. Accordingly, the disclosure constituted a serious interference with the applicant's right to respect for his private life. Furthermore, it was not an interference that was necessary in a democratic society. There were no relevant or sufficient reasons, which justified the direct disclosure by the authority to the public of the footage without obtaining the applicant's consent or masking his identity.[12]

The wording found in the ruling "to a degree surpassing that which the applicant could have possibly foreseen" bears a striking similarity to the reasonable expectation test.

The case of *Douglas v Hello! Ltd*[13] at paragraph 84, exemplifies the distinction between verbal expressions and photographs. "They are not merely a method of conveying information that is an alternative to verbal description. They enable the person viewing the photograph to act as a spectator, in some circumstances voyeur would be the more appropriate noun, of whatever it is that the photograph depicts. As a means of invading privacy, a photograph is particularly intrusive. This is quite apart from the fact that the camera, and the telephoto lens, can give access to the viewer of the photograph to scenes where those photographed could reasonably expect that their appearances or actions would not be brought to the notice of the public"

The reasonable expectation test was adopted in the Supreme Court of California's decision of *Schulman v W Productions Ltd.*[14] In this case, the court held that a woman had not suffered a breach of privacy amounting to an action, when a television filmed her being attended by paramedics at the scene of a serious road accident. This was decided on the basis that she could not have had "a reasonable expectation that members of the media would be excluded or prevented from photographing the scene" because "for journalists to attend and record the scenes of accidents and rescues is in no way unusual or unexpected".[15] In contrast, the court held that the claimant could have an objectively reasonable expectation of privacy inside a rescue helicopter because the court was "aware of no law or custom permitting the press to ride in ambulances or enter hospital rooms during treatment without the patient's consent"[16].

The reasonable expectation test does not only protect privacy in the traditional publishing avenues, although arguably the protection here is the strongest, it also extends to social media. In the remit of social media if instead of being published in a newspaper, the photographs of Ms Campbell were published by a friend via an online social network, Ms Campbell would have been unlikely to win.[17] This suggests that the protection of photographic images online still has to be developed to the same extent, and the distinction between photographs and verbal expression may be diminished.

Ferdinand v MGN Ltd[18] is the latest development in the law of privacy; it concerned a footballer, Rio Ferdinand, who had an affair. The woman he had an affair with gave information about their affair, which included the story, the details of the sexual relationship and a photograph, all of which Ferdinand believed should be protected. One of the critical factors in the defence was the fact that Ferdinand had already talked publicly about his bad behaviour, including driving bans and affairs with other women.[19] Because his affairs had been public knowledge, he did not have an expectation of privacy in regards to them. The photograph was unexceptionable in character meaning that the right was of low importance. Publication of the photograph provided limited corroboration for the story, and it supported the case that Ms Storey and the Claimant had known each other since 1997 and that was also a legitimate ingredient of the Defendant's argument as to why the Claimant had not, in fact reformed. The publication of this picture did not tip the balance in the Claimant's favour[20], following this judgement the claim was dismissed.

Although a greater protection is afforded to photographic images than verbal expressions when the reasonable expectation requirements have been satisfied; the court will permit publication of photographs when a reasonable expectation of privacy does not

5 Theakston v MGN Ltd [2002] EMLR 22
6 Theakston v MGN Ltd [2002] EMLR 22
7 Von Hannover v Germany [2005] 40 EHRR 1
8 Von Hannover v Germany [2005] 40 EHRR 1
9 Peter Carey Media Law 5th Edition
10 Murray (by his litigation friends) v Express Newspapers plc and another [2007] EWHC 1908 (Ch),
11 Peck v UK [2003] All ER (D) 255 JAN
12 Peck v UK [2003] All ER (D) 255 JAN
13 Douglas v Hello! Ltd (no 3) (2006)
14 Schulman v W Productions Ltd (1998) 18 Cal.4th 200
15 Schulman v W Productions Ltd(1998) 18 Cal.4th 200
16 NA Moreham 'Privacy in the Common Law: a doctrinal and theoretical analysis' (2005) 121 Law Quarterly Review 628.
17 Entertainment Law Review2012 Rewriting privacy: the impact of online social networks Rob Mindell
18 Ferdinand v MGN Ltd [2011] EWHC 2454 (QB) (QBD)
19 European Intellectual Property Review Case Comment Privacy considered and jurisprudence consolidated: Ferdinand v MGN Ltd Gillian Black
20 Ferdinand v MGN Ltd [2011] EWHC 2454 (QB) (QBD)

exist. This can be seen in *John v Associated Newspapers Ltd*[21] where Elton John was photographed going from his car to his house. There was no personal information conveyed and it was held that he did not meet the threshold for reasonable expectations of privacy.

In conclusion, it is clear that the law of confidence has evolved into a wider range applicability, although the high profile media cases do not as such represent a breach of confidence, but rather a misuse of private information. It has been demonstrated through case law that a clear distinction exists between verbal expressions and photographic images, and that this distinction has lead to photographs being afforded a higher level of protection. The courts have justified the distinction because photographs by nature can be particularly intrusive; allowing their publication can harm the personal autonomy of the individual, which must be protected. This distinction can be clearly observed by analysing the judgements of cases, which have been brought to the court to stop publication of news with corresponding photographs e.g. Campbell. The decision in Campbell has been followed by subsequent case law; affirming that photographs are more likely than verbal expressions to be overly intrusive.

[21] John v Associated Newspapers Ltd [2006] EWHC 1611 (QB)

After completing his Law degree, **Oliver Marriage** began an MBA in order to gain knowledge and develop business skills that could be used in conjunction with law to provide a strong foundation for future entrepreneurial ventures. Coloured tyres may not be the million pound idea, but it is buried in there somewhere. While law specifically is not his chosen field, it has proved invaluable as an analytical tool in further pursing academia, and a practical skill when arguing with librarians. "Play to your strengths". Outside university life, Oliver is a keen musician; he enjoys both singing and playing the guitar, and hopes to have recorded an EP by the end of the year.

A right to be forgotten?

by Nataly Papadopoulou | ELSA Leicester

The Internet is nowadays a major part of life for the majority of people on this planet. Its importance is immense: it aids the quick and efficient spreading of information as well as the actual storing of an infinite amount of information online, it facilitates governmental and public services; and helps organizations and businesses in carrying out everyday tasks; further, and most importantly, the Internet has provided the platform for superior and uncomplicated communications, enhanced by the creation of forums for exchanging ideas, the email service, blogging, and so on. A somewhat recent development is the growth of social media sites – such as Facebook, Twitter or LinkedIn – which currently play a key role for web users and allow the exchange of messages, images and other materials, thereby providing a platform for exchanging ideas. Social media sites were defined by Kaplan and Haenlein[1] as:

> *"a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content".*

Such platforms do not solely benefit users: new phenomena such as cyber-bullying, online sexual harassment or suicide inducements are a troubling reality for users, site managers and certainly legislators – who have a duty to protect their citizens from harm. Regulating the Internet and its dangerous end products has been a focal point for academics and commentators alike. Its regulation, or yet mere control, is far from uncomplicated, given the Internet's popularity and extensive impact upon a number of jurisdictions. A US-server, for instance, provides access to Google all over the world to jurisdictions with different laws, social norms, cultures, and therefore attitudes towards various issues such as gambling or pornography. For example, a pornographic website can be accessed both in countries with an open-minded attitude towards such content – such as the USA – and to conservative ones – such as China – near indiscriminately.

Returning to social media sites – a rather different concern and the heart of this short piece is the massive amount of personal information users of these sites share online, voluntarily or otherwise, with grave consequences that can often go undetected by users. An anonymous user writes in The Guardian[2]:

> *"One day, about 2 years ago now, I googled my own name and was horrified that in the first 4 google results it was possible to track me on the electoral roll for 8 years, uncover my full date of birth, full address including house number, names and ages of my brothers, sister and partner...I have nothing to hide, but I feel very vulnerable with all this personal information about me so readily accessible…"*

Facebook can hold information indefinably – despite, in this instance, the deletion of the user's Facebook account. In 2009, the Facebook team altered the site's terms of use, such that a user cannot permanently delete information already shared due to of concerns regarding the site's functionality if certain information suddenly disappeared[3]. Additionally, those running the platform are allowed to *use* information and material users share even after the account's deletion. This has raised great controversy, to which Mark Zuckerberg – the founder of Facebook – has responded with statements such as:

> *"We wouldn't share your information in a way you wouldn't want. The trust you place in us as a safe place to share information is the most important part of what makes Facebook work"*[4].

Furthermore – and again using Facebook as an example for clarity's sake – a picture 'tagged' by one of *your* 'Friends' containing tags also of other users probably remains online even if the 'tag is removed' by *you* as that specific photograph also appears in the other tagged users' accounts. Moreover, since that photograph appears in the accounts of every person tagged in it, the photo containing *you* might by now have been downloaded to the computers of any number of people that have access to it. This is an example of a need to be forgotten – a need that is certainly applicable to other personal data and information – such as date of birth, address or sexual orientation and individual preferences – that could be shared with commercial partners or other users, and could potentially cause inconvenience or even harassment. There are potentially serious consequences with regards to personal information being permanently, or even temporarily stored online, and naturally there have been a number of attempts to deal with this issue.

Bernal[5] quotes the EC Communication of November 2010 in defining *'the right to be forgotten'* as:

> *"... the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes.*[6] *"*

Bernal raises both fascinating issues in terms of US-based companies' interests in allowing users such rights, and concerns in terms of the 'emotional' reactions of politicians, the media, online businesses, and the aforementioned US-based companies. The practicalities are also fundamental: the number of online 'spaces' information is stored is untraceable, and the costs of producing technologies that can trace data back through these spaces are enormous.

At present, users of the web have no right to demand third parties to permanently erase personal online data.

In Europe, the European Commission proposed on January 25th, 2012 reforms to Data Protection Laws, currently the much criticized Data Protection Directive 95/46/EC[7], through a Regulation – directly applicable to Member States – that will harmonize data protection laws across Europe. Among other proposals[8] the Regulation provides for *'a right to be forgotten'* in Article 17. The *'right to erasure'* requires, upon request of the data subject, deletion of all personal data of the subject if it is no longer necessary for the purposes it was collected or processed for, or if the subject no longer consents, or if a court or regulatory authority rules that data should be erased, or if data has been unlawfully processed. A number of exceptions are provided, favoring freedom of expression, for instance, or cases where concerns regarding public interest may arise. Its practical effect would be to compel companies such as Facebook or Google to erase information upon request. The Regulation's adoption is planned for 2014, and its effects will be put into force in 2016.

Many have provided criticism, especially in terms of online freedom of speech; for US-based users, it would mean an imbalance of rights against EU citizens – given the USA's open-minded approach to freedom of speech[9]. The United Kingdom, among nine Members States, is also opposing proposals as *'unrealistic'* [10]; the UK has voted for the Regulation to be turned into a Directive to provide flexibility, and also votes for *'separate rules'* for smaller businesses[11]. It will be interesting to see what the EU officials' reaction will be, and whether the Regulation will undergo amendments.

Commentators suggest alternatives to the *'right to delete'*: developing existing law/practice by applying fines/sentences for data loses/breaches of data security; the use of software that will enhance data security via encryption – currently subject to an enormous criticism in terms of effectiveness – and finally *'changes in the community and culture'*[12]. This view is also shared by the *Open Rights Group*:

> *"A good rule of thumb is to assume everything is public and not to share sensitive or potentially embarrassing information, photos, videos or other content… Users should think twice about signing up to services that ask for a lot of information"*[13].

As Bernal[14] confirms, problems will always exist – '*human errors… nature… malice, technological error and developments, [and the need] to fight terrorism or catch abusers or murderers*' – even with proper regulation and enforcement.

As a concluding remark, I support the view that the most effective solution is to track back to the root of the problem – i.e. the culture, peoples' behavior online and offline. Regulating the Internet and social media is rather futile for a number of reasons – most importantly for me is jurisdiction – the borderless and international nature of the Internet. Educating users and highlighting the consequences of sharing an enormous amount of private and personal information online should be the focal point for governmental officials.

Why don't you try, if you haven't already done so, to 'Google' yourself – how much of *your life* is available to *anyone* with access to the online world?

Nataly Papadopoulou is a University of Leicester LLB graduate, who completed her LLM in Human Rights at Queen Mary, University of London, in 2013. She has returned to Leicester to undertake her PhD, with a focus on euthanasia and human rights. Among her modules during the LLM, Nataly took an interest in Cyberspace Law. ELSA day has given Nataly the perfect opportunity to combine her modular knowledge with her love of human rights.

1 A. Kaplan, M. Haenlein, 'Users of the world, unite! The challenges and opportunities of social media', Business Horizons 53 (1), (2010), p. 61.
2 'How easy is it to delete yourself from the web - your experiences' (April, 2013) <www.theguardian.com/technology/2013/apr/04/delete-online-profile-readers-panel> accessed 3 January 2014.
3 'Facebook controversy over right to delete personal information" (February, 2009) <http://www.telegraph.co.uk/technology/facebook/4680220/Facebook-controversy-over-right-to-delete-personal-information.html> accessed 3 January 2014.
4 'Facebook controversy over right to delete personal information', (February, 2009) <http://www.telegraph.co.uk/technology/facebook/4680220/Facebook-controversy-over-right-to-delete-personal-information.html> accessed 31 December 2013.
5 Bernal, P. A., 'A Right to Delete?', European Journal of Law and Technology, Vol. 2, No. 2, 2011.
6 EC Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(2010) 609, p.8.
7 Available at <http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf> accessed 28 December 2013.
8 For other provisions <http://www.sjberwin.com/insights/2013/11/07/update-on-draft-eu-data-protection-regulation> accessed 29 December 2013.
9 Warwick Ashford, 'US lawyer criticises principle of right to be forgotten', (February, 2012) <http://www.computerweekly.com/news/2240117365/US-lawyer-criticises-right-to-be-forgotten-principle> accessed 31 December 2013.
10 Warwick Ashford, 'UK calls for opt-out of online right to be forgotten', (April, 2013) <http://www.computerweekly.com/news/2240180878/UK-calls-for-opt-out-of-online-right-to-be-forgotten> accessed 31 December 2013.
11 'UK seeks opt-out of 'unrealistic' European 'right to be forgotten' laws', (April 2013) <http://www.out-law.com/en/articles/2013/april/uk-seeks-opt-out-of-unrealistic-european-right-to-be-forgotten-laws/> accessed 31 December 2013.
12 Ibid. (n.4)
13 Ibid. (n.3)
14 Ibid. (n.4)

Giving human rights an identity online:

Obstructing villains

by Nerijus Karlauskas | ELSA Middlesex

elsa
The European Law Students' Association
MIDDLESEX

Internet Trolls. Haters. Keyboard Warriors. These are our modern Macbeths, our Mayors of Casterbridge, our Iagos. These are the characters of today that make the works of William Shakespeare and Thomas Hardy come to life. They are the villains that are known all over the internet, filling cyberspace with man's inhumanity to man, with just a click of a button…

Cyberspace is used by real people of all ages, coming from diverse backgrounds and societies. However it appears that cyberspace does not reflect the way regular societies run. It appears that when a person delves into cyberspace, they – in the eyes of their cyber-peers, at least – are not viewed as a real-life person anymore – rather, they are simply a user. Although their name might be Bob in real life, in cyberspace they can be Steve123. He is a user, using a platform created within the cyberspace. These platforms are the sites, where everyone can be anyone they want, and can express themselves however they like – which appears to positively enable users to exercise their fundamental Human Rights. Usually in real life, whenever these rights clash or are breached, a resolution is ultimately reached. However often that is not the case within cyberspace, as some users take these rights for granted, become villains and continuously abuse others. Despite there being real life laws, rights and regulations, in cyberspace these laws become fictitious – but the outcomes of these breaches are no less real.

Cyber bullying is a form of cybercrime where one user threatens, harasses or embarrasses another – contrary to absolute freedom from torture according European Convention on Human rights (ECHR), Article 2. This type of behaviour can have a number of consequences, with some as tragic and serious as suicide. Victims such as Megan Meier[1], Jamey Rodemeyer[2], Amanda Todd[3], Hannah Smith[4], Chelsea Clark[5] and Rebecca Sedwick[6], who had been facing continuous humiliation from unidentified users, who thought that they were just having a bit of harmless fun. With most of the victims being below the age of 16, they should be under adult supervision – although there is not much that they can do, since the attacks come from the internet, well outside their region of control. This type of cyber-crime happens on popular sites that are visited by millions, such as Facebook, Twitter, Youtube, blogs, and gaming websites. Due to innocent users having no control in preventing the abuse reaching them, it should be the site's responsibility to control of what is happening on their platforms. Despite their best efforts to get as much information about user's identity, all of them still allow the users to remain anonymous. With a right to expression clashing with right to privacy, a clear balance has to be struck between ECHR articles 8 and 10. How can the present situation be resolved – or at least improved – and at the same time protect everyone's human rights?

Sadly, it appears that these kinds of sites have not done their best to protect online users. In most cases, it is clear that the damage is done when the user receives the abuse from another anonymous user. So, how can these platforms create an environment that does not prevent someone from expressing themselves, while at the same time protecting their privacy when trying to identify them?

One of the ways sites like Facebook could protect online users is by blocking as much abusive content as possible, before it reaches the intended recipient. However there is a danger that this might amount to a breach of article 8. Methods such as using automatic filters could be used – software that block offensive or hate-speech language text combinations, and image scanners that could identify offensive image contours, etc. This software would then automatically block the sender from using the site. Methods such as this would not result in breach of any rights, due to similar methods already being used in other sites such as "Google Maps"[7] and online games such as "Runescape"[8]. Recent developments of fingerprint readers could also be used in future – websites could require users to scan their fingerprint in order to sign in, and at the same time protect their identity. This feature would not breach Article 8, since it is currently used in latest phone models. Users using their unique identification means that the chances of identifying the wrongdoer increase, since it was their print that gave them the access to the offending user account.

In conclusion, Charles Dickens was right when he said that: "Electric communication will never be a substitute for the face of a man with his soul in it, encouraging another man to be brave

1 BBC News, " US 'cyber bullying' case begins", (BBC News 2008) <http://news.bbc.co.uk/1/hi/world/americas/7736078.stm> accessed 5/1/2013
2 Jon Swaine, "Boy, 14, found dead over gay bullying", (Telegraph 2011) <http://www.telegraph.co.uk/news/worldnews/northamerica/usa/8779672/Boy-14-found-dead-over-gay-bullying.html> accessed 5/1/2013
3 Katinka Dufour, "Amanda Todd case highlights issue of online bullying", (Telegraph 2012) <http://www.telegraph.co.uk/news/worldnews/northamerica/usa/9612030/Amanda-Todd-case-highlights-issue-of-online-bullying.html> accessed 5/1/2013
4 Sian Lloyd, "Hannah Smith death: Ask Fm to help Police inquiry", (BBC News 2013) <http://www.bbc.co.uk/news/uk-23596068> accessed 5/1/2013
5 Claire Carter, "Mother criticises 'evil' social networks used by teen before she committed suicide", (Telegraph 2013) <http://www.telegraph.co.uk/news/uknews/law-and-order/10430754/Mother-criticises-evil-social-networks-used-by-teen-before-she-committed-suicide.html> accessed 5/1/2013
6 BBC News, "Florida; Charges in Rebecca Sedwick 'bullying death'", (BBC News 2013) <http://www.bbc.co.uk/news/world-us-canada-24538798> accessed 5/1/2013

and true". But there is always another side to the coin. Apart from all the villains, there will always be heroes, who are so moved by need to make a difference whatever the situation is. This is why we have ELSA DAY – an opportunity to gather together and embrace the mutual understanding that you are not alone in protecting and upholding human rights, as a hero of our days!

Nerijus is currently a second year LLB course student at Middlesex University, London. His law interests include attending court trials, studying legal method and participating in extracurricular seminars, talks and trainings in various legal areas. His ambition is to become a barrister and practice in employment and tortious disputes litigation and arbitration. Nerijus is an active member of the university as well as the Students' Union and has been elected as a student representative. He received a 'Gold Status' award, which reflected his efforts for making positive changes and resolving his peers' issues in Law Board of Studies meetings.

Protecting children with the governance of pornography on the Internet

by Amy Shields | ELSA Newcastle

The wide availability of pornography on the Internet is a cause for concern for many governing bodies. There is much controversy over the fact that what can be classified as "obscene" and "illegal" in one country may be completely acceptable in another. Regulating this form of 'entertainment' is considered to be one of the most controversial topics within the range of Internet concerns[1]. Out of this debate arises the sensitive issue of child abuse through the use of child pornography. Regulation and prohibition of child pornography has become a major focus for many governments. This stems from the need to recognise that paedophiles are able to easily 'trawl' the Internet for pornographic content involving young children, subjecting them to unnecessary abuse. Many argue that while regular pornography should not be "proscribed by government based on freedom of speech, the line should be drawn at child pornography"[2]. Child pornography is particularly sensitive as it is argued to be a permanent documentation of direct child abuse. However, legislation that is currently in place in The United Kingdom does not completely eradicate or prevent child pornography. Governing bodies need to fully understand and appreciate the abuse that stems from child pornography, while differentiating it from 'regular' pornography in order to collectively enact appropriate legislation, which is both effective and protective to cover the span of the World Wide Web.

A major problem which governments are required to face is the fact that "there is no settled definition of pornography"[3]. This is because what is considered obscene differs between countries throughout the world, depending on cultural and moral values, and this creates difficulties because of the fact that the World Wide Web is available in numerous nations. Governing bodies find great difficulty in regulating a media outlet, which crosses the boundaries of many differing cultures and societies. There have been worldwide attempts by governments and legal bodies to limit and, even, restrict the availability of pornographic content on the Internet. As such, the emergence of the Internet and the availability of pornography have created a "moral panic" amongst governments and law enforcement agents[4]. This panic has extended within the realm of child pornography and The United Kingdom, in particular, as a result, has seen the enactment of the Protection of Children Act 1978 as the main legislation governing in this area.

Children are impressionable and easily fall prey to the manipulation of paedophiles working under the shadow of the Internet. These individuals lure children into sexually explicit and dangerous situations, which are then promoted and transmitted over the World Wide Web. There are, unfortunately, problems with the legislation that is currently in place in The United Kingdom, as it does not fully eradicate, nor does it appropriately prevent, the existence of child pornography on the Internet. The laws in place are weak and will allow for the continued transmission and possession of these sexually abusive images and videos on the Internet. However, Reidenberg articulates that the Internet "poses a fundamental challenge for effective leadership and governance"[5]. Despite this challenge, the need to effectively govern child pornography existence on the Internet is evident in the outcome of the case *R v T (Child Pornography)* (1993) where the defendant was able to show there was no reason to convict him of the offence under s1(1)(c) Protection of Children Act 1978. Here the defendant argued against s. 1(1)(c) of the Protection of Children Act 1978, which provides that it is an offence for a person "to have in his possession such indecent photographs [or pseudo-photographs], with a view to their being distributed or by himself or others" by saying that he had no intent to show the material to anyone but himself[6]. By allowing individuals to legally obtain pornographic material involving children, so long as they have no intent to broadcast to other individuals, the law fails to effectively regulate and criminalize the existence of child pornography on the Internet.

In response, there has been much more emphasis on the need for child protection with relation to the Internet and the dangers that it presents. It is clear that recently many more government officials and policy makers are "embracing the politics of fear regarding child sexual abuse".[7] Parents and advocacy groups promote the notion of "stranger-danger" and work together to establish a safety net for children exposed on the Internet. It is apparent that for Internet legislation to protect children from sexual abuse or exploitation to work, all societies and cultures need to consistently "draw the line at child pornography". A US legislator in a recent congressional meeting has stated: "The sexual exploitation of our children is a criminal problem; it is a social problem; it is a human rights problem"[8]. Following such advocacy arguments, Melissa Hamilton notes that: "the net-widening policy of concern here is the wholesale inclusion of child pornography offenses as a genre within the child sexual exploitation initiative. Such a policy represents a deontological perspective that judges all sexual images of children as immoral and therefore deems anyone who views such images as a criminal, who deserves strict punishment regardless of the consequences of his actions"[9]. Whether these new policies are too restrictive appears to be of minimal concern if child pornography is to be eradicated and paedophiles are to be discouraged from utilizing the Internet to lure their next child victim.

As the age of the Internet develops and expands, it is crucial for the safety of children that international legislative bodies work together to legislate against child pornography on the Internet. The US, for example, is taking a leading role in developing policy and legislation for law enforcement agencies to use so that they may crack down on the criminal nature of child pornography on the Internet. It has been claimed that the "[i]nternet offers what has been called the 'triple A engine' of anonymity, availability, and affordability that is fuelling addictive behaviour involveing cybersex"[10]. Consequently, this addictive behaviour is producing extensive collections of child pornography, which are being trafficked and constantly transmitted online[11]. By failing to create legislation that reaches across all borders, with respect to child pornography online, the National Centre for Missing and Exploited Children strongly warns that "anyone can be exposed to child pornography online very, very easily…we're growing sexual abusers; they're growing; their being cultivated and nurtured and watered and fed on the Internet"[12]. By drawing the line at child pornography and creating international legislation controlling the Internet, nations can work together to protect the child from further sexual exploitation and abuse.

The Internet is an international organ and regulation through laws is difficult to achieve as many nations differ in what is socially and culturally acceptable. However, the one constant that should be evident in Internet legislation is legislation governing the sexual exploitation and abuse of children online through pornography. Policy makers, along with law enforcement agents, need to acknowledge the harsh fact that the Internet is 'growing' with predators who will ultimately sexually abuse children. By creating a stronger 'net-wide' policy, the Internet will be able to move forward into the next generation of protecting all children, and eliminating the danger and abuse associated with child pornography.

Amy Shields is the Vice President for Academic Activities at ELSA Newcastle. She is a third year law student at Newcastle University and upon graduation aims to return to Canada to take over a sole-practitioner law firm where she will be working specifically with children and promoting their rights. She has a great passion to help with bringing justice into the lives of those who are unable to do so for themselves and feels that this is why law is her best career choice.

1 Akdeniz, Yaman. " Governance of Pornography and Child Pornography on the Global Internet: A Multi-Layer Approach" published in Edwards & Waelde, Law & the Internet: regulating cyberspace. (Hart Publishing, Oxford 1997) at p223
2 Ibid at p227
3 Ibid at p223
4 Cohen, S. "Folk Devils and Moral Panics: Creation of Mods and Rockers". (Blackwell, 1987)
5 J R Reidenberg, "Governing Networks and Cyberspace Rule-Making" (1996) Emory Law Journal 45
6 R v T (Child Pornography) (1999) 163 J.P. 349; Protection of Children Act 1978 c37
7 Hamilton, Melissa. "The Child Pornography Crusade and Its Net-Widening Effect" (2012) 33 Cardozo L. Rev. 1679 at 1680
8 In Our Own Backyard: Child Prostitution and Sex Trafficking in the United States: Hearing Before the Subcomm. on Human Rights & the Law of the Comm. on the Judiciary, 111th Cong. 1 (2010) [hereinafter In Our Own Backyard] (statement of Sen. Richard J. Durbin, Chair, Subcomm. on Human Rights & the Law)
9 Hamilton, Melissa. "The Child Pornography Crusade and Its Net-Widening Effect" (2012) 33 Cardozo L. Rev. 1679 at 1680
10 Al Cooper, Sexuality and the Internet: Surfing into the New Millennium, 1 CyberPsychology & Behav. 187 (1998).
11 Janis Wolak et al., Crimes Against Children Research Ctr., Trends in Arrests of "Online Predators" 1 (2009), available at http://unh.edu/ccrc/pdf/CV194.pdf
12 Domestic Minor Sex Trafficking: Hearing Before the Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary, 111th Cong. 54 (2010)

Does posting a picture last forever?

by Tibor Korman
ELSA Queen Mary, University of London

elsa
The European Law Students' Association
QUEEN MARY, UNIVERSITY OF LONDON

I am sure that you have heard of the law students that dressed as Somali pirates[1] for a fancy pub crawl in Edinburgh or the other 2 students that dressed as the twin towers in Manchester[2]. One of the practitioners that I have discussed this with recently had a really interesting observation to make: "Good luck to them finding a training contract". This remark puzzled me because it begs the question whether something like this can be taken down from the Internet and be forgotten about. Habeo Facebook, ergo sum[3], but for what price?

Luckily for all of us, the UK Information Commissioner's Office has warned employers in the UK that it would have very serious concerns if they were to ask for Facebook login and password details from existing or would-be employees but, across the ocean, the Florida Board of Bar Examiners (FBBE) has guidelines vague enough to suggest it can start screening the social network accounts of certain applicants to the Florida Bar.[4] The European Convention on Human Rights ("ECHR") provides in Art 8(1) that: "Everyone has the right to respect for his private and family life, his home and his correspondence." In addition, the Charter of Fundamental Rights of the European Union reads in Art 7: "Everyone has the right to respect for his or her private and family life, home and communications." Furthermore in Article 8, it states: "Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data, which has been collected concerning him or her, and the right to have it rectified."

The main challenge with the above scenario is that the pictures are by definition correct in what they represent; but was the posting of the picture an interference with private life[5] and is there a right to delete those pictures from the internet even if they are not considered an interference with private life, mainly because they were taken in a public space and consented to at the time?

Rob Mindell[6] argues that privacy claims that occurred in classic media would not be successful in virtual social media context if the facts changed a little. Imagine that the pictures of Ms Campbell leaving a rehabilitation clinic are posted by her "friend" on Social Media. Mindell´s argument is based on the fact that "friends" are mutually selected and that, by posting something, one intends to share it with the "friends" who are an exclusive limited group. Ms Campbell, to prove a "reasonable expectation of privacy," would depend on to whom the information is published to. Because knowledge of someone being a user of narcotics is of social benefit, publication to a discriminate audience of "friends" for whom the information would be of use would qualify for a defence of public interest. Similarly, Mindell argues that posting pictures of Mr Mosley to his identified "friends" on his wall would make the defence applicable. In all fairness, this ignores the fact that to post something on Facebook means that "friends" of the posting person as well as the "friends" of the person on whose wall the post is posted will see the post[7] plus it will pop up in the news feed of any person liking it or commenting on it since. This slightly undermines the logic of Mindell who sees Faceebook only from the side of the person on the picture and his or her limited group of friends.

However, how does this apply when someone posts pictures of somebody else on Facebook taken by their own camera? If the information in question is considered to be highly personal or, in some circumstances, merely frivolous, such as the distribution of an embarrassing photograph or video that contains no notable information of importance to the claimant's network of friends, it would be less likely to qualify for a successful defence of public interest. This was shown to be the case for traditional media in *Mosley v News Group Newspapers*[8], in the judgment of Eady J.: "Although no doubt interesting to the public, was this genuinely a matter of public interest? I rather doubt it."

Lennin Hernández González, concludes: "the mere fact that private information is made available to a determined public does not entail that such data have lost their attributes as private information and even less that it can be granted the same usage of public information." Therefore, one would be protected by privacy laws in the circumstances someone posted something about aspect of private life on social media against his will provided the public interest defence is not satisfied[9]. However, this seems only applicable if the pictures were taken in a situation where the person portrayed had a reasonable expectation of privacy,

1 http://www.legalcheek.com/2013/11/edinburgh-university-law-students-cause-outrage-after-blacking-up-as-somali-pirates-for-fancy-dress-pub-crawl/
2 http://www.dailymail.co.uk/news/article-2488232/Fury-British-girls-Twin-Towers-fancy-dress-costumes--daughter-pilot-flying-US-time-terror-attacks.html
3 ("I have Facebook, therefore I am"). Lennin Hernández González" Habeo Facebook ergo sum? Issues around privacy and the right to be forgotten and the freedom of expression on online social networks". Entertainment Law Review 201,Ent. L.R. 83
4 O'Brien, 'Facebook v the Florida Bar' (2011) 1 International Journal of Public Law and Policy 127
5 Von Hannover v Germany [2004] E.M.L.R. 21; (2005)
6 Rob Mindell „Rewriting privacy: the impact of online social networks" Entertainment Law Review 2012 Ent. L.R. 52
7 Depending on the privacy settings
8 [2008] EWHC 1777 (QB)
9 In the author's opinion very unlikely on Facebook for ordinary user

thus maybe arguably a private house party or similar. In case of public photography, e.g. done by a professional photographer in a club, the solution Facebook provides is to contact the person who posted the picture and untag[10] yourself. However, Facebook will not remove the picture from friend´s profile or the club´s page on which it has been posted. Therefore, something that can "threaten" your career, such as the twin towers costume, can be posted online without fear of breach of privacy if the picture has been taken in public space[11].

Similarly, after Facebook acquired Instagram it announced a policy change including a clause to the effect that Instagram can use photos and other data posted by users without seeking consent or providing prior notice to such users[12]. The terms and conditions of use further stipulates that "[i]f you remove information that you posted to the Service, copies may remain viewable in cached and archived pages of the Service, or if other Users or third parties using the Instagram API[13] have copied or saved that information."[14] This basically means pictures might be licensed to third parties and might be accessed even after they have been deleted from your account. Similarly to Facebook, Instagram has a policy setting that practically determines your "reasonable expectation of privacy" when posting pictures. One can only wonder what would happen if mistakenly (due to a default setting of an upgraded operational system on your phone for example) a picture has been posted with public settings instead of private setting and how would Instagram ensure the picture available for some time to the public is retrieved. Considering the above privacy statements it would hardly do anything about it. Therefore, anything posted by a friend or by you on Instagram has the potential to be there forever and to be made available to media.

With regard to Twitter: "[b]y submitting, posting or displaying Content on or through the Services, you grant us a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed)…"[15], which means that any picture posted by yourself can be retweeted (re-posted by different user); with breach of privacy hardly arguable because of the public nature of Twitter, even if those pictures are obviously intended to stay private[16]. If posted by someone else, your reasonable expectation of privacy will be considered and possible defence of public interest can be applicable as discussed above. Regardless of whether you or your friends or third parties post the pictures, if posted on Twitter as public, the pictures will never disappear, provided that they do not infringe privacy rights and are not removed by court order; anyone under the above licence can access, retweet and publish them.

Data Protection Directive (95/46/EC) ('the Directive') indicates that data subjects have the right to obtain from data controllers (e.g. Facebook): 'the rectification, erasure or blocking of data the processing of which does not comply with the provisions of the Directive, in particular because of the incomplete or inaccurate nature of the data' (Article 12(b) and (c)). In the UK, a data subject's right to erasure only applies to the extent that the relevant data are inaccurate, which cannot be argued with regard to our scenario. The decision as to whether a data controller should rectify, block, erase or destroy data is left to the Court. The interpretation that there is no right to be forgotten has been most recently confirmed by Advocate General Jääskinen in the *Google Spain case* C-131/12.

The EU is currently discussing a new Data Protection Regulation with intent that "[a]ny person should have the right to have personal data concerning them rectified and a 'right to erasure and to be forgotten' where the retention of such data is not in compliance with this Regulation", Graham and Cooper[17] argue that the proposed Article 17 goes beyond providing individuals with the right to have unlawful content about them deleted. It does not place any onus on the user to show that the publication complained of is harmful, or goes beyond the scope of what might reasonably be expected, based on the context of the interaction. This seems to be the solution to the unwanted pictures on Facebook. Nevertheless, it is unclear how the regulation will deal with direct quotations from a post or pictures with more than one person on them. The final version of the Regulation is expected to be enacted in 2015, which certainly will be something the Internet community should look forward to with great expectations.

The best advice one can give for use of social media is to ensure that your settings are strictly private and recommend this to all of your "friends"; because, if they are not, you have practically lost all reasonable expectations of privacy, which significantly limits the human right to private life in its protection. To conclude, check your privacy settings, think about what you post and, lastly, how you dress up for a Halloween party because some mistakes will last forever and Google search will find you years after you have forgotten about it.

Tibor Korman is a Queen Mary, University of London student in his final year studying to become a corporate lawyer in the future. He likes to challenge himself, which is the reason why he looked into this ELSA Day topic, which has been a complete unknown to him until this article was completed, even though he is a very active user of Social Media. Tibor would like to thank Nadia Tjahja for her comments and guidance provided when writing this article. The opinions expressed in this article should not be taken as legal guidance.

[10] Remove connection with ones' profile
[11] Von Hannover v Germany (40660/08 and 60641/08)
[12] „…hereby grant to Instagram a non-exclusive, fully paid and royalty-free, transferable, sub-licensable, worldwide license to use the Content that you post on or through the Service, subject to the Service's Privacy Policy" – http://instagram.com/about/legal/terms/#
[13] Development mode of use
[14] http://instagram.com/about/legal/privacy/#
[15] https://twitter.com/tos
[16] http://www.post-gazette.com/jack-kelly/2011/06/05/Weiner-s-troubling-tweet/stories/201106050183
[17] Nick Graham, Alexandra Cooper „The right to be forgotten -- what's the position now?" Data Protection Ireland, DPI 6 6 (10)

The darker side of social networks: The inadequacy of cyber bullying legislation in the UK

by Philip Wells | ELSA Sheffield

elsa
The European Law Students' Association
SHEFFIELD

Within the world of the Internet, a battle is occurring between two fundamental and essential human rights: The Freedom of Speech and The Right to Privacy.[1] Ideas of censorship and control have been raised to attempt to combat the individuals that misuse the Internet as a vessel to evade the law and commit criminal acts.[2]

The Internet has yielded significant social good for the world, creating an easily accessible system for sharing information and communicating globally. However, balanced alongside this benefit is the realisation that the Internet has also been used to circumvent laws. It has spawned 'Internet Trolls'[3], 'Cyber Pirates'[4] and, more generally, created a platform for certain individuals to share racist, sexist and homophobic views with anonymity.

The ability to share such views, often inciting fear and distress in persecuted individuals within the context of social networking websites, has led to tragic situations of self-harm and suicide. Famous incidents such as the suicide of Tyler Clementi in the US[5] and Thomas Mullaney in the UK[6] have garnered significant media attention. However, the UK Government is still grappling with how to adequately prohibit and guard against this sort of behaviour.

This article aims to provide a very brief overview of the laws and legal redress available to individuals suffering from this form of cyber bullying. In doing so, this article will highlight that while developments are underway to combat this problem; a suitable system of regulation has not yet been created.

Criminal Law

There are currently a plethora of different avenues and methods for individuals who are victims of cyber bullying to pursue, in theory. However, the practical difficulties in establishing an action, as well as the often confidential nature relating to the bullying, commonly limits what actions an individual will feel able to take.[7] Numerous pieces of criminal legislation such as section 16 of the Offences Against the Person Act 1861, section 4 of the Protection from Harassment Act 1997, section 1 of the Malicious Communications Act 1988, and section 127 of the Communications Act 2003 all exist as devices to curb and prohibit actions that could be classified as cyber bullying.[8]

These criminal laws, while good in theory, are plagued with problems for individuals seeking to use them to gain redress. This is mainly because most of the criminal laws governing actions that would be classified as cyber bullying were created in an era before the Internet and social networking was fully developed. They are outdated for dealing with this modern problem and therefore are unsuitable. For example, the Offences Against the Person Act was created in 1861, a time when today's form of electronic communication would scarcely have been imaginable. Therefore, the law, with the slight exception of a few piecemeal additions of common law, has no appropriate provisions to combat cyber bullying. As well as existing within an outdated legal framework, the criminal law is often predicated on a high level of proof.[9]

It is, therefore, the case that the criminal law has not created a suitable platform for individuals to seek redress. Moreover, the rare success of criminal actions against cyber bullying and other internet based offences has often been overshadowed by more notorious and ridiculed actions, such as *Chambers v Director of Public Prosecutions*,[10] which is colloquially referred to as the "Twitter Joke Trial".

Tort Law

Together with the limited and problematic criminal law provisions that attempt to combat cyber bullying, there is also the longstanding torts of defamation and libel. Conjointly, these actions have been used to prohibit the publication and distribution of offensive and character-damaging information. These mechanisms proved to be successful for use against newspapers and other publications; however, like the criminal law, it is ill equipped against cyber bullying on social networking sites. These torts are the product of a different age and, therefore, provide limited guidance on how to address Internet-based actions of cyber bullying.[11]

The UK Government has attempted to update the law regarding defamation to remedy this defect, as seen by the

1 See generally: Jennifer Agate and Jocelyn Ledward, 'Social media: how the net is closing in on cyber bullies' Ent. L.R. 2013, 24(8), 263-268.
2 Jade Brannan, 'Crime and social networking sites' Jur. Rev. 2013, 1, 41-51.
3 A recent well-publicised example of which can be seen in relation to the University of Cambridge Professor of Classics, Mary Beard < http://www.telegraph.co.uk/news/uknews/law-and-order/10209643/Internet-troll-who-abused-Mary-Beard-apologises-after-threat-to-tell-his-mother.html> accessed 02.01.2014.
4 For example the longstanding legal battle involving the Pirate Bay website < http://www.wired.co.uk/news/archive/2013-02/26/pirate-bay-leaves-sweden> accessed 02.01.2014.
5 http://abcnews.go.com/US/rutgers-trial-dharun-ravi-sentenced-30-days-jail/story?id=16394014 accessed 01.01.2014.
6 http://www.bbc.co.uk/news/uk-england-birmingham-14121631 accessed 02.01.2014.
7 Jennifer Agate and Jocelyn Ledward, 'Social media: how the net is closing in on cyber bullies' Ent. L.R. 2013, 24(8), 263-268.
8 Ibid.
9 Ibid.
10 Chambers v. DPP [2012] EWHC 2157.
11 Jennifer Agate and Jocelyn Ledward, 'Social media: how the net is closing in on cyber bullies' Ent. L.R. 2013, 24(8), 263-268.

Defamation Act 2013, due to come into effect in early 2014. However, many remain highly sceptical of the legislation and have seen fit to criticise it for failing to take the opportunity to overhaul the law into a more suitable and modern mechanism for redress.[12] This inadequacy of tort law is a noticeable problem internationally for common law jurisdictions and has led to certain jurisdictions, such as New Zealand, creating a new tort specifically designed to resolve Internet based issues of privacy.[13]

The Solution

Cyber bullying is an issue on the rise and a relatively common problem for a large amount of young people.[14] The current law, both civil and criminal, has simply failed to produce a clear and suitable system of regulation to restrict and prohibit this sort of abusive behaviour.

One method to resolve this problem is the introduction of stricter and more punitive laws, as has been the case in the United States of America[15] and in Canada.[16] These laws are designed to combat the modern problem of cyber bullying and are, therefore, significantly easier for an individual to bring an action. However, they are onerous pieces of legislation that many individuals fear tread into the domain of Internet censorship and over-burdensome restrictions on Freedom of Speech. Additionally, while they are the most modern attempts to regulate and remove cyber bullying, due to the rapid developments in the Internet and electronic communication, they could easily be just as obsolete and cumbersome as some of the current legislation in a relatively short period of time.

A far less onerous method to attempt to combat cyber bullying is by attempting to educate individuals better on social networking and communication. In its basic form, this approach has been adopted in the UK, instead of stringent laws, and is a now a curriculum requirement at UK Schools. This is a preventative approach that aims to avoid the emotional harm and distress that cyber bullying can cause. This approach, based on the idiom 'prevention is better than a cure' is a positive method to deal with cyber bullying in an open arena. However, it could never be relied on to completely prevent such behaviour and, therefore, the solution must also lie in suitable redress for when cyber bullying has actually occurred.

Conclusion

Overall, the issue of cyber bullying is a pressing social issue and a concern that will only develop and become more pronounced in the future. Like numerous Internet-based problems, such as cyber piracy, governments and countries have struggled to create forwarding thinking pieces of regulation. Moreover, they have also been faced with the gargantuan task of monitoring the vast realm of the Internet to even identify this sort of behaviour. Nevertheless, action must be taken and it is time for the Government to embark on serious consultations and research to attempt to formulate an adaptable and flexible method to stop cyber bullying.

Philip Wells is an Alumnus of the University of Sheffield. A former LLB and LLM student at Sheffield, Philip was involved in a variety of different projects and programmes while studying, such as being the manager of the free legal advice clinic (FreeLaw) and being the Careers Secretary for the Edward Bramley Law Society. Philip is currently undertaking a bespoke accelerated LPC at the University of Law in London, following which he will start his training contract at a magic circle law firm.

[12] http://kellywarnerlaw.com/the-uk-parliament-facebook-twitter-and-cyberbullying-ing/ accessed 01.02.2014.
[13] Jennifer Agate and Jocelyn Ledward, 'Social media: how the net is closing in on cyber bullies' Ent. L.R. 2013, 24(8), 263-268.
[14] Please see: http://www.ditchthelabel.org/cyberbullying-statistics/ accessed 02.01.2014.
[15] Lorraine McDermott, 'Legal issues associated with minors and their use of social networking sites' Comms. L. 2012, 17(1), 19-24.
[16] http://www.torontosun.com/2013/12/26/cyberbullying-becomes-a-national-issue-in-wake-of-familys-unending-nightmare accessed 02.01.2014.

Hate speech and religion: The effect of online dissemination and the potential for harmonisation of national legislation

by Alexander Adamou & Jake Wright | ELSA Sussex

With the advent of social media and the greater reliance on the Internet, the sharing of information has become easier and this information is now more available to the general public worldwide. This, however, poses a problem when such information is offensive or prejudicial against certain minority groups. In the new digital age, in order to be able to enforce the rights of these minorities, we need to be able to clearly identify the applicable national law and apply it consistently to circumstances that may occur.

The first thing that we need to consider is if a legally binding definition of 'hate speech' on the national level is possible – also, if this is possible or necessary at an international level given the worldwide nature of the communication. In The United Kingdom, it can be said that a legally binding definition of "hate speech" is more than possible and it is a reality. This is because we have legislation in this jurisdiction that deals specifically with this issue and goes so far as to define acts that can be considered "Hate Speech".

For this definition we need to look at the Public Order Act 1986[1]. By virtue of part 3 of this piece of legislation, acts of religious hatred[2] are prohibited. When looking to hate speech we need to look at section 18 of the Act, which states that:

"(1) A person who uses threatening, abusive or insulting words or behaviour, or displays any written material which is threatening, abusive or insulting, is guilty of an offence if—

(a) He intends thereby to stir up racial hatred, or

(b) Having regard to all the circumstances racial hatred is likely to be stirred up thereby.[3]

So, whilst this does not mention hate speech per se, this covers verbal acts that are religiously charged and thus can reasonably be considered to be a definition for hate speech within the United Kingdom[4].

This gives us a legally binding definition from which to work from. However, although legally binding, we must consider the sheer breadth of this definition and the balancing act that must be done with the right to freedom of expression guaranteed by Article 10 of the European Convention on Human Rights (ECHR)[5], which has been codified in section 12 of the Human Rights Act (HRA)[6]. This has somewhat been resolved by the addition of Section 29J[7] in the Racial and Religious Hatred Act 2006[8].

Now, we must consider whether this is necessary or possible at an international level. On the issue of possibility there are several attempts at an international level to define hate speech, for example, in The International Covenant on Civil and Political Rights (ICCPR) Article 20[9] and the Additional Protocol to the Convention on Cybercrime Article 2[10]. This would seem to indicate that there is a call for such a definition on a supra-national level, but considering the reservations that some countries have to these protocols there is a discrepancy in opinion that may be hard to reconcile due to different cultural backgrounds and political philosophies.

In conjunction with this, there have been those who have argued that a general international definition leads to problems with interpretation at a municipal level and adds a layer of needless complexity as to what hate speech is[11]. Thus, moving further away from the sought aim and actually making things more difficult in terms of resolving certain human rights issues.

Looking towards necessity there would be those that would argue that hate speech has become more of a global problem with the advent of social media and easier communication between countries and parts of the world. In this vein, a generalised international definition of hate speech would be an indicator to the wider community that such actions are not tolerated and may even call for a review of domestic legislation.

On the other hand, there is a strong argument to say that this is an internal matter[12] for states and that they most simply suffer the same problem but, however, they should be left to define and tackle the problem in their own way. Many would argue the awareness is most effectively raised at the domestic level and that the appropriate institution to reconcile these particular issues would be the national legislating bodies and domestic courts. This has some basis on the lack of enforceability of international law[13] and many would say its lack of impact on a domestic setting[14].

Having considered the definition, we must now look at what the key contextual elements are to identify a 'hate speech' and whether the multiplying and wider effect of online dissemination always means higher potential impact of online hate speech. The law on hate speech in the United Kingdom is fragmented amongst multiple statutes developed over twenty years since the commencement of the Public Order Act 1986. Hate speech originated from a public offence, defined under section 4 as using "fear or provocation of violence", which is aggravated by hate elements in sentencing under section 31 of the Crime and Disorder Act 1998. This aggravation is defined under section 28 as demonstrating hostility "towards the victim of the offence… based on the victim's membership of a [racial] membership" or motivated by membership of a racial or religious group[15]. Another element of hate crime originates in section 18 of the Public Order Act 1986[16] as discussed above.

The stirring of 'racial hatred' was included under this public offence and results in a conviction when intent to cause hate and that racial hatred was likely to have been caused in regard to all the circumstances[17]. While originally limited to hate based on skin colour, race, ethnic origin or nationality[18], 'racial hatred' was expanded later under the Racial and Religious Hatred Act, which inserted Part 3A into the Public Order Act 1986 to include hatred with reference to a religious belief or lack of belief[19]. The Criminal Justice and Immigration Act 2008 amended Part 3A further to include hatred with reference to sexual orientation.

Helpfully, Lord Carswell in *DPP v Collins*[20] described hate speech as any words "that reasonable citizens, not only members of the ethnic minorities referred to by the terms, would find… grossly offensive"[21].

Neither the Public Order Act 1986 nor the Crime and Disorder Act 1998 apply a multiplying effect for dissemination of hate speech to a wider audience, let alone online. The Act provides two distinct categories from which hate speech can be disseminated: public and private[22], both of which are equally applicable for a charge of hate speech. Inexplicably, there has been a strong neglect of the multiplying effect and higher potential impact of online hate speech, despite the most recent amendment being in 2008, a time of peak internet usage. This can be partly explained by the timing of the Act; the Internet was not used for mainstream applications during the 1980's. However, it is even difficult to argue by analogy through publications of offensive material or broadcasting as these mediums are used as mere examples of how hate speech may be expressed, rather than examples of greater 'damage'. Thus, it is reasonable to conclude that the Public Order Act 1986 does not recognise the possibility of greater impact through communicating with a wider audience.

An explanation for this is provided by the United Nations Committee on the Elimination of Racial Discrimination, which suggests "the United Kingdom government firmly believes that it strikes the right balance between maintaining the country's long standing traditions of freedom of speech and protecting its citizens from abuse and insult"[23]. Thus it seems that the confidence of the UK government in the statute's efficacy left no desire to radically reform the definition of the offence, refusing to amend what is not allegedly broken. However, this explanation can be further developed; perhaps the House of Commons initially intended the Public Order Act 1986 to restrict anti-social and violent behaviour such as rioting and assaults in large communities such as districts of London. In the Hansard Report for the passing of the Bill, the Secretary of State for the Home Department (then Mr Douglas Hurd) commented on the need to reduce "abusive and loutish behaviour" on the most vulnerable sections of a community – namely ethnic minorities and elderly citizens[24]. The House of Commons were in complete agreement that Part III of the Act went far enough to provide sufficient protection to ethnic minorities whilst still maintaining the fundamental freedom of speech, demonstration and liberty[25].

Despite the UK's lack of legal recognition for online hate speech, the Crown Prosecution Service recognises s. 127 of the

1 http://www.legislation.gov.uk/ukpga/1986/64/contents
2 ibid defined in Section 17 as" hatred against a group of persons by reason of the group's colour, race, nationality (including citizenship) or ethnic or national origins"
3 ibid Section 18
4 It is also worth noting that The Criminal Justice and Immigration Act 2008 amended Part 3A of the Public Order Act 1986. The amended section adds the offence of inciting hatred on the ground of sexual orientation in England and Wales
5 http://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=#n1359128122487_pointer
6 http://www.legislation.gov.uk/ukpga/1998/42/contents
7 To protect Freedom of Expression this section states that *"Nothing in this Part shall be read or given effect in a way which prohibits or restricts discussion, criticism or expressions of antipathy, dislike, ridicule, insult or abuse of particular religions or the beliefs or practices of their adherents, or of any other belief system or the beliefs or practices of its adherents, or proselytising or urging adherents of a different religion or belief system to cease practising their religion or belief system."*
8 http://www.legislation.gov.uk/ukpga/2006/1/schedule
9 This Article states that "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law"
10 Found at http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm
11 Hate Speech Rules Under International Law, Toby Mendel Executive Director Centre For Law And Democracy, February 2010
12 Similar to the "wholly internal situation" doctrine of the single market shown in case C-448/98 Guimont [2000]. i.e. if there were a domestic principle of equal treatment whereby such discriminatory treatment would be unlawful. This relies on national principles in a European context and may be the more prudent manner in which to tackle this issue rather that a generic definition that satisfies no one.
13 F. Kirgis "Enforcing International Law" The American Society Of International Law (ASIL) Insights January 1996
14 Rosalyn Higgins Problems and Process: International Law and How We Use It (1994) 205-6
15 Crime and Disorder Act 1998, s. 28(1)(a), Part 2
16 Op Cit No 1
17 Op Cit no 1
18 Op Cit No 1 Section 17
19 Racial and Religious Hatred Act 2006 s. 1
20 [2006] UKHL 40
21 Ibid; at para 8-9 per Lord Carswell
22 Public Order Act 1986, s. 18(2), Part 3
23 United Nations Committee on the Elimination of Racial Discrimination (1996), *'Fourteenth periodic reports of parties due in 1996: United Kingdom of Great Britain and Northern Ireland'*
24 Hansard HC Deb 13 January 1986 vol 89 col 793
25 Ibid, cc 820-852

Communications Act 2003 as an alternative avenue for charges of hate crime[26]. This section criminalises grossly offensive messages that the public of a multi-racial society would find offensive, thus it has a much broader scope for application than the legislation cited above and includes offensive messages[27], hacking, cyber bullying and stalking[28].

This brings up an interesting idea about the notions of "intimidation" and "provocation"; how 'incitement to hatred', intimidation and 'provocation' can be considered different from hate speech. Due to the lack of a dedicated hate crime offence, intimidation shares a wider definition as 'harassment, alarm and distress'[29] in the United Kingdom under the Public Order Act 1986. A specific definition of these synonyms is also missing from the Act and no explanatory notes have been published, but case law helps provide a practical definition of what could constitute harassment. *R v. Joseph Smith*[30] demonstrates that the precise definitions are vague and run the real risk of verging into common assault. Incitement to hatred is defined as 'stirring racial hatred' under the Public Order Act 1986 but no specific definition is provided.

Judging by the different wording of the two Acts, incitement to hatred is more focused around the disseminating of information that tries to spread an active feeling of hatred in public, or in a private audience. Conversely, provocation and intimidation is much more personal between the provoker and the victim, leading to a fear of immediate unlawful violence based on the victim's membership of a racial or religious group.

This brings us to the concept of hate speech and religion. This can be a tricky concept to deal with because of the fact that there can be a difference between blasphemy (defamation of religious beliefs) and hate speech based on religion. We must consider how national legislation distinguishes between the two.

Blasphemy and hate speech under the English Legal System have two very distinct histories and are different in substance. Currently, there is no longer an offence for blasphemy under English law. Despite this, the historical context is very important as it signposts important shifts in ideology that are clearly reflected in the newer public offences under the Public Order Act 1986. Under common law, blasphemy, while abolished by the Criminal Justice and Immigration Act 2008[31], began in the 16th century in *Taylor's Case*. It was described as an incredibly heinous crime and purportedly against God, English law and society[32]. Since the 19th century, convictions were very rare, with the last recorded conviction being in 1924[33], but blasphemy was constantly asserted as still relevant to the common law as late as 1977 in the case of *R v Lemon*, favourably described as a "safeguard [to] the tranquility of the kingdom"[34].

Interestingly, Lord Scarman noted that blasphemy acts as an important measure to respect religious beliefs that many hold dear and protection from "scurrilous ridicule"[35], which greatly expanded the original purpose of blasphemy (a crime against God) and began to encroach on the newer statutory public offences of 'stirring up religious hatred' under the Racial and Religious Hatred Act 2006 by focusing on the sensitivity of practicing Christians.

The similarity is even more startling when considered with the recorded Parliamentary speech of Lord Macaulay in 1833: "It is monstrous to see any Judge try a man for blasphemy under the present law. Every man ought to be at liberty to discuss the evidences of religion… But, no man ought to be at liberty to force, upon unwilling ears and eyes, sounds and sights which must cause irritation"[36]. Comparatively, section 29A of the Public Order Act 1986 (amended by Racial and Religious Hatred Act 2006) details that religious hatred is made against "a group of persons defined by reference to religious belief or lack of religious belief"[37], thus the level of convergence is notable with both offences pointing towards contempt made at a particular group of individuals.

On the other hand, statutory public offences seem to extend beyond mere insult and discussion on the non-existence of God into genuine incitement of hatred and discrimination against a group of individuals. Furthermore, the Public Offences Act 1986 requires a likeliness to cause "harassment, alarm or distress"[38] rather than something merely insulting or scurrilous in nature.

Furthermore, the old law on blasphemy focused specifically on the predominant religion of the land: protestant Christianity. Referring back to the elements of the defense, this was due to its integral ties to the contemporary British society and stems from a reluctance to curtail free speech and public criticism. Judge Alderson of Yorkshire framed the requirement well by stating "a person may, without being liable to prosecution for it, attack Judaism or Mahometanism; or even any sect of the Christian religion, save the established religion of the country"[39]. Contrarily, the new Public Order Act 1986 provides protection for all groups in relation to a religious belief, including lack of belief.

Regardless, both statutory and common-law forms of blasphemy were abolished on July 2008 with the enactment of s. 79 Criminal Justice and Immigration Act 2008. Led by Dr. Evan Harris MP, the repeal of all forms of blasphemy was made with criticism by numerous members of the House of Lords and the Archbishop of York. Whilst the Lords were in favour of protecting private individuals and the numerous faith groups contained in Britain from harassment, they were reluctant to remove the public protection afforded to the Christian faith and wanted to recognise its contribution to the fabric of British society[40].

To conclude, national legislation and common law did not make any attempt to distinguish between hate speech and blasphemy, the two offences only slightly intersect in time, over approximately two years. Despite this, the influence of previous legislative efforts and (predominantly) common law is clear to see: the two offences blur together during the end period of blasphemy and the statutory commencement of the public offence under the Public Order Act 1986.

Finally, we can look at the potential for harmonisation of national legislation. Of course, in these circumstances, we must consider the principle of proportionality. The current protection from hate speech is highly uneven in its scope and conflicted in definition: some legal systems suggest that the element of 'hate' on a group is sufficient to trigger a criminal offence, whilst others argue that there should be an amalgamation of hatred, intimidation and or harassment in order to be categorised as 'hate speech'. For instance, the National Council for Crime Prevention in Sweden defines hate speech as speech which "[threatens] or expresses contempt for a national, ethnic or other such group of persons"[41], removing the intention element and focusing on the words used; that is, any expression that makes a person of an identified group feel inferior. Conversely, Russia requires an evidential element of hatred to be present[42], which is much more difficult to prove as it is based on the subjective discretion of law enforcement present. Furthermore, with the continuous issues of xenophobia, anti-Semitism and sexual orientation in Russia, hate speech may not be covered at all in practice. Equally, the historical difference between European nations means that certain groups may have greater statutory protection over others: such as the history of anti-Semitic policies in Germany, Austria and Italy.

From a European perspective, this is unacceptable as there should not be different levels of protection depending on geographic location or a selected 'group'. Sufficient respect must be given to historical context of the differing nations in Europe for a compromise to be met. Instead, legislation of Member States should be harmonised by focusing on individuals rather than groups[43] of a certain characteristic.

Efforts have been made already to unite legislative efforts; the Office for Democratic Institutions and Human Rights has published legislative guidelines in order to try to bring these conflicted approaches together, focusing on any "malice or ill will towards individuals on grounds of race, religion, sexual orientation etc"[44]. In addition, the Council of Europe has issued a Convention on Cybercrime and, additionally, what should constitute an offence for online hate speech. The Articles in the Protocol require the criminalisation of racial and xenophobic motivated threats[45], insults[46], disseminating racist or xenophobic material and denial of genocides that occurred over human history[47] on a computer system. This Convention brings uniformity in definition and objectives between nation states without impinging on *how* these objectives will be incorporated[48]. Although, paragraph 2b of Articles 5 (insult) and 6 (Holocaust denial) allow a signing party to derogate away from criminal liability, critically depriving this Convention of its uniform intentions. In addition, the United Kingdom and Ireland have not signed this particular Convention[49], leaving harmonisation in jeopardy.

---

26 Crown Prosecution Service, Communications Offences, *'Improper Use of Postal and Electronic Communications'* Available from: http://www.cps.gov.uk/legal/a_to_c/communications_offences/ [Last accessed: 26th September 2013]
27 [2006] UKHL 40
28 Crown Prosecution Service, Op cit.
29 Public Order Act 1986, s. 4A(1), Part 3, Queen Elizabeth II
30 [2013] EWCA Crim 11
31 S. 79 Criminal Justice and Immigration Act 2008
32 *R v Lilburne* (1649) 4 St. Tr. 1269, at para 1307 per Lord Keble
33 Lauterpacht E. (1992) C. J. Greenwood, *International Law Reports*, Cambridge University Press, pp. 426-8
34 [1979] AC 617 per Lord Scarman at para 658
35 Ibid
36 Kenny C. (1922) *'The Evolution of Blasphemy'*, Cambridge Law Journal vol. 2 p. 135
37 s. 29A Public Order Act 1986
38 Public Order Act 1986, s. 5(1)
39 Kenny (1922) op cit. p. 141 per Judge Alderson
40 HL Deb 5th March 2008 vol. 699
41 The Swedish Penal Code, Chapter 16, s. 8 (Law 1988:835)
42 Garland J. and Chakraborti N. (2012) European Journal of Criminology, *'Divided by a common concept? Assessing the implications of different conceptions of hate crime in the European Union'*, vol. 9(1) 38-51, SAGE Publications, p. 42
43 bid; p. 40
44 Akdeniz Y. (2001) Electronic Business Law Reports, 1(3) *'Case Analysis of League Against Racism and Antisemitism (LICRA), French Union of Jewish Students, v Yahoo! Inc. (USA), Yahoo France, Tribunal de Grande Instance de Paris (The County Court of Paris), Interim Court Order, 20 November 2000.'*, p. 110-120
45 Council of Europe, Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems CETS No. 189, Article 4, 28th January 2003, Available at: http://www.refworld.org/docid/47fdfb20f.html [Last accessed: 12th October 2013]
46 Ibid; Article 5
47 Ibid; Article 6
48 Ibid; para 2

Even with these efforts to harmonise the national legislations of Europe, the very nature of the Internet means that any attempts are futile without the consent of the United States government. The majority of the Internet is hosted and based in the United States, thus it seems imperative to ensure that a shared legislative framework with Europe governs this large section of the Internet.

Unfortunately, case precedent shows that the United States is not willing to compromise the constitutionally guaranteed right to free speech. For example, in the case of *Yahoo! Inc v League Against Racism and Anti-Semitism (LICRA)*, a French anti-hate student union attempted to prevent Yahoo! from hosting an auction for the sale of Nazi memorabilia. The French High Court held that Yahoo! should impose a mechanism that filtered out French IP addresses and a declaration of nationality within three months or it would face a fine of 100,000 francs every day afterwards[50]; such measures would have an estimated 90% success rate. Subsequently, however, Yahoo! sought a hearing from the United States District Court of California to rule the French verdict invalid on the grounds of violation of the First Amendment Right to Free Speech. This is an example of the conflicts and continuous issues involved in attempting to harmonise legislation, the United States did not experience the same level of anti-Semitism, racism and devastation perpetrated by the fascist regimes in Europe during the early to middle 20th century.

Wolf illustrates the difficulties with controlling content on the Internet by likening it to "chasing cockroaches"[51]; content can reappear within days elsewhere outside of the ambit of the harmonised framework, like the US, and mirrors of articles may never disappear if there is no public link from the original website. Therefore, it is highly impractical to attempt to chase individual perpetrators of this content. Instead of focusing on a top-down imposition of Internet regulation, horizontal efforts should be made by Internet Service Providers and charities.

In regards to the principle of proportionality, the force of legislation can have a disproportionately negative restriction on freedom of expression on the Internet. If a domestic government legislated to place responsibility on ISPs to filter-out online hate speech and content, the ISPs would inevitably take a more precautionary and strict approach to avoid any inclusion of content that may be deemed to be offensive[52]; radically restricting freedoms to express oneself and the Internet itself for that country.

Perhaps then, due to the issues with proportionality, differing historical contexts, and a need to include the United States in any effort to unify an approach to online hate speech, there needs to be a 'softer' approach that does not bind individual states to legislation, but pressures Internet Service Providers specifically to create an agreeable Code of Conduct. Already movements have been made in the United Kingdom with the Internet Watch Foundation (IWF) that attempts to bring down websites containing child abuse and criminally obscene sexual content. In fact, Italy, Austria, Belgium, France, Germany, Ireland, Norway and the United Kingdom all have industry bodies with mutually agreed codes completely outside of the jurisdiction of legislation[53] so there is no lack of willingness on the parts of European governments, just a lack of co-ordination.

Alexander Adamou is a third-year student at the University of Sussex in Brighton. He hopes to pursue a career in corporate law, with the ambition of joining the bar. Hate crime and media law are new territory for Alexander, and so he took on this article as an interesting and enjoyable challenge. In writing this article, Alex feels that he has learned much about the importance of media law in everyday life and he would like to take this opportunity to thank Nadia Tjahja for her helpful comments and guidance that she provided during the process of writing this article.

Jake Wright is the current President of ELSA Sussex, and through working with ELSA he has developed a picture of how he can use his degree in a constructive way to benefit our society. Through researching for this article, Jake's interest in hate speech as a legal specimen has been magnified, and he has already implemented his findings into his current degree studies. With a revival of Euro-scepticism and the looming threat of a returning 'island mentality' in the UK, Jake understands the importance of keeping the debates around these issues free of the muddying influences of racial slurs and incitements of violence.

[49] Council of Europe, Treaty Office, 'Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems CETS No. 189' Available at: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=28/08/2011&CL=ENG [Last accessed: 12th October 2013]

[50] Akdeniz Y. Op cit.

[51] Wolf C. (2009) Anti-Defamation League, 'Hate Speech on the Internet and the Law', Available at: http://adl.org/osce/osce_legal_ analysis.pdf [Last accessed: 4th October 2013]

[52] Leonardi D. Marsden C. Tambini D. (2008) 'Codifying Cyberspace: Communications self-regulation in the age of Internet convergence', Routledge: London and New York, p. 281

[53] Ibid; p. 132

The dark side of free speech: Combatting the increasing use of the Internet as a method of propagating extremism

by Sam Sutton | ELSA University of East Anglia

The Internet has become a fundamental part of our lifestyle over the past two decades, forming an essential part of our working and social lives. Children of this millennium will never know a time where it was not possible to instantly contact someone on the opposite side of the world at little to no cost, or find a wealth of information on any topic within seconds. The substantial increase in the mobile Internet access has further augmented this change in our society, and never before has human civilization been more interconnected on a global scale.

It is clear, however, that this massive expansion of the interconnectivity of the human race has had more sinister consequences. In the shadows of this age of universal access, dark forces have hijacked the growing freedom of information to spread messages of hate and fear to the four corners of the Earth, in an effort to spread their own twisted doctrines to new audiences. Below the seemingly benign surface of the internet lies the so-called 'Deep Web' – an un-indexed, unregulated Wild West of online content, forums, and marketplaces – where it is possible to obtain anything from hard drugs to bomb plans. Nestled among the architects of anarchy hidden in the Deep Web, one can encounter radicals and extremists, preying on the minds of unwary web users. Whilst the number of individuals being radicalised purely through the Internet has, up until recently, remained relatively low, it is clear that this number is now steadily increasing – to disturbing levels (Institute for Strategic Dialogue, 2011)[1].

What is perhaps the most worrying aspect of this situation is the fact that, for the first time in our history, radicalism can be effectively spread without requiring physical proximity between master and acolyte. In fact, in many cases, such physical contact never occurs, with preachers reaching across many thousands of miles to spread their message. One notable example is the website Azzam.com, which was accused by the US Government in 2002 as serving as a 'recruitment hub for Islamic extremists' – particularly in the USA and UK (North, 2002)[2].

Of course, not all radicalisation takes place in such a covert manner as this. Over the course of 2013, Facebook became embroiled in controversy surrounding the posting of videos showing the beheading of captives. Despite initially banning these videos in May 2013, Facebook later rescinded the ban, citing human rights protection as one of the reasons. In a statement released by the social networking giant in October 2013, Facebook said:

> *"Facebook has long been a place where people turn to share their experiences, particularly when they're connected to controversial events on the ground, such as human rights abuses, acts of terrorism and other violent events. People are sharing [these videos] on Facebook to condemn it. If the video were being celebrated, or the actions in it encouraged, our approach would be different." – Facebook, October 2013 (Kelion, 2013)*[3]

The problem lies in the incredibly fine and subjective distinction between free speech and hate speech. However principled Facebook's policy on extremist content, it is clear that such content does serve to spread the message of extremists and terror organisations, *effectively acting* as an indirect recruiting tool for such organisations. With children as young as 13 now permitted to have access to all of Facebook's content, the organisation cannot continue to maintain its neutral stance on such content. Whilst there must be a forum for such content to be revealed, it is less clear that Facebook, or indeed any mainstream social networking service, is the most appropriate venue for this. Without the introduction of full-scale content monitoring and filtering (which Facebook itself has already acknowledged as technically impossible, given the number of users), it is difficult to see how an effective and comprehensive block of this content would be possible.

Nevertheless, we can see that such filtering has been both encouraged and instituted at a national level across Europe. In the United Kingdom, the Cameron ministry has introduced an 'opt-in' filter on internet pornography, requiring domestic internet users to explicitly opt-in to access such content. Whilst the stated goal of the program – the protection of vulnerable minors – is laudable, this creates a worrying precedent. What there is to prevent future governments from widening the scope of the filter to include other 'obscene' content, or even 'immoral' content? Such nebulous descriptions, combined with imperfect automated filtering, could result in a wide range of perfectly legitimate content being blocked, such as sites for sex education or for abuse victims. We have already seen examples of this happening, with BT blocking sites relating to 'gay and lesbian lifestyles' in its initial roll out of the opt-in filter, before public outcry forced them to remove this search term from its filtering system. (Robbins, 2013)[4]

In the end, whilst electronic surveillance and interdiction can serve as a useful tool in monitoring the spread of extremism, radicalisation and extreme content on the internet, it cannot directly prevent the expansion or growth of such activity, other than through the crude and ineffective method of pursuing individuals through the criminal justice system. While this may be appropriate for the extreme cases, it does not provide an effective response to lower level hate speech or to individuals who have only just started down the path to radicalisation. These cases must be pursued as opportunities to prevent further radicalisation by challenging the views of the newly converted, and forcing them to justify the message with which they have been implanted. At the same time, it is important to avoid forcing these young radicals to 're-educate', lest we be accused of the same cultural imperialism that has caused countless conflicts over the course of human history. Above all, care must be taken as to where we draw the line between minority views and extremism. While hate speech should rightly be challenged and marginalised, we must remain vigilant to the chilling effects of restrictions on free speech, and the impact that such restrictions might have on the genuine open discourse that is one of the basic foundations of a mature democracy.

Sam Sutton is a 4th year LLB Law and French Law student from the University of East Anglia with a particular passion for Human Rights law and the interaction between European and national legal orders. Sam is hoping to pursue further studies in European Law, and is currently preparing his LLM applications for next year, with a view to joining one of the European institutions in the future.

1 Institute for Strategic Dialogue. (2011). *Radicalisation: The role of the internet.* London: Institute for Strategic Dialogue.
2 North, A. (2002, Febrary 2). *Pro-jihad website draws readers.* Retrieved from British Broadcasting Corporation: http://news.bbc.co.uk/1/hi/uk/1823045.stm
3 Kelion, L. (2013, October 21). *Facebook lets beheading clips return to social network.* Retrieved from British Broadcasting Corporation: http://www.bbc.co.uk/news/technology-24608499
4 Robbins, M. (2013, December 23). *Cameron's internet filter goes far beyond porn – and that was always the plan.* Retrieved from The New Statesman: http://www.newstatesman.com/politics/2013/12/camerons-internet-filter-goes-far-beyond-porn-and-was-always-plan

Awaiting strategy: An assessment of the EU's commitment to the promotion of global digital freedom

by Antonia Margaret Hantusch | ELSA York

elsa
The European Law Students' Association
YORK

"Everyone has the right to freedom of opinion and expression; 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." [1]

Introduction

The growth of the internet has been' revolutionary'[2], generating new opportunities and dangers for human rights, especially individuals' right to freedom of expression. Regardless of the transformative changes posed by the internet, the legal framework for international human rights remains pertinent[3], and nation states across the world must now consider how digital freedom can best be protected.

The recent crises in Egypt and Syria have given impetus to the debate regarding whether and how freedom of expression should be regulated online[4]. Globally, this debate has divided nation states, with Russia and China believing a heavy government presence in internet regulation is required, whilst the EU presses for the maintenance of a multiple stakeholder approach[5].

Through exploring the meaning of digital freedom, the credibility of EU initiatives to protect it, and why the EU's involvement is important, this article seeks to examine the EU's commitment to the promotion of global digital freedom. Ultimately, it is argued that, whilst the EU's efforts should be welcomed, if the institution is to promote digital freedom in its external policies effectively a clear and consistent strategy is required.

The meaning and significance of 'digital freedom'

Freedom of expression has long been regarded by the UN Human Rights Council as a fundamental human right[6]. In facilitating a range of economic, social, civil, and political rights, the internet has developed a new way to promote the exercise of freedom of expression[7]. The applicability of the right online has been confirmed by the UN, with the UN Special Rapporteur Frank La Rue concluding that Article 19 of the Universal Declaration of Human Rights was drafted with the foresight to include and accommodate such technological developments[8].

The relevance of freedom of expression on the internet as recently emphasised by Syrian government's repression of activists[9] has given rise to talk of 'digital freedom', which has been defined as:

"The right of individuals and organisations to express their opinions in the manner of their choosing using any type of device connected to the Internet. The Internet should be seen within a comprehensive framework for freedom of expression and within the context of individual freedom generally." [10]

One of the key issues regarding the promotion of this concept is how the internet should be governed. The internet is unique from other twentieth century technological developments since it did not immediately induce government regulatory control[11]. This was due to fears of the possible adverse effects on freedom of expression[12]. The inherent tension between government and private sector control of the internet has contributed to a lack of consensus concerning the right approach to take in devising an internet governance framework that promotes freedom of expression[13]. In this context, it is fitting to consider how the EU has and should play a role.

EU Initiatives

The EU has acknowledged that it should "take the lead in globally promoting and protecting digital freedoms[14]". To this end, the EU has adopted and started to develop a number of initiatives to help promote global digital freedom. These include its external 'No-Disconnect Strategy', imposition of export controls on surveillance technologies, and policy documents that have sought to define the EU's commitment to promoting digital freedom.

1 United Nations, Universal Declaration of Human Rights, Article 19
2 United Nations Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (A/HRC/17/27, 16 May 2011) 6 <http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf> accessed 10th January 2014
3 Ibid, 7
4 Marietje Schaake, 'Digital Freedoms and Human Rights in a Hyper-Connected World' (Internet & Gesellschaft Collaboratory)<http://en.collaboratory.de/w/Digital_Freedoms_and_Human_Rights_in_a_Hyper-Connected_World> accessed 10th January 2014
5 Brian Pellot, 'Index Policy Paper: Is the EU heading in the right direction on digital freedom?' (Index on Censorship, 20th June 2013) < http://www.indexoncensorship.org/2013/06/is-the-eu-heading-in-the-right-direction-on-digital-freedom/> accessed 10th January 2014
6 Ibid, (n 1)
7 Ibid (n 3)
8 Ibid
9 Ibid (n 4)
10 'Digital Freedom: Principles and Concepts' (Global Voices Advocacy, 25th March 2013)< http://advocacy.globalvoicesonline.org/2013/03/25/digital-freedom-principles-and-concepts/> accessed 10th January 2014
11 Wolfgang Kleinwachter, 'Internet Governance and governments: enhanced cooperation or enhanced confrontation?' [2007] Communications Law 111
12 Ibid,
13 Ibid, 113
14 Report A7-0374/2012 OF 15th November 2012 on a Digital Freedom Strategy in EU Foreign Policy [2012] < http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2012-0374+0+DOC+PDF+V0//EN&language=EN> accessed 10th January 2014

No-Disconnect Strategy

The EU's 'No Disconnect Strategy' aims to support activists and ensure network resilience during political crises[15] and represents the EU's first notable attempt to address digital rights in its external work[16]. As a relatively recent development, the policy has so far delivered few tangible outcomes[17], but it holds much potential as a key means by which the EU can ensure human rights on the internet are protected. In particular, the policy offers a way for the EU to track surveillance, censorship and other disruptions to internet access around the world, alongside offline political and legal developments[18].

Whilst the policy on the whole shows a marked commitment to the promotion of global digital freedom, its credibility is hampered by the small budget which it has been allocated, which has limited its scope, as well as its ability to act quickly in the event of a human rights crisis[19]. These constraints emphasise how its nature is as an ad hoc policy and it consequently fails to illustrate a deep level of commitment from the EU regarding the promotion of global digital freedom.

Export Controls

The use of export restrictions by the EU in its bid to secure digital freedom in its external work was most recently deployed against Syria. One such control imposed on Syria comprised:

> *"a prohibition on the sale, supply, transfer or export of equipment or software intended for use by the Syrian regime in monitoring or interception of internet and telephone communications. Provision of technical or installation assistance in support of such items will also be prohibited. There is an exemption for pre-existing contracts."* [20]

Whilst this action demonstrates a commitment to promoting global digital freedom, it again presents another ad hoc policy measure on the EU's part. It has been suggested that a more committed EU might develop a comprehensive and general export programme for digital arms so that the countries at fault cannot find some other way to instigate their grave human rights breaches[21]. Furthermore, the credibility of the EU's commitment was undermined by the two-month time delay between the EU Council's announcement of the measures and their implementation[22]. This represented an unsatisfactorily slow response to what were serious human rights breaches in Syria.

Defining the EU's commitment

The EU is currently in the process of developing guidelines on freedom of expression which could provide the basis for more active external policies and encourage a strategic approach to digital freedom[23]. These guidelines are anticipated to be used when the EU is carrying out human rights assessments and to aid the EU's human rights dialogues with non-member states[24].

In addition, the EU has already published a report on Digital Freedom Strategy for EU foreign policy, which recognised the need for a more comprehensive strategy that could be employed in all of the EU's external actions and treated digital freedoms as "indispensable prerequisites for enjoying universal human rights "[25].

Overall, these developments represent a fairly entrenched commitment by the EU to take global digital freedom issues seriously since they may set a yardstick for internal EU policies on freedom of expression[26]. Nevertheless, the guidelines' credibility is weakened by their nature as a mere Common Foreign and Security Policy document, which means their development features no civic consultation[27], and that there is an absence of internal focus. Altson and Weiler have highlighted that a lack of internal EU commitment and regard for promoting human rights policy would be dangerous as internal and external policies could contradict which would emphasise inconsistency and make it difficult for the EU to be taken seriously on the global stage[28]. This indicates that the EU internally is not taking the issue of global digital freedom seriously, which undermines its commitment to protecting freedom of expression on the internet.

Despite the internet's evolution through a multiple stakeholder process, the EU's commitment to the promotion of global digital freedom is important, as some degree of leadership on the issue is essential if this open process is to be protected[29]. The EU is well suited to take on this leadership role because it constitutes the world's largest trading block and is also a beacon for fundamental human values given its European Convention on Human Rights and other rights-related work[30]. Such characteristics indicate that the EU has the capacity to frame clear freedom of expression policies and priorities on international digital freedom issues[31].

Conclusion

This article has only touched the surface of the deep-rooted questions about the protection of the right to freedom of expression on the internet. The EU has started to take positive practical measures that show a commitment to the promotion of global digital freedom but the credibility of these policies is damaged by their ad hoc nature, limited scope, slow development, and low key prioritisation by EU leaders and member states. The EU's export controls on Syria have cast doubt on the effectiveness of policies already in operation.

A clear comprehensive strategy that matches the rapid, dynamic and expansive phenomenon of the internet is needed to ensure EU leaders and member states are seriously committed to tackling the issues raised by freedom of expression on the internet both domestically and globally. Only this approach would enable the EU to make a consistent and tangible contribution to the safeguarding of digital freedoms worldwide and to assess member states' own observation of online freedom of expression. The European Parliament's 2012 report represented a chance to found this strategic approach, especially through its recognition that internal engagement with freedom of expression needs to be addressed. However, a year on from this report, the EU still awaits a clear and overarching strategy that would enable it to promote global digital freedom in line with its duty to protect fundamental human rights.

Antonia Margaret Hantusch is a second-year law student at the University of York and the Secretary General for ELSA York.

15 Marietje Schaake, 'Digital Freedoms and Human Rights in a Hyper-Connected World' (Internet & Gesellschaft Collaboratory)<http://en.collaboratory.de/w/Digital_Freedoms_and_Human_Rights_in_a_Hyper-Connected_World> accessed 10th January 2014

16 Brian Pellot, 'Index Policy Paper: Is the EU heading in the right direction on digital freedom?' (Index on Censorship, 20th June 2013) < http://www.index-oncensorship.org/2013/06/is-the-eu-heading-in-the-right-direction-on-digital-freedom/> accessed 10th January 2014

17 Ibid

18 'Digital Agenda: Karol-Theordor zu Guttenberg invited by Kroes to promote internet freedom globally' (Europa, 12th November 2011) < http://europa.eu/rapid/press-release_IP-11-1525_en.htm?locale=en> accessed 10th January 2014

19 Ibid (n 16)

20 'Embargoes and Sanctions on Syria (Department for Business, Innovation & Skills) <https://www.gov.uk/sanctions-on-syria> accessed 10th January 2014

21 Ibid (n 15)

22 Ibid (n 21)

23 Ibid (n 16)

24 Ibid

25 Ibid (n 14) 14

26 Ibid (n 16)

27 Ibid

28 Phillip Alston & JHH Weiler, 'An 'Ever Closer Union' in Need of a Human Rights Policy' [1998] EJIL 658, 664

29 Ibid (n 15)

30 Ibid

31 Ibid (n 16)

ELSA The United Kingdom
February 2014

Editor
Nadia Tjahja

Copy editors
Ashley Robertson
Andrew Glenister

Front cover design
Hector Melendez

Contact
vpmarketing@elsa-uk.org.uk

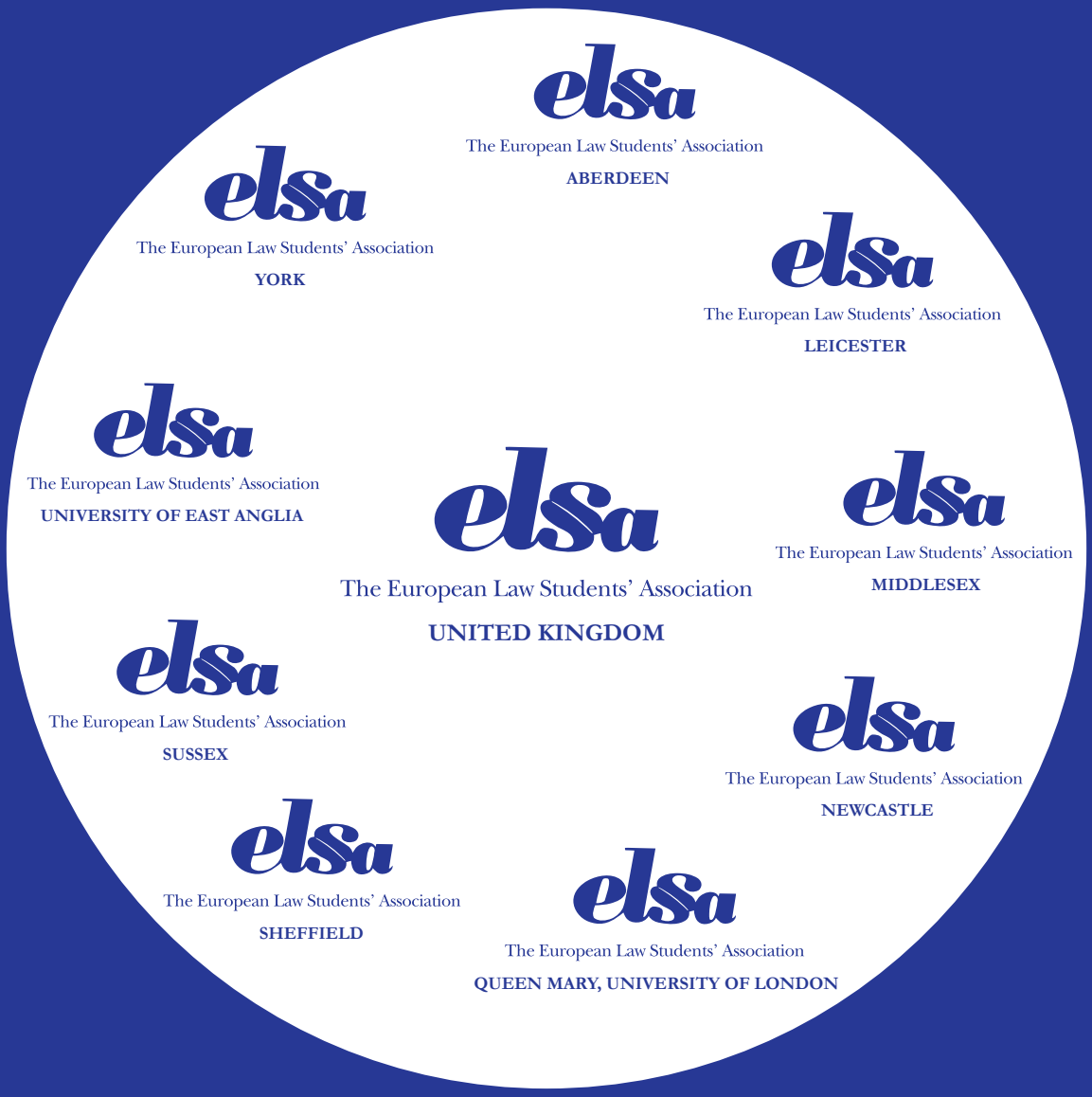
Website
uk.elsa.org

Twitter
@ELSA_UK

Facebook
www.facebook.com/ELSAUnitedKingdom

Find an ELSA Day Event

near you!



#weareELSAUK

http://bit.ly/ELSADayUK2014