NOTE

IN THE WORLD OF SOCIAL MEDIA, WHEN DOES “PRIVATE” MEAN PRIVATE? A CRITIQUE OF GERMANY’S PROPOSED AMENDMENTS TO ITS FEDERAL DATA PROTECTION ACT

Lauren Locklear*

“I must confess that I’ve never trusted the Web. I’ve always seen it as a coward’s tool. Where does it live? How do you hold it personally responsible? Can you put a distributed network of fiber-optic cable ‘on notice’? And is it male or female? In other words, can I challenge it to a fight?”

I. INTRODUCTION

You use it in the car and on the train. You use it in the library, while you’re on the phone, and during class. You use it every single day of the week, including weekends. You use it when you’re sad and when you’re happy. You use it for business and for pleasure. You use it in the rain, in the snow, and on the beach. You will probably use it before, during, and after your wedding. You definitely used it last night and again this morning. You used it five minutes before reading this. You love it and you hate it, but you definitely can’t live without it—you are addicted to social media.1

Don’t be ashamed, you are not alone. As of June 2010, there were 1.97 billion Internet users worldwide.3 Of these nearly two billion users, 600 million had Facebook accounts and 175 million used Twitter, and there were approximately 152 million blogs on the Internet.4 During December 2009, the average global user

---


4. Id.
spent over five and a half hours on websites (sites) like Facebook and Twitter, making social networks and blogs the most popular online category of entertainment when compared to instant messaging and games. During that same month, Japan had 46.6 million unique visitors to social media sites, the average Australian spent seven hours communicating through social media, and the number of unique visitors to Twitter in the United States increased by 579%.5

With users sharing so much personal information online, a new question arises: what reasonable expectation of privacy should individual users have regarding this information? More specifically, when should individuals expect that their information is protected from view by their potential employers during the job application process? When does “private” really mean private?

On August 25, 2010, Germany’s Federal Cabinet approved a draft law (Draft Law) amending its Federal Data Protection Act, or Bundesdatenschutzgesetz (BDSG).7 The Draft Law would expand the BDSG’s regulation of workplace data privacy in order to balance the value of information to employers with the value of personal data to employees.8 Most importantly for the purposes of this Note, it would prohibit employers from using social networking sites like Facebook when researching job candidates.9 The law surrounding the use of social media to perform background checks and to obtain information on employees10 is decidedly

---

5. *Led by Facebook, Twitter, Global Time Spent on Social Media Sites up 82% Year over Year*, NIELSEN BLOG (Jan. 22, 2010), http://blog.nielsen.com/nielsenwire/global/led-by-facebook-twitter-global-time-spent-on-social-media-sites-up-82-year-over-year/ [hereinafter *Led by Facebook, Twitter*].

6. *Id.* A unique visitor is an individual who visits a website more than once and is identified by their unique IP address. *Unique Visitor Definition*, WEBOPEDIA, http://www.webopedia.com/TERM/U/unique_visitor.html (last visited Sept. 30, 2012).


10. Under the Bundesdatenschutzgesetz (BDSG), an “employee” is any individual who has applied for a job, currently holds a job, or is in rehabilitation for an illness that prevents her from holding a job. See BDSG, supra note 7, at 7.
unsettled both in the United States and abroad. Germany is one of the first countries to enact specific legislation aimed at regulating how employers may use professional and social networking sites when hiring and monitoring both potential and current employees.

As with the majority of new data privacy legislation, the Draft Law suffers from two major problems. First, the rationale behind the law is to protect individuals’ online data privacy by regulating what online information employers are permitted to view. If Germany’s goal is to protect its citizens, it should be encouraging discretion regarding the information its citizens put online about themselves. This is the most effective form of privacy protection and puts the power in the individual’s hands to protect themselves rather than merely trying to tie the hands of the employer.

Second, the Draft Law is too nuanced because it relies on too many balancing tests and vague terms. The Draft law will be unsuccessful if its practical purposes are to decrease litigation and provide courts with guidance, for cases involving the use of social networking for recruiting purposes. Ultimately, countries should encourage individuals to be very cautious about what information they put online through social networking sites. Once an individual puts information online in this matter, regardless of the privacy settings on the site, the information is no longer private—it is public.

This Note will argue that the most effective form of data privacy protection is to encourage individual discretion when posting information online. If, however, a state wants to enact legislation protecting potential or current employees from the use of their


13. See discussion infra Part II.C.
The law needs to be very specific with clearly defined terms. Part II of this Note will provide a background on social media and how employers are using social media to screen and investigate both current and potential employees. Part II will also provide an overview of the data privacy laws that govern the use of social media by employers in the United States, European Union, and Germany and it will analyze Germany’s Draft Law. Part III will identify potential problems with both the purpose behind and substantive provisions of the Draft Law, and then offer solutions to these identified problems. Finally, Part III will briefly evaluate the Draft Law’s potential implications for the development of international data privacy law.

II. BACKGROUND

Google CEO Eric Schmidt predicts that “people will one day change their name and reinvent themselves in order to escape their digital past.” Today, what an individual says online through message boards, blogs, or social networking sites is equivalent to what employees used to talk about in the hallways or in the cafeteria during lunch. Therefore, some commentators urge that governments pass legislation in order to protect their citizens from losing their right to privacy in today’s digital world. The following subsections will address the rise in prevalence of social networking sites and how the United States, European Union, and Germany are currently addressing the problems created by this surge in social media usage. It will conclude with a summary of the structure of Germany’s Draft Law.

A. Social Media Background: Twitter, Facebook, and MySpace, Oh My.

Social media is a broad term encompassing the different technologies individuals use to create online communities such as forums, blogs, photo and video sharing networks, podcasts, and

---

14. This Note, however, will primarily address how employers are using information from social media sites to screen potential employees.


16. See NETWORK INTERFERENCE, supra note 11, at 1.

17. See 2-15 INTERNATIONAL COMPUTER LAW § 15.01 (LexisNexis 2010) (“[T]he commercial appropriation of personal data implies and requires that the law grant individuals a property right in their personal data.”).
Social networks enable individuals to use electronic communication to share personal information with other users in a certain online community. Social networking sites are “web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.” Facebook, MySpace, and Twitter are examples of social networking sites that capitalize on social media as a communication tool, allowing individuals around the world to interact with one another.

Social networking sites exploded in popularity because they allow individual users to make their social network visible to others. The default privacy setting on these sites varies from requiring the user to have a paid account to see other members, to simply asking the user if she would like a public or “Friends only” profile. Once an individual is a member of a social networking site, she may publicly post pictures and thoughts on her individual profile page, send “friend requests” to other members so that third parties may see there is a “friendship” between the individual and the other member, and comment on other users’ pictures or thoughts. Social networking sites developed in the United States are open to individuals around the world, but many different...
countries have their own uniquely popular site. The global reach of social networks, as well as the easy access that employers have to the Internet, has created a new unique way for employers to perform background checks on potential employees.

It is not just individuals who are becoming addicted to social media. Employers are using social media to recruit new employees, advertise the company’s services, stay abreast of current market trends, and investigate the backgrounds of potential job candidates. Many companies have social media policies that set guidelines for their employees’ use of social media. Examples of social media policies include the National Football League’s Social Media Policy, the General Service Administration’s Social Media Guidelines, the Australian Public Service Commission’s Interim Protocols for Online Media Participation, the British Broadcasting Corporation’s Social Networking Policy, and TNT’s Social Media Guidelines in Italy.

26. See Boyd & Ellison, supra note 20. Friendster became popular in the Pacific Islands, Orkut was the most popular social networking site in Brazil, and LunarStorm was the majority choice in Sweden. Id.

27. See THE NIELSEN CO., GLOBAL FACES AND NETWORKED PLACES: A NIELSEN REPORT ON SOCIAL NETWORKING’S NEW GLOBAL FOOTPRINT 2 (2009), available at http://blog.nielsen.com/nielsenwire/wp-content/uploads/2009/05/nielsen_globalfaces_mar09.pdf. Two-thirds of the Internet population in the United States, Brazil, United Kingdom, France, Germany, Italy, Spain, Switzerland, and Australia visit a social network or blogging site. Id.


33. GSA POLICY, supra note 18.


Using social media to perform background screening of potential job candidates has become so common that companies now exist for the sole purpose of collecting individuals’ online personal information online and this information to anyone who will pay. In the United States, 70% of recruiters and human resources professionals have rejected candidates based on online information. In the United Kingdom, the percentage is slightly lower at 41%, and in Germany and France the numbers are 16% and 14%, respectively. In Germany, human resources professionals and recruiters are three times more likely to look for online reputational information than corporate policies dictate.

While it is widely acknowledged that employers and recruiters look at social networking sites when making job decisions, the legality of doing so is unclear. The next section will examine existing data privacy laws in the United States, European Union, and Germany to help clarify the potential impact of Germany’s Draft Law.

B. A Survey of Existing Data Privacy Protections for Employees

Article 12 of the United Nation’s Universal Declaration of Human Rights (UDHR), which provides the baseline for privacy protection for all members, states that “[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.” The Universal Declaration of Human Rights is a contract between governments and their citizens.


39. Id.

40. Id.

41. See Jean M. Roche, Note, Why Can’t We Be Friends?: Why California Needs a Lifestyle Discrimination Statute to Protect Employees from Employment Actions Based on Their Off-Duty Behavior, 7 HASTINGS BUS. L.J. 187, 190 (2011).


43. See Network Interference, supra note 11, at 42.
Privacy will affect the potential impact and success of Germany’s Draft Law.

Privacy law in the United States has mostly grown through state-created common law and commercial identity and trade secret protection.\(^4\) This body of law is based on the theory that individuals have a right to be protected from “highly offensive invasions into a person’s hidden world.”\(^4\) Specific federal laws geared towards preventing discrimination and protecting specific categories of people protect the data of current employees and applicants for employment.\(^4\) Examples include the Children’s Online Privacy Protection Act of 1998,\(^4\) the National Labor Relations Act,\(^4\) Title VII of the Civil Rights Act,\(^4\) the Americans with Disabilities Act,\(^4\) the Age Discrimination in Employment Act,\(^4\) and the Genetic Information Nondiscrimination Act.\(^4\) In order for an applicant or current employee to have a right to privacy as applied to “off-duty” activities, the specific state the employee works in must provide for this right in its constitution or through statute.\(^4\) The recognition of people’s property right in their own personal data presents another method of protection.\(^4\) Thus, some commentators believe that there exists sufficient legal protection for individuals to address privacy issues and no further government intervention is required.\(^5\)

---

\(^4\) See Robert Sprague, \textit{Rethinking Information Privacy in an Age of Online Transparency}, 25 \textit{Hofstra Lab. \\ \\ \\ \\ \\ & Emp. L.J.} 395, 402 (2008); see also \textit{2-15 International Computer Law § 15.01, supra note 17} (noting that individuals have few instruments with which to combat the invasion of their privacy rights).

\(^4\) Sprague, \textit{supra} note 44, at 404–05.

\(^4\) \textit{Id. at 399–401.}


\(^4\) Genetic Information Nondiscrimination Act, 42 U.S.C. § 2000ff-1 (2008). An employer may be found liable under these statutes if it finds employee information online pertaining to any protected class under the aforementioned statutes and uses this information to make an adverse employment decision. \textit{See} Roche, \textit{supra} note 41, at 192–93.


\(^5\) \textit{See} \textit{2-15 International Computer Law § 15.01, supra note 17}.

Like the United States, many European countries have relied on a patchwork scheme of privacy laws, discrimination laws, and labor and employment laws to protect the data privacy of individuals in the employment setting. While it is understood that private employers have the right to monitor employees’ actions while on-duty, the law is unclear as to whether employers can use social networking sites when evaluating potential employees or when researching the off-duty activities of current employees.

In contrast to the United States’ sectoral approach to data privacy, European countries that are members of the European Union must also ensure that their domestic laws meet the data privacy standards implemented by Directive 95/46/EC and Directive 2002/58/EC. These Directives do not bind individual citizens, rather they set the minimum standards countries must follow when enacting their own data privacy laws. The goal of these Directives is to balance a high level of individual privacy protection with free movement of personal data throughout the European Union. If a member fails to adequately implement these Directives through its own laws, it may face charges before the European Court of Justice. To ensure compliance with Directive 95/46/EC

(quoted the vice president of the European Commission as saying that the United States does not wish to discuss data protection improvements with the European Union).

56. See Gail Lasprogata et al., Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy Through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada, 2004 Stan. Tech. L. Rev. 4, ¶ 14 (2004) (“Most of the Member States of the EU have a civil law legal system where the role of case law is less relevant and the need for more precise legislation is mandated.”).

57. Roche, supra note 41, at 190 (“The law is still somewhat ambiguous on the subject of what material is private when posted online.”).


61. See Directive 95/46/EC, supra note 59, arts. I, V. Directive 95/46/EC binds E.U. member states and gives them discretion to specify the conditions for the processing of personal data for their own citizens. See id.


63. See Network Interference, supra note 11, at 42–43 (explaining that the United Kingdom is currently under fire for failing to guarantee the confidentiality of certain elec-
EC, the European Commission set up the “Working Party on the Protection of Individuals with Regard to the Processing of Personal Data,” also known as the “Article 29 Working Party” (Working Party). 64 This is an independent body that advises the European Union on data protection and privacy, 65 as well as the status of the data privacy codes of conduct drawn up at a community level. 66

The Working Party issued an opinion on online social networking that defined social networking services as “data controllers,” and subscribers to these services as “data subjects.” 67 This opinion stated that social networking services located outside of the European Union are still required to respect E.U. regulations on data processing. 68 The opinion declared that if a subscriber’s information is only available to a self-selected group of individuals and the information is shared beyond that network, “the same legal regime will then apply as when any person uses other technology platforms to publish personal data on the web.” 69

When a member of the European Union wants to transfer data between a non-member state and a member state, it must comply with the standards under Directive 95/46/EC article 25, “Transfer of Personal Data to Third Countries.” 70 For example, because the European Union feels that the United States has inadequate data privacy protections, United States employers cannot transfer employee data from the European Union to the United States unless the employer has taken greater security precautions than

---

64. Directive 95/46/EC, supra note 59, art. 29.


66. Directive 95/46/EC, supra note 59, art. 30(1).


68. Id. at 6.

69. Id.

70. Directive 95/46/EC, supra note 59, art. 25 (discussing that before transfer, “the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country” must be evaluated).
those required under U.S. law. In order to establish a more predictable framework for data transfers between the European Union and the United States, the United States Department of Commerce issued “Safe Harbor Privacy Principles.”

If a company decides to comply with these principles and publicly announces this intent, any member of the European Union wishing to transfer data to this particular company may assume the company has adequate data privacy protection in compliance with Directive 95/46/EC.

Germany is a member of the European Union, and thus is required to comply with the Directives listed above. Germany has an incredibly strict data protection scheme, largely due to the use of personal information during World War II to persecute large classes of individuals. During the war, the Nazis used census records and other personal information about the German population to maintain control. The result was a strong right to privacy in the German Constitution and the passage of the first data privacy legislation in the German state of Hesse.

The data privacy of employees in Germany is protected under the BDSG, which covers the processing of personal data for commercial or administrative purposes. The purpose of the BDSG is to protect the right to privacy of all German citizens against the mishandling of their personal information. It applies to both public and private bodies of the German Federation unless a pri-
private entity is processing or using data for personal or domestic activities.  

Under the BDSG, “private bodies” are natural or legal persons, companies, and other private-law associations. The term “personal data” includes “any information concerning the personal or material circumstances of an identified or identifiable natural person (‘data subject’).” When the BDSG refers to “employees,” it includes all of the following: (1) individuals who are currently employed, (2) individuals who are participating in rehabilitation measures, (3) home-based workers, (4) civil servants, (5) those who have applied for employment, and (6) those who were previously employed.

Section 32 of the BDSG governs “data collection, processing, and use for employment-related purposes.” The applicable provisions state the following:

(1) An employee’s personal data may be collected, processed or used for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract. [Sentence omitted relating to data collection for crime prevention purposes].

(2) Subsection 1 shall also apply when personal data are collected, processed or used without the help of automated processing systems, or are processed and used in or from a non-automated filing system or collected in such a filing system for processing or use.

In addition to its provisions relating to data collection in the employment context, the BDSG also explains that prior to using a subject’s data, an entity must notify the subject of the specifics of the data collected. For example, the first time an entity collects an individual’s information, the controller must notify the individual of the collection, including who the collector is and how the

82. Id. at 8 (“Personal data shall be collected from the data subject. They may be collected without the data subject’s participation only if (1) allowed or required by law, or (2) (a) the data must be collected from other persons or bodies due to the nature of the administrative task to be performed or the commercial purpose, or (b) collecting the data from the data subject would require disproportionate effort and there are no indications that overriding legitimate interests of the data subject would be adversely affected.”).

83. Id. at 6. This Note will only address laws applicable for private entities.

84. Id.

85. Id. at 7.

86. Id. at 37. “‘Collection’ shall mean the acquisition of data on the data subject. . . . ‘Processing’ shall mean the recording, alteration, transfer, blocking and erasure of personal data. . . . ‘Use’ shall mean any utilization of personal data other than processing.” Id. at 6.

87. Id. at 37.

88. See id.
information is being collected or used. One important exception to this notification requirement states that a subject does not need to be notified if: (1) the recording or transfer of the data is expressly allowed under existing law, or (2) the data was recorded for the entity’s own purposes and was either acquired from a generally accessible source and notification would require a disproportionate effort due to the large number of subjects.

The BDSG contains various enforcement and punishment provisions in order to ensure compliance. If an individual is harmed through the unlawful collection, processing, or use of her personal data, the controller or its supporting organization must compensate the individual for damage suffered unless the controller exercised due care.

Although the BDSG does not specify what types of “damage” it protects against, it does specify that both financial and non-financial harm may be compensated. It is a criminal offense for an individual to willfully commit an administrative offense in exchange for some form of payment, for the purpose of enriching herself or another person, or for the purpose of harming another person. This individual may be imprisoned for up to two years or may be fined. Government authorities may only prosecute a criminal offense if the individual whose rights were violated, the controller, or the Federal Commissioner for Data Protection files a complaint.

As illustrated above, data privacy protections are so individualized that they vary from continent to continent, as well as country to country within the European Union. Within this complex

89. Id. at 8, 37. The BDSG does not specify who would notify the subject; however, the text of the law seems to imply that the “controller” of the data would be the notifying party. See id. at 7 (“Controller’ shall mean any person or body which collects, processes or uses personal data on his, her or its own behalf, or which commissions others to do the same.”).
90. Id. at 37.
91. See generally id.
92. Id. at 16. However, the BDSG also states the following:
   If a public body harms a data subject through collection, processing or use of his or her personal data which is unlawful or improper under this Act or other data protection provisions, the body’s supporting organization shall be obligated to compensate the data subject for damage suffered irrespective of any fault.
93. Id.
94. Id. at 49.
95. Id.
96. Id.
framework, Germany recently proposed amendments to the BDSG that would regulate the use of social media by employers when researching potential employees for recruiting purposes. This Draft Law is still currently being debated by Parliament after receiving Chancellor Angela Merkel’s approval.

C. Germany’s Draft Law and Its Proposed Data Privacy Amendments

On August 25, 2010, Germany’s legislature proposed a draft law on data privacy protection that would amend the BDSG, entitled GE Beschäftigtendatenschutz. The goal of the Draft Law is to protect employees by creating a comprehensive set of regulations regarding data privacy. It would balance the value of information to employers with the value of personal data to employees with the ultimate goal of creating a trusting work environment. The Draft Law would accomplish its goal by allowing only data that is necessary for employment-related purposes to be collected, processed, and used. The law would protect employees against spying by the employer and will provide employers with reliable compliance requirements.

The Draft Law would insert a new chapter into the BDSG, entitled “Data Collection, Processing, and Use for Employment-Related Purposes.” Section 32 of the BDSG would be divided into different subsections that each address different issues relating to the use of personal data in the employment context, including: (1) how employers can use social networking sites to research job applicants (Employer Internet Searches); (2) when employers may require medical exams from employees; and (3) when an employer may monitor an employee’s telephone, Internet, and e-mail.

99. Id.
100. Draft Law, supra note 7 at 1.
101. Id.
102. Neither “employment-related” nor “job-related” are explicitly defined in the Draft Law, a problem that this Note suggest needs to be addressed before the law is permanently adopted. See infra Part III.B.

103. See Draft Law, supra note 7, at 1. This is in accordance with rulings by the German Federal Labor Court. Id.
104. See id.
105. Id. at 5, art. 1.
The Draft Law would address more practical matters by adding the following definitions: (1) employment data is the personal data of employees; and (2) employers are public and private bodies that employ, employed, or intend to employ "employees" as defined in paragraph 11 of the BDSG.\footnote{Draft Law, \textit{supra} note 7, art. 2.} It also expands Part III of the BDSG, the general provision governing data processing by private bodies and commercial enterprises,\footnote{BDSG, \textit{supra} note 7, at 2.} so that it applies to employment data collected, processed, or used by the employer for previous, existing, or future employment-related purposes.\footnote{Draft Law, \textit{supra} note 7, at 5, art. 1.}

In addition to breaking up section 32 of BDSG into twelve different subsections, the Draft Law also makes more substantive changes.\footnote{See generally id.} An employer may collect the name, address, phone number, and e-mail address of any employment applicant without a specific employment-related purpose.\footnote{Id.} Second, employers may also collect other personal data from applicants as long as the data is required to determine the suitability of the individual for the job she is applying for.\footnote{See id.} An employer may also collect data regarding the individual’s technical and personal skills, knowledge and experience, as well as past training and any previous employment history, as long as the information is job-related.\footnote{See id.} An employer may only collect data on the religious beliefs, political views, and/or trade union membership of an employee as long as it is related to a justified occupational requirement.\footnote{See id.}

Under the Draft Law, the employer may collect generally accessible employee data without the participation of employees unless the legitimate interest of the employee in excluding the collection outweighs the legitimate interest of the employer.\footnote{See id.} With regards to Internet data, the law states that an employee’s interest in data that could be obtained from social networks that serve as a means of electronic communication outweighs the employer’s interest in such data; however, this does not apply to social networks that are intended to represent the vocational qualifications of its mem-


\footnotesize{\textbf{107.} Draft Law, \textit{supra} note 7, art. 2.}
\footnotesize{\textbf{108.} BDSG, \textit{supra} note 7, at 2.}
\footnotesize{\textbf{109.} Draft Law, \textit{supra} note 7, at 5, art. 1.}
\footnotesize{\textbf{110.} See generally id.}
\footnotesize{\textbf{111.} Id.}
\footnotesize{\textbf{112.} See id.}
\footnotesize{\textbf{113.} See id. This provision does not limit the information an employer may use when making an employment decision if the individual voluntarily grants the information. See id.}
\footnotesize{\textbf{114.} See id.}
\footnotesize{\textbf{115.} See id.}
Therefore, according to the Draft Law, even if information about an employee is generally accessible via a social networking site online, the employer may not access it because the employee’s privacy interest is too high. If the purpose of the site is to demonstrate the individual’s professional accomplishments, however, the employer’s interest may outweigh the employee’s.

Generally accessible data includes data seen on the news, heard on the radio, discoverable through a general search engine, or available through a public profile. If an individual intended that the data only be accessible to only a limited circle of acquaintances (e.g., selected friends), then the information may not be classified as generally accessible, regardless of how an employer or company obtained it. Under the Draft Law, employers are not allowed to collect or process data obtained from social networking sites that are principally used for electronic communication unless the purpose of the social network is for “presentation to potential employers.”

When determining if an employer’s interest in the information outweighs the employee, the length of time the publication has been on the Internet, the context in which the information is presented online, and whether the employee has had a chance to address the “disclosure” of the information, should be taken into consideration. This complicated provision, which uses amorphous terms within a balancing test, is one reason why Germany must amend the law before it is passed. The following Section will present two specific critiques of Germany’s Draft Law, along with potential solutions.

III. Analysis

The most effective way a country can protect the data privacy of its employees is by encouraging individual discretion regarding what information they put online or voluntarily share with others through the Internet. If, however, a state wants to enact legislation protecting potential or current employees from the use of their

---

116. Id. at 4.
117. Recall, under the BDSG and Draft Law, the term employee encompasses applicants for employment as well as current and past employees. Supra note 10.
118. Draft Law, supra note 7, at 6, art. 1.
119. Id.
120. This list is not exhaustive. Id. at 16.
121. Id.
122. Id.
123. Id.
online information by the employer, the law needs to be very specific with clearly defined terms. Germany’s Draft Law suffers in two distinct ways: purpose and practice.

First, the purpose of the Draft Law is to protect the data privacy of employees by enacting a set of regulations for employers to adhere to regarding the collection of employee data and by strictly enforcing these regulations. This purpose conforms with the European Union’s emphasis on the immutability of privacy as a fundamental human right. What the rationale behind the Draft Law does not do, and what the data privacy strategy of the European Union does not do, however, is place any of the responsibility on employees to protect their own personal data. The government must properly balance employer regulation and punishment with individual regulation and punishment, even if the punishment is just allowing an employer to view information an employee left unprotected. The data privacy law is fundamentally unfair to the employer and ultimately to the individual herself.

Second, the Draft Law is impracticable and will create confusion among both employees and employers by making them question their rights and duties in the area of data privacy. The Draft Law utilizes terms that are too ambiguous to have any true meaning, such as the terms: “generally accessible,” “sites for the primary purpose of demonstrating an individual’s professional qualifications,” and sites used for “professional purposes.” Parts III(A) and III(B) below explore these two topics—purpose and practicality—in depth. Part III(C) offers suggestions for how governments can address the issue of data privacy within the context of social media. Part III(C) concludes by addressing a potential global answer to the question: when does private really mean private?

A. A Misguided Purpose Equals a Misguided Law

The rationale behind Germany’s Draft Law is well-intentioned but, ultimately, misplaced. Germany’s ultimate goal is to protect
the privacy rights of its citizens at all costs.\textsuperscript{129} This desire stems from Germany’s past role in World War II and the Nazi’s use of personal data to discriminate against and persecute large groups of individuals.\textsuperscript{130} The problem is that Germany’s desire to protect its citizens is at odds with its all-encompassing data privacy laws, as its Draft Law demonstrates.

Germany’s Draft Law will not help protect the data privacy of its citizens in the long run, because it does not encourage its citizens to take accountability for the information they put on the Internet. Social media is quickly becoming the number one way individuals choose to communicate with the world.\textsuperscript{131} In the employment context, social media is a method employers are using to recruit potential employees and it is also how potential employees are starting to market their skills and qualifications.\textsuperscript{132} If Germany’s solution to the problem of data privacy is to specifically regulate what information employers may look at online when they are researching a potential applicant,\textsuperscript{133} Germany will have to constantly enact increasingly stringent data privacy laws to keep up with changes in technology.\textsuperscript{134}

Individuals in the digital age are not thinking about what information they are sending out into the world through social media.\textsuperscript{135} Today’s job applicants and employees would rather post first and remove later,\textsuperscript{136} but the problem is that “later” may be too late.\textsuperscript{137} Instead of amending the BDSG through its Draft Law, Ger-

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{129}See Heydrich, \textit{supra} note 75, at 417; Kotzker, \textit{supra} note 76, at 748.
\item \textsuperscript{130}See Heydrich, \textit{supra} note 75, at 417; Kotzker, \textit{supra} note 76, at 748.
\item \textsuperscript{131}See generally \textit{Led by Facebook, Twitter}, \textit{supra} note 5 (discussing the significant amount of time consumers spend on social media); \textit{Network Interference}, \textit{supra} note 11, at 1 (“What employees talked about at the water cooler now appears as tweets on Twitter.”).
\item \textsuperscript{132}See generally \textit{Network Interference}, \textit{supra} note 11, at 39–56 (exploring the legal implications of the rise of social media within the workplace); \textit{Cross-Tab}, \textit{supra} note 38, at 5–6. The Draft Law does allow employers to look at employee information on professional networking sites, Draft Law, \textit{supra} note 7, art. 1, at 6, but many individuals use social networking sites to obtain employment as well, Farhad Manjoo, \textit{How to Find a Job Online, Slate} (Mar. 17, 2009), http://www.slate.com/id/2213976/.
\item \textsuperscript{133}See Draft Law, \textit{supra} note 7, at 1.
\item \textsuperscript{134}See generally Michael Higgins, \textit{High Tech, Low Privacy}, 85 A.B.A. J. 52 (1999) (discussing how a federal law clarifying employee privacy rights will not be effective because a statute could not be drafted to cover all potential situations with the rate technology is changing).
\item \textsuperscript{135}See Nick, \textit{Preserve Your Facebook Privacy, Post Cautiously, RETREVO BLOG} (May 13, 2010, 10:59 PM), http://www.retrevo.com/content/blog/2010/05/preserve-your-facebook-privacy-post-cautiously.
\item \textsuperscript{136}See id. 54% of individuals under the age of twenty-five have posted something online that they regretted. \textit{Id.}
\item \textsuperscript{137}See Bradley, \textit{supra} note 15.
\end{itemize}
\end{footnotesize}
many should focus on encouraging self-regulation when using social media. The current version of the BDSG,\textsuperscript{138} combined with the frameworks laid out by Directives 95/46/EC and 2002/58/EC, provide more than enough data privacy protection for job applicants.\textsuperscript{139} Enacting another regulation, on top of those already in place, is not the most effective way to alleviate an individual’s fear that an employer will violate her right to data privacy.\textsuperscript{140} The most effective way to address any fears that German citizens may have regarding data privacy is to encourage discretion, because, ultimately, the individual is the one with complete control over what information she shares through social media.\textsuperscript{141} Once users voluntary share information online, the right to privacy may be diminished.\textsuperscript{142}

B. For Germany’s Draft Law, Practice Will Not Make Perfect

The second reason Germany’s Draft Law is flawed is because of its text. The law utilizes terms that, despite attempts to define them,\textsuperscript{143} are so ambiguous as to have no true meaning.\textsuperscript{144} Employers and employees who try to interpret the Draft Law may do so in a way that will have unintended negative consequences.\textsuperscript{145} Additionally, the Draft Law will suffer from enforcement problems because it uses balancing tests rather than bright-line rules.\textsuperscript{146} Laws prohibiting specific employer behavior when hiring employees are already generally difficult to enforce because it is hard to prove that the employer refused to hire the individual for an illegal

\begin{itemize}
\item \textsuperscript{138} See BDSG, \textit{supra} note 7.
\item \textsuperscript{139} There is not that much of a difference between new workplace privacy issues in the digital age and traditional ones, except that technology makes it easier for unscrupulous workers to get into trouble. Higgins, \textit{supra} note 134, at 54.
\item \textsuperscript{140} Not to mention the fact that increased regulations may cause employer costs to rise. Gary L. Kaplan, \textit{Privacy Property, Confusion and Waste}, 4 CONSUMER FIN. SERVS. L. REP. 19, 20 (2001) (“Consumers should not merely be asked if they consider their private information important, but how much they would be willing to pay to assure protection of their personal information.”).
\item \textsuperscript{141} For example, “[i]n Canada, the right to informational privacy has been described as ‘the right of the individual to determine for himself when, how, and to what extent he will release personal information about himself.’” Lasprogata, \textit{supra} note 56, ¶ 11.
\item \textsuperscript{142} Sprague, \textit{supra} note 45, at 405, 407.
\item \textsuperscript{143} See Draft Law, \textit{supra} note 7, at 16, art. 6 (defining “generally accessible” and other terms).
\item \textsuperscript{144} See Kaplan, \textit{supra} note 140, at 19 (clarifying that the main challenge when creating a new property right for personal data is defining the right clearly, using consistent terms).
\item \textsuperscript{146} See Draft Law, \textit{supra} note 7, at 6, art. 1.
\end{itemize}
reason. Any attempt at enforcing a law that uses uncertain terms and balancing tests to prohibit an employer from looking at specific types of information from specific types of sites when researching job candidates will be even more difficult.

1. The Negative Impact of Ambiguous Terms

The first practical problem with the Draft Law is that too many of its terms are ill defined and ambiguous. Germany utilizes a civil law legal system, diminishing the role of case law and demanding the need for precise litigation. The Draft Law starts out clearly: during the hiring process, an employer may always ask an individual for basic contact information and for any information clearly relating to the qualifications of that specific job. After this initial provision, the Draft Law employs terms that are either undefined or so poorly defined that a clear interpretation is impossible. Terms such as “employment-related purposes,” and “legitimate interest of the employers,” are used throughout the Draft Law without being defined.

The most troubling aspect of the Draft Law’s ambiguity revolves around the use of the term “generally accessible.” The law states that an employer may “collect an applicant’s generally accessible data” and that this includes “collect an applicant’s generally accessible data” and that this includes “data . . . available through the press or the radio . . . or discoverable through a general search engine.” However, information that is limited to a specific circle of acquaintances or is found on a social network used principally for electronic communications is not generally accessible. The plain meaning of these terms is unclear.

The Draft Law defines “generally accessible” data in a way that perhaps makes it even more confusing than if the drafters had not

---

148. See Lasprogata, supra note 56.
149. Draft Law, supra note 7, art. 1, at 6.
151. See Draft Law, supra note 7, at 6, art. 1.
152. Id. at 16.
153. Id.
154. Id. If individuals use the social network to present information to potential employers, employers may collect information from this website. Id.
attempted to define it at all.\textsuperscript{155} The term “general search engine” could include all types of search engines, or it could include search engines available through subscription only.\textsuperscript{156} The Draft Law also does not address a situation that may occur if a current employee obtains information about a job applicant through “generally accessible” means and then reports this information to the person in charge of making the hiring decision.

Most importantly, the Draft Law makes no clear distinction between social networking sites and professional networking sites.\textsuperscript{157} Facebook, traditionally thought of as a social networking site, is also used by individuals for professional purposes.\textsuperscript{158} It is also unclear what the Draft Law means when it states that information found on a “social network used for electronic communications” is off-limits to employers.\textsuperscript{159} In such a new area of law\textsuperscript{160} and with a regime so protective of the data privacy of its citizens, affecting millions of people worldwide in the ever-growing realm of social media,\textsuperscript{161} this Draft Law should be as close to clear as possible.

2. Balancing Tests and Enforcement Issues

The Draft Law will be complicated to enforce because it will be difficult for an applicant to know when an employer has potentially violated the Draft Law, it will be difficult to prove that the employer has violated the Draft Law, and the ambiguities discussed above will make it difficult for the judicial body presiding over a complaint to determine if the employer violated the Draft Law.\textsuperscript{162} Moreover, the Draft Law utilizes ambiguous balancing tests rather than bright-line rules.

\textsuperscript{155} See id.
\textsuperscript{156} Id. at 16.
\textsuperscript{157} Id.
\textsuperscript{158} See Manjoo, supra note 132. See generally Dryer, supra note 11 (noting how social media and Facebook is beginning “to morph from a fun and easy way to stay socially connected with friends into a dynamic and interactive way of doing business and practicing law”).
\textsuperscript{159} See Draft Law, supra note 7, at 6. For example, if an employee posts information to her Facebook account but does not restrict who may see the information, this may be considered “generally accessible”; however, the Draft Law places an apparently broad restriction on the use of information from social networking sources. Id.
\textsuperscript{160} See Kaplan, supra note 140 (stating that when new privacy laws are inconsistent and unclear, business may feel pressured to adopt costly safeguards that outweigh their benefits).
\textsuperscript{161} See Heydrich, supra note 75.
\textsuperscript{162} See supra Part III.B.1.
First, an applicant for employment will have a difficult time determining when an employer violates the Draft Law by using information obtained through a prohibited Internet search. For example, in *Gaskell v. Univ. of Ky.*, Gaskell applied for a job at the University of Kentucky but was rejected after the University performed an Internet search and found information on Gaskell’s private website that it felt made him unsuited for the job. Gaskell only became aware of potential discriminatory animus after the University asked him questions regarding his religious beliefs during his interview. If an employer does not ask an applicant questions during the interview that indicate the employer has potentially violated the Draft Law by collecting information from prohibited sources, the applicant will have no way of knowing the employer violated the law.

Second, it will be difficult to enforce the Draft Law because it will be hard to collect evidence to prove the employer committed an illegal act. The Draft Law, similar to other employment laws, is complaint-driven, and the employer has control over most of the evidence needed to prove a complaint. Therefore, once an applicant for employment, the controller, or the Federal Commissioner for Data Protection figures out that an employer may have performed an illegal Internet search, it will be very difficult to prove this fact.

Third, although the Draft Law attempts to create a bright-line rule regarding the ability of employers to electronically look at different kinds of employee data, in practice, the law creates a balancing test. Bright-line rules are preferable to balancing tests because


164. Michelle Sherman, *Social Media Research + Employment Decisions: May Be a Recipe for Litigation*, SOC. MEDIA L. UPDATE (Jan. 18, 2011), http://www.socialmedialawupdate.com/2011/01/articles/social-media/social-media-research-employment-decisions-may-be-a-recipe-for-litigation (“In his complaint, Dr. Gaskell alleges that Dr. Cavagnero asked about his religious beliefs, and allegedly said that Dr. Gaskell’s religious beliefs and his ‘expression of them would be a matter of concern’ to the dean.”).

165. *See Cross-Tab*, *supra* note 38, at 10 (stating that only 36% of recruiters and HR professionals in Germany tell job candidates if online information factored into their employment decision).


167. BDSG, *supra* note 96, at 49.

168. Although it is not clear from the BDSG or the Draft Law what exactly an individual would need to prove a breach of data privacy, it is likely that the employee would need some level of proof that the employer acted wrongfully.
balancing tests are hard to comply with and to enforce.\textsuperscript{169} The Draft Law contains provisions addressing the employer’s ability to look at “generally accessible data” and data found on social networking sites or professional networking sites.\textsuperscript{170} In addition, the Draft Law states that he employer may collect generally accessible data, unless “the employee’s legitimate interest in to not having this data collected outweighs the employer’s legitimate interest in collection.”\textsuperscript{171} Considerations to take into account when deciding whether this issue weighs in favor of the employer or employee are the length of time the generally accessible publication has been on the Internet and whether the employee has had a chance to address the “disclosure.”\textsuperscript{172}

According to these provisions of the Draft Law, even if information about an employee is generally accessible, the employer may be unable to access it because the employee’s privacy interest at stake is too high.\textsuperscript{173} This broad balancing test would consistently be difficult to administer because an employee will always have an incredibly high interest in keeping potentially damaging information private, and an employer will always have a clear stake in finding out as much information about a job applicant as possible, in order to make the correct hiring decision.\textsuperscript{174} Additionally, although the BDSG makes no distinction between the privacy expectations of an applicant for employment and a current employee,\textsuperscript{175} a court or other enforcement body may also have to take this factor into consideration when utilizing the Draft Law’s balancing test, thus creating another layer of difficulty.\textsuperscript{176}

Thus, the Draft Law will be difficult to enforce for three reasons. First, it will be very difficult for an individual to determine when an employer has utilized information from a prohibited source when making its employment decision. Second, if an individual, the con-

\textsuperscript{170}. See discussion supra Part III.B.1.
\textsuperscript{171}. Draft Law, supra note 7, at 6, art. 1.
\textsuperscript{172}. Id. at 16.
\textsuperscript{173}. See id. at 6, art. 1.
\textsuperscript{174}. Employers may face potential liability for the misconduct of their employees under the doctrine of negligent hiring if they do not research their job applicants thoroughly. Robert Sprague, Rethinking Information Privacy in an Age of Online Transparency, 25 Hofstra Lab. & Emp. L.J. 395, 397–401 (2008).
\textsuperscript{175}. See BDSG, supra note 7, at 7.
controller, or the Federal Commissioner for Data Protection discovers that an employer may have violated the Draft Law, there will be problems of proof because the employee will have to show that the employer actually performed the forbidden search. Third, the Draft Law’s use of a balancing test rather than a bright-line rule will have a negative effect on its practical application. If Germany’s goal is to create a comprehensive system of data protection that is staunchly protective of employee rights in the workplace, it needs to utilize clearly defined rules. This will ensure that employers and employees are aware of what information an employer may look at online and what information is inaccessible.

C. Potential Ways to Reconcile Data Privacy Protection with the Development of Social Media

Through its Draft Law, Germany is attempting to provide clear, comprehensive legislation that will give increased legal certainty to employers and employees in the arena of data privacy. As described above, however, enacting legislation that places greater restrictions on employers is neither the most efficient nor the most effective way to ensure data privacy. The following analysis will offer four different ways for Germany to protect the data privacy of employees while taking into account the increasingly rapid development and prevalence of social networking sites and the freedom needed by employers to thoroughly research potential job applicants.

First, Germany needs to encourage its citizens to monitor what information they put online through social media. Only 35% of women and 30% of men in Germany always consider their online reputation when editing or posting content on the Internet. This is the lowest percentage for women among the individuals surveyed in the United States, United Kingdom, and France, and the second lowest percentage for men.

The best way for Germany to encourage self-regulation rather than simply enacting more and more regulations against employers, is to relax the restrictions on employers proposed by the Draft Law. Unlike Germans, citizens of the United States view the

177. Higgins, supra note 139, at 55 (clarifying that most workplace privacy cases that rely on vague balancing tests create a patchwork of standards so that there really is no national policy to protect employee privacy).
178. Draft Law, supra note 7, at 1.
179. See discussion supra Part II.A.
180. See Cross-Tab, supra note 38, at 18. For survey methodology, see id. at 22.
181. See id.
responsibility for protecting their online reputation as their own.182 If employers are able to use any information found online, including information found through social networking sites, when making employment decisions, then individuals will be more likely to limit the potentially harmful information they post online.183 Germany should also educate its citizens on the appropriate methods of protecting online information by advocating for primary and secondary schools, as well as universities, to teach courses in online safety and ways to protect personal information in the digital age.184 Events such as “European Data Protection Day” should be available via webcam through the European Commission’s website, instead of consisting of a series of closed workshops at the European Parliament.185

Second, instead of focusing so heavily on the regulation of employers and how employers are processing information found through illegal Internet searches, Germany should concentrate on regulating social media companies. Strict regulation of social media companies is preferred over employer regulation because the only way many social networking sites make a profit is by commercially exploiting the data of users and other third parties.186 When employers are accessing applicant data through social media sites they are attempting to uncover as much information as possible regarding the applicant’s ability to perform the job.187 Therefore, in order to make sure that social media companies are protecting the data of their users, Germany should encourage courts to enforce contractual rights instituted by user agree-

---

182. See id. at 19 (explaining that out of the individuals surveys in the United Kingdom, France, Germany, and the United States, the United States was the only country where a slight majority of respondents claimed sole responsibility for protecting their reputation).

183. Some individuals may find fault with the idea of self-censorship insofar as they do not understand why a person must be more careful with his or her speech simply because it may be captured in a permanent form by a social media site. My response is that the advent of technology has created a way for an individual’s speech to be recorded permanently with or without her permission, and there is no more effective way to ensure privacy in the electronic age than through self-censorship online.

184. This education should include information on how users can use social media to create a strong personal brand and affect job applications in a positive way. See Cross-Tab, supra note 38, at 10 (noting that human resources professionals believe that the use of online reputational data will increase in coming years and that positive branding already influences a candidate’s application).


186. See Network Interference, supra note 11, at 40.

187. See Cross-Tab, supra note 38, at 3.
ments and demand that social networking sites have precise, prominently displayed instructions on how to adjust privacy settings or remove content.

Third, if Germany decides to enact strict employer regulations rather than individual user regulation, it will need to enact a law that is more precise and more detailed. The Draft Law’s ambiguous terms and balancing tests provide a confusing framework for employees, employers, and enforcement bodies to adhere to. As discussed in Part III(B), above, the Draft Law should specifically define every term it uses to describe social networking sites, generally accessible data, and legitimate interests of the employer versus the employee. Additionally, instead of purporting to institute bright-line rules but instead enacting indiscriminate balancing tests, the Draft Law should very clearly state what an employer may or may not do when researching a potential employee. Solely requiring that each regulation ultimately depend on the balancing of privacy interests between the employee and employer is not an effective way to provide greater legal certainty to employees and employers.

Fourth, Germany should amend its Draft Law to include a provision that Internet searches of job applicants should only be performed by individuals who are otherwise removed from the hiring decision. For example, if the human resources department of a company is in charge of all online research of job applicants and then that department sends the relevant information to the individual making the employment decision, there is less of a chance that a breach of the applicant’s data privacy will hurt the applicant. This method of researching job applicants will help ensure that even if the employer violates the Draft Law the job prospects of the applicant will not be adversely affected.

In addition to taking into account the recommendations listed above, Germany also needs to be aware that its Draft Law will have significant implications for the future of global data privacy. In 2010, the European Union proposed to strengthen its existing regulatory approach and suggesting that social networking sites should be treated under the same legal regime as any other web platform publishing users’ personal information).

188. See Network Interference, supra note 11, at 40–42 (noting the lack of a uniform regulatory approach and suggesting that social networking sites should be treated under the same legal regime as any other web platform publishing users’ personal information).

189. See id. (highlighting the inability of users to remove content and lack of clarity in privacy policies on social networking sites).

190. See discussion supra Part III.B.1.

191. See supra Part III.B.2.

192. See Sherman, supra note 164.

193. Id.
Internet privacy laws in order to address new challenges presented by social networks like Facebook, and due to the increasingly international scope of most businesses, there will eventually be a need for a global social media policy. The Safe Harbor Privacy Principles discussed above, are merely a short-term solution to a long-term problem.

The European Union needs to set an example of how a governing body can properly balance the need for protecting the data privacy rights of individuals with business autonomy and self-regulation. If the European Union models its amendments after Germany’s Draft Law, the problems addressed in Parts III(A) and III(B) will be replicated on a global scale. Instead, the European Union needs to take into consideration the suggestions listed above when developing an international binding legal instrument addressing data privacy. The goal of this instrument should be to encourage individual self-regulation of data privacy while also providing certain levels of protection over online information that the individual is unable to control. The instrument should utilize clearly defined terms and bright-line rules, and it should not attempt to parse out the different types of websites an employer may visit when researching a potential job applicant. It should differentiate between the privacy expectations of job applicants and current employees, and it should emphasize the importance of separating the individual performing the Internet search from the individual making the employment decision.

IV. CONCLUSION

Social media has changed the way employees talk to one another, how employers and employees communicate, and how employers decide who they want to be their employees in the first place. Germany’s Draft Law attempts to combat the increased use of social media by employers when researching employees; how-


196. Safe Harbor Decision, supra note 58.

197. See supra Parts III.A–B.

198. See Data Protection on the Agenda of the Next G8?, supra note 195 (noting the rising concern about challenges to data protection and lack of a globalized, legal solution).
ever, the rationale behind the Draft Law and the substance of the law itself will not adequately protect the privacy of individuals while balancing the concerns of employers. The European Union has stated that this ultimate principle is at the heart of its policy regarding data privacy, and Germany's Draft Law fails to adequately take this into account.

The Draft Law puts all the responsibility on the employer to control what information it uses when researching potential employees online and fails to put any responsibility on the individual to be discreet with the information she makes available on the Internet, especially through social networking sites. The structure of the Draft Law is flawed because it relies on balancing tests and vague classifications that will not be helpful for courts attempting to enforce the law, nor for employees or employers when attempting to understand their rights in the workplace. Instead of using the Draft Law as a model for its amendments to the data privacy laws, the European Union should use it as a lesson for what to avoid when structuring its potential international data privacy instrument. The world is becoming increasingly digital, and any attempt at regulating what specific websites an employers may look at online before hiring an employee will be futile.