Kentucky Law Journal

Volume 103 | Issue 3 Article 5

2015

Data Privacy as a Civil Right: The EU Gets It?

Raymond Shih Ray Ku
Case Western Reserve University School of Law

Data Privacy as a Civil Right: The EU Gets It?

Raymond Shih Ray Ku[1]

INTRODUCTION

Can an employer fire an employee based upon information gleaned from Facebook or other social media? Should this information be protected as private even when it is shared with "friends"? This Article explores how differences between privacy law in the United States (US) and the European Union (EU) highlight an important, if subtle, distinction between two competing conceptions of privacy. The first treats autonomy as an aspect of privacy. The second treats privacy as an aspect of autonomy. In other words, how, if at all, do the two legal regimes protect an individual's personal information or what is often referred to as "data privacy"? This Article argues that both legal regimes generally approach data privacy protection by treating autonomy as an aspect of privacy. As such, privacy law primarily focuses upon the individual's right to control the disclosure and collection of information, and the debate surrounding privacy law revolves around the circumstances in which privacy law should protect an individual's right to consent to the collection and disclosure of information.

However, the EU also excludes certain classes of information from collection and processing, such as race, ethnic origin, political opinion, or even sex life. This exclusion provides an important complimentary approach in which data privacy is a means of protecting individual autonomy and dignity. These provisions of EU privacy law prevent employers from making decisions based upon certain categories of information analogous to laws protecting individuals from discrimination. This approach could and should be an important part of the data privacy debate in the US. In addition to discussing the circumstances in data collection that are permissible, the data privacy debate should also focus upon what categories of information, if any, should be protected and under what circumstances should decision makers be prevented from relying upon protected information.

This Article begins by discussing the recurring controversy surrounding employers' employment decisions based upon information gleaned from an employee's or a potential employee's social media accounts. These examples are representative of the sometimes-troubling practice of schools, employers, and others basing important decisions upon information gathered online. This Article

[1] Professor of Law, Director, Center for Cyberspace Law & Policy, Case Western Reserve University School of Law. I would like to thank the editors of the Kentucky Law Journal especially Benjamin Monarch and Jeffrey Kaplan for the hard work and patience. The ideas expressed in this essay were inspired by the works of numerous privacy scholars, including Daniel Solove, Julie Cohen, and Alan Westin.

then provides a brief description of data privacy laws in the US and the EU. This discussion explains how these two sets of laws protect data privacy. The social media problem is then considered through these laws and illustrates how, despite their differences, both legal regimes focus upon protecting an individual's right to control information about him or herself. Finally, the Article identifies an alternative approach toward data protection that is closer to civil rights and anti-discrimination laws than privacy. The social media example also demonstrates why protecting data privacy requires protecting an individual's right to be free from discrimination.

I. DATA PRIVACY: THE SOCIAL MEDIA PROBLEM

The growth in individuals using social media, as well as the growing ubiquity of data about those individuals online in general, increasingly challenge the legitimacy of individual expectations of privacy. By one measure, worldwide social media usage will grow from just under one billion users in 2010 to a projected 2.44 billion users in 2018.[2] It is common for individuals using these services to share a wide range of information, from nude images of themselves to their opinions on political, philosophical, and religious questions. In some cases, this information is shared with only one other or a small circle of confidants. However, a great deal of information is shared with a much larger group of individuals, including coworkers, employers, and even the public at large.

It should come as no surprise then that decision makers, including employers and school admissions committees, gather and use this data when evaluating prospective employees and students.[3] However, individuals were in fact surprised to find themselves fired because of Facebook posts or denied admission because of something they tweeted. Cases demonstrating the negative consequences of social media usage have been widely reported. Consider the following examples. A young man posts a picture of himself smoking what appears to be an illegal substance. His employer, a Facebook friend, fires him.[4]

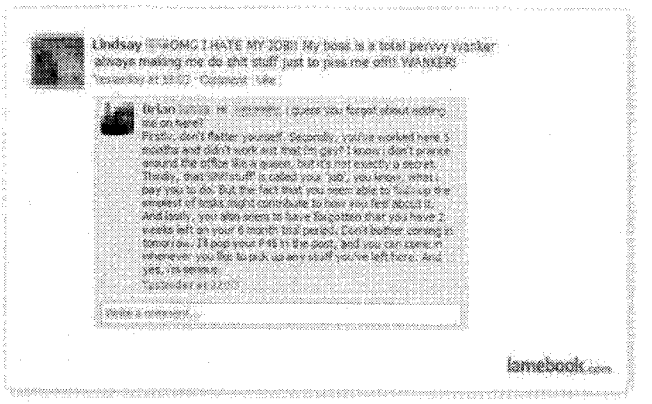
---

[2] *See Number of Social Network Users Worldwide from 2010 to 2018*, STATISTA, http://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/ (last visited Jan. 26, 2015).

[3] *See, e.g.*, Daniel Bean, *11 Brutal Reminders that You Can and Will Get Fired for What You Post on Facebook*, YAHOO! (May 6, 2014), https://www.yahoo.com/tech/11-brutal-reminders-that-you-can-and-will-get-fired-for-84931050659.html; Jessica Holdman, *Employees Fired for Facebook Post*, BISMARCK TRIBUNE (Sept. 9, 2013, 4:59 PM), http://bismarcktribune.com/business/local/employees-fired-for-facebook-post/article_2117b7f8-199b-11e3-806d-001a4bcf887a.html; Heather Leigh, *4-Year-Old Expelled from Preschool for Mom's Facebook Post*, NEWS4JAX (Aug. 27, 2014, 11:22 PM), http://www.news4jax.com/news/4yearold-expelled-from-preschool-for-moms-facebook-post/27740108.

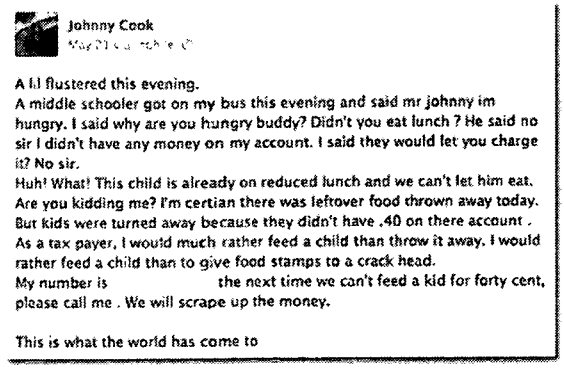
[4] Bean, *supra* note 3.

A woman is fired after complaining about her job and insulting her boss.[5]



A school teacher is fired for posting a picture of herself on vacation holding alcoholic beverages.[6] Or, a school bus driver is fired after expressing his opinion about the plight of a hungry child on his bus and offering to help "scrape up the money."[7]

[5] *Id.*
[6] *Id.*
[7] *Id.*


Johnny Cook

A lil flustered this evening.
A middle schooler got on my bus this evening and said mr johnny im hungry. I said why are you hungry buddy? Didn't you eat lunch ? He said no sir I didn't have any money on my account. I said they would let you charge it? No sir.
Huh? What? This child is already on reduced lunch and we can't let him eat.
Are you kidding me? I'm certian there was leftover food thrown away today.
But kids were turned away because they didn't have .40 on there account .
As a tax payer, I would much rather feed a child than throw it away. I would rather feed a child than to give food stamps to a crack head.
My number is the next time we can't feed a kid for forty cent, please call me . We will scrape up the money.

This is what the world has come to

These examples are used as cautionary tales of the dangers of social media, generating "dos" and "don'ts" of social media usage.[8] Some of the "don'ts" would appear to be obvious: do not post evidence that you live "like a pre-rehab Lindsay Lohan," or demonstrate that you are "getting chatty with the competition," for example.[9] Other examples may come as a surprise, such as refraining from expressing opinions on "politics, race, class, or gender" or bragging about your "beautiful baby, boyfriend, or boat."[10]

Given the growing recognition that important decisions may be based upon information shared on social media, individuals have begun to "manage" their social media identities.[11] And, consultants now offer professional advice on how to manage that identity.[12] Some go as far as offering to expunge your online identity.[13]

While the way in which this information is shared and is gathered is clearly new, arguably the "arbitrariness" or "unfairness" of such decisions is not new. For example, in the United States, private employment is generally based upon the principle of employment at will.[14] Under this approach, employers may generally refuse to hire or may decide to fire individuals for any reason. For example, an employee may be fired for supporting a rival football team[15] or political candidate.[16]

[8] *See, e.g.*, Kathy Kristof, *6 Things You Should Never Reveal on Facebook*, YAHOO! (Sept. 14, 2010, 3:00 AM), http://finance.yahoo.com/news/pf_article_110674.html; Amy Levin-Epstein, *Facebook & Your Job: 5 Ways to Get Fired*, CBS NEWS (Mar. 16, 2011, 12:10 PM), http://www.cbsnews.com/news/facebook-your-job-5-ways-to-get-fired/.

[9] Levin-Epstein, *supra* note 8.

[10] *Id.*

[11] *See, e.g.*, Anna Vander Broek, *Managing Your Online Identity*, FORBES (June 2, 2009, 10:00 AM), http://www.forbes.com/2009/06/01/manage-online-reputation-technology-identity.html; Phyllis Korkki, *Is Your Online Identity Spoiling Your Chances?*, N.Y. TIMES, Oct. 9, 2010, http://www.nytimes.com/2010/10/10/jobs/10search.html?_r=0.

[12] Mary Beth Moore, Dir. of Emp'r Outreach & Externships, Remarks at the Workshop on Personal Branding and Social Media at Case Western Law School (Oct. 23, 2014) (during the writing of this essay, the Career Development Office at Case Western organized a workshop on managing students' online social identities).

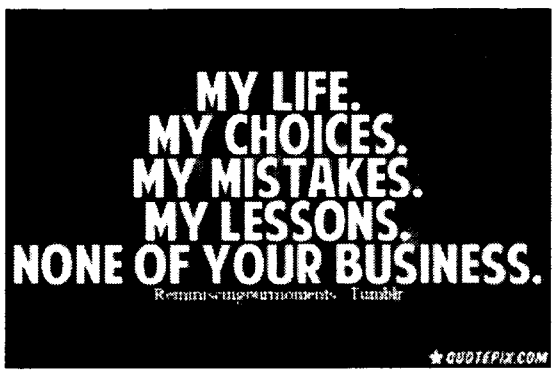
[13] *See, e.g.*, REPUTATION.COM, http://www.reputation.com/ (last visited Jan. 26, 2015).

[14] BLACK'S LAW DICTIONARY 641 (10th ed. 2014).

[15] Kim Janssen, *Packer Backer Fired for Wearing Green Bay Tie*, SOUTHTOWN STAR (Sept. 24, 2012, 6:25 AM), http://southtownstar.chicagotribune.com/news/3476381-418/tie-stone-fired-bears-packers.html.

As such, employers are generally free to discriminate against individuals unless specifically prohibited by certain laws, such as under anti-discrimination laws, which prohibit them from discriminating based upon an individual's race, color, religion, sex, or other protected categories.[17]

If the use of this information as the basis for decision-making should come as no surprise, it should also come as no surprise that individuals have objected to this use.[18] The following Internet meme nicely illustrates these objections.



Often, these objections are framed or interpreted in terms of individual privacy.[19] In other words, an employer, school, or other decision-maker should not base their decisions on this information because it is (or should be) considered private. Of course, the difficulty with this position is the fact that claiming information you have already revealed to others is nonetheless private, smacks of inconsistency. The remainder of this Article examines this objection beginning with a comparison between data protection in the US and the EU.

---

[16] Timothy Noah, *Bumper Sticker Insubordination*, CHATTERBOX (Sept. 14, 2004, 6:30 PM), http://www.slate.com/articles/news_and_politics/chatterbox/2004/09/bumper_sticker_insubordination.html.

[17] *See* 42 U.S.C. § 2000e-2 (2012).

[18] Greg Fish & Timothy B. Lee, *Employers, Get Outta My Facebook*, BLOOMBERG BUSINESSWEEK, http://www.businessweek.com/debateroom/archives/2010/12/employers_get_outta_my_facebook.html (last visited Jan. 26, 2015); Rachel Ryan, *Yes, Employers Will Check Your Facebook Before Offering You a Job*, HUFFINGTON POST (May 4, 2013, 5:12 AM), http://www.huffingtonpost.com/rachel/ryan/hiringfacebook_b_2795047.html.

[19] *See, e.g.*, Patricia Sanchez Abril, *A (My)Space of One's Own: On Privacy and Online Social Networks*, 6 NW. J. TECH. & INTELL. PROP. 73, 73–74 (2007); James Delaney, *Employer Use of Facebook and Online Social Networks to Discriminate Against Applicants for Employment and Employees*, 64 LAB. L.J. 86, 91–95 (2013); Saby Ghoshray, *The Emerging Reality of Social Media: Erosion of Individual Privacy Through Cyber-Vetting and Law's Inability to Catch Up*, 12 J. MARSHALL REV. INTELL. PROP. L. 551, 552–53 (2013).

II. APPROACHES TOWARD PRIVACY IN THE US AND EU

In order to understand and evaluate the privacy claims posed by social media, this section compares data privacy protection in the US and the EU. The purpose of this discussion is not to provide an in-depth analysis of data privacy laws but to illustrate how these two regimes approach the protection of information. As discussed below, while both regimes focus upon protecting the individual's right to control information, the EU supplements these protections with prohibitions against the use of certain information such as political opinion or data concerning one's sex life.

In the US, data or information privacy is not governed by a single statute.[20] Rather, information is protected on a case-by-case basis. For example, separate statutes protect information regarding health information,[21] driver licenses,[22] and even video rentals.[23] Varying common law causes of action also protect aspects of privacy.[24] Government surveillance is covered by the Fourth Amendment,[25] communication interception statutes,[26] and the Foreign Intelligence Surveillance Act.[27] However, the one unifying theme or underlying principle to privacy protections in the United States is that the law protects only reasonable expectations of privacy.

So when are expectations of privacy reasonable? The answer to this question can be reduced to choice. Individuals have a reasonable expectation of privacy until they choose to make that information accessible to others. Courts have concluded that there is no reasonable expectation of privacy in information in plain view,[28] including when private property can be viewed from the air,[29] shared with third parties,[30] or contained or transmitted through an employer's property including emails and telephone calls.[31] As a common understanding of privacy might suggest, information is private until the individual decides to share that information or acts in a manner that makes the information available to others. Consequently, debates about privacy focus largely upon the circumstances in which an individual can be

[20] *See* DANIEL SOLOVE & PAUL SCHWARTZ, PRIVACY LAW FUNDAMENTALS 2–4 (2d ed. 2011).

[21] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 1173, 110 Stat. 1936, 2024–26.

[22] Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (2012).

[23] Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195.

[24] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 (1890) (explaining the foundational work on the common law right of privacy); *see also* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 126–27 (2007) (exemplifying more recent scholarship on this topic).

[25] U.S. CONST. amend. IV.

[26] 18 U.S.C. §§ 2510–22 (2012).

[27] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783.

[28] Coolidge v. New Hampshire, 403 U.S. 443, 465–67 (1971).

[29] Dow Chemical Co. v. United States, 476 U.S. 227, 239 (1986).

[30] Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

[31] *See* Smyth v Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996).

said to have shared information or that information is accessible to others, but nonetheless should be protected.[32]

For example, in 2000, the Federal Trade Commission outlined four key principles governing the fairness of information practices in the online marketplace. Internet Data Collection is fair when these four prongs are met:

> 1. Notice—Web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (*e.g.*, directly or through non-obvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.
>
> 2. Choice—Web sites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (*e.g.*, to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities).
>
> 3. Access—Web sites would be required to offer consumers reasonable access to the information a Web site has collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information.
>
> 4. Security—Web sites would be required to take reasonable steps to protect the security of the information they collect from consumers.[33]

Under this interpretation, individuals have a reasonable expectation in online privacy when they have been made aware of the circumstances in which their information will be collected and used, and they are given the opportunity to choose whether they share that information. In other words, individuals lose any reasonable expectation of privacy when they make the informed choice to share that information.

Given the centrality of notice and choice, it should come as no surprise that in the US, states have responded to the use of social media in employment decisions by following those principles. Currently, to protect the individual's right to determine when to share information, fourteen states limit an employer's ability to demand access to an employee's social media.[34] These states, however, do not

[32] *See generally* Richards & Solove, *supra* note 24.

[33] DIV. OF FIN. PRACTICES, FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE iii (2000), *available at* http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

[34] *See* SEYFARTH SHAW, SOCIAL MEDIA PRIVACY LEGISLATION: DESKTOP REFERENCE 6–9 (2014), *available at* http://www.seyfarth.com/uploads/siteFiles/practices/131317SocialMediaSurveyM13.pdf

prohibit an employer from obtaining and relying upon publicly available information.

The concept of informed choice is also central to data privacy in the EU. Unlike the ad hoc approach followed in the US, the EU's Directive on Data Protection[35] provides a comprehensive set of legal principles for data privacy and requires member states to implement those principles. For example, EU Directive 95/46 requires member states to guarantee that personal data is: "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes,"[36] and that personal data may only be processed if "the data subject has unambiguously given his consent."[37]

In response to the 95/46 Directive, the US negotiated various safe harbor principles. US data collection will be considered consistent with the 95/46 Directive when:

> Notice: An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party(1).
>
> Choice: An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party(1) or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.
>
> For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.
>
> Onward Transfer: To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer

(summarizing state social medial protections); *see also* Michael Loatman, *Social Media Privacy Bills Facing More Scrutiny*, BLOOMBERG BNA SOC. MEDIA BLOG (May 16, 2014), http://www.bna.com/social-media-privacy-b17179890555/.

[35] Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

[36] *Id.* art. 6(1)(b), at 40.

[37] *Id.* art. 7(a).

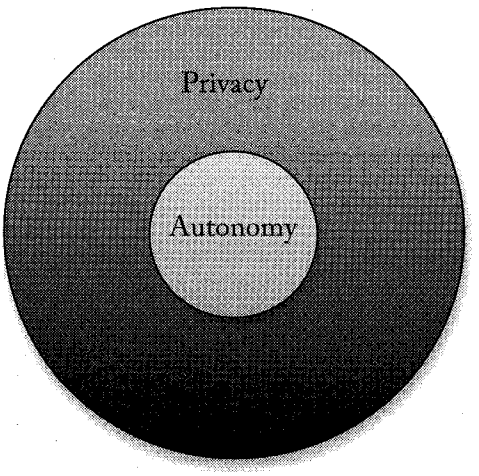
> information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.
>
> Security: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.
>
> Data Integrity: Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.
>
> Access: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.
>
> Enforcement: Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.[38]

Accordingly, while the EU provides greater protection for the integrity of data, individual access to data, and the requirement for enforcement of data protection, informed consent through notice and choice can be considered the core principles of EU data protection as well.

Conceptually, this approach toward data protection treats individual autonomy as an aspect or element of privacy. While this element is critical, choice serves

[38] U.S. Dep't of Commerce, *Safe Harbor Privacy Principles*, EXPORT.GOV (July 21, 2000), http://www.export.gov/safeharbor/eu/eg_main_018475.asp.

privacy and not the other way around. Visually, the relationship between autonomy and privacy would look like this:



Conceived in this manner, whether information is private, and therefore, legally protected, is a function of the autonomous choice of the individual. In general, when the individual exercises her autonomy by choosing to share information, she no longer has a privacy interest in that information.

Given this conceptual approach and that data protection in both the US and the EU turns upon principles of notice and choice, it should be no surprise that claims that information shared on social media is private or that the use of this information by others is unfair are met with skepticism. After all, individuals knowingly share this information with others. They choose to make this information available to others. In some cases, this may include having an employer as a Facebook friend or tweets that are generally open to the public. As such, it could be said that individuals "foolishly trade away their privacy to 'broadcast themselves.'"[39] Nonetheless, a persistent unease and objection to decision making based upon truthful information gleaned online remain. As the following section argues, the EU Directive offers an alternative approach that evaluates the fairness of these decisions based upon another relationship between privacy and autonomy.

III. DATA PROTECTION & ANTI-DISCRIMINATION

If objections to employers or other decision makers relying upon information on social networks cannot be firmly grounded in terms of privacy, civil rights or freedom from discrimination offers a complimentary paradigm. As this section discusses, this approach is suggested by Directive 95/46 and is one consistent with a model of privacy that recognizes privacy as an aspect of autonomy.

As discussed above, a popular objection to decision makers relying upon information available online is the claim that this information is "none of your

[39] Abril, *supra* note 19, at 83.

business." While this can readily be considered an objection based upon privacy, it is also a claim that the information should not be part of decision making even if the information is not protected by a right of privacy. Once again, consider Directive 95/46. While the US and EU both approach data protection through the twin principles of notice and choice, the EU opens up the possibility of going one important step further. Specifically, Directive 95/46 prohibits "the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[40]

Accordingly, the Directive recognizes that the use of certain categories of information should be prohibited, and one might suggest that under Directive 95/46 an employer would be prohibited from making employment decisions based upon this information. Such a conclusion would appear to give social media users the remedy they seek. The Directive, however, recognizes two important exceptions. First, the prohibition does not apply if the individual has given her explicit consent unless the member state does not permit such consent.[41] Second, the prohibition may not apply "to data which are manifestly made public by the data subject."[42] As such, it may not give prospective and current employees or students the protections they desire.

However, because the Directive is implemented by member states and allows for variation based upon the laws of the member state, it should come as no surprise that there are differences in how these provisions have been interpreted. For example, French law closely tracks the Directive and its exceptions,[43] and as such it may not provide any additional protections. In contrast, Spain protects an individual's right to refuse to state "his ideology, religion or beliefs"[44] and prohibits the collection of data "for the sole purpose of storing personal data which reveal the ideology, trade union membership, religion, beliefs, racial or ethnic origin or sex life."[45] With respect to personal data revealing "ideology, trade union membership, religion and beliefs," Spain requires that this information may only be collected "with the explicit and written consent of the data subject."[46] Likewise, Italy restricts the use of this "sensitive data" to circumstances in which the data is indispensable.[47]

[40] Council Directive 95/46, *supra* note 35, art. 8(1), at 40.

[41] *Id.* art. 8(2)(a).

[42] *Id.* art. 8(2)(e), at 41.

[43] Loi 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Law 2004-801 of August 6, 2004 on the Protection of Individuals with Regard to Data Processing of Personal Data and Amending the Law 78-17 of January 6, 1978 Relating to Data, Files and Liberties], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Aug. 7, 2004, *available at* http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=20040807&numTexte=2&pageDebut=14063&pageFin=14077.

[44] Protection of Personal Data Law art. 7 ¶ 1 (B.O.E. 1999, 4390) (Spain).

[45] *Id.* art. 7 ¶ 4.

[46] *Id.* art. 7 ¶ 2.

[47] *See* Decreto Legislativo 30 giugno 2003, n. 196 (It.).

While it remains to be seen whether differences in the implementation of Directive 95/46 will provide legal protections beyond those afforded by a right of privacy premised upon notice and consent, it opens the door to treating data protection as a civil right rather than a privacy right.

Instead of asking whether information is private, should we be asking when and under what circumstances decision makers should be permitted to use information available to them? Tracking Directive 95/46, instead of asking whether my racial or ethnic origin should be protected as private, should we be asking how is my racial or ethnic origin, political opinions, religious or philosophical beliefs, or sex life relevant to whether I will be a good student or employee? In this respect, the objection that some information is "none of your business" is not so much an objection to decision makers obtaining the information and thus intruding upon one's private life so much as it is an argument that the information is not relevant. In other words, "if it doesn't directly affect you, then it's probably none of your business."[48]

Should objections to data gathering be treated as civil rights objections? Consider a recent story reported in the *New York Times* about a prospective college student. Apparently, while the student attended the college's information session, she posted disparaging comments about other attendees, and because the college tracked its social media coverage, it discovered her tweets.[49] According to the college, the student was denied admission based upon her credentials, but according to the Dean of Admissions and Financial Aid, "had her credentials been better, those indiscreet posts could have scuttled her chances."[50] Why would someone's admission decision turn on her tweets? The Dean explained, "We would have wondered about the judgment of someone who spends their time on their mobile phone and makes such awful remarks."[51]

Richard Posner argued that we should not recognize a right of privacy under these circumstances because it would deny the decision maker important, relevant information.[52] To paraphrase Judge Posner, admitting a student in the absence of this information would be akin to admitting a defective student, and the school should be entitled to investigate the soundness of the applicant.[53] One might tend to agree with the outcome in the preceding example or with the outcome of earlier examples, such as the employee smoking illegal drugs or skipping work to attend a Halloween party. The same justification can be used to support perhaps more troubling examples, such as the firing of the teacher who posted pictures of herself with alcohol on Facebook, the bus driver expressing his frustration over a hungry

[48] *See* Nisha Patel, *25 Famed Nosey People Quotes*, SLODIVE, http://slodive.com/inspiration/25-famed-nosey-people-quotes/ (last visited Jan. 26, 2015).

[49] Natasha Singer, *They Loved Your G.P.A. Then They Saw Your Tweets*, N.Y. TIMES, Nov. 10, 2013, at BU3.

[50] *Id.*

[51] *Id.*

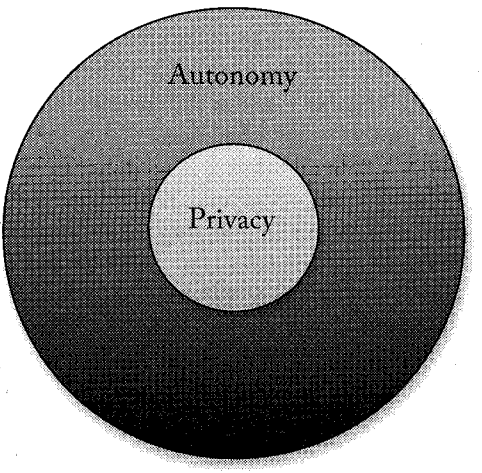
[52] *See* Richard A. Posner, *An Economic Theory of Privacy*, REGULATION, May–June 1978, at 19–20.

[53] *See id.* at 21–22.

child, or a student denied readmission to college because he had shared the fact that he is gay with his friends on Facebook. In these later cases, was this information relevant? Was it evidence that they were somehow "defective" employees or students?

Even assuming these preceding examples could be considered evidence of poor judgment, this issue still begs the question of whether such behavior necessarily carries over into the classroom or workplace. Nevertheless, any assumption that individual behavior under one set of circumstances is evidence of how that individual will behave in other circumstances is inconsistent with our understanding of human behavior.[54] Individuals are capable of and do assume different personae depending upon whether they are at home, with friends, or in the workplace. This situational identity is not only common, but also arguably necessary for human flourishing.

Viewed in these terms, autonomy is not an instrument of privacy evidenced by individual decisions to share or withhold information, but rather privacy is an instrument for protecting individual autonomy. Visually, this relationship would be depicted as follows:



In other words, limiting the circumstances in which individuals may obtain information about others allows those individuals to live a life of their choosing. More importantly, recognizing privacy as an element of autonomy forces society to recognize that concluding that the use of information is not a threat to individual privacy is not the same as concluding that the use of information does not threaten individual autonomy.

Much like the debates over the relevance of race or gender or any of the categories of human traits we protect through anti-discrimination laws, contemporary debate over data protection should focus upon identifying when individual behavior (past or present) is relevant to the task at hand and when judgments based upon behavior are misleading and inaccurate. However, instead of

[54] *See* Abril, *supra* note 19, at 84–85.

legal or constitutional debates involving which physical characteristics are irrelevant or the circumstances in which individuals with those characteristics require protection, this is a policy debate about the categories of information and the circumstances in which that information is relevant, if at all.

CONCLUSION

While it is both important and fair for laws in the US and the EU to protect the individual's right to be fully informed about the circumstances in which data will be collected and used and to protect the individual's right to decide whether to share that information, notice and choice are only part of the solution. As illustrated by the privacy problems generated by the sharing and accessibility of information through social media, privacy as defined by the individual's ability to control personal information does not adequately capture the full range of data protection interests. While the Directive of 95/46 suggests an important alternative approach consistent with the civil rights paradigm, it may not go far enough.

Data protection laws must recognize that individual autonomy distilled as individual choice is not simply a tool for protecting and defining the boundaries of an individual's right to privacy. Instead, data protection laws should recognize that the right of privacy is also a tool for protecting individual autonomy. Recognizing privacy as an aspect of autonomy clarifies the interests that individuals using social media are seeking to protect even when they share information online—certain information about what I believe, what I have done, or what I am doing are not relevant to decisions being made about me. While some of such claims can readily be dismissed as unreasonable and self-serving, such as abusive behavior or illegal conduct, others merit in-depth consideration. Why should a bus driver be fired for expressing frustration for a passenger? Why should a student be denied admission because he shared his sexual orientation on Facebook? Questions like these suggest the need for broader discussions in the US and the EU on how decisions impacting the lives of individuals should be made and what it means for individuals to be judged on their merits.

Highlighting the differences between autonomy as privacy and privacy as autonomy is not a suggestion that the two are separate or mutually inconsistent. Both protect individual freedom and autonomy although through different legal mechanisms. Anti-discrimination protections are useful remedies for preventing overt discrimination. In contrast, privacy protections address subtle discrimination and unconscious bias. Both approaches are required in order to fully protect individual autonomy and freedom.