Wimberly Lawson
Wright Daves & Jones, PLLC
Attorneys & Counselors at Law

Briefly

August 2021 Volume 21, Issue 8

THE USE OF PRONOUNS: NOT AS SIMPLE AS WE ONCE THOUGHT

Edward H. Trent

"[M]ost were taught as children, that boys are 'he/him' and girls are 'she/her.' Now, however, the use or alleged misuse of pronouns may result in employment law claims under Title VII."

The societal debate over what the term "sex" means regarding an individual's gender continues to draw battle lines and create confusion in all sectors of society. In June 2020, the United States Supreme Court issued its decision in *Bostock v. Clayton County, Ga.* addressing whether Title VII's prohibition on discrimination because of "sex" covered discrimination based on sexual orientation and/or transgender status, the latter more broadly viewed within the context of gender identity. Because discrimination based on characteristics not covered under Title VII do not create a legal claim for discriminatory termination under the civil rights statute, it would seem logical the Court would first address what the term "sex" means in the statute. In reaching its conclusion, however, the Court determined that it did not need to reach that question but proceeded in its analysis "on the assumption that 'sex' signified what the employers suggest, referring only to biological distinctions between male and female."

While the Court was willing to accept, for purposes of argument, that sexual orientation and transgender status were "factors other than sex" under Title VII, the Court nevertheless concluded in a 6-3 decision that an employer's termination of an employee because of the employee's sexual orientation or transgender status was so inextricably intertwined with the employee's sex as male or female that termination on the basis of sexual orientation and/or transgender status violated Title VII's prohibition on discrimination "because of ... sex." The Court, however, expressly left open questions of sex-specific dress codes, restroom and locker room access, and religious objections in various potential scenarios. As a result, the Court left more muddled than clear the question of whether an employer is required to treat an employee consistent with the employee's gender identity or with the employee's biological sex. The breadth of this debate is far beyond the narrow focus of this article, which addresses the use of pronouns when referring to persons - namely what most were taught as children, that boys are "he/him" and girls are "she/her". Now, however, the use or alleged misuse of pronouns may result in employment law claims under Title VII.

Interpreting Title VII and bolstered by the Court's *Bostock* decision, the United States Equal Employment Opportunity Commission (EEOC) updated its guidance on the application of Title VII when it comes to sexual orientation and gender identity. Specifically with regard to pronouns, the EEOC's 2021 "*Protections Against Employment Discrimination Based on Sexual Orientation or Gender Identity*" states at No. 11 that "in certain circumstances . . . intentionally and repeatedly using the wrong name and pronouns to refer to a transgender employee could contribute to an unlawful hostile work environment." This guidance, which the EEOC notes does not have the force of law, is consistent with prior guidance issued under the Obama Administration that the use of names and pronouns when referring to individuals should be consistent with the individual's gender identity, even when the gender identity is inconsistent with the individual's biological sex.

This very issue was before the Sixth Circuit Court of Appeals in March 2021 in the case of *Meriwether v. Shawnee State University*. There, Professor Meriwether was a 25-year veteran with a spotless record. In his philosophy classes, he addressed his students as "Mr." or "Ms." believing a more formal addressing of his students added to the weight of the topics discussed in class, which could include controversial topics being debated in contemporary society. As a devout Christian, he maintains that "God created human beings as either male or female, that this sex is fixed in each person from the moment of conception, and that it cannot be changed, regardless of an individual's feelings or desires." As a result, Professor Meriwether objected to referring to a male student

Continued on page 4

HOW CYBER-SECURE IS YOUR 401(K)?

Mary C. Moffatt

"The case has been noted as a wakeup call for all involved, including employers as plan sponsors, and participants."

Scary Scenario: One bright morning you hear the stock market futures are set to go high, so later in the day, you decide to see how much your 401(k) has increased. After years of consistently maxing out your 401(k), you've managed to develop a healthy nest-egg of almost $250,000. So, you log on, using the secure credentials, and double-security verification. Hmmm. That's odd. The balance shows $0 – must be a mistake, right? You quickly contact the help desk and to your shock, they confirm, yep – your account is $0. You later learn the entire balance has been transferred to an account at a well-established local bank but by the time you are able to contact the bank, the money has been transferred, again, overseas.

Such was the scenario for the plaintiff in the case of *Bartnett v. Abbott Labs, Alight Solution, LLC* (No. 20-cv-2127, N.D. Ill., April 3, 2020). In that case, the plaintiff sued the plan administrator, sponsor, service provider and recordkeeper, alleging they each failed to use the level of care, skill, prudence, and diligence required of an ERISA fiduciary to protect the plan assets, resulting in the theft of $245,000 (the entire balance) from her 401(k) account. In early 2021, the Court dismissed the claims against the sponsor and plan administrator, but did so "without prejudice," noting that the parties were engaged in limited discovery that might allow plaintiff to cure certain deficiencies and renew the actions against these defendants. The Court allowed the claims against the service provider/recordkeeper, Alight, to move forward, and ultimately the case settled in July 2021. The case has been noted as a wakeup call for all involved, including employers as plan sponsors, and participants.

According to the United States Department of Labor (DOL), as of 2018, there are 106 million defined contribution plan participants, covering estimated assets of $6.3 trillion. The Employee Retirement Income Security Act of 1974 (ERISA) includes standards applicable to most private retirement plans - such as 401(k) plans - and the standards are intended to protect the assets of plan participants. With the increased use of third-party service providers through outsourcing and the increased risks of cyberattacks and data breaches, the DOL recently responded to the increased calls for cybersecurity guidance. On April 14, 2021, the Employee Benefits Security Administration (EBSA) issued "*New Cybersecurity Guidance for Plan Sponsors, Plan Fiduciaries, Record-Keepers, Plan Participants*." In addition, the DOL has recently begun an audit initiative - sending requests to plan sponsors and service providers for the production of significant information, including all documentation relating to cybersecurity programs/policies and/or information security protocols and policies, evidence of cybersecurity training, and reports of any security breaches.

As an agency within the DOL with responsibility to assure the security of the retirement benefits of U.S. workers and their families, the EBSA notes that *without sufficient protections, these assets may be at risk from cybersecurity threats and that ERISA requires plan fiduciaries to take appropriate precautions to mitigate these risks*. The EBSA Guidance consists of three separate documents, as discussed in more detail below: (1) Cybersecurity Program Best Practices, (2) Tips for Hiring a Service Provider, and (3) Online Security Tips.

1. Cybersecurity Program Best Practices.

In the first portion of the Guidance, the EBSA recommends the use of service providers which, among other recommendations, (1) have a formal well-documented cybersecurity program; (2) ensure that any assets or data stored in the cloud or managed by the third-party service provider are subject to appropriate security reviews and independent security assessment; (3) encrypt sensitive data, stored and in transit; (4) have a reliable annual third-party audit of security controls and (5) have an effective business resiliency program addressing business continuity, disaster recovery and incident response.

In the Guidance, the EBSA specifically notes that it is "directed at plan sponsors and fiduciaries regulated by ERISA, and plan participants and beneficiaries," and furthermore, that "ERISA requires plan fiduciaries to take appropriate precautions to mitigate" internal and external cybersecurity threats.

Under ERISA, a "fiduciary" generally includes any person who (1) exercises any discretionary authority or control over plan management; (2) exercises any authority or control over the management or disposition of plan assets; (3) renders investment advice with respect to plan money or property for a fee or other compensation; or (4) has discretionary authority or responsibility for plan administration. 29 U.S.C. §1002 (21) (A).

Employer-sponsored retirement plans have one or more "named fiduciaries" with the authority to control

Continued on page 3

and manage the operation and administration of the plan. The named fiduciary is identified in the plan document or pursuant to a procedure specified in the plan. 29 U.S.C. §1102. A person who is not named as a fiduciary may nonetheless be a fiduciary with respect to a particular function they perform. Plan fiduciaries could include, for example, plan trustees, plan administrators, plan sponsors, record keepers, custodians, third-party administrators, or members of the investment committee.

2. Tips for Hiring a Service Provider.

In the second portion of the Guidance, the EBSA provides tips to help plan sponsors and fiduciaries prudently select a service provider with strong cybersecurity practice. Among the recommendations are: (1) asking about the service provider's information security standards, practices and policies, and audit results, and (2) comparing them to the industry standards adopted by other financial institutions. Specifically, the EBSA recommends the use of service providers that follow "a recognized standard for information security and use an outside auditor to review and validate cybersecurity."

In addition, sponsors of 401(k) and pension plans should ask their service provider how it validates its practices and what levels of security standards it has met and implemented. Sponsors should also ask their service provider whether it has experienced past security breaches, what happened, and how the service provider responded. EBSA further recommends asking the service provider if it has any insurance policies that would cover losses caused by cybersecurity breaches, identity theft breaches, misconduct by the service provider's own employees or contractors, or breaches caused by external threats, such as third-party hijacking of a plan participant's account. Finally, the EBSA recommends that plan sponsors ensure that when they contract with a service provider, that the contract requires "ongoing compliance with cybersecurity and information security standards" and to beware of contract provisions that "limit the service provider's responsibility for IT security breaches."

In the Tips document, the EBSA also suggests such contracts include terms that would enhance cybersecurity protection for the plan such as: information security reporting; clear provisions on the use and sharing of information and confidentiality; notification of cybersecurity breaches; compliance with records retention/destruction, privacy, and information security laws; and insurance coverage such as professional liability, errors and omissions liability insurance, cyber liability, and privacy breach insurance and/or fidelity bond/blanket crime coverage.

3. Online Security Tips.

In the third document included in the Guidance, the EBSA makes several online security tips which will sound familiar to many. To reduce risks of online security, the EBSA recommends that plan participants: routinely monitor their online accounts; use strong and unique passwords; use multifactor authentication; keep personal contact information current; close or delete unused accounts; be wary of using free Wi-Fi such as in airports, hotels or coffee shops; beware of phishing attacks and learn how to recognize phishing attacks; use antivirus software and keep the software current and updated; and know how to report identity theft and cybersecurity incidents to the FBI/Department of Homeland Security.

While all these steps sound familiar to many readers having been publicized in numerous articles and commonly recommended, with the issuance of the EBSA Guidance, plan fiduciaries may have increased responsibility to reiterate these recommendations in participant educational materials, and/or training.

The EBSA Guidance may be accessed here: https://www.dol.gov/agencies/ebsa/key-topics/retirement-benefits/cybersecurity

While this Guidance does not have the full force of law, if a plan sponsor or other fiduciary fails to respond adequately to the Guidance, it could arguably increase the potential liability of plan sponsors or fiduciaries in the event of cybersecurity breaches. Employers who sponsor retirement plans should act now to review and document their own internal cybersecurity programs. Plan sponsors should also act to verify that their service providers are in compliance with the Guidance and have strong cybersecurity policies that serve to protect plan participants. Employers should also consult with their employment counsel regarding the specifics of the Guidance, and any of the attorneys at Wimberly Lawson may assist in this regard.

who identified as female by "Ms." or female pronouns and vice versa. This became an issue in 2016 when the university emailed all faculty that they were now required to refer to students "by their 'preferred pronoun[s]'." When he approached his Department Chair about possible accommodations given his religious beliefs, Professor Meriwether was told there were no exceptions. During the conversation, the Department Chair was derisive of the professor's religious beliefs and even professed that the "presence of religion in higher education is counterproductive."

Two years later, Professor Meriwether was teaching his Political Philosophy class when he responded to a student's question with "Yes, sir." After class, the student approached the professor "demanding" to be addressed as female because the student identified as a woman. Professor Meriwether declined, believing that to do so would be acknowledging a falsity, namely that a male student could become female. The professor recommended a compromise of referring to the student by the student's last name. The student objected, making several complaints - to which the university responded by demanding that Professor Meriwether use the student's preferred pronouns or eliminate all sex-based pronouns and titles (an impossibility). At one point during the saga, the professor offered to use the student's preferred pronouns provided he be permitted to place on his syllabus an explanation that he was doing so under protest and stating his views on the subject. The school refused this latter accommodation claiming that should the professor state his views on the subject, his expression would be in violation of the university's anti-discrimination policy.

Although the student continued to participate in class without incident and ultimately received a high grade, the university instituted an investigation, which was viewed as highly flawed by the Court, and ultimately issued a formal reprimand to the professor. He was told that any further violation would result in further disciplinary action, up to and including termination. His appeal was summarily dismissed with the university refusing to even consider his religious views on the matter, but instead "equating his views to those of a hypothetical racist or sexist."

The Sixth Circuit reversed the dismissal of the professor's constitutional claims asserting violations of free speech and of both the Free Exercise and Establishment of Religion clauses of the First Amendment. The Court noted there was no basis to find that Professor Meriwether's actions created a hostile educational environment. The Court explained:

> "When the university demanded that Meriwether refer to Doe using female pronouns, Meriwether proposed a compromise: He would call on Doe using Doe's last name alone. That seemed like a win-win. Meriwether would not have to violate his religious beliefs, and Doe would not be referred to using propounds Doe finds offensive. Thus, on the allegations in this complaint, it is hard to see how this would have 'create[d] a hostile learning environment that ultimately thwarts the academic process.'"

It is this observation that will likely have significance for private employers.

The EEOC has noted that while Title VII requires employers to accommodate employee's religious practices and beliefs, employers are not required "to accommodate religious expression that creates, or threatens to create, a hostile work environment." Employers certainly should take steps to ensure that no employee is harassed or mistreated based on sexual orientation, gender identity, or religious beliefs on these or other matters. While it is not always easy to balance the interests of an employee with a gender identity inconsistent with the individual's biological sex and another person's sincerely held religious beliefs concerning human sexuality, it can be done.

The *Meriwether* court points out that it is not either/or but can be both/and. There was no disputing that requiring Professor Meriwether to affirm that a person can change sexes through the manner and words used to address the person would violate his religious beliefs. It was also clear that the student had a right to fully participate in the educational program. The court found that both interests were protected using Professor Meriwether's proposed compromise, even though not to the student's full satisfaction.

Employers may be called upon to address similar issues in the workplace. In doing so, the starting point is that all employees deserve to be treated with dignity and respect and that there should be a compromise that everyone can live with, even if one or both is not entirely happy with the outcome. This may vary depending on the work environment, the level and frequency of interaction between the employees, and frankly the willingness of the employees to see and respect the other's point of view.

While the Supreme Court declined to address issues such as pronouns, dress codes, or restroom and locker room access in its *Bostock* decision, employers will be forced to address those issues. The EEOC has concluded that an employee's professed gender identity is dispositive of all of these questions without regard to the thoughts, feelings, or religious convictions of any other employee. The courts, however, will continue to wrestle with these questions in light of Bostock. More immediately, employers will first have to address them in their workplaces, and will hopefully do so in a manner that seeks to uphold and respect the dignity of all of their employees.