SPECIAL ADVERTISING FEATURE TO COLUMBUS BUSINESS FIRST

COLUMBUS BAR ASSOCIATION

Legal Connections

CBA www.cbalaw.org

LEGAL EXPERTISE FOR THE BUSINESS COMMUNITY

NOVEMBER 13, 2020

Check out our Community Conversations on Inclusive Democracy: Elections & Voting at cbalaw.org

Jill Snitcher McQuain, Esq.
Executive Director
jill@cbalaw.org

PROTECTING YOUR PRIVACY BY SAVING YOUR TRASH: HOW LAW ENFORCEMENT CAN OBTAIN YOUR DNA PROFILE FROM YOUR DISCARDED COFFEE LID—WITHOUT A WARRANT

In the context of the Fourth Amendment, courts have generally held that a person does not have a reasonable expectation of privacy in an item that they have voluntarily abandoned by, for instance, throwing the item in the trash or leaving footprints behind at the scene of a crime. If an item is deemed to be "voluntarily abandoned," most courts will find that law enforcement is not required to obtain a search warrant in order to search and/or seize that item.

Law enforcement has relied upon that doctrine to bypass the search warrant requirement of the Fourth Amendment before collecting, extracting, sequencing and analyzing unavoidably shed DNA material that has been left behind on voluntarily abandoned objects such as cigarette butts or soda cans. However, given the breadth of sensitive information that may be learned about a person just from their DNA, the privacy interests in unavoidably shed DNA is of

HOLLY CLINE, ESQ.,
The Tyack Law Firm Co., LPA

JAMES TYACK, ESQ.,
The Tyack Law Firm Co., LPA

a different magnitude than the interest in physical items placed in the trash, footprints or fingerprints. To be sure, courts have long recognized that a person has a legitimate and reasonable expectation of privacy in their DNA material and all the information it can reveal.

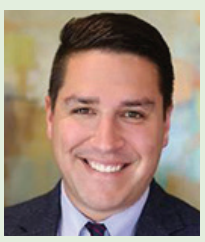
Moreover, while it may be common knowledge that physical items left in public are readily accessible to law enforcement, it is not common knowledge—or even reasonably foreseeable—that any member of the public or law enforcement would seize a physical item and send that item to a lab to have DNA material extracted, sequenced and profiled. And, unlike physical items, the contents of DNA are never actually visible to the public, as sophisticated technology is required to extract DNA material from a physical object. People do not voluntarily assume the risk of "turning over a comprehensive dossier" of their private genetic information because there is simply no reasonable way for a person to avoid leaving behind a constant trail of their DNA material as they move about in the world.

Thus, even if law enforcement's warrantless seizure of a physical item voluntarily abandoned is lawful, such logic cannot—and should not—be extended to the DNA material that has been unavoidably and inadvertently shed onto that object. Once an item believed to contain DNA material is seized and secured by law enforcement, no exception to the warrant requirement of the Fourth Amendment to the United States Constitution and/or Article I, Section 14 of the Ohio Constitution applies to the warrantless extraction, sequencing, analyzing, profiling, and comparison of the DNA material contained thereon. As the U.S. Supreme Court has repeatedly cautioned, "[a]s technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, [courts must seek] to 'assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" Courts must therefore avoid "mechanically applying" older doctrines to new types of searches made possible by modern technologies, which can reveal myriad "privacies of life" in ways that are "remarkably easy, cheap, and efficient compared to traditional investigative tools." ■

JOIN US ON NOV. 18 FOR OUR ANNUAL EASTMAN & SMITH EMPLOYMENT LAW UPDATE, ALL ABOUT EMPLOYMENT LAW IN THE TIME OF COVID-19: CBALAW.ORG

CONSIDER DIGITAL ASSETS IN PLANNING YOUR ESTATE:

As our level of reliance on digital mediums in our daily lives increases, the need for fiduciaries to access digital assets is more important now than ever. Under Ohio's Revised Uniform Fiduciary Access to Digital Assets Act (ORC §2137), a fiduciary has the general authority to access and use the digital assets of: (1) a principal under a power of attorney, (2) a decedent under a last will and testament, (3) a trust under the terms of such trust and (4) a ward under guardianship.



ANDREW MARVIN, ESQ.,
Carlile Patchen & Murphy LLP

Digital assets are assets existing in electronic format that have an associated right of use. Digital assets often carry sentimental and/or financial value and contain important personal information (e.g., an email account containing electronic bank statements or a cloud storage account containing photographs and important documents in electronic format).

Though it is important to appoint fiduciaries that can access digital assets, it is equally important that such fiduciaries have the ability to access, manage and terminate digital assets without unnecessary burden. It is wise to provide a fiduciary with an inventory of digital assets and associated passwords and/or login information. Having such information in a safe location along with other estate planning documents will give a fiduciary a more efficient means of dealing with digital assets.

Certain companies are now providing their users the option to decide who may access digital assets upon a user's incapacitation or death (e.g., Facebook allows for designation of a "legacy contact" and Google allows for designation of an individual to access an account that has been inactive for a designated period of time). Though this practice by companies is welcomed, a complete estate plan should include a strategy for dealing with digital assets upon incapacitation or death. In the absence of such plan, digital assets may be permanently inaccessible or a court order may be required to allow access to the assets. As our lives continue to be less dependent on tangible items, so too should our estate plans. ■