No. 12-1776

In the Supreme Court of the United States

UNITED STATES OF AMERICA,

Petitioner,

v.

MARK ZUCKERMAN,

Respondent.

On Writ of Certiorari to
the United States Court of Appeals
for the Thirteenth Circuit

BRIEF FOR THE RESPONDENT

TEAM 5
JOSEPH HOGUE & ELLORA ROY
COUNSEL FOR THE RESPONDENT

QUESTIONS PRESENTED

I. This Court has held that it is reasonable, under the Fourth Amendment, to perform a timely, warrantless search of an arrestee's person for the purpose of preserving evidence. The Evans DNA Collection Act authorizes law enforcement officials to perform a warrantless extraction of DNA from a pre-conviction arrestee regardless of relevance of DNA to the criminal investigation. Does this statutory narrowing of the Fourth Amendment cause the Evans DNA Collection Act to be facially invalid?

II. This Court has used a totality-of-the-circumstances test when assessing the constitutionality of a warrantless search. Relying only on the Evans DNA Collection Act and with no showing of probable cause, a court ordered Mark Zuckerman, a pre-conviction arrestee, to provide a DNA sample. Did Mr. Zuckerman's specific privacy interest in his bodily integrity outweigh the government's general interest in law enforcement and cause the Evans DNA Collection Act to be invalid as applied to him?

III. This Court employs the two-pronged *Katz* privacy test to determine whether a privacy interest should be protected by the Fourth Amendment. Mr. Zuckerman, a pre-conviction arrestee, clearly indicated that his Facepoke information was private by not disclosing his password, making use of built-in privacy features, and limiting his number of Facepoke friends. Is society prepared to recognize Mr. Zuckerman's privacy interest in private information available on his Facepoke page as reasonable?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases from the Supreme Court of the United States:

Other Materials:

OPINIONS BELOW

The unreported opinion of the United States Court of Appeals for the Thirteenth Circuit is available in the Transcript of the Record at pages 12-23. As relevant for the current matter, the court of appeals reversed Mr. Zuckerman's convictions, found the Evans DNA Collection Act to be unconstitutional as applied to Mr. Zuckerman, and directed the district court to order Mr. Zuckerman's DNA sample destroyed and removed from the Evans DNA database.

The unreported opinion of the United States District Court for the Eastern District of Evans is available in the Transcript of the Record at pages 4-10. As relevant for the current matter, the district court entered judgment on the jury verdict finding Mr. Zuckerman guilty of assault on a federal officer and embezzlement. Additionally, the district court found the Evans DNA Collection Act to be constitutional.

JURISDICTION

The judgment of the court of appeals was entered on September 5, 2012. The petition for a writ of certiorari was granted on October 1, 2012. The jurisdiction of this Court rests on 28 U.S.C. 1254(1).

STATUTORY AND REGULATORY PROVISIONS INVOLVED

The following two constitutional provisions are particularly relevant for this matter: U.S. Const. art. VI, cl. 2; and U.S. Const. amend. IV.

The following three statutes are particularly relevant for this matter: 18 U.S.C. § 111 (2012), 18 U.S.C. § 656 (2012), and Evans Code 2010, §337.

Pertinent text of the statutory and regulatory provisions, with the exception of the Evans Code which is unavailable, is provided in Appendix A.

STANDARD OF REVIEW

Questions pertaining to the application of constitutional law are reviewed de novo. *See Pierce v. Underwood*, 487 U.S. 552, 558 (1988). In this matter, the Court has identified two issues relating to the applicability of the Fourth Amendment of the United States Constitution to facts involving emerging technologies. As such, the Court should use a de novo standard of review for both issues.

STATEMENT OF THE CASE

I. Introduction

Mark Zuckerman, a man with no prior criminal record, was arrested following a physical confrontation with a federal officer. As part of the criminal investigation, the police performed two warrantless searches that were irrelevant to the alleged assault and could not be supported by

reasonable suspicion, let alone probable cause. First, a DNA sample was forcibly extracted from Mr. Zuckerman after he refused to willingly provide one. Second, an investigator used coercion to gain access to Mr. Zuckerman's private Facepoke account after attempts to access the account through public channels were unsuccessful and a noncoercive request for access to the account was denied.

II. DNA Extraction

The Evans DNA Collection Act authorizes law enforcement authorities to collect DNA samples from individuals arrested for any crime involving violence, regardless of whether DNA evidence is needed to investigate the crime at hand or identify the suspect. Evans Code 2010, § 337. The codified legislative purposes for this broadly-worded statute are to assist law enforcement in carrying out their duties, to solve past crimes, and to prevent future criminal activity. Evans Code 2010, § 337.1. Once collected, DNA material is stored in the Evans DNA Database. (R. at 9.)

Pursuant to the Evans DNA Collection Act, investigators attempted to take a DNA sample while Mr. Zuckerman was in police custody following his aforementioned arrest; however, Mr. Zuckerman refused to consent to the sample. (R. at 8.) Following his refusal, the government brought a motion before the United States District Court for the Eastern District of Evans seeking authorization to proceed with the sample. (R. at 8.) The motion was granted, and the investigators proceeded to forcibly extract a DNA sample from Mr. Zuckerman using a cheek buccal swab. (R. at 13.)

Following the extraction, the DNA sample was forwarded to the Evans State Police Crime Lab where it was added to the Evans DNA Database. (R. at 13.) At the time of the extraction, the investigators were aware that Mr. Zuckerman was a person-of-interest in a sexual

assault investigation, but he had not been charged in that matter. (R. at 8.) To date, Mr. Zuckerman still has not been charged for any crimes due to his DNA sample, and the DNA sample was not relevant evidence in the two crimes for which he was indicted in this matter. (R. at 8.)

III. Search of Facepoke Account

As a condition of his employment at Evans Software Technologies, Inc. ("EST"), Mr. Zuckerman was required to sign an agreement to provide his Facepoke password to EST. (R. at 5.) Per its own written policy, EST recognized the confidentiality of Facepoke passwords and only authorized itself to use the passwords to investigate suspected use of Facepoke against EST or its customers. (R. at 5.) Mr. Zuckerman initially objected to providing his password "as a matter of principle" (R. at 17), but he eventually relented in order to be hired (R. at 5).

Approximately nine months after Mr. Zuckerman began his employment, the president of EST began to suspect that Mr. Zuckerman was not competently performing his duties. (R. at 5.) Despite not suspecting Mr. Zuckerman of wrongdoing, the president ordered that an "Employee Review Procedure" be performed for Mr. Zuckerman. (R. at 18.) During the Employee Review Procedure, it was discovered that Mr. Zuckerman's Facepoke password did not work. (R. at 5.) When Mr. Zuckerman refused to provide the correct password, EST terminated him. (R. at 5.) Following his termination, Mr. Zuckerman was involved in a physical confrontation with a federal officer attempting to escort him from the building which led to his subsequent arrest. (R. at 5.)

During investigation into the matter, police investigators attempted to access Mr. Zuckerman's Facepoke account but were unsuccessful due to his privacy settings. (R. at 18.) Rather than respect Mr. Zuckerman's clear desire for privacy, a police investigator reached out to

one of Mr. Zuckerman's friends to gather more information regarding Mr. Zuckerman's use of Facepoke. (R. at 6.) During this interview, it was discovered that Mr. Zuckerman and the interviewee were Facepoke "friends," so the investigator requested Mr. Zuckerman's friend to allow the police investigator to review Mr. Zuckerman's Facepoke page. (R. at 6.) Mr. Zuckerman's friend refused until the police officer informed him that he would seek a subpoena for the access. (R. at 6.)

In reviewing Mr. Zuckerman's Facepoke page, it was discovered that Mr. Zuckerman had made an innocuous post the month after he was hired, visible only to his Facepoke friends, regarding the lax financial controls at EST. (R. at 19.) After further investigation revealed that approximately $232,000 was missing from EST, Mr. Zuckerman's Facepoke post served as the primary evidence supporting his embezzlement charge. (R. at 19.)

IV. Procedural History

Mr. Zuckerman was indicted for assaulting an FBI officer and embezzlement. (R. at 2.). Subsequently, Mr. Zuckerman moved to suppress the evidence secured in violation of his Fourth Amendment rights, specifically the DNA swab sample and information from his Facepoke page (R. at 3), but his motion was denied by the United States Court for the Eastern District of Evans (R. at 4). Following a trial, the district court entered judgment on a jury verdict finding Mr. Zuckerman guilty of both charges of the indictment and sentenced him to five years in a federal penitentiary. (R. at 7.) As part of its reasoning, the district court noted that Mr. Zuckerman "had no expectation of privacy" in his Facepoke page. (R. at 7.) Additionally, the district court revisited its prior denial of Mr. Zuckerman's motion to suppress the DNA evidence and, in a finding collateral to his assault and embezzlement charges, found the Evans DNA Collection Act

constitutional, in part by analogizing DNA sampling to traditional fingerprinting. (R. at 10.) Mr. Zuckerman appealed the court's judgment and sentence. (R. at 11.)

The United States Court of Appeals for the Thirteenth Circuit reversed Mr. Zuckerman's convictions and directed the district court to enter an order for his DNA sample to be destroyed and removed from the Evans DNA database. (R. at 12.) With regard to Mr. Zuckerman's convictions, the court of appeals reasoned that Mr. Zuckerman had a "legitimate expectation of privacy in the contents of his Facepoke page" and that "society recognizes that expectation as reasonable." (R. at 21.) Further, the court of appeals reasoned that based on a "totality of the circumstances," Mr. Zuckerman's interests in the privacy of his DNA "outweigh[ed]" the government's general interests in collecting DNA and found the Evans DNA Collection Act unconstitutional as it applied to Mr. Zuckerman. (R. at 16.) This Court granted certiorari. (R. at 24.)

SUMMARY OF ARGUMENT

Two large public policy issues underlie this case: (1) how much privacy from warrantless searches must be established due to advances in science and technology such as one's DNA and private social media accounts; and (2) what diminished expectation of privacy, if any, should one expect as a pre-conviction arrestee.[1]

[1] Since the issues identified by this Court for briefing did not specifically indicate a challenge to the reversal of Mr. Zuckerman's two convictions, this brief does not explore either of the federal statutes on which the convictions were based. However, a plain reading of each federal statute makes clear that neither conviction could survive even a plain-error standard of review, as the Record contains evidence disproving key elements of each alleged crime. The assault conviction must fail because the federal officer was not engaged in performance of his official duties at the time of the assault (R. at 5) as required by the federal statute, 18 U.S.C. § 111(a)(1) (2012). The embezzlement conviction must fail because Evans Software Technologies, Inc., is not a bank or similar organization (R. at 5) as required by the federal statute, 18 U.S.C. § 656 (2012).

This Court is often tasked with evaluating the scope of the Fourth Amendment in light of advances in science and technology. Since, with most disputes, a subjective expectation of privacy has been expressed, the cases often turn on whether, objectively, society is prepared to recognize an expectation of privacy as being reasonable. For both of the matters before this Court in this case, society finds it reasonable to view the information as private. It does not take a medical degree to understand the massive amounts of personal information contained in DNA (e.g., DNA testing to identify risk-factors for genetic diseases is becoming more commonplace and popular television shows highlight uses of DNA evidence in criminal investigation). Additionally, the "social media age" has made society more aware of the difference between things shared with the world and things shared only with a private group (of friends, colleagues, business partners, vendors, etc.).

Further, while this Court has considered what diminution in rights, if any, a pre-conviction arrestee should expect, it has not encroached upon the arrestee's Fourth Amendment rights for any purposes other than officer safety, preservation of evidence, or rudimentary identification procedures. Nothing in the facts of this case suggest that Mr. Zuckerman's status as a pre-conviction arrestee, a man presumed innocent until proven guilty, should have allowed for a warrantless DNA extraction or a warrantless search of his private Facepoke account.

ARGUMENT

I. The Evans DNA Collection Act is facially invalid because no set of circumstances exists where it would comply with the Fourth Amendment's protection of all people from unreasonable searches of their persons. It is never reasonable to extract a DNA sample from an arrestee without a showing of probable cause supporting the need for a DNA sample.

Mr. Zuckerman's Fourth Amendment right to be secure in his person against unreasonable searches was violated when police investigators, pursuant to a court order not supported by probable cause, extracted a DNA sample using a buccal swab. This Court has clearly established guidelines for reasonableness with regard to warrantless searches, and it has never held that it is reasonable to conduct a warrantless search on a pre-conviction arrestee without a showing of probable cause. While proponents of pre-conviction DNA sampling of arrestees argue that it is no different than fingerprinting, in actuality, fundamental differences exist between a fingerprint and a DNA sample causing such an analogy to be misplaced.

A. A person has a constitutionally-protected right to be free from unreasonable bodily searches, and this Court has clearly developed the guidelines of reasonableness.

As relevant for the matter at hand, the Fourth Amendment states: "The right of the people to be secure in their persons . . . against unreasonable searches . . . shall not be violated[.]" U.S. Const. amend. IV. It is also worth noting that this Court has recognized that the Fourth Amendment also protects United States citizens from unreasonable searches by state government officials, thus foreclosing any loopholes that could be exploited by collaboration of state and federal investigators. *See Mapp v. Ohio*, 367 U.S. 643, 655 (1961) (extending prohibition against using evidence obtained in violation of the Fourth Amendment to state courts by virtue of the Due Process Clause of the Fourteenth Amendment).

With the constitutional protection of the Fourth Amendment in mind, it is important to also consider another aspect of the Constitution. As relevant for this matter, the Supremacy Clause states: "This Constitution . . . shall be the supreme law of the land; and the judges in every state shall be bound thereby, anything in the constitution or laws of any state to the contrary notwithstanding." U.S. Const. art. VI, cl. 2. Reading the Fourth Amendment and

Supremacy Clause side-by-side, it is clear that a state statute cannot allow behavior by law enforcement officials that is contrary to the protections of the U.S. Constitution. As such, to determine the constitutionality of the Evans DNA Collection Act, an analysis of this Court's reasonableness guidelines is warranted.

The easiest way to avoid an unconstitutional search is to simply obtain a search warrant. *See Arizona v. Gant*, 556 U.S. 332, 338 (2009) ("[O]ur analysis begins, as it should in every case addressing the reasonableness of a warrantless search, with the basic rule that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.'") (citation omitted). With regard to warrants, this Court has held that execution of a search pursuant to a validly obtained warrant does not violate the Fourth Amendment. *L.A. Cnty., Cal. v. Rettele*, 550 U.S. 609, 616 (2007). The importance of warrants is embedded in the Fourth Amendment, which in relevant part states: "[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched[.]" U.S. Const. amend. IV. A strict reading of this clause from the Fourth Amendment calls into question a state's ability to remove the element of probable cause from a reasonable search, since warrants are the best example of a reasonable search, and a warrant must necessarily be based upon probable cause. Since the Evans DNA Collection Act purports to bypass both the warrant and probable cause requirements, building an argument for reasonableness becomes challenging, and ultimately, not possible.

B. A buccal swab for DNA is a search as contemplated by the Fourth Amendment, so it must comply with guidelines laid out by this Court to be reasonable.

This Court has held that the government taking of bodily fluids is a search for Fourth Amendment purposes. *See Ferguson v. City of Charleston*, 532 U.S. 67, 77 n.9 (2001) (noting that the Court has routinely treated urine screens as Fourth Amendment searches)*; Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 618 (1989) (distinguishing taking of blood samples and taking of urine samples, but finding both to be searches contemplated by the Fourth Amendment). In *Skinner*, this Court was charged with assessing the constitutionality of railroad regulations designed to curb drug abuse by railroad employees. *Id.* at 606. Prior to reaching the merits of the constitutional challenge to the regulations, this Court first analyzed whether both blood draws and urine samples were even covered by the Fourth Amendment. *Id.* at 616-17. Without much analysis, this Court relied on its precedents to hold that blood draws do implicate the Fourth Amendment. *Id.* at 616 (quoting *Schmerber v. California*, 384 U.S. 757, 767-768 (1966)) (noting that the Court has long recognized "compelled intrusio[n]" for blood samples is a search contemplated by the Fourth Amendment). With regard to the urine sample, the Court considered the degree of intrusion, the amount of information contained in a urine sample, and society's expectation of privacy regarding urine. *Id.* at 617. Weighing these factors, this Court concluded that a urine sample, too, was a search contemplated by the Fourth Amendment, despite its minimum intrusion, because extensive medical information is available in a urine sample and society has long recognized as reasonable an expectation of privacy in one's urine. *Id.* at 617.

Applying a similar analysis to that used in *Skinner*, a DNA buccal swab is clearly a search that implicates the protections of the Fourth Amendment. While the degree of intrusion is certainly less than a blood draw, it is definitely more intrusive than a urine screen (an entirely external process) since it involves a swab inside the mouth. Additionally, if the amount of

information available in a urine sample is troubling to the Court, the amount of information available from a DNA sample alone should put a DNA buccal swab under the protection of the Fourth Amendment. Finally, and perhaps most importantly, applying the *Katz* privacy test, which has been favored by this Court to assess a person's "reasonable expectation of privacy," *see United States v. Jones*, 132 S.Ct. 945, 950 (2012), any pre-conviction arrestee would have an immense privacy interest in their DNA, and society views that privacy interest as being reasonable, *see Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"). Since all of the factors favor a DNA buccal swab being a search that implicates the Fourth Amendment, law enforcement officials must either obtain a warrant or demonstrate that the DNA buccal swab fits into an exception recognized by this Court for a DNA buccal swab to be constitutional.

C. A person's status as an arrestee for a violent crime does not diminish his privacy rights to the point that a constitutional search can be conducted without probable cause.

Having established the authority of the Fourth Amendment and the applicability of the Fourth Amendment to the behavior in question, the burden is on the government to establish the reasonableness of the search. *See United States v. Jeffers*, 342 U.S. 48, 51 (1951) ("[T]he burden is on those seeking the exemption to show the need for [lack of adherence to judicial processes].") (citation omitted). The government may consider the following two arguments to support a reduction in privacy rights of pre-conviction arrestees: (1) a warrantless search is valid using the Search-Incident-to-Custodial-Arrest ("SICA") exception to the warrant requirement; or (2) a warrantless search of pre-conviction arrestees serves a special need other than law

enforcement, so it is valid using the Special-Needs exception to the warrant requirement. A closer examination of each of these exceptions to the warrant requirement will make clear that neither is applicable to pre-conviction arrestees.

The SICA exception to the warrant requirement was recently clarified by this Court in *Arizona v. Gant*, 556 U.S. 332 (2009). In *Gant*, this Court explains the rationale supporting the reasonableness of the custodial-arrest exception as "deriving from interests in officer safety and evidence preservation." *Id.* at 338 (citing *United States v. Robinson*, 414 U.S. 218, 230–234 (1973)); *see also United States v. Edwards*, 415 U.S. 800, 802-03 (1974) ("[W]arrantless searches incident to custodial arrests . . . ha[ve] traditionally been justified by the reasonableness of searching for weapons, instruments of escape, and evidence of crime when a person is taken into official custody and lawfully detained.") (citations omitted). In closing its decision in *Gant*, the Court notes that searching an arrestee's vehicle, incident to the arrest, requires a warrant unless one of three things is true: (1) the arrestee is within "reaching distance" of the passenger compartment prior to the search; (2) "it is reasonable to believe the vehicle contains evidence of the *offense of the arrest*"; or (3) some other exception to the warrant requirement exists. *Gant*, 556 U.S. at 351 (emphasis added).

Applying the SICA exception to the warrant requirement as a constitutional justification for a warrantless DNA extraction for all pre-conviction arrestees ignores the purpose of this exception. DNA extraction does not implicate officer safety or preservation of evidence, rationale discussed in *Edwards* and reiterated in *Gant*, because officer safety is not called into question simply because an arrestee has DNA (every human does) and there is no way that an arrestee could do something to hide or destroy his DNA should it be determined that the DNA is relevant to the crime committed. Just as a police officer must attain a warrant to search an

arrestee's vehicle, absent fitting into the three narrow exceptions discussed in *Gant*, it stands to reason that an officer must attain a warrant for the far more intrusive search of a DNA extraction.

The applicability of a Special-Needs exception can be disposed of much more easily. In order to fit into one of the narrow Special-Needs exceptions, this Court requires a showing that there is something other than a general law enforcement purpose for the search. *See Ferguson v. City of Charleston*, 532 U.S. 67, 74 n.7 (2001) (summarizing the Special-Needs exception as searches justified by needs other than the normal need for law enforcement). As such, the Evans DNA Collection Act fails on its face because the express purpose stated in the act is to assist law enforcement personnel with carrying out their duties. (R. at 14 (citing Evans Code 2010, §337.1).) Additionally, even if the government were to argue, notwithstanding the express statement of purpose in the statute, that there is a special need to monitor pre-conviction arrestees, and that pre-conviction arrestees have a reduced expectation of privacy, this Court would be required to expand the Special-Needs doctrine because the exception has not previously been applied to pre-conviction arrestees. *See Samson v. California*, 547 U.S. 843, 846 (2006) (allowing suspicionless search of a parolee); *United States v. Knights*, 534 U.S. 112, 122 (2001) (allowing warrantless searches of probationers based upon a reasonable suspicion of wrongdoing); *Hudson v. Palmer*, 468 U.S. 517, 526-28 (1984) (holding that inmates have no right to privacy in their cells or protection from unreasonable seizures of their personal effects); Brian Gallini, *Step Out of the Car*, 62 Ark. L. Rev. 475, 494 (2009) (summarizing the six categories of Special-Needs exceptions unrelated to a reduced expectation of privacy for prior conviction). *But see United States v. Mitchell*, 652 F.3d 387 (3d Cir. 2011) (holding federal statute allowing suspicionless DNA extraction of pre-conviction arrestee constitutional based, in part, on a diminished expectation of privacy); *Anderson v. Commonwealth*, 650 S.E.2d 702, 706

(Va. 2007) (holding state statute allowing supicionless DNA extraction of pre-conviction arrestee constitutional by analogizing the extraction to fingerprinting).

Since neither the SICA exception nor the Special-Needs exception applies, neither can properly be used as justification for the government to perform a warrantless extraction of DNA from a pre-conviction arrestee.

D. DNA samples are so fundamentally different from fingerprints that the two cannot be construed as analogous under the Fourth Amendment.

The government may try to avoid subjecting DNA sampling to Fourth Amendment scrutiny by analogizing the collection of DNA samples to fingerprinting. This argument has three flaws that must be explored. First, fingerprinting of arrestees, while socially accepted, has never been subjected to a Fourth Amendment analysis by this Court. Second, while fingerprinting and DNA sampling both may be used for identification, DNA samples contain so much additional information that the two should not be analogized. Last, even assuming arguendo that fingerprinting of arrestees would pass this Court's Fourth Amendment scrutiny and that DNA sampling is merely a technological progression of fingerprinting, DNA sampling of arrestees must still be subjected to its own Fourth Amendment scrutiny.

While issues regarding fingerprinting of arrestees have been discussed by this Court, the Court has never ruled on the direct issues. *See, e.g.*, *Hayes v. Florida*, 470 U.S. 811, 815-17 (1985) (discussing, in dicta, that this Court's precedent may permit fingerprinting based only on reasonable belief that fingerprinting may absolve or incriminate a suspect); *Davis v. Mississippi*, 394 U.S. 721, 728 (1969) (holding that fingerprints obtained without probable cause or consent were inadmissible). Assuming that fingerprinting of arrestees did come under judicial scrutiny by this Court, it would most likely pass because there is no longer a societal expectation of

privacy to one's fingerprint upon arrest. *See* Bureau of Justice Statistics, U.S. Dep't of Justice, Public Attitudes Toward Uses of Criminal History Information, 43 (2001), *available at* http://bjs.ojp.usdoj.gov/content/pub/pdf/pauchi.pdf (finding that 94 percent of adults find the fingerprinting of arrestees to be either "very acceptable" or "somewhat acceptable"). However, simply because fingerprinting of arrestees has become commonplace, and thus societally accepted, does not mean that it would have passed a Fourth Amendment analysis when it first came into use and began shaping societal expectations.

It is also very important to consider that fingerprints are fundamentally different than DNA samples. One need look no further than the fact that hundreds of convicted prisoners have been freed based on DNA evidence, *see* Molly Hennessy-Fiske, *DNA Evidence Exonerates 300th Prisoner Nationwide*, L.A. Times, Oct. 1, 2012, at A5, despite the wide availability of fingerprint evidence, to recognize that DNA must be fundamentally different than fingerprints.

Another way to highlight differences is to consider use in a criminal investigation. While the usefulness of fingerprinting stops at identification, DNA can also be used to develop a profile of an unknown suspect, including appearance, gender, medical conditions, family, and behavioral characteristics. *See* Bert-Jaap Koops & Maurice Schellekens, *Forensic DNA Phenotyping: Regulatory Issues*, 9 Colum. Sci. & Tech. L. Rev. 158, 161-65 (2008) (discussing use of DNA to compose suspect profiles). An appropriate analogy might be the relationship between typewriters and computers: both can be used to type words onto paper, but typing words onto paper is really only a capability, not the purpose, of the computer. Extending that analogy to DNA and fingerprints: both DNA and fingerprints can be used for identification, but identification is only a capability of DNA, while it is the purpose of fingerprints. And, it is those

larger capabilities, known and unknown, that should cause suspicionless DNA sampling to be heavily scrutinized by this Court.

Finally, even if one was to accept that DNA sampling is simply a technological progression of fingerprinting, this does nothing to excuse the practice from Fourth Amendment scrutiny. Many of this Court's holdings with regard to the Fourth Amendment concern appropriate integration of new technologies into criminal investigation. *See United States v. Jones*, 132 S.Ct. 945, 949 (2012) (determining constitutionality of warrantless use of GPS device); *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (determining constitutionality of warrantless use of "sense-enhancing" technology); *California v. Ciraolo*, 476 U.S. 207, 214 (1986) (determining constitutionality of warrantless aerial observation). Justice Brennan adequately summarized this Court's view of the Fourth Amendment when he noted: "The Constitution would be an utterly impractical instrument of contemporary government if it were deemed to reach only problems familiar to the technology of the eighteenth century[.]" *Lopez v. United States*, 373 U.S. 427, 459 (1963) (Brennan, J., dissenting). This Court has never simply given a "free pass" to a new criminal investigative technique because it appeared to be nothing more than a technological progression on an accepted technique.

II. The Evans DNA Collection Act is invalid as applied to Mr. Zuckerman because Mr. Zuckerman's reasonable expectation of privacy in his DNA was not outweighed by the state's general interest in assisting law enforcement personnel with their public responsibilities. It was unreasonable to extract a DNA sample from Mr. Zuckerman without a warrant based on a showing of probable cause.

Even if the Evans DNA Collection Act is not facially invalid, its application to Mr. Zuckerman violated his Fourth Amendment rights. For warrantless searches, this Court uses a totality-of-the-circumstances test to assess reasonableness. Since Mr. Zuckerman's privacy

interests in his DNA clearly outweigh the government's general interest in law enforcement, a warrantless extraction of Mr. Zuckerman's DNA is unreasonable and violates the Fourth Amendment. Additionally, as the government's use of Mr. Zuckerman's DNA is a harm that is ongoing (and possibly increasing) and this Court can redress the injury by affirming the order of the lower court to destroy the DNA sample and remove the DNA sample from the Evans DNA Database, this matter can and should be decided by this Court.

A. Using this Court's totality-of-the-circumstances test, Mr. Zuckerman's privacy interest in his DNA outweighed the state's general interest in law enforcement.

This Court uses a totality-of-the-circumstances test when determining the constitutionality of a Fourth Amendment search. *See Samson v. California*, 547 U.S. 843, 848 (2006) (quoting *United States v. Knights*, 534 U.S. 112, 118 (2001)); *Ohio v. Robinette*, 519 U.S. 33, 39 (1996) (noting that "reasonableness" is the "touchstone of the Fourth Amendment" and that reasonableness is measured by the "totality of the circumstances"). In examining the totality of the circumstances, this Court weighs the "intru[sion] upon an individual's privacy" against the "promotion of legitimate government interests." *Samson*, 547 U.S. at 848 (quoting *United States v. Knights*, 534 U.S. 112, 118-19 (2001)).

As discussed previously, a buccal DNA swab is a search as contemplated by the Fourth Amendment. *See supra* Argument I.B. Since the law enforcement officials chose to rely on a court order based on a state statute (as opposed to executing a search after obtaining a warrant based on a showing of probable cause), it is necessary and appropriate to subject the reasonableness of the state's extraction of Mr. Zuckerman's DNA to the totality-of-the-circumstances test. *Compare L.A. Cnty., Cal. v. Rettele*, 550 U.S. 609, 616 (2007) ("When officers execute a valid warrant . . . the Fourth Amendment is not violated."), *with United States*

v. Knights, 534 U.S. 112, 118 (2001) (upholding validity of a warrantless search based on a totality of the circumstances).

Even as an arrestee for a violent crime, Mr. Zuckerman maintained a privacy interest in his DNA. *See United States v. Edwards*, 415 U.S. 800, 808-09 (1974) (noting that pre-conviction arrestees have a diminished expectation of privacy of their persons, but limiting it to a reasonable time and scope). A DNA extraction clearly violates the scope limitation contemplated by even a broad reading of *Edwards*. There is little that the government could forcibly take from an individual that would be more intrusive and invasive than a sample of his DNA, which is believed to literally contain every piece of genetic information of a specific human being. As the science and technology of DNA continues to evolve, the depth of this intrusion into an individual's privacy rights, and rights to bodily integrity, will only increase. *See* Charles Q. Choi, *Cloning of a Human*, Sci. Am., June 2010, at 36, 36-38 (discussing the inevitability of human cloning); Bert-Jaap Koops & Maurice Schellekens, *Forensic DNA Phenotyping: Regulatory Issues*, 9 Colum. Sci. & Tech. L. Rev. 158, 169 (2008) (discussing precautions the Dutch have taken to prevent revelation of "unknown" personal characteristics to suspects, despite allowing DNA phenotyping in criminal investigation)

Additionally, Mr. Zuckerman's privacy interest would certainly pass the *Katz* privacy test. *See Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). First, Mr. Zuckerman clearly had a subjective expectation of privacy, given that he refused to give consent for the DNA extraction. Second, it is reasonable to conclude that society views that expectation as being reasonable, even for an arrestee, given the vast amount of information available in a DNA sample. *See* Jessica L. Roberts, *The Genetic Information Nondiscrimination Act as an Antidiscrimination Law*, 86 Notre Dame L. Rev 597, 615-16 (2011) (discussing societal fears

with genetic testing due to feared repercussions); *see also* Genetics & Public Policy Center, John Hopkins University, U.S. Public Opinion on Uses of Genetic Information and Genetic Discrimination 2 (2007), *available at* http://www.dnapolicy.org/resources/GINAPublic_Opinion_Genetic_Information_Discrimination.pdf (reporting that 54 percent of adults trust law enforcement with genetic information little or not at all). *But see* 42 U.S.C. § 14135a(a)(1)(A) (2012) ("The Attorney General may . . . collect DNA samples from individuals who are arrested[.]"); Evans Code 2010, §337 (allowing suspicionless DNA sampling from arrestees). With both prongs of the *Katz* privacy test satisfied, there is little doubt that Mr. Zuckerman had a privacy interest that should be protected by the Fourth Amendment.

On the other hand, looking at legitimate government interests being promoted, none has been presented. Looking only at the statute, its stated purpose is to "assist law enforcement officials in carrying out their duties and in furtherance of solving and preventing past and future criminal activity." (R. at 14 (citing Evans Code 2010, §337.1).) This can fairly be summarized as a general interest in law enforcement. This Court, however, has held that a general interest in law enforcement is not sufficient to support a warrantless search. *See, e.g.*, *Ferguson v. City of Charleston*, 532 U.S. 67, 86 (2001) (striking down an obstetric patient drug-testing policy because it was deemed to have general law enforcement as an underlying rationale); *City of Indianapolis v. Edmond*, 531 U.S. 32, 48 (2000) (deeming checkpoint program unconstitutional because its purpose was "indistinguishable from the general interest in crime control"). Additionally, considering that Mr. Zuckerman had no prior criminal record (R. at 16) and that DNA evidence had no relevance to the crime for which Mr. Zuckerman was arrested (R. at 16),

there would appear to be no specific interest in law enforcement that extraction of Mr. Zuckerman's DNA might further.

Imputing an identification purpose onto the language of the statute, though clearly not contemplated by the express language of the legislature, also falls short, primarily for two reasons. First, as discussed previously, a DNA sample is fundamentally different than a fingerprint. *See supra* Argument I.D. Second, and perhaps more relevant for a totality-of-the-circumstances analysis, Mr. Zuckerman's identity was not in question. (R. at 16.) As such, even if in some cases a DNA sample may be necessary for identification purposes, in the unique facts of this case, that could not be put forth as a legitimate government interest.

Considering the totality of the circumstances, the Evans DNA Collection Act is unconstitutional as applied to Mr. Zuckerman. One would have to argue that Mr. Zuckerman, as a pre-conviction arrestee, had no privacy interest in his DNA in order for the government to prevail in this matter, given its complete lack of showing a legitimate government interest in collecting the DNA. This would clearly be a losing argument considering the prior holdings of this Court and protections afforded post-conviction arrestees in the confidentiality of their DNA. *See United States v. Edwards*, 415 U.S. 800, 808-09 (1974) (noting that pre-conviction arrestees have a diminished expectation of privacy of their persons, but limiting it to a reasonable time and scope); *see, e.g.*, 42 U.S.C. § 14135e(c) (2012) (authorizing criminal penalties for misuse of DNA information collected under the federal statute); Cal. Penal Code § 299.5 (West 2012) (authorizing fines and prison time for misuse of DNA information collected under the California statute).

B. Despite the collection of Mr. Zuckerman's DNA being a collateral issue to the subsequent criminal proceedings, the state's collection, storage, and distribution of Mr. Zuckerman's DNA has caused him an actual injury that

is likely to be redressed by affirmance of the order of destruction of his DNA sample and removal from the Evans DNA database.

This Court may consider issues of justiciability sua sponte. *See, e.g.*, *Adarand Constructors, Inc. v. Mineta*, 534 U.S. 103, 110 (2001) (noting that, in some matters, this Court is obliged to examine standing sua sponte); *Reno v. Catholic Soc. Servs., Inc.*, 509 U.S. 43, 57 n.18 (1993) (noting that this Court has the power to raise questions of ripeness on its own motion); *Memphis Light, Gas & Water Div. v. Craft*, 436 U.S. 1, 7-8 (1978) (noting that this Court has the power to consider question of mootness even if it was not raised by parties in their briefs). Thus, although the government has not challenged the justiciability of Mr. Zuckerman's DNA collection in the lower courts (*see generally* R.), a few words regarding the justiciability of this collateral issue are appropriate.

Since the district court cited *United States v. Mitchell*, 652 F.3d 387 (3d Cir. 2011), when discussing the justiciability of the DNA issue (R. at 8), it is important to distinguish that case, which involved an interlocutory appeal by the government, from the matter at hand. In *Mitchell*, the defendant was arrested for attempted possession with intent to distribute cocaine. *Mitchell*, 652 F.3d at 389. Pursuant to a federal statute, the government sought to collect a DNA sample, pre-conviction, but was prohibited from doing so by the district court. *Id.* The government filed an interlocutory appeal challenging the prohibition. *Id.* at 391.

Before deciding the issue on its merits, the Third Circuit Court of Appeals made two findings as to the justiciabiity of the matter before it: (1) the government did have a statutory basis for its appeal in the criminal matter, *id.* at 392; and (2) this particular interlocutory appeal fit into the narrow exception established by the collateral order doctrine, *id.* at 398. Statutory basis had been called into question in *Mitchell* because, without it, the prosecution is generally not allowed to appeal a criminal matter. *Id.* at 391-92 (citing United States v. Farnsworth, 456

F.3d 394, 399 (3d Cir. 2006)). Our matter relates to an appeal by Mr. Zuckerman, not the prosecutor, so determining the statutory basis for a prosecutorial appeal is of limited importance to our case. The collateral order doctrine was relevant in *Mitchell* because the government sought an interlocutory appeal, which is an exception to the "final judgment" rule. *Id.* at 392 (citing *Cohen v. Beneficial Indus. Loan Corp.*, 337 U.S. 541, 546 (1949)). Since the present case does not involve an interlocutory appeal, but rather an appeal after final judgment by the district court, the collateral order doctrine, too, is of limited importance to our case. Assuming arguendo that an interlocutory appeal was sought by Mr. Zuckerman, it should have been denied by the district court because he would have failed the third prong of the collateral order doctrine because this matter is still effectively reviewable on appeal from final judgment. *See Coopers & Lybrand v. Livesay*, 437 U.S. 463, 468 (1978) (summarizing the three prongs of the collateral order doctrine). The government's concerns, present in *Mitchell*, regarding an inability to appeal if the defendant was acquitted are clearly not present for Mr. Zuckerman who, as the defendant, maintains a right to appeal a conviction after final judgment.

Looking specifically at the issue of mootness, a main concern of *Mitchell*, this Court has recently reiterated that as long as a court can grant some "effectual relief," the case is not moot. *Knox v. Serv. Emps. Int'l Union, Local 1000*, 132 S.Ct. 2277, 2287 (2012) (quoting *Church of Scientology of Cal. v. United States*, 506 U.S. 9, 12 (1992)). In that same decision, the Court further reinforced the notion that "as long as the parties have a concrete interest, however small, in the outcome of the litigation, the case is not moot." *Id.* (quoting *Ellis v. Railway Clerks*, 466 U.S. 435, 442 (1984)). In this matter, Mr. Zuckerman does have a concrete interest—the government has an improperly attained sample of his DNA and he wants it destroyed and removed from the Evans DNA Database. Further, this Court can provide complete relief to Mr.

Zuckerman by affirming the lower court order for destruction and removal of the DNA sample. Given that the facts of this matter align with this Court's recent interpretation of the mootness doctrine, the case is not moot.

III. Mr. Zuckerman has a reasonable expectation of privacy in his private Facepoke information that is protected by the Fourth Amendment because he clearly demonstrated a subjective belief in that privacy and society is prepared to recognize that expectation as reasonable. It was a violation of Mr. Zuckerman's Fourth Amendment rights to perform a warrantless search of his private Facepoke information.

Since *Katz v. United States*, 389 U.S. 347 (1967), this Court has recognized that the right to privacy against unreasonable governmental interference under the Fourth Amendment contains two prongs: subjective and objective. Mr. Zuckerman clearly demonstrated a subjective interest in his private Facepoke account information and society is prepared to recognize that as a reasonable interest. Consequently, this Court should find that the government's warrantless search and seizure of Mr. Zuckerman's Facepoke profile were not only unlawful, but interfered with Mr. Zuckerman's legitimate expectation of privacy.

A. Mr. Zuckerman had a subjective privacy interest that was not destroyed by using Facepoke to communicate with a select few friends and house personal information.

In *Katz*, this Court considered various components that ultimately led to this Court's shaping of an individual's reasonable expectation of privacy. *See supra* Argument I.B. The specific facts in *Katz* are noteworthy for the case at hand. In *Katz*, FBI agents installed recording equipment to a public phone booth's exterior that eventually resulted in a man's eight-count conviction for conducting illegal wagers. *See Katz v. United States*, 389 U.S. 347, 348 (1967). The Court addressed the location involved in the search and seizure, and held that "the Fourth

Amendment protects people, not places." *Id.* at 351. The Court further reasoned that "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* The Court went on to explain that warrantless searches are still unlawful despite facts that demonstrate probable cause. *Id.* at 356.

The Court ultimately held that the search and seizure of the recorded conversations violated the Fourth Amendment. *Id.* at 359. In his concurrence, as discussed previously, Justice Harlan explained that Fourth Amendment privacy protections require the following two factors: (1) a person must have an actual or subjective expectation of privacy; and (2) that the expectation must be objectively reasonable. *Id.* at 361 (Harlan, J., concurring).

In *United States v. Ziegler*, the Ninth Circuit Court of Appeals considered the legitimate expectation of privacy when an employee had images of child pornography on his workplace computer. *United States v. Ziegler*, 474 F.3d 1184, 1187 (9th Cir. 2007). The FBI received a tip from the company's owner that an employee had viewed child pornography from his office computer. *Id.* at 1185. After attaining the company's attorney's approval, the management entered the employee's office and copied his hard drive. *Id.* at 1185. The employee was eventually charged, and he later appealed the district court's denial to suppress the evidence. *Id.* at 1188.

The *Ziegler* court held that the search was reasonable because the office and the computer were purchased and maintained by the consenting and controlling company. *Id.* at 1191. The court also held that because the employer notified its employees that a department monitors the computers, employees could not reasonably expect privacy. *Id.* at 1192. As a result, the court held that the lower-level court was correct to deny the employee's motion to suppress the evidence because the evidence was obtained from a lawful search. *Id.* at 1193.

Mr. Zuckerman had an actual expectation of privacy because he expressly articulated his disagreement with the company's employment condition and told the hiring manager that his reluctance to release his password was "a matter of principal." (R. at 5.) Further, Mr. Zuckerman only shared his Facepoke information with select friends. (R. at 7.) Mr. Zuckerman took further measures to ensure privacy when he limited his Facepoke profile's visibility to only the Facepoke friends he accepted. (R. at 7; R. at 20.) Similar to *Katz*, Mr. Zuckerman sought to keep his profile private even in an area that could be accessible to the public, but was in fact not visible to the public. In fact, Mr. Zuckerman changed his profile password again to further secure that privacy interest. (R. at 5.) The case-at-hand is a stark contrast from the *Ziegler* case because Mr. Zuckerman's Facepoke account was an account that he registered, maintained, and controlled before his employment. Mr. Zuckerman's ownership advances his subjective expectation to privacy, unlike the facts that surrounded the *Ziegler* court's decisive holding.

B. Society as a whole recognizes a person's privacy interest in private Facepoke information and distinguishes between publicly-available and private Facepoke information.

Earlier this year, this Court discussed the expectations of privacy in *United States v. Jones*, 132 S.Ct. 945 (2012). In *Jones*, a nightclub operator sought to suppress evidence that government agents obtained when they placed a tracking device under his vehicle. *Id.* at 948. The Government claimed that the tracking device did not interfere with the car owner's expectation of privacy because "the exterior of a car is thrust into the public eye, and thus to examine it does not constitute a search." *Id.* at 952 (citing *New York v. Class*, 475 U.S. 106, 114 (1986)).

The Court held that the government did violate the car owner's Fourth Amendment rights when agents attached the device and consequently, occupied the private property to observe the

car's travels on city streets. *Id.* at 949. In her concurring opinion, Justice Sotomayor suggested that perhaps it is time to reevaluate the modern basis that people do not have a reasonable expectation of privacy in information consensually released to third parties. *Id.* at 957 (Sotomayor, J., concurring). Justice Sotomayor opined: "[In] the digital age . . . people reveal a great deal of information about themselves to third parties[.] . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every website they had visited[.]" *Id.* at 957 (Sotomayor, J., concurring).

There is enough discussion and action to conclude that Facepoke profiles are objectively private if the user engages the appropriate privacy settings. In the present case, even the hiring manager expressed that "she understood his concern [to reveal his password]," and that the "company acknowledges that Facepoke passwords are private." (R. at 17.) Despite this concession, the hiring manager repeated that surrendering the password was a condition of employment and that the company would keep [the passwords] confidential." (R. at 17.) Mr. Zuckerman's expectation to privacy was objectively reasonable, especially considering the emergence of new legislation regarding privacy in social media profiles. *See* Jason Keyser, *Illinois Facebook Password Law Bars Employers From Asking For Social Media Logins*, Huffington Post Chicago (Aug. 1, 2012, 3:49 PM), http://www.huffingtonpost.com/2012/08/01/illinois-facebook-law_n_1730077.html (discussing an Illinois statute codifying an expectation of privacy relating to Facebook information).

C. There are no exceptions to the warrant requirement that the government could use to avoid a warrant based on the unique facts of this situation.

Since *United States v. Jeffers*, 342 U.S. 48 (1951), and more recently in *Georgia v. Randolph*, 547 U.S. 103 (2006), this Court has held that the Fourth Amendment provides clear

protection against the illegal and warrantless search of a person's private space when the government agents did not obtain valid consent.

In *Georgia v. Randolph*, this Court considered legal precedent and numerous factors that ultimately led to their decision in favor of an individual's privacy rights. In *Randolph*, warrantless police searched the defendant's house for drugs, pursuant to consent from his estranged wife. *See Randolph*, 547 U.S. at 107. However, in doing so, the police ignored the withholding of consent by the defendant (and homeowner) who was also present. *Id.* Following his drug possession charge, the defendant filed a motion to suppress the evidence obtained in the search. *Id.*

In resolving this matter, first, this Court acknowledged that there is an exception to the general rule that a warrantless entry of a person's home is unreasonable per se. *Id.* at 109. This Court reviewed *Illinois v. Rodriguez*, 497 U.S. 177 (1990) and *United States v. Matlock*, 415 U.S. 164 (1974), and reviewed their respective analyses pertaining to valid consent. In *Rodriguez*, the Court explained the two forms of valid consent: (1) the property owner's actual voluntary consent; or (2) consent from a third party who retains common authority over the property. *Rodriguez*, 497 U.S. at 181. In *Matlock*, the Court examined the contours of "common authority" as a "mutual use of the property by persons generally having joint access or control for most purposes." *Matlock*, 415 U.S. at 171. The *Randolph* Court also explained that the core element in Fourth Amendment consent cases is not found in property law, but instead, in generally shared social expectations or the customary expectation of courtesy. *Randolph*, 547 U.S. at 111-113 (citing *Minnesota v. Olson*, 495 U.S. 91 (1990) and *United States v. Jeffers*, 342 U.S. 48, 51 (1951)).

Ultimately, the *Randolph* Court held that the warrantless search of the home was not reasonable because when a present co-occupant denies police entry to the space, the refusal prevails over the consent of the other occupant. *Id.* at 122-123. Additionally, this Court stated that "we have, after all, lived our whole national history with an understanding of the ancient adage that a man's house is his castle to the point that the poorest man may in his cottage bid defiance to all the forces of the Crown." *Id.* at 115.

In a case with persuasive precedential value involving common authority over private computer information, Illinois's Third District Court of Appeals considered applicable exceptions to the warrant requirement when a man was convicted of possessing child pornography on his computer when his father permitted the police to search. *See People v. Blair*, 748 N.E.2d 318, 322 (Ill. App. Ct. 2001). The man was arrested before the search when he videotaped kids at a zoo. *Id.* Subsequent to his arrest, the man's parents allowed the police to enter, and the subsequent search of the man's computer revealed bookmarks storing child pornography. *Id.*

The Third District Court of Appeals held that the burden to establish an exception to the warrant requirement falls on the prosecutor to prove by a preponderance of evidence. *Id.* at 323. The court reviewed *Matlock* and held that, even in instances of common authority, a resulting seizure requires probable cause. *Id.* The court ultimately held that probable cause did not exist, and that the police violated the man's Fourth Amendment rights. *Id.*

In the case-at-hand, it is uncontested that Mr. Zuckerman did not provide the agents with actual consent because the agents never asked Mr. Zuckerman's permission to search and seize the contents of his private Facepoke profile. When Mr. Zuckerman was in the government's custody for the assault, the police tried to enter into Mr. Zuckerman's profile from a Google

search but were unsuccessful in their attempt. (R. at 6.) The police didn't asked Mr. Zuckerman to view his private profile, nor did they obtain a warrant to access the profile. Instead, the police went through Mr. Zuckerman's work e-mail address book and tracked down one of Mr. Zuckerman's Facepoke friends. (R. at 6.) The police asked the third party if they could view Mr. Zuckerman's Facepoke profile contents, and the third party initially refused. (R. at 6.) It was only after the police used daunting legal language that the third party compellingly accessed Mr. Zuckerman's personal profile. (R. at 6.) However, Mr. Zuckerman's Facepoke friend did not have common authority to allow police access to his private profile.

Although Mr. Zuckerman did restrict the amount of friends to view his profile, there is no evidence to support that Mr. Zuckerman authorized his friend to have "common authority" with the mutual use of joint access to the intangible property. While it is uncontested that the police were unsuccessful at viewing Mr. Zuckerman's profile because of his restrictive privacy settings, the Record is silent as to whether Mr. Zuckerman's approval was required if a friend wanted to post something on Mr. Zuckerman's profile page. (R. at 18.) Furthermore, nothing in the Record indicates that the third party had control of Mr. Zuckerman's profile. *Black's Law Dictionary* defines "control" as "[t]o exercise power or influence over." Black's Law Dictionary 378 (9th ed. 2009). In addition, when the police seized the nine-month-old contents of the post, they didn't have the requisite probable cause that would validate a reasonable person with the belief that the seized contents contained evidence of crime. *See Texas v. Brown*, 460 U.S. 730, 741 (1983). Mr. Zuckerman is also afforded the right to privately criticize his employer's careless management.

Although Fourth Amendment violations are generally based on the state's action, there are instances where a private citizen's actions can transform into the government's actions. In

the Ninth Circuit Court of Appeals, an assistant manager at a hotel contacted police that one of the guests may be using and selling drugs from their hotel room and requested that police escort the manager as he checked the room. *United States v. Reed*, 15 F.3d 928, 930 (9th Cir. 1994). When the manager entered the unoccupied hotel room, he described his discovery of drug paraphernalia to the officers in the doorway. *Id.* When the guest returned to his room, he disallowed the police to search his room. *Id.* After obtaining a search warrant, the police recovered drugs and a gun from the guest's room, and subsequently obtained a warrant for his arrest. *Id.*

The Ninth Circuit held that the initial search of the hotel room was a Fourth Amendment violation because the manager was acting as a warrantless de facto government agent. *Id.* at 931. The Ninth Circuit considered two factors to determine if the manager was acting as a private citizen or as a government instrument. *Id.* First, the court found that the agents allowed the warrantless manager to interfere with the room and the agents acted as lookouts. *Id.* Moreover, the court found that the manager assisted the police with the warrantless search. *Id.* at 932.

In the facts of our case, the police both allowed and induced the warrantless third party to interfere with Mr. Zuckerman's private profile. (R. at 6.) Irrespective of the police coercive conduct to access Mr. Zuckerman's profile, the third party did aid the police because the police did not have the probable cause to secure a warrant to search the profile. The police maliciously relied on the third party's private citizen status as a way to elude the probable cause requirement to continue with their probing mission.

Absent a warrant, probable cause, valid consent, and exigent circumstances, the agents unlawfully searched Mr. Zuckerman's profile and unlawfully seized his profile's nine-month-old post. Mr. Zuckerman's status as a pre-conviction arrestee does not diminish any expectation to

privacy or trigger any exceptions to the warrant requirement. To provide for such an exception would undermine our judicial system, which is premised on the fundamental principle that a person is innocent until proven guilty. Consequently, the government's illegal action resulted in the violation of Mr. Zuckerman's Fourth Amendment privacy rights because no exceptions to the warrant requirement applied.

D. Warrantless searches of a space protected by the Fourth Amendment implicate the totality-of-the-circumstances test which the government fails by not putting forth a legitimate government interest.

This Court held in *Ohio v. Robinette*, 519 U.S. 33 (1996) that although the Fourth Amendment standard is reasonableness, that reasonableness is determined through the totality of the circumstances. *Robinette*, 519 U.S. at 39. The lack of facts that the government has to establish reasonableness in its conduct makes this search tantamount to a fishing expedition. The Record indicates that before Mr. Zuckerman was in police custody, he had no prior criminal record. (R. at 16.) Nowhere in the Record does it indicate that agents received a tip, or any information that explains the government's interest to access Mr. Zuckerman's Facepoke profile. The only thing the agents knew was that Mr. Zuckerman pushed and hit the person who escorted him after he was terminated from his job. (R. at 5.) The government failed to establish a causal connection between Mr. Zuckerman's physical distress over his termination and his private information on Facepoke. The Record is silent as to what the government was seeking. The evidence the agents did unlawfully obtain also didn't extend any support to any real issue the agent might have been aware of before his intrusion. The nine-month-old post the agents obtained discussed how it was good a thing Mr. Zuckerman was an "honest" man because the management did not properly monitor their accounts. (R. at 6.) The post itself did not contain anything that blatantly suggested he conducted any wrongdoing.

CONCLUSION

Mr. Zuckerman's Fourth Amendment rights were violated in two different ways. First, without probable cause, police used an unconstitutional statute, one that purported to reduce the protections of the Fourth Amendment, as authority to perform a DNA extraction. Second, without probable cause, police conducted a warrantless search of Mr. Zuckerman's private Facepoke account, a space for which society recognizes a reasonable expectation of privacy.

For these reasons, we respectfully ask that you affirm the Thirteenth Circuit Court of Appeals holding reversing Mr. Zuckerman's convictions for assault of a federal officer and embezzlement. Additionally, we respectfully ask that you affirm on alternate grounds the Thirteenth Circuit Court of Appeals holding regarding the constitutionality of the Evans DNA Collection Act by finding it facially unconstitutional and direct the district court to order Mr. Zuckerman's DNA sample to be destroyed and removed from the Evans DNA database.

CERTIFICATE OF COMPLIANCE

The undersigned counsel certifies that the Respondent's Brief complies with the word limitation specified in Rule C(3)(d) of the ALA Moot Court Competition Rules. Pursuant to the word-count feature of Microsoft Word, the brief contains 9,870 words, excluding the Cover Sheet, Table of Contents, Table of Citations, Certificate of Compliance, and Appendix.

Respectfully submitted:

/s/ Joseph Hogue /s/ /s/ Ellora Roy /s/
Team #5
Attorneys for Respondent

APPENDIX

U.S. Const. art. VI, cl. 2.

This Constitution, and the Laws of the United States which shall be made in pursuance thereof; and all treaties made, or which shall be made, under the authority of the United States, shall be the supreme law of the land; and the judges in every state shall be bound thereby, anything in the constitution or laws of any state to the contrary notwithstanding.

U.S. Const. amend. IV.

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

18 U.S.C. § 111 (2012).

(a) In general.--Whoever--

(1) forcibly assaults, resists, opposes, impedes, intimidates, or interferes with any person designated in section 1114 of this title while engaged in or on account of the performance of official duties; or

(2) forcibly assaults or intimidates any person who formerly served as a person designated in section 1114 on account of the performance of official duties during such person's term of service,

shall, where the acts in violation of this section constitute only simple assault, be fined under this title or imprisoned not more than one year, or both, and where such acts

involve physical contact with the victim of that assault or the intent to commit another felony, be fined under this title or imprisoned not more than 8 years, or both.

(b) Enhanced penalty.--Whoever, in the commission of any acts described in subsection (a), uses a deadly or dangerous weapon (including a weapon intended to cause death or danger but that fails to do so by reason of a defective component) or inflicts bodily injury, shall be fined under this title or imprisoned not more than 20 years, or both.

18 U.S.C. § 656 (2012).

Whoever, being an officer, director, agent or employee of, or connected in any capacity with any Federal Reserve bank, member bank, depository institution holding company, national bank, insured bank, branch or agency of a foreign bank, or organization operating under section 25 or section 25(a) of the Federal Reserve Act, or a receiver of a national bank, insured bank, branch, agency, or organization or any agent or employee of the receiver, or a Federal Reserve Agent, or an agent or employee of a Federal Reserve Agent or of the Board of Governors of the Federal Reserve System, embezzles, abstracts, purloins or willfully misapplies any of the moneys, funds or credits of such bank, branch, agency, or organization or holding company or any moneys, funds, assets or securities intrusted to the custody or care of such bank, branch, agency, or organization, or holding company or to the custody or care of any such agent, officer, director, employee or receiver, shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both; but if the amount embezzled, abstracted, purloined or misapplied does not exceed $1,000, he shall be fined under this title or imprisoned not more than one year, or both.

As used in this section, the term “national bank” is synonymous with “national banking association”; “member bank” means and includes any national bank, state bank, or bank and trust company which has become a member of one of the Federal Reserve banks; “insured bank”

includes any bank, banking association, trust company, savings bank, or other banking institution, the deposits of which are insured by the Federal Deposit Insurance Corporation; and the term "branch or agency of a foreign bank" means a branch or agency described in section 20(9) of this title. For purposes of this section, the term "depository institution holding company" has the meaning given such term in section 3 of the Federal Deposit Insurance Act.