THIRTY-FOURTH ANNUAL
DEAN JEROME PRINCE MEMORIAL EVIDENCE COMPETITION

No. 18 - 2417

Supreme Court of the United States

ELIZABETH JORALEMON,
Petitioner,

--against--

UNITED STATES OF AMERICA,
Respondent.

ON WRIT OF CERTIORARI

TO THE COURT OF APPEALS FOR THE FOURTEENTH CIRCUIT

RECORD ON APPEAL

TABLE OF CONTENTS

Indictment **1**

Documents **4**

Transcript: Argument on Motion to Suppress **14**

Transcript: Ruling on Motion to Suppress **27**

Transcript: Trial Excerpts **31**

Circuit Court Opinion **43**

Certified Questions **53**

UNITED STATES DISTRICT COURT
DISTRICT OF WESTNICK
– – – – – – – – – – – – – – – X

UNITED STATES OF AMERICA

- against -

ELIZABETH JORALEMON,

Defendant.

– – – – – – – – – – – – – – – X

INDICTMENT

Cr. No. 16-43
(T. 18, U.S.C., §§ 1030(a)(2) and 1030(b))

THE GRAND JURY CHARGES:

INTRODUCTION

At all times relevant to this Indictment, unless otherwise indicated:

1. The defendant ELIZABETH JORALEMON was a resident of the state of Westnick. JORALEMON was employed as a junior aide to United States Congressman Jerry Livingston, who represented Westnick's Second Congressional District.

2. In the summer and fall of 2016, Livingston ran for reelection. Livingston's opponent was Torey Malconey.

3. On or about June 3, 2016, the office of Congressman Livingston was contacted by the Chaotic DERP Squad ("C-DERPS"), a group of hackers located in Galtanon, a foreign country. The hacking group offered to provide Livingston's campaign with emails hacked from the accounts of Torey Malconey and members of her staff in return for cash.

4. Between June 3, 2016 and August 9, 2016, members of Livingston's senior staff agreed to the proposal made by C-DERPS, the hacking group.

5. On or about August 9, 2016, defendant JORALEMON met with Marin Rapstol, a member of the hacking group, at Fullerton Park in Westnick. JORALEMON came to the meeting with a briefcase containing $50,000, and Rapstol came to the meeting with a similar-looking briefcase

containing thumb drives with emails hacked from the accounts of Torey Malconey and members of her staff. Each left the meeting with the briefcase the other had brought.

6. On or about September 7, 2016, defendant JORALEMON had a second meeting with Rapstol at the same park in Westnick. Once again, JORALEMON came to the meeting with a briefcase containing $50,000, and Rapstol came to the meeting with a similar-looking briefcase containing thumb drives with emails hacked from the accounts of Torey Malconey and members of her staff. Each left the meeting with the briefcase the other had brought.

7. The emails hacked from the accounts of Torey Malconey and members of her staff were obtained by accessing computers owned and operated by Malconey's campaign (the "Malconey computers").

8. Neither JORALEMON nor Rapstol, nor anyone working with them, had authority to access the Malconey computers.

9. The hacked emails obtained from the Malconey computers included, among other things, the following: (1) messages seeking contributions from persons residing out of state; (2) messages inviting persons residing out of state to speak at rallies in support of Malconey; and (3) messages arranging for Malconey to speak at various venues outside of Westnick. Accordingly, the Malconey computers were used in interstate commerce and were "protected computers" as defined in 18 U.S.C. § 1030(e)(2)(B).

COUNT ONE

(Conspiracy to Commit Computer Intrusions)

10. The allegations contained in paragraphs 1 through 9 are realleged and incorporated as if fully set forth in this paragraph.

11. In or about and between June 2016 and September 2016, both dates being approximate and inclusive, within the District of Westnick and elsewhere, the defendant ELIZABETH

JORALEMON, together with Marin Rapstol and others, did knowingly and willfully conspire to access one or more computers without authorization and exceed authorized access, and thereby to obtain information from one or more protected computers, which information had a value in excess of $5,000, contrary to Title 18, United States Code, Sections 1030(a)(2)(C), 1030(b), 1030(c)(2)(A) and 1030(c)(2)(B)(iii).

12. In furtherance of the conspiracy and to affect its objects, within the District of Westnick and elsewhere, the defendant ELIZABETH JORALEMON and others, committed and caused to be committed, among others, the following:

OVERT ACTS

a. On or about August 9, 2016, defendant JORALEMON met with Marin Rapstol, a member of the hacking group, at a park in Westnick, delivered a briefcase to Rapstol, and received a briefcase from him.

b. On or about September 7, 2016, defendant JORALEMON met with Marin Rapstol, a member of the hacking group, at a park in Westnick, delivered a briefcase to Rapstol, and received a briefcase from him.

(Title 18, United States Code, Sections 1030(b) and 3551 et seq.)

A TRUE BILL

Gustavo N. Flores

GRAND JURY FOREPERSON
FEBRUARY 10, 2017

Arnold Stevens

ARNOLD STEVENS
UNITED STATES ATTORNEY
DISTRICT OF WESTNICK

THE
EXTRA NEWS

ALL ABOUT THE BIG WORLD WE LIVE IN *EXCLUSIVE NEWS TODAY*

ELECTION EDITION

New Polls Show Race for Westnick's 2nd Congressional District Tightening After Orphanage Memorial Incident

August 1, 2016
By Ben Studler

ARBOR TOWN - Two new polls show the race between incumbent Representative Jerry Livingston and challenger Torey Malconey for Westnick's 2nd Congressional District has tightened significantly in the last few weeks.

A New York Times/Upshot poll reported that Livingston, currently serving his fourth term, and Malconey were tied at 44% support each with 8% undecided, while a SurveyUSA poll has Rep. Livington up 46% to 44%. Both polls have a margin of error of +/- 5%, meaning the race is essentially tied. Just one month ago Livingston was up double digits in both polls.

The polls were taken shortly after a viral video released last week of Livingston laughing during a recent memorial ceremony for three staff members of Arbor Town's only orphanage, who were killed in a recent fire that also destroyed the orphanage. Livingston has apologized, blaming the laughter on a private joke made by his wife.

"This was one very brief moment in a two hour ceremony. But my constituents know I'm the only candidate who will get the federal funds necessary to rebuild the orphanage. I get results," Livingston said to a gaggle of reporters outside a recent campaign event.

Malconey responded to the video in a statement stating in part, "Our district needs a representative who relates to the grief in our community, not a cynic who has been hardened by Washington and has become distant from the real needs of his constituents."

1300 Pennsylvania Avenue NW
Washington, DC 20004

U.S. Customs and Border Protection

MEMORANDUM

FROM: Clinton O'Keefe
CBP Officer

DATE: 20 August 2016

SUBJECT: Confiscation of Smartphone for Forensic Search

On 20 August 2016, I was stationed at the international port-of-entry at Washington Dulles International Airport, where I conducted the immigration, customs and agriculture components of the inspection process for passengers disembarking international flights. At approximately 18:30, a woman identified by her valid United States issued passport and Westnick state driver's license as ELIZABETH JORALEMON approached me for inspection. The woman appeared anxious and irritated, so I selected her for a search of her person and luggage. The woman consented to a body x-ray scan and a search of her luggage, neither of which revealed any contraband. I then asked the woman to enter the password to unlock her smartphone, which she refused to do. I informed the woman that CBP would need to conduct a digital forensic analysis of her smartphone, and that the phone would be confiscated and returned to her after the digital forensic analysis was complete. The woman then turned her smartphone over to me and proceeded through the U.S. port-of-entry. I labeled the smartphone for identification and sent it to the forensic analysis laboratory for digital forensic analysis.

FEDERAL BUREAU OF INVESTIGATION
302 - INVESTIGATIVE REPORT

22 AUGUST 2016

I, Madison Throop, am a Special Agent with the Federal Bureau of Investigation. In August 2016, I was assigned to an investigation based upon an anonymous tip that was left on the Bureau's voice mailbox on 21 August 2016. The tipster described overhearing a "very suspicious" exchange between a female bar patron and a bartender at Ed's Fast Fun Inn, a bar in Southeast Washington, D.C. frequented by young people working on Capitol Hill. The tipster overheard the female patron discussing her discomfort with her boss assigning her to make drop-offs with some type of foreign agent. The tipster also overheard the female patron say she wanted to quit her job but could not because she just found out from a genetic test that she is certain to get Ashwells Disease. I researched Ashwells and discovered it is a rare degenerative neurological disease. On average, it begins in a person's late thirties, and most patients die within 10 years of onset, absent intensive treatment. The female patron said she needed to retain the health insurance that comes with her job now that she knows she will develop Ashwells. As follow up, the agency plans to reach out to genetic testing services to obtain a list of customers who have tested positive for Ashwells.

SA Madison Throop
22 August 2016

FEDERAL BUREAU OF INVESTIGATION
302 - INVESTIGATIVE REPORT

26 AUGUST 2016

I, Adira Pierrepont, am a Special Agent with the Federal Bureau of Investigation. My contact, a former FBI agent by the name of Mark Givens, is an employee at 23andyou.com, a service that collects and analyzes DNA in order to tell customers about their genetic makeup, including their ethnic background and some information about certain genetic conditions. On 23 August 2016, pursuant to a lead that a suspect had been diagnosed with Ashwells disease, a rare genetic condition affecting one in 100,000 individuals, I asked Mr. Givens to search the database of 23andyou.com for any individual within a 20-mile radius of Washington, D.C. with that condition. After consulting with in-house attorneys at 23andyou.com, Mr. Givens consented to conduct this search and orally share the results with me. The search indicated that one ELIZABETH JORALEMON, a resident of Westnick, satisfied the conditions of the search. A public records search indicated that JORALEMON resides at 452 Delft Avenue in Arbor Town, Westnick, a popular suburb of Washington, D.C. A search of Capitol Hill directories indicates that JORALEMON is a junior aide on the staff of Representative Jerry Livingston, who represents Westnick's Second Congressional District. I have ordered that surveillance begin on JORALEMON at the earliest possible opportunity.

apierre

SA Adira Pierrepont
26 August 2016

FEDERAL BUREAU OF INVESTIGATION
302 - INVESTIGATIVE REPORT

08 SEPTEMBER 2016

I, Orlando Remsen, am a Special Agent with the Federal Bureau of Investigation. On 7 September 2016, Special Agents of the Federal Bureau of Investigation arrested and interviewed MARIN RAPSTOL. The agents identified themselves as FBI agents before conducting the interview. After the agents administered *Miranda* warnings, the subject agreed to speak to us without counsel present. RAPSTOL provided the following information about ELIZABETH JORALEMON, along with additional information about her not included here:

In June 2016, the hacking conglomerate known to cybercrime agents as the Chaotic DERP Squad ("C-DERPS") began a sophisticated mercenary campaign to influence United States elections for profit from their base in the nation of Galtanon. In the past, the group had engaged in similar activities in the United States and other countries. C-DERPS targeted candidates in battleground states, as they believed those candidates would be the most amenable to demands for payment in return for the sensitive information that C-DERPS could provide.

In June 2016, C-DERPS sent Rosa Feil, Livingston's campaign manager, an email with a link to an encrypted messaging service called TextApp promising damaging information on Livingston's challenger. Initially C-DERPS received no response. In August 2016, however, the hackers began communicating with Congressman Livingston's campaign team on TextApp. The hackers promised to provide emails and other information stolen from the computer of Livingston's challenger, Torey Malconey, in exchange for $100,000 in cash. The hackers eventually scheduled the first of two exchanges for 9 August 2016. RAPSTOL completed the exchange on that date in Westnick by providing JORALEMON with a briefcase containing a flash drive with the illicitly obtained information on it. JORALEMON delivered a briefcase containing $50,000 in cash to RAPSTOL at this exchange. RAPSTOL stated that he was aware that the flash drive contained information stolen from a rival's computer and that the $50,000 he received was partial payment for the flash drive. According to RAPSTOL, JORALEMON never said or did anything that might suggest that she knew what was on the flash drive at this first meeting.

RAPSTOL made a second exchange with JORALEMON on 7 September 2016. At this drop, RAPSTOL provided a second flash drive with illicitly obtained material in a briefcase to JORALEMON, and JORALEMON again provided $50,000 in a briefcase to RAPSTOL. At this

meeting, RAPSTOL asked JORALEMON if the campaign was satisfied with the previously provided material. RAPSTOL said that JORALEMON told him she did not know what he was referring to and that she just wanted to swap the brief cases and leave so that she could keep her job. This meeting was surveilled by myself and other agents. After RAPSTOL left the meeting, he was apprehended at a location from which JORALEMON would not observe the arrest.

SA Orlando Remsen
8 September 2016

1300 Pennsylvania Avenue NW
Washington, DC 20004

U.S. Customs and Border Protection

MEMORANDUM

FROM: Dean Nostrand
Forensic Analyst

DATE: 09 September 2016

SUBJECT: Forensic Analysis of Elizabeth Joralemon's Smartphone

---

On 21 August 2016, our lab received a request from CBP officer Clinton O'Keefe for a digital forensic analysis of ELIZABETH JORALEMON's smartphone. The analysis was completed on 7 September 2016 and brought back 985 pages of material. The results of the analysis contained no findings of illegal contraband and no evidence of any suspicious electronic financial transactions. One text message conversation, however, aroused some suspicion. The messages came from the text messaging app "TextApp," which encrypts users' messages and automatically deletes them after thirty days. The conversation, between JORALEMON and another user identified as "Cheryl" in JORALEMON's phone, detailed an arrangement whereby JORALEMON and "Cheryl" would meet and "exchange." The messages are sparse, and both users appeared to use code, deliberately avoiding explicit reference to what JORALEMON and "Cheryl" planned to exchange. The word "cash," however, appears twice in the conversation, but without meaningful context. The only TextApp messages the analysis recovered are from this conversation. The messages do not reveal enough information to recommend a criminal investigation, but for future notice, I have added this memo, along with a transcript of the TextApp conversation, to the Interagency Border Inspection System.

FEDERAL BUREAU OF INVESTIGATION
302 - INVESTIGATIVE REPORT

21 OCTOBER 2016

I, Madison Throop, am a Special Agent with the Federal Bureau of Investigation. In August 2016, I was assigned to an investigation concerning ELIZABETH JORALEMON. On 20 October 2016, I searched the databases of all federal law enforcement agencies, including the Interagency Border Inspection System ("IBIS"), for any information concerning JORALEMON. My search of IBIS brought back a Customs and Border Protection ("CBP") memorandum and report, dated 9 September 2016, detailing the results of a forensic examination of JORALEMON's cellphone. The CBP report contained a transcript of a text message conversation from the messaging app "TextApp." The conversation revealed that JORALEMON had been planning meetings with a TextApp user by the name of "Cheryl." I then made the report known to the rest of the investigation team. At the time, I was aware that TextApp automatically deleted messages after thirty days and that, consequently, the messages would be unavailable by the time the FBI could secure a search warrant for JORALEMON's smartphone.

SA Madison Throop
21 October 2016

U.S. Department of Justice
United States Attorney
District of Westnick

277 Dutchman's Plaza
Breuckelyn, Westnick 11201
11 April 2017

By ECF and Hand
Rebecca Cadman, Esq.
216 Dutchman's Plaza East
Breuckelyn, Westnick 11201

Re: United States v. Elizabeth Joralemon
Criminal Docket No. 16-CR-43

Dear Ms. Cadman,

Pursuant to our recent correspondence and Rule 16 of the Federal Rules of Criminal Procedure, enclosed please find the email exchange regarding the DNA database information request made by FBI Special Agent Adira Pierrepont. Please do not hesitate to contact me with any questions or concerns.

Cordially,

Washington

Amara Washington
Assistant U.S. Attorney

Enc.

From: Adira Pierrepont [Adira.Pierrepont@doj.gov]
To: Mark Givens [Mark.Givens@23andyou.com]
August 23, 2016 [2:45 AM]

Mark –

How have you been? It was great seeing you and Joan last week, and I really couldn't be happier about your new job. It is perfect for you.

Meanwhile, I was wondering if I might ask you for some help. Do you have time for a phone call sometime tomorrow morning? Let me know.

Best,
Adira

From: Adira Pierrepont [Adira.Pierrepont@doj.gov]
To: Mark Givens [Mark.Givens@23andyou.com]
August 23, 2016 [9:23AM]

Great speaking to you just now. Like I said, we are ok for you to clear it with your boss. We are confident there is nothing in the law or your own policies that would prevent this from going forward.

More importantly, I hope you will think about all the good you and your company can do by helping us with this. This might be our only chance to get a lead and get this case closed. I know you're just as ticked off about the corruption in DC as I am. An indictment like this would reverberate far beyond this one case. It would put that entire town on notice that the sheriff is in town and not afraid to enforce the law.

Hope to hear from you soon,
Adira

From: Mark Givens [Mark.Givens@23andyou.com]
To: Adira Pierrepont [Adira.Pierrepont@doj.gov]
August 26, 2016 [2:03 PM]

Adira, I was able to speak with our lawyers. They agree that there is nothing wrong with this and that I am ok to run a search. However, they have told me to share only the relevant information over the phone. I cannot release any of the results directly. I will call in a moment.

From: Adira Pierrepont [Adira.Pierrepont@doj.gov]
To: Mark Givens [Mark.Givens@23andyou.com]
August 26, 2016 [2:16 PM]

Mark –

You've done the whole country a great service. Looking forward to that beer with you very soon.

Adira

UNITED STATES DISTRICT COURT

DISTRICT OF WESTNICK

----------X

UNITED STATES OF AMERICA No. 16-CR-643

-against-

ELIZABETH JORALEMON,

Defendant.

----------X

JUNE 9, 2017

TRANSCRIPT: ARGUMENT ON MOTION TO SUPPRESS

Before: Hon. Robert Pitler

APPEARANCES:

For Defendant Elizabeth Joralemon:	Rebecca Cadman Cadman & Henry LLC
For the United States of America:	Amara Washington Assistant U.S. Attorney
Court Reporter:	John Crain

COURT: Good morning, counsel. Pending before me is Defendant's motion to suppress certain DNA information obtained by the FBI, as well as the fruits of a forensic search of the Defendant's phone. First, let's discuss the DNA. This was, as I understand it, information the company 23andyou.com possessed after Ms. Joralemon submitted her DNA sample to them for analysis.

Let me begin by asking the prosecution for some background. How exactly did the government come into possession of this genetic information, and why shouldn't the government be required to obtain a warrant before accessing such private, sensitive information?

WASHINGTON: Judge, as set out in our papers, agents received an anonymous tip, based on a conversation overheard in a bar, suggesting that someone who likely worked on Capitol Hill and who had Ashwells disease might be involved in some sort of corruption. So, the agents sought to answer a simple question: Is there any way to find out if there is someone living in the Washington, D.C. area with Ashwells? Agents knew Ashwells was very rare. They also knew that various commercial DNA analysis companies, including 23andyou, test for Ashwells. And so they contacted 23andyou and asked for identifying information of anyone with Ashwells living in the Washington, D.C. metropolitan area. And that inquiry led to the identification of Elizabeth Joralemon.

Judge, it's clear the agents didn't need a warrant to obtain this information. The law is settled, and has been for decades,

that when someone shares information with a third party -- whether it's the phone numbers called on a landline telephone or the deposits and withdrawals made from a bank account -- that person surrenders any reasonable expectation of privacy in that information. The key Supreme Court cases on point regarding the third-party doctrine are United States v. Miller, where the Court held that there is no expectation of privacy in bank records, and Smith v. Maryland, where the Court held that police could collect pen register information without a warrant. Defendant chose to share her DNA with 23andyou, and she invited 23andyou to analyze it, and then she consented to that information being sold. That's why we didn't need a warrant to retrieve this information from the third party.

COURT: Thank you. I'd like to hear now from Ms. Cadman on this issue. Ms. Cadman, why does the third-party doctrine not apply?

CADMAN: Thank you, your Honor. We disagree with the way the prosecution has characterized the third-party consent doctrine. The prosecution began its argument with the exception rather than the rule. The rule, per Katz v. United States, is that where a person seeks to keep something private, and where that expectation of privacy is reasonable, Fourth Amendment protections apply, and investigators need a warrant. Miller and Smith provide an exception to that general rule insofar as they hold that an individual who relinquishes information to a third party may no longer have a

reasonable expectation of privacy in that information. But it's clear that the information the FBI gathered in this case is protected by the Fourth Amendment even though it was provided to a third party.

The Supreme Court has recognized that, Miller and Smith notwithstanding, some information is so private that an individual retains a reasonable expectation of privacy with respect to that information, even after sharing it with a third party, particularly if it is the type of information commonly shared when using ubiquitous modern technology. In U.S. v. Jones, for instance, Justice Sotomayor agreed with the majority that investigators needed a warrant to place a GPS monitor on a suspect's car. But while the majority in Jones based its holding on the physical invasion involved in placing a GPS locator on the car, Justice Sotomayor came to the same result by saying that, per Katz, an individual has a reasonable expectation that every movement over an extended period of time is not being tracked.

COURT: Are you saying I should apply a concurrence here?

CADMAN: Not at all, your Honor. We are simply arguing that there is good authority from the Supreme Court for saying that, where new technology causes us to share information we would previously have kept private, and where that information is extremely sensitive and personal, we retain a reasonable expectation of privacy even if we

share it with a third party. And investigators therefore need a warrant to get it.

COURT: Which cases are you referring to?

CADMAN: First, in Kyllo v. U.S., the Court -- and this was Justice Scalia writing -- expressed its concern with preserving the privacy interests originally protected by the Fourth Amendment. So, the Court in effect concluded that where a new device allows access to private information that could not previously have been reached without a physical intrusion, Fourth Amendment protections apply. Second, in Riley v. California, the court found an expectation of privacy in a personal smartphone. Our position relies upon a logical extension of these two holdings: a DNA database contains deeply personal data, just like the smartphone in Riley and the geolocation data in Jones, and that data has only recently become accessible thanks to a new technology, as described in Kyllo.

COURT: I'm just not sure how different DNA is from the information shared with the third parties in Smith and Miller. Can't I learn a great deal about a person from bank records and pen registers? Can't I learn, for instance, where the person is spending money and what on? Can't I learn whether the person is calling a radiologist, a paramour, the DNC or the RNC?

CADMAN: There is an important distinction, your Honor. Bank transactional records or records of phone calls are lists of

discrete information. It would be impossible to infer much from them without significant additional data.

COURT: Thank you, Ms. Cadman. Ms. Washington, why aren't Miller and Smith distinguishable, as Ms. Cadman contends? Aren't the differences she identifies compelling?

WASHINGTON: No, your Honor. Here, Defendant, like the defendants in Miller and Smith, must have understood, or at least reasonably should have understood, that the information she freely provided would be seen by third parties -- the analysts and other employees of 23andyou. Moreover, 23andyou requests a specific release of information from its clients when they sign up. In fact, Defendant was specifically told that her data would be shared with additional third parties who paid for it, and that she could decline to consent to having her data shared. But she clicked the box indicating that she consented.

COURT: All right, but I'm guessing nothing in the release mentioned that the information might be turned over to law enforcement?

WASHINGTON: True, your Honor, but that's not the point. The defendants in Miller and Smith didn't consent to having their information turned over to law enforcement either, at least not explicitly. The point is not that the Defendant consented explicitly to allowing law enforcement to access her personal data, but rather that she understood, in a general sense, that others

would see the information, and therefore she could not reasonably expect that it would be private.

Defendant also seems to be arguing that DNA is different. But it's not. In Maryland v. King, the Supreme Court made clear that the Fourth Amendment doesn't treat DNA differently. This case, like King, involves a narrow, limited use of non-sensitive DNA information. The fact is that the FBI knows nothing private or sensitive about Defendant that they didn't know before they obtained the DNA analysis results. They know that she is a Congressman's aide with Ashwells disease, which they already knew from the tip.

COURT: Okay, counselors, you've given me a lot to think about. Let's now turn our attention to the cellphone issue. Ms. Cadman, you are moving to suppress text messages found on the messaging app TextApp that the government intends to offer at trial. You raise no evidentiary objections at this time -- you allege only Fourth Amendment violations. Why should these messages be suppressed?

CADMAN: Your Honor, the government violated my client's constitutionally protected right to privacy by seizing her cellphone for an extended period of time in order to conduct an exhaustive, intrusive search of the phone's contents without any level of suspicion. This search was conducted in violation of the Fourth Amendment, and the government should not be permitted to use at trial what they discovered.

COURT: Ms. Washington is it true you are offering the fruits of a search that was conducted without any level of suspicion?

WASHINGTON: Yes, your Honor. However, the search was not illegal because it was made at the border and it therefore falls under the long-recognized border search exception to the Fourth Amendment. The government is prepared to concede that the officers who seized and searched the Defendant's phone had neither probable cause nor reasonable suspicion. But the search was reasonable and lawful, simply by virtue of where it took place: at the border.

CADMAN: If I may your Honor, this search was not reasonable simply because it was conducted at the border. As the Supreme Court recognized in Riley v. California, modern smartphones contain such an extraordinary trove of personal data that searches of them are exponentially more intrusive than a search of something like a backpack or a briefcase, in which a person can store only so much information. Moreover, laptops and cellphones are necessities for modern travel. You can't leave home without them.

COURT: All right, counselors, I think we are getting ahead of ourselves. Ms. Cadman, could you tell me exactly what happened here?

CADMAN: Of course, your Honor. In August 2016, Ms. Joralemon was returning from a family vacation abroad. Upon her return to the country, as she passed through Dulles airport, a border agent stopped her and searched her. For absolutely no reason at all, your

Honor, the border agent seized Ms. Joralemon's phone and, upon realizing that it was password protected, confiscated it and told her that the phone would be sent for a forensic search and would not be returned for weeks. Ms. Joralemon was certainly confused by this since, as the government just conceded, the agent acted without any particularized suspicion whatsoever. Nevertheless, she complied graciously.

And your Honor, a forensic search can recover gigabyte upon gigabyte of personal data -- including data that has been deleted or that is stored in the digital cloud. To allow the data that was found on my client's phone to be admitted into evidence without the government having to establish, at the very least, reasonable suspicion, would violate my client's constitutional rights.

COURT: Now correct me if I'm wrong, but after your client was arrested, the government received a warrant to conduct a forensic search on your client's phone. So why don't these messages fall under the inevitable discovery doctrine?

CADMAN: You're right about the warrant, your Honor. But the inevitable discovery doctrine doesn't apply here because of the nature of the messaging app that was used. On TextApp the messages are deleted and irretrievable after thirty days. So, at the time the government executed its warrant, the messages could no longer be seen and would not have been discovered.

COURT: So Ms. Cadman, what evidence from the search are you specifically trying to preclude the government from introducing at trial? I understand that it was messages from this TextApp application. But why are those messages important to this case?

WASHINGTON: Your Honor, perhaps I can jump in here. The messages, in our view, were sent to arrange the meetings described in the indictment where briefcases with cash and thumb drives containing hacked data were exchanged. There are references to cash. And the circumstances under which the messages were created, including the use of the app that causes the messages to disappear after 30 days, all suggest consciousness of guilt. We submit that these messages are compelling proof that the Defendant knew she was involved in a criminal conspiracy.

COURT: Could agents have retrieved these messages without a forensic search of the phone?

CADMAN: No, your Honor. We spoke with a developer for TextApp, and the developer told us that, because of the encrypted nature of the messages and the fact that access to the app itself is password-protected, the only way a third party could access the information was through a forensic search.

COURT: So, Ms. Washington, what is your response to the argument that the border search exception does not apply in this case?

WASHINGTON: Your Honor, it is the long-standing right of the United States government to protect itself, its people, and its sovereignty

by stopping and examining people and things crossing the border. This nation has a strong interest in protecting its territorial integrity -- including protecting itself from smuggled contraband -- and this interest is at its strongest at the border. Defendant suggests that the applicability of the border search exception should depend on the nature of the object being searched. But cellphones, or any other electronic storage devices, should be treated similarly to luggage or other containers a person brings across the border. And the exception unquestionably applies to such containers. While we acknowledge that the law has to come to grips with technological advances, we stress that a great deal of contraband is already coming into the country in digital form.

COURT: Okay, say I were to agree that a phone or a laptop could be searched for contraband. It's one thing to search for contraband from what is readily apparent from opening an electronic device. But isn't it something else to perform an exhaustive forensic search and obtain every keystroke the owner of the phone has ever made?

WASHINGTON: No, Your Honor. In fact, detailed searches are necessary to effectuate the purpose of the exception. First, most phones are password protected. Indeed, that was the case with Defendant's phone. Electronic techniques were necessary to unlock the phone. Second, once the phone was unlocked, a forensic analysis was necessary to determine if there was contraband somewhere in the

files stored on the phone that was not readily accessible from the phone's home screen.

CADMAN: If I may, your Honor, the government is advocating for a boundless expansion of the border search exception. As your Honor suggested, it's one thing for the government to open a laptop and view the contents that appear on the screen, but a forensic search is different in both character and degree. And in Flores-Montano, the Supreme Court held that the border search exception does not apply to all searches conducted there. In that case, and in every subsequent circuit court decision to address the issue, courts have differentiated between routine and nonroutine searches and agreed that nonroutine searches require some level of suspicion.

WASHINGTON: Your Honor, we acknowledge that the border search exception as it stands does not apply to all searches conducted at the border. But this is not the kind of invasive bodily search that the Supreme Court is concerned with. It's a search of an object, Judge. This was a routine search, the type that the First Congress, the one that ratified the Fourth Amendment, empowered border agents to conduct.

CADMAN: Excuse me, your Honor. The right we invoke is as old as the Bill of Rights itself. The Fourth Amendment has always prohibited searches without probable cause. The Supreme Court has carved out a very narrow exception for searches that occur at the border. But that exception doesn't apply here.

COURT: Last word, Ms. Washington?

WASHINGTON: Your Honor, today's cellphones contain the ability to store large amounts of dangerous contraband, and thus, at the border, the government's interest in searching them has never been greater.

COURT: Okay. Thank you, counsel, for this very thorough discussion of these two issues. I will reserve ruling. I'd like to meet back here on June 26th, and I hope to have decisions ready to deliver from the bench then. Thank you. We're adjourned.

UNITED STATES DISTRICT COURT

DISTRICT OF WESTNICK

----------X

UNITED STATES OF AMERICA No. 16-CR-643

-against-

ELIZABETH JORALEMON,

Defendant.

----------X

JUNE 26, 2017

TRANSCRIPT: RULING ON MOTION TO SUPPRESS

Before: Hon. Robert Pitler

APPEARANCES:

For Defendant Elizabeth Joralemon: Rebecca Cadman
Cadman & Henry LLC

For the United States of America: Amara Washington
Assistant U.S. Attorney

Court Reporter: John Crain

COURT: Good afternoon, counsel. I will now render my decision on Defendant's motions to suppress.

First, I address the DNA evidence collected by federal agents. There is nothing so unique about DNA to warrant excluding it from the third-party doctrine. Smith and Miller both held that, by voluntarily sharing information with a third party, an individual loses her reasonable expectation of privacy in that information, and that law enforcement officers therefore do not need a warrant to access it. Here, Defendant not only shared her DNA with 23andyou.com, she asked that it be analyzed. She also clicked a box indicating that her information could be shared with third parties who paid for the data. Because she provided her information voluntarily and should have known her information could be seen by third parties, Defendant's DNA information falls squarely within the ambit of the third-party doctrine.

Defendant's comparison of genetic data to the cellphone information in Riley is unpersuasive. Genetic information is not so deeply revealing or so comprehensive per se that it should be excluded from the third-party doctrine. In this case, the FBI used Defendant's DNA only to identify her, not to track her movements or reveal any comprehensive information about her daily routine, her heritage, or even her physical characteristics. As the Supreme Court said in King, using DNA in this limited way does not raise any significant privacy concerns. For all of these reasons,

Defendant's motion to suppress the DNA evidence is denied.

I now turn to Defendant's request to suppress text messages from the app TextApp. The government recovered these messages through a forensic search of Defendant's cellphone after seizing the phone as Defendant was re-entering the United States. Forensic searches of electronic devices seized at the border conducted with or without reasonable suspicion are constitutional under the border search exception to the Fourth Amendment. No binding precedent indicates that, in determining whether a particular border search may be conducted without reasonable suspicion or probable cause, a court must consider how extensive the information the search is likely to yield is. Moreover, judicial restraint is warranted here, because the question of what is permissible at the border is an area typically controlled by Congress.

Defendant argues that forensic searches of electronic devices require special Fourth Amendment consideration because they might reveal extensive personal data. I find this reasoning unpersuasive. To conduct thorough searches of objects crossing through our borders, the government regularly rips open the linings of suitcases and takes apart the inner workings of large vehicles without violating the Fourth Amendment. A forensic search of an electronic device is not so different as to call for a contrary rule.

The Supreme Court has carved out an exception to the border search doctrine and required reasonable suspicion for certain government examinations of the person conducted at the border. An example of this exception is laid out on page 541 of United States v. Montoya de Hernandez, reported at 473 U.S. 531. The search of Defendant's cellphone, however, was clearly not an invasive bodily search implicating the same personal dignity concerns as a government-conducted x-ray of one's internal organs.

The power of the government to search persons and objects entering our border is a well-settled cornerstone of our Fourth Amendment jurisprudence. The Court finds that the government's interest in control over its borders does not change depending on whether a person is carrying documents stored in a suitcase or documents stored in an electronic device. Defendant crossed an international border with her cellphone. By doing so, she relinquished her Fourth Amendment privacy rights in all objects in her possession at the time, including the contents of her phone. Defendant's motion to suppress the TextApp messages found on her cellphone is accordingly denied.

UNITED STATES DISTRICT COURT

DISTRICT OF WESTNICK

----------X

UNITED STATES OF AMERICA No. 16-CR-643

-against-

ELIZABETH JORALEMON,

Defendant.

----------X

OCTOBER 23, 2017

TRANSCRIPT: TRIAL EXCERPT

Before: Hon. Robert Pitler

APPEARANCES:

For Defendant Elizabeth Joralemon:	Rebecca Cadman Cadman & Henry LLC
For the United States of America:	Amara Washington Assistant U.S. Attorney
Court Reporter:	John Crain

WASHINGTON: Your Honor, the United States calls FBI Agent Orlando Remsen to the stand.

CLERK: Agent Remsen, please state your name and spell it for the record.

REMSEN: Orlando Remsen, O-R-L-A-N-D-O R-E-M-S-E-N.

CLERK: Do you swear to tell the truth, the whole truth, and nothing but the truth, so help you God?

REMSEN: I do.

WASHINGTON: Good afternoon, Agent Remsen. What is your current occupation?

REMSEN: I am a Special Agent for the Federal Bureau of Investigation in Washington, D.C. I work in the cyber crime division.

Q: And how long have you been in that position?

A: Five years.

Q: Have you held any other positions at the FBI?

A: Yes, before that I was in the counter-terrorism division for seven years.

Q: Did you participate in the investigation of Elizabeth Joralemon?

A: Yes.

Q: As part of that investigation did you question an individual named Marin Rapstol?

A: Yes. We observed Mr. Rapstol meeting with Ms. Joralemon on September 7, 2016 in Fullerton Park. After Mr. Rapstol left that meeting, we questioned him.

Q: And what, if anything, did Mr. Rapstol tell you during this interview?

CADMAN: Objection, Your Honor, hearsay.

WASHINGTON: Your Honor, the statements we intend to elicit are all admissible as admissions against interest pursuant to Rule 804(b)(3). The declarant is deceased, and the statements, when made, exposed the declarant to criminal liability.

COURT: Objection overruled. The witness may answer.

WASHINGTON: Thank you, Your Honor. In light of the interruption, allow me to repeat the question. What, if anything, did Mr. Rapstol tell you during this interview?

A: He told us he was employed as a courier for a foreign subversive hacking conglomerate that sought to profit from American elections by obtaining private information from candidates and selling the information to their opponents for a fee.

Q: Did Mr. Rapstol discuss what occurred at the meeting you observed between him and Ms. Joralemon?

A: Yes, he told us that at the meeting we observed, and at another meeting about one month earlier, he showed up with a flash drive in a briefcase containing information hacked from computers used by Congressman Livingston's opponent, and that he exchanged the

briefcase with the flash drive for a similar looking briefcase containing 50,000 US dollars.

Q: Did you surveil any of those meetings?

A: Yes, I surveilled the second meeting in September.

Q: Do you recognize the person who met with Mr. Rapstol on that occasion?

A: Yes.

Q: Do you see that person in this courtroom?

A: Yes.

Q: Could you please point that person out to us.

A: It was her. In the blue pantsuit.

COURT: Let the record reflect that Agent Remsen has pointed to the Defendant.

Q: Now, to be clear, Mr. Rapstol said he accepted a briefcase with 50,000 dollars in cash at the meeting you surveilled?

A: Yes.

Q: And Mr. Rapstol said he delivered the flash drive at that same meeting?

A: Yes.

Q: And did you witness this exchange?

A: Yes.

Q: When you interrogated Mr. Rapstol, did you ask him if he knew what was in the briefcase he was delivering?

A: Yes.

Q: What did he say?

A: Rapstol told me he knew he was delivering a flash drive containing information hacked from accounts belonging to the political rival of the Congressman the Defendant was working for.

Q: And during that interrogation, did you ask Mr. Rapstol if he knew what was in the briefcase the Defendant had delivered to him?

A: Yes.

Q: And what did he say in response?

A: He acknowledged that the briefcase he got from the Defendant contained 50,000 dollars, and that the cash was partial payment for the information contained on the flash drive.

Q: Did Rapstol still have the briefcase he'd received from the Defendant with him when you brought him in for questioning?

A: Yes.

Q: And did you open that briefcase and look inside?

A: Yes. It contained $50,000 in cash.

Q: Now, have you investigated other hacking operations similar to this one in the past, Agent Remsen?

A: Yes. Last year we uncovered a ring of hackers that were blackmailing certain Congressional aides in an attempt to stymy certain legislation from reaching the committee stage.

Q: When you say we does that mean you worked on the case specifically or the FBI in general uncovered the ring?

A: I was the head of the team that investigated that case.

CADMAN: Your Honor, we have a Federal Rule of Evidence 106 application.

COURT: Please approach and let's keep this quick counsel. We're almost done for the day.

[THE FOLLOWING OCCURRED AT SIDEBAR]

COURT: Counsel, what's the issue?

CADMAN: Agent Remsen has omitted the second half of the statement made by Mr. Rapstol during the interrogation. The full statement ought to come in given how dramatically the second half changes the meaning of the first. Without the second half of the statement, the jury will infer that Ms. Joralemon had the same level of knowledge about the exchange that Mr. Rapstol did. And that's precisely why the government is offering it, your Honor.

WASHINGTON: Your Honor, the rest of Agent Remsen's 302 report about his interview with Mr. Rapstol is hearsay and not admissible.

CADMAN: Your Honor, its admission is absolutely necessary to avoid misleading the jury, especially right before they go home for the day. Agent Remsen has completely left out the second part of the 302. In this omitted portion, Mr. Rapstol was asked whether the woman he met with -- a woman Agent Remsen has now identified as my client -- ever said or did anything that might suggest she knew what was in the briefcases, and he responded no. And in fact, when Mr. Rapstol asked Ms. Joralemon at their second meeting if the Livingston campaign was satisfied with previously provided

material, Ms. Joralemon responded that she didn't know what he was referring to and that she just wanted to swap the briefcases and leave so that she could keep her job. And the government must prove knowledge, your Honor. It's an essential element of the offense.

WASHINGTON: Your Honor, I'm looking at Rule 106, and by its very language it doesn't apply to oral statements. Even if we conceded that this was necessary for context, which it isn't, the statement can't come in. It's hearsay, plain and simple.

CADMAN: The rule applies to oral statements by virtue of Rule 611(a), your Honor. It is essential that this second portion of the statement comes in today.

COURT: That's an interesting argument, counsel. Is there any authority for that position, given that the plain text of the Rule seems to support the government's argument and foreclose the possibility of this coming in?

CADMAN: Yes, your Honor. The Second, Seventh, and Tenth Circuits have all held that oral testimony should be admissible under Rule 106. The common law rule of completeness allowed for the admission of oral statements when fairness dictated they be admitted in their entirety. This is exactly such a situation. The jurors can't be allowed to leave without hearing this statement.

WASHINGTON: Again, your Honor, the Defendant's position is wrong for at least two reasons. First, the Rule explicitly states that the rule of completeness applies only to written and recorded

statements. I'm not fully prepared with cases right now, but I know that at least one circuit -- I think the Ninth Circuit -- categorically does not allow any oral statements in under Rule 106. Why are we reading something into the rule that isn't there? Second, and regardless of all of that, this is hearsay, and Rule 106 does not render otherwise inadmissible evidence admissible. It solely governs the order of proof.

COURT: Ms. Cadman?

CADMAN: The First Circuit and the D.C. Circuit have both held that Rule 106 renders otherwise inadmissible evidence admissible. If Rule 106 were concerned only with the order of proof, then it would be unnecessary since Rule 611 already affords the Court wide discretion to control the order of proof. Rule 106 must play a substantive role or it would be mere surplusage.

WASHINGTON: Your Honor, Defendant is trying to use this procedural rule as a Trojan horse to bring in self-serving, exculpatory testimony.

CADMAN: Your Honor, these jurors will be seriously misled if they go home tonight without hearing the full statement. This is precisely the purpose the rule is meant to serve.

COURT: I understand your point counsel. But there are always breaks in a trial, and this is one of them. And I'm reading the rule and it says, quote "writing or recorded statement" end quote. This is

neither of those. I am inclined to deny your application, although I am a little curious about this supposed circuit split.

WASHINGTON: Your Honor, the Rule says what it says. We can't let the Defendant use this to bring in whatever she wants.

CADMAN: We're not trying to bring in whatever we want, your Honor. I simply want to make sure the jury is not misled by the deliberate omission of the second part of Mr. Rapstol's statement.

COURT: How about this, counsel, both of you can send me cases tonight and I'll read them and then rule from the bench tomorrow.

CADMAN: Well, we still contend that the jury should hear the rest of the statement now. But I see that's not in the cards. So the Court's invitation is acceptable to us. Thank you, your Honor.

WASHINGTON: Again, this seems like a pretty cut and dry issue to me, but we will also send a letter brief tonight.

COURT: Just try to have them to me by 7:00 PM. Monday Night Football is on, and I won't read anything once the game starts. Let's call it a day. Let's go back on the record, so I can dismiss the jurors for the day. It's already late as it is.

UNITED STATES DISTRICT COURT

DISTRICT OF WESTNICK

----------X

UNITED STATES OF AMERICA No. 16-CR-643

-against-

ELIZABETH JORALEMON,

Defendant.

----------X

OCTOBER 24, 2017

TRANSCRIPT: TRIAL EXCERPT

Before: Hon. Robert Pitler

APPEARANCES:

For Defendant Elizabeth Joralemon:	Rebecca Cadman Cadman & Henry LLC
For the United States of America:	Amara Washington Assistant U.S. Attorney
Court Reporter:	John Crain

COURT: Good morning everyone.

CADMAN: Good morning, your Honor.

WASHINGTON: Good morning, your Honor.

COURT: Before we bring in the jury, I wanted to make a final ruling on yesterday's Rule 106 application. I had a chance to read over the cases you each submitted. While I am cognizant of the circuit split, I stand by my previous decision and deny the application. The full statement cannot come in.

First, based on its plain language, Rule 106 applies only to written and recorded statements. While the Second, Seventh, and Tenth Circuits have held otherwise, this Court agrees with the approach taken by the Ninth Circuit in United States v. Liera-Morales, which can be found at 759 F.3d 1105. The language of the rule is clear. Had the drafters wanted to include the oral statements aspect of the common law doctrine, they could have done so. They didn't. This omission was deliberate, and it serves an important practical purpose. It is much easier for the Court to examine documents or recorded statements before deciding to admit them. When it comes to oral statements, however, it is impossible to know how something will play out until the witness starts testifying. At that point, it may be too late to put the genie back into the bottle.

While I could have decided the issue on that ground alone, I nonetheless address the government's second argument. I agree with

the government's position that Rule 106 does not render otherwise inadmissible evidence admissible. I find persuasive the Sixth Circuit's reasoning in United States v. Costner, reported at 684 F.2d 370. There, the court held that Rule 106 is intended to eliminate the misleading impression created by taking a statement out of context. The Rule simply covers an order of proof problem; it is not designed to make admissible something that should otherwise be excluded. The Second, Fourth, and Ninth Circuits have all reached similar conclusions when deciding this issue.

Thus, while I do find that the second half of the statement likely does affect how a jury would interpret the first half, I must still deny the defense's application. The second half of the statement will not be admitted. Now let's bring the jury in and get back on track with this trial.

WASHINGTON: Thank you, your Honor.

CADMAN: I want it on record that I am preserving this issue for appeal.

COURT: Knock yourself out, counsel. Please bring in the jury.

UNITED STATES COURT OF APPEALS
FOR THE FOURTEENTH CIRCUIT

----------X No. 18-076

ELIZABETH JORALEMON,
Defendant-Appellant,
-against-
UNITED STATES OF AMERICA,
Appellee.

----------X

ARGUED: July 10, 2018

DECIDED: August 3, 2018

Before: CAPLOW, BENTELE, and FALK, Circuit Judges:

OPINION OF THE COURT

FALK, *Circuit Judge*:

Background

Defendant Elizabeth Joralemon was convicted after a jury trial of conspiring to access and obtain information from a protected computer without authorization, in violation of 18 U.S.C. § 1030(a)(2). Defendant contends that the District Court erred when it denied the following: (1) her pretrial motion to suppress data obtained from her cellphone after it was seized from her at the border; (2) her pretrial motion to suppress her genetic information obtained without a warrant from a non-medical DNA analysis service; and (3) her application during trial, under Federal Rule of Evidence 106, to introduce the remainder of an oral statement that she claims should in fairness have been considered by the jury at the same time as the portion of the statement introduced by the government. We affirm the decisions of the District Court in their entirety.

Facts

On August 21, 2016, FBI agents received an anonymous tip indicating that a woman in a bar was complaining that her boss had asked her to exchange packages with a foreign agent. When the bartender suggested she quit her job, the woman responded that she could not because she had been diagnosed with a rare disease known as Ashwells and needed to maintain her health insurance to pay for the treatments.

The agent who received the tip knew that the bar where the conversation was overheard was frequented by staffers working on Capitol Hill, and the FBI decided to pursue the lead. Another agent contacted a retired former colleague working at 23andyou.com, a commercial DNA analysis service. 23andyou.com customers can use the service to obtain information about their genealogies and to test for their propensity for certain genetic diseases, including Ashwells. The agent asked the former colleague whether the 23andyou database included anyone with Ashwells

disease living in the D.C. metropolitan area. The colleague came back with the name of a single individual: Defendant Elizabeth Joralemon. By reviewing various agency and congressional directories, FBI agents quickly determined that Defendant was employed as a junior aide on the staff of a sitting United States congressman, Representative Jerry Livingston.

The agents decided to place Defendant under surveillance. On September 7, 2016, as they watched her, Defendant travelled to a park in a D.C. suburb in the State of Westnick. Once she arrived, agents witnessed her meet with another individual. The two exchanged what appeared to be identical briefcases. The agents followed and ultimately arrested the other individual, who agreed to speak to them. The individual, Marin Rapstol, referred to here as "the Courier," explained that he worked for an organization that hacks into computers and sells the information it steals. At some point in August 2016, the Courier's organization reached an agreement with senior members of Representative Livingston's campaign staff to sell the campaign information hacked, or stolen, from the computers of a rival candidate.

According to the Courier, at the meeting observed by the agents, the Courier gave the other individual, identified by the Courier as Defendant, a briefcase containing a thumb drive with data stolen from the rival candidate's computers, and, in exchange, Defendant gave him a briefcase containing $50,000 in cash. The Courier further stated that he had engaged in a similar exchange with Defendant about a month earlier. Finally, and of particular significance to this appeal, the Courier reported that Defendant never said or did anything to suggest that she knew what the briefcases contained. In fact, the Courier claimed that when he asked Defendant at the second meeting whether the Livingston campaign was satisfied with the information it had received during the first exchange, Defendant replied that she did not know what the Courier was referring to and was at the meeting only to swap the briefcases so she could keep her job. The Courier died before Defendant's trial.

As part of their investigation, FBI agents checked the databases of other law enforcement agencies for additional information about Defendant. As a result of their inquiry, they learned that, on August 20, 2016, Defendant flew into the Washington Dulles International Airport on her way back from a family vacation abroad. While she was going through the customs process at the airport, a Customs and Border Patrol ("CBP") Agent decided, without reasonable suspicion or probable cause, to seize Defendant's cellphone and subject the phone to a forensic examination. Defendant was informed that the search would take a number of weeks and that her phone would be returned after the search was completed.

The CBP agents who conducted the forensic search uncovered encrypted messages that had been sent through TextApp, a cellphone messaging application that deletes, after thirty days, all traces of incoming and outgoing messages sent through the application. Because the messages were encrypted, they could be found only through a forensic search. The search revealed that Defendant had received TextApp messages referring to "meetings" and "exchanges" and making vague references to "cash." The government offered this evidence at trial as indicative of Defendant's guilty state of mind and knowing participation in the charged conspiracy.

Discussion

A. Forensic Search Without Reasonable Suspicion at the Border

Defendant first argues that the District Court erred when it denied her motion to suppress messages found on her cellphone and concluded that the search was permissible under the border search exception to the Fourth Amendment. According to Defendant, the border search exception should not apply to a search as intrusive as a forensic analysis of a smartphone because of the large volume and the sensitive nature of the information smartphones contain. Rather, contends Defendant, the government should be required to demonstrate at least reasonable suspicion before conducting such a forensic search.

Support for Defendant's argument may be found in decisions of the Fourth and Ninth Circuits, both of which have recently held that, even at the border, forensic searches of electronic devices are "nonroutine" searches that require a showing of particularized reasonable suspicion. *See United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018); *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013). On the other hand, when the Eleventh Circuit recently considered the issue, it held that forensic searches of electronic devices conducted at the border should be considered "routine searches" that do not require reasonable suspicion. *See United States v. Touset*, 890 F.3d 1227 (11th Cir. 2018). We find the reasoning of the Eleventh Circuit compelling and adopt it here.

Under the Fourth Amendment, warrantless searches are per se unreasonable unless an established exception applies. Here, one does. The border search exception to the Fourth Amendment's probable cause and warrant requirements is well-recognized and long-established. *United States v. Ramsey*, 431 U.S. 606, 617 (1977). Under this exception, United States officers may conduct "routine" searches and seizures of persons and property at a United States border without a warrant, probable cause, or even reasonable suspicion. *See id.* at 619.

The border search exception is grounded in the recognition that, as a sovereign nation, the United States has the right to control who and what may enter the country. *See id.* at 620. Indeed the First Congress, which also ratified the Fourth Amendment, afforded border agents "full power and authority" to search without a warrant any item entering the country. Act of July 31, 1789, c.5, §24, 1 Stat. 29. As the Supreme Court has noted, "The historical importance of the enactment of this customs statute by the same Congress which proposed the Fourth Amendment is . . . manifest." *Ramsey*, 431 U.S. at 616-17.

It is often said that the "touchstone of the Fourth Amendment is reasonableness." *Florida v. Jimeno*, 500 U.S. 248, 250 (1991). What is reasonable depends on both the nature of a particular search or seizure and all of the circumstances surrounding that search or seizure. *New Jersey v. T.L.O.*, 469 U.S. 325, 337-42 (1985). Consistent with Congress's power to protect the United States by examining persons and things being brought into the country, the "balance of reasonableness is qualitatively different at the international border than in the interior." *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). Indeed, suspicionless searches at the border are considered reasonable simply because they occur at the border. *See Ramsey*, 431 U.S. at 616.

The Supreme Court has distinguished between "routine" and "nonroutine" border searches, the latter of which require reasonable suspicion. *Montoya de Hernandez*, 473 U.S. at 538-41. But

the search in *Montoya de Hernandez* was an intrusive search of an individual's person. The Supreme Court has yet to hold that any particularized suspicion is required for the search of a person's effects at the border. *See United States v. Flores-Montano*, 541 U.S. 149, 152-54 (2004). Nor has the Court distinguished between searches of different types of property. *See id.* at 149, 155; *United States v. Alfaro-Moncada*, 607 F.3d 720, 727-29 (11 Cir. 2010). Other circuits have determined that non-forensic searches of electronic devices are permissible. *See, e.g.*, *United States v. Stewart*, 729 F.3d 517 (6th Cir. 2013).

We see no reason why the Fourth Amendment should require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property. A forensic search of an electronic device is not a like a strip search or an x-ray; it does not expose intimate body parts or require border agents to touch the person in question. Because the search here was of an electronic device and was not an invasive physical search of the Defendant's body, we conclude that it was a routine search and therefore that reasonable suspicion was not required. We are unpersuaded by Defendant's argument that the border search exception should yield in light of the Supreme Court's decision in *Riley v. California*, 134 S. Ct. 2473, 2480 (2014). Border searches by their nature are reasonable. A forensic search of a cellphone is a routine search that falls squarely within the border search exception to the Fourth Amendment. The District Court's decision to deny Defendant's motion to suppress the data obtained from her cellphone is, therefore, affirmed.

B. Warrantless Search of Commercial DNA Tests

Defendant next argues that FBI agents violated her Fourth Amendment right to be free from unreasonable searches and seizures when they obtained, without a warrant, the genetic testing profile the company 23andyou.com kept at the request of and pursuant to a contract with Defendant. The government contends that no warrant was required because Defendant chose to share her genetic information with 23andyou.com, a third party.

The Supreme Court has held that "the Fourth Amendment protects people, not places." *Katz v. United States*, 389 U.S. 347, 351 (1967). According to the Court, "what [an individual] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* Therefore, the Fourth Amendment protects "what an individual seeks to preserve as private" so long as the individual has a reasonable expectation that it will be kept private. *See, e.g., Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018).[1]

Under the third-party doctrine, developed after *Katz*, an individual who voluntarily gives information to a third party has no reasonable expectation of privacy with respect to that information. *See Smith v. Maryland*, 442 U.S. 735, 743 (1979); *United States v. Miller*, 425 U.S. 435, 443 (1976). The instant case requires this Court to determine whether the facts at hand justify application of the third-party doctrine or whether, in light of *Carpenter*, the circumstances here suggest that a warrant was required to obtain Defendant's genetic information in general and the test result indicating Defendant was afflicted with Ashwells in particular. In *Carpenter*, the Supreme Court held that, despite the third-party doctrine, law enforcement must obtain a warrant

[1] The Supreme Court rendered its decision in *Carpenter v. United States* on June 22, 2018, well after Defendant's conviction and sentencing in the District Court.

under the Fourth Amendment to retrieve GPS phone tracking data from cellphone service providers. 138 S. Ct. at 2221.

However, the Court was careful there to limit the scope of its holding to the facts before it. *Id.* at 2220. *Carpenter* addressed only geolocation data. *Id*. Defendant reads too much into the *Carpenter* decision when she argues that it calls upon us to discard the long-established third-party doctrine and the holdings of *Smith* and *Miller*. In reaching this conclusion, we join the many courts that have continued to apply the third-party doctrine since *Carpenter* was decided, even in light of modern technologies that reveal sensitive personal information. *See, e.g., Palmieri v. United States*, 896 F.3d 579, 588 (D.C. Cir. 2018).

Contrary to Defendant's arguments, nothing about DNA itself compels a different outcome. The Supreme Court has held that DNA used only for the purpose of identification is no different than a thumbprint or other identifying information, and that it therefore raises no privacy concerns sufficient to overcome the presumption of constitutionality that usually attaches to a search incident to arrest. *See Maryland v. King*, 569 U.S. 435, 465 (2013). While the Court stated in dicta in *King* that a search of DNA for medical information would raise different privacy concerns, the present case does not involve a sifting of medical information, but rather a narrow search for an identifying feature in a database. *See id.* at 464.

We acknowledge that the actions of the investigators here involve an intrusion into privacy—perhaps one greater than the intrusions at issue in *Miller* and *Smith*. Nevertheless, we do not find the narrow access to genetic information at issue here so different from access to bank or telephone records as to compel deviation from well-settled Fourth Amendment doctrine. *Carpenter* may counsel sensitivity to changing technologies in the Fourth Amendment context, but it also urges sensitivity to the facts of particular cases. The federal agents here conducted a narrowly tailored search for information the Defendant had already disclosed to a third party. The District Court properly denied Defendant's motion to suppress that information.

C. Oral Statements Under Rule 106

The third and final issue raised by Defendant is one of first impression in this Circuit: whether Federal Rule of Evidence 106 ("Rule 106") applies to oral statements. During the trial, the government called an FBI agent to testify about statements made by the Courier after he was arrested. Because the Courier, having died, was unavailable to testify at trial, and because his statements were against his penal interest, the District Court permitted the government to introduce portions of the Courier's statements through the testimony of the FBI agent who interviewed him. *See* Fed. R. Evid. 804(b)(3).

Immediately after the prosecution elicited a portion of the Courier's statements, defense counsel made a Rule 106 application requesting that additional statements made by the Courier during the same interrogation be admitted at the same time. Defense counsel argued that the jury needed to hear the remainder of the oral statements to put in context the portions offered by the government. The portion defense counsel wished to enter included arguably exculpatory statements Defendant made to the Courier. These arguably exculpatory statements were otherwise inadmissible hearsay because they were not made against the Courier's penal interest.

After hearing argument and accepting briefing on the question overnight, the District Court denied defense counsel's application, and the remainder of the oral statement was never received in evidence. After reviewing the District Court's decision for abuse of discretion, we affirm that decision for the following two reasons: (1) Rule 106 does not apply to oral statements; and (2) Rule 106 does not allow the admission of otherwise inadmissible evidence.

As the late Justice Scalia once wrote, "The text is the law, and it is the text that must be observed."[2] While this case is about a rule of evidence, and not a statute, we still need look no further than the text of the Federal Rule at issue to answer the question before us. Rule 106 codifies the Rule of Completeness, a common law rule that covered all forms of communication made outside the courtroom. *See* Fed. R. Evid. 106 advisory committee's note; 21A Charles Alan Wright & Arthur R. Miller, Federal Practice & Procedure, § 5072.1 (2d ed.). But, by its own words, Rule 106 is limited to "writings" and "recorded statements." At common law, "the rule of completeness applied broadly to all types of evidence, whether documentary or oral testimony." Collin D. Hatcher, *The Whole Truth or Anything but …: How Fairness, Reliability, and the Rule of Completeness Affect the Jury's Truth-Seeking Function*, 39 Am. J. Trial Advoc. 683, 697 (2016). Thus, we know from the text of the rule that oral statements were deliberately left out. The Advisory Committee Notes support this interpretation. *See* Fed. R. Evid. 106 advisory committee's note.[3] Several of our sister circuits agree that the plain language of Rule 106 sufficiently answers the question of whether it applies to oral statements. *See, e.g., United States v. Liera-Morales*, 759 F.3d 1105, 1111 (9th Cir. 2014).

While we are confident that a plain reading of the text of the rule is sufficient to answer the question before us, we also address practical considerations involving Rule 106's application at trial. There are many practical reasons not to apply Rule 106 to oral statements. While a court may reliably confirm the entirety of the contents of a document or recorded statement, recollections of oral statements offer no such reliability or known limitations.

Moreover, the remainder of the oral statement Defendant sought to offer under Rule 106 was inadmissible hearsay. Some of our sister circuits have suggested that oral statements, including statements that are otherwise inadmissible, may be introduced under Rule 106, particularly when the Rule is read together with Federal Rule of Evidence 611(a). We, however, disagree.

Rule 611(a) is not a substantive rule of admission. It simply governs an order of proof issue with respect to admissible evidence. The same is true for Rule 106. *See, e.g., U.S. v. Costner*, 684 F.2d 370, 373 (6th Cir. 1982). While petitioner stresses the exculpatory nature of the excluded statements, the "fact that some of the omitted testimony arguably was exculpatory does not, without more, make it admissible under the rule of completeness." *United States v. Lentz*, 524 F.3d 501, 526 (4th Cir. 2008).

Here, the oral statements Defendant sought to offer at trial were buried by not just one, but two layers of inadmissible hearsay. The first level was that of the Courier speaking to the agent. The excluded portions of the oral statements made to the agent by the Courier were not made

---

[2] Antonin Scalia, *Common Law Courts in a Civil-Law System: The Role of the United States Federal Courts in Interpreting the Constitution and Laws*, *in A Matter of Interpretation: Federal Courts and the Law* 3, 22 (1997).

[3] This Court recognizes that Advisory Committee members are not authors of the rules and their notes have no binding effect. *See Tome v. United States*, 513 U.S. 150, 167-68 (1995) (J. Scalia, concurring) (the Advisory Committee Notes "bear no special authoritativeness" and cannot "change the meaning that the Rules would otherwise bear.").

against penal interest, and no other hearsay exception applies to them. The second layer consisted of statements, allegedly made by Defendant to the Courier, in which she minimized her involvement in the crime. Allowing admission of such "self-serving, exculpatory statements made by a party which are being sought for admission by that same party" cannot be permitted under Rule 106, even when the Rule is read together with Rule 611. *Lentz*, 524 F.3d at 526.

For all these reasons, we hold that the District Court did not abuse its discretion when it denied Defendant's Rule 106 application at trial.

Conclusion

For the foregoing reasons, the judgment of conviction is *affirmed*.

CAPLOW, *Circuit Judge*, dissenting:

The majority acknowledges that the "touchstone of the Fourth Amendment is reasonableness." *Florida v. Jimeno*, 500 U.S. 248, 250 (1991). Yet, with its feet planted firmly in the twentieth century and its head in the sand, it insists on rigidly applying to our modern age of digital media doctrines developed in an age of paper. The results, unsurprisingly, are anything but reasonable.

A. A Forensic Search of an Electronic Device Seized at the Border Conducted Without Reasonable Suspicion is Unconstitutional

Recent Supreme Court cases have re-imagined Fourth Amendment protections in light of advancing technology. *See,Carpenter v. United States,* 138 S. Ct. 2206 (2018)*; Riley v. California*, 134 S. Ct. 2473 (2014); *Kyllo v. United States*, 533 U.S. 27 (2001). Despite this trend, the majority insists on applying to our current reality a doctrine initially adopted in 1789 by the First Congress. Act of July 31, 1789, c.5, §24, 1 Stat. 29. Now, anyone entering the United States must accept the possibility that their entire digital lives will be scrutinized by the government for absolutely no reason at all.

Prior to today's decision, the majority of circuits ruling on this issue held that reasonable suspicion is required for forensic searches of electronic devices seized at the border. *See United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018), *as amended* (May 18, 2018); *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013). The Supreme Court, moreover, has endorsed limiting even long-recognized doctrines when advancing technology requires it. *See Riley v. California*, 134 S. Ct. 2473 (2014). As the Fourth Circuit held in *Kolsuz*, the border search doctrine should likewise be so limited. 890 F.3d at 145. Because modern electronic devices contain such vast amounts of highly personal data, the privacy interests of individuals in their personal electronic devices outweigh the interests of the government in preventing contraband from entering the country.

Following the Eleventh Circuit's opinion in *United States v. Touset*, the majority apparently reasons that a forensic search of a smartphone is no different than a search of a truck crossing the border. This argument makes little sense. While the number of documents stored in a

truck and a smartphone may be comparable, the nature of the information stored is not. Literally attached to our hips, smartphones have become almost an extension of our very beings; the information stored on them is not only vast, it is extremely personal. People cross the border with extensive digital archives of their most private conversations with loved ones, but few drive a truck filled with physical records of those conversations.

Forensic searches of electronic devices are particularly invasive. Forensic searches of smartphones reveal data stored on the devices, including "personal contact lists, emails, messenger conversations, photographs, videos, calendar, web browsing history, and call logs, [and] physical location down to precise GPS coordinates." *Kolsuz*, 890 F.3d at 139. Because of their expansive nature, these particular searches should be not be considered "routine" searches within the ambit of the border search doctrine. *See, e.g.*, *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985).

The disturbing circumstances of the case before the court today highlight the need for a requirement of reasonable suspicion for these particular searches. Defendant was traveling back from a family vacation when a CBP officer, for no particular reason, seized Defendant's personal smartphone. CBP proceeded to send the phone miles away, for several weeks, to conduct a forensic analysis, which recovered essentially every piece of data contained on the phone. After the lab completed the search, CBP officers stored some of Defendant's digital data, including private text conversations, in a file on a federal database, which the FBI accessed weeks later. Defendant's cellphone contained no contraband; the government simply used the border search exception to achieve access to Defendant's private text conversations without a warrant.

While the Eleventh Circuit declined to require reasonable suspicion in *Touset*, the court nevertheless concluded that the seizure there was based on reasonable suspicion because the Defendant was on the Department of Homeland Security's "look out" list for child pornography. *Touset*, 890 F.3d at 1230-31. Before us today, by contrast, is a search and seizure that the government concedes was conducted without any justification whatsoever other than the fact that it took place at the border. The messages retrieved from Defendant's personal electronic device should have been suppressed.

B. The Third-Party Doctrine Does Not Apply to DNA Evidence Obtained from a Commercial Service Without a Warrant

The majority repeats the error it makes with respect to the border search exception by rotely applying the third-party doctrine to genetic testing. In doing so, it irreparably erodes the protections of the Fourth Amendment.

The Defendant's Fourth Amendment right to be free from unreasonable searches and seizures was violated when the government obtained, without a warrant, Defendant's genetic testing profile and medical information from 23andyou.com. A plain reading of the text of the Fourth Amendment alone should be enough to dispense with this case. It explicitly states, "The right of the people to be secured in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. Amend. IV. The protections of the Fourth Amendment are not, as some suggest, limited to the contents of a person's home. Indeed, the Supreme Court long ago made clear that "the Fourth Amendment protects people, not places." *Katz v. United States*, 389 U.S. 347, 351 (1967). It is difficult to imagine something more

inherently encompassed within someone's "person" than his or her genetic profile. The majority's willingness to extend the third-party doctrine to information as sensitive as the results of DNA testing is utterly improper.

The third-party doctrine was developed to address bank records and telephone numbers. That kind of relatively innocuous and limited data has little in common with the sensitive, detailed, health-related information generated by DNA analysis. Thus, while *Smith* and *Miller* are binding on this Court, their application to the present circumstances is hardly obvious. Indeed, "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, 'what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.'" *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (citing *Katz v. United States*, 389 U.S. 347, 351-52 (1967)). Before blindly applying doctrines developed in another era, courts must consider whether subsequent technological developments allow for previously unforeseen intrusions upon privacy rights. *See Kyllo v. United States*, 533 U.S. 27, 40 (2001).

Like smartphone data, genetic information is simply too private to be obtained without a warrant. In *Carpenter*, the Court found that the government had violated the defendant's Fourth Amendment rights when it obtained cell-site geolocation data without a warrant. 138 S. Ct. at 2218. The Court held *Smith* and *Miller* to be inapposite, because "a cell phone [is] almost a 'feature of human anatomy.'" *Id.* (quoting *Riley v. California*, 134 S. Ct. 2473, 2484 (2014)). Genetic test results are even more clearly a feature of human anatomy. The majority relies on *Maryland v. King*, 569 U.S. 435 (2013) in a desperate attempt to justify its holding. However, a careful reading of that decision undercuts the majority's reasoning. *See King*, 569 U.S. at 464-65 ("If in the future police analyze samples to determine, for instance, an arrestee's predisposition for a particular disease or other hereditary factors not relevant to identity, that case would present additional privacy concerns not present here.") The majority misses the forest for the trees and sanctions an encroachment upon privacy interests the Fourth Amendment protects.

C. Rule 106 Should Apply to Oral Statements, Even if Otherwise Inadmissible

Finally, the majority's narrow reading of Federal Rule of Evidence 106 not only renders the Rule mere surplusage in light of Rule 611(a), it seriously endangers the ability of Defendants accused of serious crimes to adequately defend themselves. Rule 106, properly understood and reasonably applied, permits the admission of otherwise inadmissible oral statements, so long as those statements ought in fairness be considered contemporaneously with statements already admitted. While the abuse of discretion standard is deferential, it is met here; the lower court erred when it refused to admit the second half of the Courier's statement under Rule 106.

First, Rule 106 allows for the admission of oral statements when read in conjunction with Rule 611(a). I acknowledge that whether Rule 106 is intended to be a substantive rule or merely a procedural rule that affects the order of proof is a tricky question. Nevertheless, I am persuaded by both the language of the rule and its placement within the Federal Rules of Evidence that it is meant to address more than only the order of proof. *See United States v. Lopez-Medina*, 596 F.3d 716, 734 (10th Cir. 2010) ("While Rule 106 applies only to writings and recorded statements, we have held the rule of completeness embodied in Rule 106 is substantially applicable to oral testimony . . . by virtue of Fed. R. Evid. 611(a), which obligates the court to make the interrogation and presentation effective for the ascertainment of the truth.") (internal citations omitted). Indeed, Rule

611 directs courts to "exercise reasonable control over the mode and order of examining witnesses and presenting evidence so as to . . . make those procedures effective for determining the truth." Fed. R. Evid. 611(a). How is allowing the government to bring in the first half of a statement that inculpates the defendant while refusing to allow the defendant to bring in the second half that seems to exculpate her, merely because the statement was made orally, following procedures effective for determining the truth?

The Seventh Circuit has laid out a four-part test to determine when the remainder of an admitted statement should also be received. *United States v. Li*, 55 F.3d 325 (7th Cir. 1995). "To determine whether a disputed portion is necessary, the District Court considers whether (1) it explains the admitted evidence, (2) places the admitted evidence in context, (3) avoids misleading the jury, and (4) insures fair and impartial understanding of the evidence." *Id.* at 330. That test is met here, and it should not matter whether the disputed evidence is a portion of a written document or an oral statement.

The majority compounds its error by holding that Rule 106 applies only to otherwise admissible evidence. As the facts of this case demonstrate, this narrow reading of the rule undermines its purpose. That is why the D.C. Circuit was correct when it stated, "Rule 106 can adequately fulfill its function only by permitting the admission of some otherwise inadmissible evidence when the court finds in fairness that the proffered evidence should be considered contemporaneously. A contrary construction raises the specter of distorted and misleading trials and creates difficulties for both litigants and the trial court." *United States v. Sutton*, 801 F.2d 1346, 1368 (D.C. Cir. 1986).

The idea that Rule 106's proper function transcends the other rules limiting admissibility is based on its placement in Article I of the Federal Rules of Evidence, "which contains rules that generally restrict the manner of applying the exclusionary rules." *Id*. (citing C. Wright & K. Graham, Federal Practice and Procedure: Evidence § 5078, at 376 (1977 & 1986 Supp.)). Further, "every major rule of exclusion in the Federal Rules of Evidence contains the proviso, 'except as otherwise provided by these rules,' which indicates 'that the draftsmen knew of the need to provide for relationships between rules and were familiar with a technique for doing this.'" *Id*. This language was deliberately excluded from Rule 106, "which indicates that Rule 106 should not be so restrictively construed." *Id*.

Although the majority will likely conjure up images of criminal defendants run amok bringing in self-serving, exculpatory testimony, these fears are unfounded. The Rule applies only when "a misunderstanding or distortion created by the other party can only be averted by the introduction of the full text of the out-of-court statement." *United States v. Awon*, 135 F.3d 96, 101 (1st Cir. 1998). Trial judges retain great discretion to keep out blatantly self-serving testimony that a party seeks to admit under Rule 106.

Simply put, Rule 106 was intended for exactly the type of situation raised by this case. Defendant should have been permitted to bring in the second half of the Courier's statement, although it was inadmissible hearsay, because Rule 106 and the rule of completeness, not to mention fundamental fairness, required correction of the distortion created when the government selectively elicited inculpatory testimony from the FBI agent.

For the foregoing reasons, I dissent.

No. 18 - 2417

Supreme Court of the United States

ELIZABETH JORALEMON, Petitioner,

--against--

UNITED STATES OF AMERICA,
Respondent.

DATE: November 16, 2018

The petition for a writ of certiorari to the United States Court of Appeals for the Fourteenth Circuit is granted, limited to the following questions:

I. Whether, under the Fourth Amendment, the government must secure a warrant issued upon probable cause to directly obtain, from a non-medical commercial service that performs DNA analysis, genetic information related to a medical condition.

II. Whether, under the Fourth Amendment, the government must have reasonable suspicion to perform a forensic search of an electronic device seized at the United States border.

III. Whether Federal Rule of Evidence 106 applies to the remainder of or related oral statements, and whether the Rule permits the receipt of otherwise inadmissible evidence.