# UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF NEW YORK

**----------------------------------------------------------x**

**:**

**UNITED STATES OF AMERICA :**

**:**

**:**

**:**

**v. : 13-cr-761 (VM)**

**:**

**YUDONG ZHU : Electronically Filed**

**YE LI, :**

**:**

**Defendants. :**

**----------------------------------------------------------x**

**MEMORANDUM OF LAW IN SUPPORT OF**

**DEFENDANT YUDONG ZHU'S MOTION FOR RECONSIDERATION OF THE COURT'S DENIAL OF MOTION TO SUPPRESS EVIDENCE SEIZED FROM LAPTOP COMPUTER AND THE FRUITS OF SUCH EVIDENCE**

John D. Cline

Law Office of John D. Cline

235 Montgomery Street, Suite 1070 San Francisco, CA 94104

(415) 322-8319 (telephone)

Maurice H. Sercarz Sercarz & Riopelle, LLP

810 Seventh Avenue, Suite 620 New York, NY 10019

(212) 586-4900 (telephone)

*Attorneys for Dr. Yudong Zhu*

# Page

ARGUMENT 1

CONCLUSION 5

# CASES

*Georgia v. Randolph*,

# TABLE OF AUTHORITIES

**Page**

547 U.S. 103 (2006) 4

*Riley v. California*,

2014 U.S. LEXIS 4497 (U.S. June 25, 2014) *passim*

*United States v. Davis*,

2014 U.S. Dist. LEXIS 15003 (S.D.N.Y. Feb. 4, 2014) 1

**OTHER AUTHORITIES**

U.S. Const. Amend. IV *passim*

Dr. Yudong Zhu submits this memorandum in support of his motion to reconsider the Court's denial of his motion to suppress the contents of the laptop computer that he surrendered to NYU in May 2013. Docs. 28-31 (motion), 34-36 (opposition), 37-38 (reply), 40 (order). Reconsideration is warranted in light of the Supreme Court's intervening decision in *Riley v. California*, 2014 U.S. LEXIS 4497 (U.S. June 25, 2014). *See, e.g., United States v. Davis*, 2014

U.S. Dist. LEXIS 15003, at \*9 (S.D.N.Y. Feb. 4, 2014) ("'intervening change in controlling law'" is a ground for reconsideration) (quoting *Kolel Beth Yechiel Mechil of Tartikov, Inc. v. YYL Irrevocable Trust*, 729 F.3d 99, 104 (2d Cir. 2013)).

*Riley* establishes that cell phones--and, by its reasoning, other portable personal computers such as laptops--occupy a uniquely protected category for Fourth Amendment purposes, because of the extraordinary volume of intensely personal information they contain. *Riley* expresses a strong preference for a warrant when the government intends to search such a device. Just as *Riley* refused to apply ordinary search incident to arrest doctrine to a cell phone, this Court should decline to apply what it found to be ordinary third-party consent analysis to the contents of the laptop computer.

# ARGUMENT

On May 27, 2014, this Court denied Dr. Zhu's motion to suppress the contents of the laptop computer and the fruits of that evidence. Doc. 40. The Court found that Dr. Zhu had a reasonable expectation of privacy in the contents of the computer. *Id*. at 7-14. It concluded, however, that NYU gave valid third-party consent to the FBI's search of the laptop's password- protected and encrypted contents. *Id*. at 14-17. The Court recognized that "the laptop's passwords and encryption weigh against finding that NYU had access, similar to locks on a door." *Id*. at 16. But it found that a form Dr. Zhu signed in October 2008 sufficed to give NYU

both access to and common authority over the contents of the laptop, despite Dr. Zhu's express refusal to grant NYU access when requested in May 2013. *Id*. at 16-17.1

On June 25, 2014, the Supreme Court decided *Riley*. The unanimous opinion addressed the warrantless search of cell phones incident to arrest. The Court observed that when (as here) law enforcement officials undertake a search to discover evidence of a crime, "reasonableness [under the Fourth Amendment] generally requires the obtaining of a judicial warrant." *Riley*, 2014 U.S. LEXIS 4497, at \*15 (quotation omitted). Turning to the warrant exception on which the government relied--search incident to arrest--the Court found that "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." *Id*. at \*33. The Court summarized the unique privacy concerns of a cell phone:

The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information--an address, a note, a prescription, a bank statement, a video--that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.

Finally, there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower. *See* Harris Interactive,

1 For the reasons stated in our prior pleadings, we respectfully disagree with the Court's ruling in this respect.

2013 Mobile Consumer Habits Study (June 2013). A decade ago police officers searching an arrestee might have occasionally stumbled across a highly personal item such as a diary. *See, e.g., United States v. Frankenberry,* 387 F.2d 337 (CA2 1967) (per curiam). But those discoveries were likely to be few and far between. Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives--from the mundane to the intimate. *See Ontario*

*v. Quon,* 560 U. S. 746, 760 (2010). Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.

*Id*. at \*35-\*37. The Court observed that the data on a cell phone differs from physical records qualitatively as well as by quantity. A cell phone search reveals internet browsing information, location data, and apps that contain (and give access to) an enormous range of information. As the Court observed, "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form--unless the phone is." *Id*. at \*39-\*40 (emphasis in original).

Given the privacy intrusion that occurs when the police search a cell phone, the Court rejected the government's reliance on the search incident to arrest exception. The Court's holding was "not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest." *Id*. at \*47. The Court added: "Our cases have historically recognized that the warrant requirement is an important working part of our machinery of government, not merely an inconvenience to be somehow 'weighed' against the claims of police efficiency." *Id*. (quotation omitted). It recognized that where time does not permit police to obtain a warrant, the exigent circumstances exception to the warrant requirement may apply to permit the search of a cell phone. *Id*. at \*48-\*49.

The *Riley* Court's privacy analysis applies equally to laptop computers such as the one at issue here. Laptops, like cell phones, can contain an extraordinary amount of highly personal data, including documents, emails, photographs, financial and health information, and internet search histories. The laptop at issue here contained a wealth of such information. As Dr. Zhu explained in his declaration, "I used [the laptop] for the full range of professional and personal purposes. In addition to sensitive information relating to MRI-related work that I and others carried out, I kept on the laptop personal information relating to my family's and my finances, health, and other private matters." Doc. 30 at 2 ¶ 5.2 In addition to their extraordinary storage capacity, laptops are portable and thus, like cell phones, may reveal location data.

Just as the heightened privacy interest in a cell phone (or a laptop) bars use of the search incident to arrest exception to the warrant requirement, it should similarly bar use of the third- party consent doctrine, at least where--as here--the third-party lacks physical access to the contents of the device and the user expressly refuses consent. *Cf. Georgia v. Randolph*, 547 U.S. 103, 109 (2006) (rejecting third-party consent exception where defendant was present and objected to search of his home); *id.* at 135 (Roberts, C.J., dissenting) ("To the extent a person wants to ensure that his possessions will be subject to a consent search only due to his *own* consent, he is free to place these items in an area over which others do *not* share access and control, be it a private room or a locked suitcase under a bed.") (emphasis in original).

Absent exigent circumstances or Dr. Zhu's consent--neither of which was present here-- the government's proper course before searching the laptop was spelled out succinctly in *Riley*: "get a warrant." 2014 U.S. LEXIS 4497, at \*51. Because the government failed to take this step

2 We incorporate in this memorandum by reference the declarations and accompanying exhibits submitted in connection with Dr. Zhu's motion to suppress. Docs. 29, 30, 37.

despite ample time and full knowledge that Dr. Zhu sought to protect his privacy with passwords and encryption, the search of the laptop violated his Fourth Amendment rights. Suppression is required.

# CONCLUSION

For the foregoing reasons, and for the reasons stated in Dr. Zhu's initial motion and reply, the Court should enter an Order suppressing all evidence obtained from the search of the laptop computer that Dr. Zhu surrendered to NYU in May 2013, and the fruits of that evidence.

Dated: July 15, 2014

Respectfully submitted,

/s/ John D. Cline

JOHN D. CLINE

Law Office of John D. Cline

235 Montgomery Street, Suite 1070 San Francisco, CA 94104 415.322.8319 (telephone)

415.524.8265 (facsimile)

Email: cline@johndclinelaw.com

/s/ Maurice Sercarz

MAURICE SERCARZ

Sercarz & Riopelle, LLP 810 Seventh Ave., Suite 620 New York, NY 10019 212.586.4900 (telephone)

212.586.1234 (facsimile)

Email: msercarz@sercarzandriopelle.com

# CERTIFICATE OF SERVICE

This is to certify that on this the 15th day of July, 2014, I caused to be filed a true and correct copy of the instant Memorandum and annexed declarations using the Southern District of New York's Electronic Case Filing system ("ECF") which will send a notice of filing to all counsel of record.

/s/ John D. Cline JOHN D. CLINE